Administrator-Handbuch

v9.0

SecurityGateway für E-Mail-Server
Administrator-Handbuch

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Die Produkte, die in diesem Dokument genannt werden, können eingetragene Marken oder Warenzeichen ihrer jeweiligen Inhaber sein oder beinhalten.

v9.0.3 - Juni 2023

Inhaltsverzeichnis

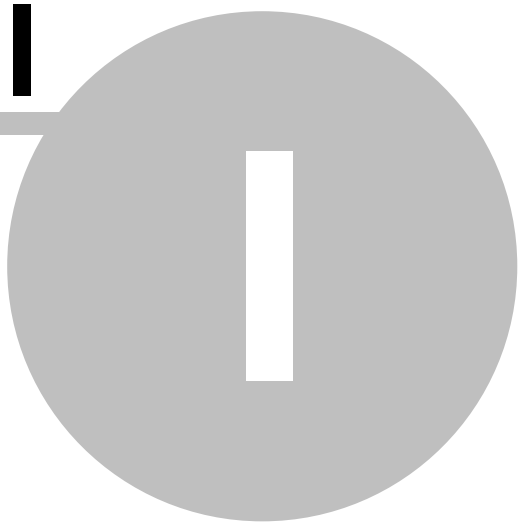
Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kapitel



1 SecurityGateway

1.1 Übersicht

MDaemon Technologies hat auf der Grundlage jahrelanger Erfahrung mit der Technologie der Mailserver einen E-Mail-Firewall für Nutzer beliebiger SMTP-E-Mail-Server entwickelt. SecurityGateway für E-Mail-Server bietet mehrstufige Abwehrmaßnahmen, die an der Außengrenze Ihres Netzwerks umfassend wirken und Gefahren für Ihre E-Mail-Kommunikation durch Spam, Viren und andere Bedrohungen abwehrt. Der E-Mail-Firewall SecurityGateway für E-Mail-Server ist auf der Filtersprache SIEVE aufgebaut, einem Industriestandard, und bietet Leistungsstärke und Flexibilität in der Verwaltung des eingehenden und abgehenden E-Mail-Verkehrs.

Der E-Mail-Firewall SecurityGateway bietet zahlreiche Vorteile:

- **Genaue Erkennung**—SecurityGateway bietet mehrere Analysewerkzeuge, um Bedrohungen von legitimen E-Mail-Nachrichten zu unterscheiden und setzt die besten, erprobten Techniken für Anti-Spam 155, Anti-Virus 187, Anti-Spoofing 190 und Anti-Abuse 222 wirksam ein. Damit werden eine 99-prozentige Abwehrquote für Spam erreicht und falsche positive Treffer nahezu vollständig vermieden.
- **Einfache Verwaltung**—Eine intuitiv zu bedienende, aufgabenorientierte Benutzerschnittstelle stellt für alle Hauptfunktionen von SecurityGateway je eine Leitseite zur Verfügung. Die Leitseiten enthalten Übersichten gemeinsamer Aufgaben und Verknüpfungen zu den Seiten, von denen aus die einzelnen Aufgaben erledigt werden können. Diese Herangehensweise gestattet es den Administratoren 60, gemeinsame Aufgaben mit geringstem Aufwand auszuführen. Aufgaben der Systemadministratoren können auch an Domänen-Administratoren delegiert werden, und diese Domänen-Administratoren können eine oder mehrere Domänen verwalten, die ihnen ein Globaler Administrator zuweist. Schließlich können die Benutzer selbst bestimmen 32, wie mit einzelnen Nachrichten verfahren werden soll; sie brauchen sich dazu nicht an einen Administrator zu wenden.
- **Schutz gegen Datenverlust**—SecurityGateway filtert nicht nur eingehenden sondern auch abgehenden E-Mail-Verkehr. Eine einfach zu bedienende Benutzerschnittstelle gestattet das Festlegen von Regeln, welche die unbefugte Übermittlung vertraulicher Informationen aus dem Netzwerk nach außen erkennen und verhindern können.
- **Leistungsstarke Filterfunktionen**—Die umfassenden Filterfunktionen von SecurityGateway stützen sich auf die Filtersprache SIEVE, die besonders zum Filtern von E-Mail geschaffen wurde. Administratoren können den Funktionsumfang von SecurityGateway auch durch den eingebauten Inhaltsfilter für Nachrichten 252 und den Editor für SIEVE.Skripte 284 erweitern und eigene SIEVE-Skripte erstellen.
- **Umfassende Berichtsfunktionen**— Die umfassenden Berichtsfunktionen 324 von SecurityGateway helfen, Strukturen und Verhaltensmuster im E-Mail-Verkehr und mögliche Probleme zu erkennen. Alle Berichte lassen sich durch Anklicken tiefer detailliert darstellen und bieten so weiter gehende Möglichkeiten der Analyse.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **Flexible mehrstufige Abwehrmaßnahmen**—Administratoren können wahlweise die Reihenfolge beeinflussen, in der die einzelnen Stufen der Abwehrmaßnahmen von SecurityGateway in Tätigkeit treten. Sie können damit die Sicherheitsregeln an die individuellen Bedürfnisse und Verhaltensmuster für ihren Mailverkehr anpassen.

Übersicht über die Funktionen

Das Navigationsmenü von SecurityGateway im linken Bereich der Benutzeroberfläche enthält sechs Untermenüs, und jedes dieser Untermenüs steuert einen Teil der Funktionen von SecurityGateway. Es folgt eine kurze Übersicht über diese sechs Untermenüs:

Das Dashboard

Das Dashboard ist die erste Seite, die dem Benutzer nach der Anmeldung an SecurityGateway für E-Mail-Server angezeigt wird. Die Leitseite des Dashboards bietet einen schnellen Überblick über den momentanen Zustand von SecurityGateway und zeigt die Zusammenfassungen einiger Berichte 324 über die Aktivität der letzten 24 Stunden.

Im oberen Bereich des Dashboards befindet sich der Abschnitt Server-Status. Dieser Abschnitt zeigt an, ob der SMTP-Dienst ausgeführt wird, und er bietet Verknüpfungen, um den Dienst zu starten und zu beenden. Das Dashboard zeigt außerdem den Umfang des Lizenzschlüssels und Verknüpfungen zum Verwalten der Produkt-Lizenz 150 und der Produkt-Aktivierung, und es gibt Auskunft über die Zahl der Domänen und Benutzer, die im System vorhanden sind. Es stellt ferner eine Verknüpfung zur Liste der Domänen 48 her, über welche die Domänen und Benutzer verwaltet werden können. Ist eine neue Version der Software 149 verfügbar, so steht in diesem Abschnitt auch eine Verknüpfung zur Verfügung, über die nähere Informationen zu der neuen Version aufgerufen werden können. Den globalen Administratoren wird außerdem der freie Speicherplatz auf dem Datenträger angezeigt. Weiter werden die Zahl der gerade aktiven eingehenden und abgehenden SMTP-Verbindungen angezeigt. Im Abschnitt Warteschlagen-Status werden die Zahl der Nachrichten in den Eingangs-, Zustellungs- und Defekt-Warteschlangen angezeigt. Im selben Abschnitt wird den globalen Administratoren die Zahl der Nachrichten in der administrativen Quarantäne und der Quarantäne der Benutzer angezeigt. Schließlich steht für die Einträge der Eingangs- und Zustellungs-Warteschlagen eine Option zur Verfügung, um die Verarbeitung der Warteschlagen anzuhalten und wieder zu starten.

Unter dem Abschnitt Server-Status befindet sich der Abschnitt Server-Statistik. Dieser Abschnitt enthält sechs der grafischen Berichte, die SecurityGateway zur Verfügung stellt: Eingehende/Abgehende Nachrichten 324, Gesamt-Bandbreite für E-Mail 324, Normale/Spam-Nachrichten 324, Aufschlüsselung der Spam-Nachrichten 324, Aktivste E-Mail-Empfänger 326 und Aktivste Spam-Quellen 328. Jeder Bericht enthält die Statistik über die letzten 24 Stunden.

Im Menü für das Dashboard im linken Bereich ist eine Verknüpfung mit der Leitseite für das Dashboard enthalten, und es stehen Verknüpfungen zu den Optionen für Mein Benutzerkonto 32 zur Verfügung, welche die Verwaltung der Einstellungen, der Quarantäne und des Nachrichtenprotokolls für das eigene Benutzerkonto gestatten.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Domänen-Administratoren[60] haben dabei Zugriff auf Statistiken und Optionen nur für die Domänen, für die sie auch über die Administratorrechte verfügen.

Einstellungen/Benutzer[46]

Das Menü *Einstellungen/Benutzer* ist in sieben Abschnitte untergliedert, die Verknüpfungen zu den Kernbereichen der Konfiguration von SecurityGateway enthalten. Die Optionen in diesen Abschnitten dienen der Einrichtung von Domänen und Benutzerkonten, der Konfiguration der Zustellung von Nachrichten, der Quarantäne, der Datensicherung und Wiederherstellung sowie der Optionen für die Datenbank und anderer Einstellungen. Das Menü Einstellungen/Benutzer zerfällt in folgende Abschnitte:

- **Benutzerkonten**[47]—Der Abschnitt Benutzerkonten im Menü *Einstellungen/Benutzer* enthält Optionen und Einstellungen für die Benutzerkonten und Domänen, die SecurityGateway betreut. Dieser Abschnitt enthält fünf Verknüpfungen für Funktionen im Zusammenhang mit Benutzerkonten, wie etwa das Erstellen von Domänen und Benutzerkonten, die Einrichtung von Datenquellen für die Benutzerprüfung, Vorgaben für verschiedene Benutzereinstellungen und vieles mehr.
- **E-Mail-Konfiguration**[78]—Der Abschnitt E-Mail-Konfiguration verweist auf fünf Seiten, die verschiedene Nachrichten-bezogene Funktionen steuern. Sie können die Optionen in diesem Abschnitt etwa nutzen, um festzulegen, auf welchen Servern die E-Mail-Konten Ihrer Benutzer eingerichtet sind, die Einstellungen für die Quarantäne festzulegen, verschiedene Einstellungen zur Nachrichtenzustellung zu bearbeiten und andere technische Einstellungen zu verwalten.
- **Disclaimer (Kopftexte / Fußtexte)**[119]—Disclaimer für Nachrichten sind Textbausteine, die der Server oberhalb oder unterhalb des Nachrichtentexts in eingehende, abgehende und lokale E-Mail-Nachrichten einfügen kann. Mithilfe dieses Konfigurationsdialogs können Sie die Disclaimer erstellen und verwalten.
- **System**[125]—Der Abschnitt System im Menü *Einstellungen/Benutzer* enthält Verknüpfungen mit verschiedenen Systemfunktionen, wie etwa der Verschlüsselung, den Optionen für die HTTP-Schnittstelle, den Verzeichnispfaden und der Verwaltung des freien Speicherplatzes.
- **Datenbank**[143]—Die über diesen Abschnitt erreichbaren Optionen legen Art und Umfang der Daten fest, die SecurityGateway speichert. Sie steuern weiter die Funktionen zur automatischen Datensicherung und die Optionen für die Wiederherstellung des Servers aus Datensicherungen.
- **Lizenzverwaltung**[150]—Im Abschnitt Lizenzverwaltung werden die Informationen zur Lizenz für das Produkt angezeigt; dazu gehören der Name der Person oder die Firma des Lizenznehmers, der Lizenzschlüssel und der Status der Lizenz.

Weitere Informationen können Sie den Übersichten über die einzelnen Abschnitte und den Hilfeseiten zu den einzelnen Abschnitten entnehmen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Sicherheit 154

Das Menü *Sicherheit* ist in acht Abschnitte untergliedert und gestattet den Zugriff auf verschiedene Werkzeuge, mit deren Hilfe Sie Ihre Domänen und Benutzer gegen Spam, Viren, missbräuchliche Nutzung des E-Mail-Systems und andere Sicherheitsrisiken schützen können. Es folgt ein kurzer Überblick über die einzelnen Abschnitte. Weitere Informationen können Sie den Hilfeseiten der einzelnen Abschnitte entnehmen.

- **Anti-Spam** 155—Der Abschnitt Anti-Spam im Menü Sicherheit enthält Optionen, die Ihnen bei der Bekämpfung von Spam und unerwünschten Junk-Nachrichten helfen. Der Abschnitt enthält acht Anti-Spam-Funktionen; dazu gehören Funktionen zur Erkennung und Bekämpfung von Spam durch Heuristische Verfahren, die Bayes'sche Analyse, Schwarze Listen für DNS (DNSBL) und URI (URIBL), die Graue Liste und vieles mehr.
- **Anti-Virus** 187—Der Abschnitt Anti-Virus im Menü Sicherheit enthält Optionen, die Ihnen die Erkennung durch Viren infizierter Nachrichten erleichtern und verhindern, dass diese Nachrichten Ihre Benutzer erreichen. SecurityGateway unterstützt zwei Anti-Virus-Produkte und bietet mit ihrer Hilfe umfassenden Schutz gegen Viren: Clam AntiVirus (ClamAV™) und IKARUS Anti-Virus. ClamAV ist ein quelloffenes, unter der Lizenz GPL veröffentlichtes, Anti-Virus-Modul, das besonders für E-Mail-Gateways entwickelt wurde. IKARUS Anti-Virus bietet zuverlässigen Schutz gegen bösartige und möglicherweise schädliche Programme. Diese Software verbindet herkömmliche Methoden der Virenabwehr mit den neuesten vorausschauend arbeitenden Methoden. SecurityGateway enthält darüber hinaus auch die Outbreak Protection 157, und stellt hierdurch eine zusätzliche Schutzschicht gegen Ausbrüche von Viren und Massenangriffe zur Verfügung.
- **Anti-Spoofing** 190—Der Abschnitt Anti-Spoofing enthält Werkzeuge, die Ihnen bei der Erkennung von Nachrichten helfen, die unter gefälschten ("gespooften") Absender-Adressen versandt werden. In diesem Abschnitt stehen sechs Anti-Spoofing-Methoden zur Verfügung, wie etwa die DKIM-Prüfung, Sender-ID, Prüfung durch Rückruf und viele mehr.
- **Anti-Abuse** 222—Der Abschnitt Anti-Abuse enthält Werkzeuge, die Ihnen helfen, den Missbrauch Ihres E-Mail-Systems durch Dritte zu unterbinden. Zu diesem Missbrauch gehören die Durchleitung von Spam-Nachrichten im Relaisbetrieb, die übermäßige Inanspruchnahme von Übertragungs-Bandbreite, der übermäßig häufige Verbindungsaufbau mit dem Server und ähnliche Verhaltensweisen. Der Abschnitt Anti-Abuse enthält sechs Werkzeuge.
- **Filterung**—Der Abschnitt Filterung enthält zwei Funktionsbereiche: Filterung der Inhalte der Nachrichten 252 und Filterung von Dateianlagen 263. Mithilfe der Filterung der Inhalte der Nachrichten können Filter-Regeln angelegt werden, die verschiedene Aktionen ausführen können. Nachrichten, die bestimmten Kriterien entsprechen, können abgewiesen, kopiert, an eine andere Adresse umgeleitet, in Quarantäne gegeben und auf vielfältige andere Weise behandelt werden. Mithilfe der Optionen zur Filterung von Dateianlagen können Dateitypen festgelegt werden, die zum Abweisen oder zur Quarantäne der Nachricht führen, in der sie gefunden werden. Sie können die Filterung systemweit und nach Domänen getrennt steuern.
- **Schwarze Listen** 265—In den Schwarzen Listen können E-Mail-Adressen, Hosts und IP-Adressen erfasst werden, deren Nachrichten Sie abweisen lassen oder in Quarantäne geben wollen. Per Voreinstellung werden solche

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nachrichten bereits während der SMTP-Verbindung abgewiesen; Sie können die entsprechenden Einstellungen jedoch auf der Seite Aktion der Schwarzen Liste ändern und die Nachrichten stattdessen in Quarantäne geben lassen. Die gewünschte Vorgehensweise kann systemweit und nach Domänen getrennt vorgegeben werden, und auch die Schwarzen Listen selbst können systemweit und nach Domänen getrennt geführt werden.

- **Weiße Listen** 275—In den Weißen Listen können E-Mail-Adressen, Hosts und IP-Adressen erfasst werden, deren Nachrichten von einigen Sicherheitsbeschränkungen ausgenommen sind. Die Funktionen Heuristik, Bayes, DNSBL, DKIM-Prüfung und auch fast alle anderen Sicherheitsfunktionen von SecurityGateway können so konfiguriert werden, dass Absender, Hosts und Nachrichten von der Bearbeitung durch diese Funktionen ausgenommen sind, falls sie einen Treffer auf einer Weißen Liste auslösen. Jede Weiße Liste kann systemweit und nach Domänen getrennt geführt werden.
- **Sieve-Skripte** 284—SecurityGateway nutzt die zum Filtern von E-Mail entwickelte Filtersprache Sieve für viele seiner Funktionen, und die Übersicht über die Sieve-Skripte erlaubt einen Einblick in die Reihenfolge, in der die Funktionen ausgeführt werden. Es steht auch ein Editor für Sieve-Skripte zur Verfügung, mit dessen Hilfe Sie eigene benutzerdefinierte Skripte erstellen können.

Nachrichten/Warteschlangen 306

Nach Auswahl des Menüpunkts Nachrichten/Warteschlangen erhalten Sie Zugriff auf zwei Abschnitte:

- **Nachrichten-Protokoll** 307—Das Nachrichten-Protokoll enthält zu jeder Nachricht, die Ihre Benutzer senden und empfangen, einen eigenen Eintrag. Darin sind Datum und Uhrzeit, zu denen die Nachricht verarbeitet wurde, Absender und Empfänger, sowie der Betreff der Nachricht vermerkt. Das Protokoll gibt außerdem Aufschluss über die Ergebnisse der Zustellversuche, insbesondere, ob die Nachricht zugestellt oder nicht zugestellt wurde. Wurde eine Nachricht nicht zugestellt, so ist auch der Grund aufgeführt, etwa, dass der Absender in einer Schwarzen Liste erfasst war, dass die Nachricht eine gesperrte Dateianlage enthielt, oder ähnliches. Auch die Größe der Nachricht und die Bewertung der Nachricht 185 werden erfasst. Sie können sich zu jeder Nachricht aus dem Nachrichten-Protokoll detaillierte Informationen anzeigen lassen, insbesondere den Mitschnitt der Übermittlung der Nachricht, ihren Inhalt und ihre Quelle (soweit verfügbar). Sie können Nachrichten als Spam oder als normale Nachrichten kennzeichnen und damit die Bayes'schen Lernverfahren von SecurityGateway verfeinern helfen, sodass Nachrichten genauer bewertet werden können.
- **Post-Warteschlangen**—Dieser Abschnitt enthält Verknüpfungen zu vier verschiedenen Warteschlangen für Nachrichten: Quarantäne für Benutzer, Administrative Quarantäne, Nachrichten, die auf die Zustellung warten, und defekte Nachrichten. Die Quarantäne für Benutzer 308 hält eingehende Nachrichten zurück, die bestimmte Sicherheitsprüfungen nicht bestehen. Die Benutzer können sich bei SecurityGateway anmelden und die Inhalte ihrer Quarantäne-Ordner einsehen. Aus der entsprechenden Übersicht können sie sich Nachrichten anzeigen lassen, sie löschen oder sie aus der Quarantäne freigeben, sodass sie normal zugestellt werden können. Die Administrative Quarantäne 310 ist der Quarantäne für Benutzer ähnlich, sie betrifft jedoch abgehende Nachrichten und Nachrichten, die Viren enthalten. Der Zugriff auf die Administrative Quarantäne ist auf Administratoren beschränkt. Die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Warteschlange für Nachrichten, die auf die Zustellung warten[311] enthält alle Nachrichten, die noch nicht zugestellt sind; hierzu gehören auch Nachrichten, deren Zustellung fehlgeschlagen ist, und die auf die erneute Zustellung warten. Sie können sich alle Nachrichten in dieser Warteschlange anzeigen lassen, Nachrichten an die Absender zurück leiten, die Zustellung einer Nachricht unterbinden sowie eine sofortige erneute Zustellung für ausgewählte oder alle Nachrichten in der Warteschlange veranlassen. Die Warteschlange für Defekte Nachrichten[312] enthält Nachrichten, die wegen nicht behebbarer Fehler in der Zustellung nicht zugestellt werden konnten; dies sind beispielsweise Nachrichten in einer Endlosschleife, die die *Höchstzahl der Zwischenstationen*[95] bereits erreicht haben. Sie können sich alle Nachrichten in dieser Warteschlange anzeigen lassen, Nachrichten an ihre Absender zurück leiten, löschen sowie eine sofortige erneute Zustellung für ausgewählte oder alle Nachrichten in der Warteschlange veranlassen.

Protokollierung[316]

Nach Auswahl des Menüpunkts Protokollierung erhalten Sie Zugriff auf drei Abschnitte:

- **Nachrichten-Protokoll**[317]—Diese Verknüpfung führt ebenfalls zu dem Nachrichten-Protokoll, das bereits im Abschnitt Nachrichten/Warteschlangen weiter oben beschrieben wurde. Die Verknüpfung wird aus Gründen der einfacheren Bedienung für den Administrator auch an dieser Stelle angeboten.
- **Protokolldateien**[318]—Im Abschnitt Protokolldateien erhalten Sie Zugriff auf die verschiedenen Protokolldateien, die SecurityGateway im Verzeichnis für Protokolle[134] ablegt. Im Gegensatz zum Nachrichten-Protokoll werden diese Protokolle nicht in der Datenbank abgelegt. Sie können daher nicht als sortierfähige Listen angezeigt werden, und ihre Einträge sind nicht nach Ereignissen gruppiert oder getrennt. Sie liegen vielmehr als Nur-Text-Dateien vor, in denen die Mitschnitte der verschiedenen SMTP-Verbindungen und der anderen Aktionen verzeichnet sind, die SecurityGateway bearbeitet. Die Seite Alle Protokolldateien im Abschnitt Protokolldateien macht alle Protokolldateien zugänglich, die im Ordner "logs" (Protokolle) enthalten sind. Dazu gehören die aktuellen Protokolldateien und frühere[320] Protokolldateien, die archiviert wurden. Von dieser Seite aus können Sie alle dort aufgeführten Dateien einsehen. Die anderen Seiten im Abschnitt Protokolldateien enthalten Verknüpfungen mit den jeweils aktuellen Protokolldateien, die SecurityGateway führt; dazu gehören das System-Protokoll, die Eingangs- und Ausgangs-Protokolle und Protokolle über die AntiVirus-Aktualisierung.
- **Konfiguration**[320]—Der Abschnitt Konfiguration enthält eine Verknüpfung mit der Seite für die Konfiguration des Protokolls, auf der die Einstellungen und Optionen für die Protokollierung eingerichtet werden. Auf dieser Seite können Sie festlegen, in welchem Detaillierungsgrad die Eingangs-, Ausgangs- und HTTP-Protokolle geführt werden. Sie können auch wählen, in welcher Weise die Protokolldateien angelegt werden sollen: Zur Auswahl stehen ein Standardsatz Protokolldateien, ein neuer Satz Protokolldateien für jeden Tag, deren Dateinamen das Erstellungsdatum enthält, und ein neuer Satz Protokolldateien, der nach Wochentagen getrennt angelegt wird, und dessen Dateinamen die Namen der Wochentage enthalten. Schließlich können Sie auch verschiedene Einstellungen zur Pflege der Protokolle festlegen; hierzu gehören eine Größenbegrenzung, bei deren Erreichen eine Protokolldatei archiviert und eine neue Datei begonnen werden, die Anzahl solcher archivierter Protokolldateien, die auf dem System höchstens verbleiben

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

sollen, und die Zeit, für die ein Protokoll höchstens bestehen kann, bevor es in jedem Falle archiviert wird.

Berichte 324

Im Abschnitt Berichte stehen interaktive, detailreiche grafische Berichte über die Aktivität von SecurityGateway zur Verfügung. Sie können Berichte erstellen, die die Anzahl der eingehenden im Vergleich zu den abgehenden Nachrichten zeigen, eine Übersicht über die Arten von Spam- oder Junk-Nachrichten geben, die Bandbreitennutzung aufschlüsseln, die aktivsten Absender nach Gesamt-Nachrichtengröße zeigen, Übersichten über erkannte Viren geben, und viele weitere Angaben enthalten. Jeder Bericht kann außerdem mithilfe besonderer Optionen konfiguriert werden. So kann ein Bericht etwa Daten nur für eine bestimmte Domäne oder für alle Domänen enthalten, der Maßstab der Daten lässt sich nach Stunden, Tagen und Monaten auflösen, und der Bericht kann sich wahlweise auf festgelegte Zeiträume beziehen, etwa einen Tag, eine Woche, einen Monat, oder den Zeitraum zwischen zwei Daten. Unterhalb jedes Berichts wird ihr Inhalt tabellarisch dargestellt. Diese Darstellung enthält Verknüpfungen mit dem Nachrichten-Protokoll, die eine Anzeige nur derjenigen Daten aus dem Protokoll bewirken, die sich auf die Daten aus dem Bericht beziehen. Eine solche Verknüpfung kann beispielsweise alle eingehenden Nachrichten anzeigen, die zu einer bestimmten Stunde empfangen wurden, die auch im Bericht dargestellt wird, alle Nachrichten, die einen Virus enthielten und an einem bestimmten Tag eingingen, und alle Nachrichten, die durch den aktivsten Empfänger in einer Domäne empfangen wurden.

System-Anforderungen

Sie erhalten einen Überblick über die neuesten System-Anforderungen und die Empfehlungen für SecurityGateway in dem in englischer Sprache verfügbaren Artikel SecurityGateway für E-Mail-Server - System-Anforderungen. Sie können über die Website www.mdaemon.com auf diesen Artikel zugreifen.

So erhalten Sie weitere Hilfe

Die neuesten Informationen zur technischen Unterstützung für SecurityGateway sowie unter anderem Unterstützung über E-Mail und Telefon, eine Wissens-Datenbank, häufig gestellte Fragen (FAQ), Foren und vieles mehr erhalten und erreichen Sie unter www.mdaemon.com/Support/.

SecurityGateway 9.0.3 - Juni 2023

1.2 Neuigkeiten in Version 9.0

Zur besonderen Beachtung

- 9.0.3 — Das Leistungsmerkmal Outbreak Protection 157 ist wieder verfügbar. Bitte prüfen Sie Ihre Einstellungen für die Outbreak Protection; es ist möglich, dass diese auf die Voreinstellungen zurückgesetzt wurden.
- 9.0.2 — Cyren Anti-Virus wurde durch IKARUS Anti-Virus ersetzt. Cyren hat kürzlich die Absicht mitgeteilt, den Geschäftsbetrieb kurzfristig einzustellen. Hieraus hat sich die Notwendigkeit ergeben, einen neuen Anti-Virus-Partner zu finden. In einem gründlichen Auswahlprozess hat sich IKARUS Anti-Virus durch seine exzellente Erkennungsrate und Geschwindigkeit herausgehoben. IKARUS Anti-Virus bietet zuverlässigen Schutz gegen bösartige und möglicherweise schädliche Programme. Diese Software verbindet

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

herkömmliche Methoden der Virenabwehr mit den neuesten vorausschauend arbeitenden Methoden. IKARUS Anti-Virus aktualisiert die Virendefinitionen automatisch alle 10 Minuten.

- 9.0.2 — Das Modul Cyren Outbreak Protection wurde entfernt. Cyren hat kürzlich die Absicht mitgeteilt, den Geschäftsbetrieb kurzfristig einzustellen. Es werden mögliche Anti-Spam-Techniken derzeit auf Eignung geprüft, um sie möglicherweise den bestehenden Maßnahmen gegen Spam in den Software-Produkten hinzuzufügen.
- 9.0.0 — Postfachnamen, die Pluszeichen (+) enthalten, werden ab jetzt per Voreinstellung als subadressiert 77 behandelt. Im Rahmen der Benutzerprüfung wird die Subadresse als Alias behandelt. Ein Beispiel hierzu: Der Benutzer `benutzer+ordner@example.com` wird aufgelöst in `benutzer@example.com` und in einen Alias, bei dem `benutzer+ordner@example.com` auf `benutzer@example.com` verweist. Bei neu zu erstellenden Benutzerkonten sind Pluszeichen im Postfachnamen nicht mehr zugelassen. Bei bestehenden Benutzerkonten werden etwa in den Postfachnamen vorhandene Pluszeichen nicht automatisch entfernt; auch werden die Benutzerkonten selbst nicht entfernt. Sie können bereinigt werden, indem auf der Seite Datenquellen für Benutzerprüfung 63 der Vorgang Benutzer prüfen ausgeführt wird. Im Rahmen der Bereinigung können die Postfachnamen umbenannt oder zusammengeführt werden. Wahlweise kann auch die bisherige Verhaltensweise beibehalten werden; hierfür steht im Menü Benutzer-Optionen 73 die neue Option "*Pluszeichen (+) in Postfachnamen der Benutzer zulassen*" zur Verfügung. Wenn diese Option aktiv ist, werden Postfachnamen, die Pluszeichen enthalten, nicht wie Aliasnamen und Subadressen behandelt. Ein Beispiel hierzu: `benutzer+ordner@example.com` wird als eigener Benutzer und nicht als Alias von `benutzer@example.com` behandelt.

Besonders wichtige neue Leistungsmerkmale

Auswertung der Absenderkopfzeile From 220

Im Menü Sicherheit 154 wurde dem Abschnitt Anti-Spoofing 190 die neue Seite Auswertung der Absenderkopfzeile From 220 hinzugefügt. Mithilfe der in ihr enthaltenen Optionen können in betrügerischer Absicht gefälschte Absenderkopfzeilen (From) entdeckt werden, die Spammer in Nachrichten einfügen, und die den Benutzern vorspiegeln sollen, dass die Nachricht aus einer vertrauenswürdigen Quelle stammt.

Verbesserungen in der Handhabung der Web-Schnittstelle

- Die Dialogfunktionen für die Suche lassen sich jetzt anzeigen und ausblenden. Darüber hinaus wurde die Haupt-Symbolleiste um eine Schaltfläche zum Abbruch einer Suche erweitert.
- Den Übersichtsseiten für Nachrichten 307 können jetzt bis zu vier weitere Suchmuster für Kopfzeilen, Ergebnisse und Gründe hinzugefügt werden. Die Muster für Kopfzeilen können mithilfe eines Symbols auf der Symbolleiste durch UND/ODER (AND/OR) getrennt werden. Ergebnisse und Gründe werden immer durch ODER (OR) getrennt.
- Die Symbolleiste auf den Seiten Liste der Domänen 48 und Liste der Benutzer 57 wurde um eine einfache Suchfunktion erweitert.
- Popup-Fenster können jetzt in der Größe verändert, verschoben und maximiert werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- Es wurde ein Listen-Editor hinzugefügt, der für Mobilgeräte besonders geeignet ist.
- Die Übersicht über die archivierten Nachrichten wurde um Schaltflächen zum Vor- und Zurückspringen erweitert.
- In der unteren rechten Ecke der Seiten zum Durchsuchen archivierter Nachrichten[109] erscheint jetzt bei Bedarf eine Meldung, dass Nachrichten wieder hergestellt wurden.

Verbesserungen auf dem Dashboard für Administratoren

- Das Dashboard[9] und das Menü Einstellungen/Benutzer » System » Speicherplatz[135] zeigen den globalen Administratoren jetzt den auf den Datenträgern verfügbare Speicherplatz an.
- Das Dashboard zeigt jetzt die Zahl der aktiven ein- und abgehenden SMTP-Verbindungen an.
- Das Dashboard zeigt den globalen Administratoren jetzt die Zahl der Nachrichten an, die sich in administrativer Quarantäne und Quarantäne der Benutzer befinden.
- Die Eingangs-Warteschlange und die Warteschlange für externe Zustellung können jetzt angehalten werden.

Weitere Leistungsmerkmale und Änderungen

- Im Menü Einstellungen | System | HTTP-Server steht eine neue Option zur Verfügung, mit deren Hilfe in die HTTPS-Antworten der Header HTTP Strict Transport Security (HSTS)[132] eingefügt werden kann. Diese Option ist per Voreinstellung aktiv. Empfängt ein Browser, der HSTS unterstützt, einen HSTS-Header, und ist das SSL-Zertifikat gültig, so werden alle weitere HTTP-Anforderungen an dieselbe Domäne automatisch auf HTTPS umgestellt.
- SecurityGateway unterstützt auf neueren Versionen von Microsoft Windows jetzt TLS 1.3. Auf Microsoft Windows Server 2022 und Microsoft Windows 11 ist TLS 1.3 per Voreinstellung aktiv. Microsoft Windows 10 beinhaltet ab Version 2004 (Build 19041) experimentelle Unterstützung für TLS 1.3. Sie kann für eingehende Verbindungen durch Bearbeiten des folgenden Schlüssels in der System-Registrierungsdatenbank aktiviert werden:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Securit
  yProviders\SCHANNEL\Protocols\TLS 1.3\Server

DisabledByDefault (DWORD) = 0

Enabled (DWORD) = 1
```

- Benutzer können jetzt die Nachrichten einsehen, die in ihren Quarantäne-Berichten aufgeführt sind. Ob diese Vorgehensweise zulässig ist, bestimmen die globalen Administratoren mithilfe einer neuen Option im Menü Einstellungen/Benutzer » E-Mail-Konfiguration » Quarantäne-Konfiguration[86] oder unter Hauptmenü » Mein Benutzerkonto » Einstellungen[34].
- Wenn für das gerade genutzte Gerät oder den gerade genutzten Browser eines Benutzers die Option Anmeldung auf diesem Gerät speichern und beibehalten[73] aktiv ist, dann erscheint auf der Seite Mein Benutzerkonto » Einstellungen des Benutzers[34] jetzt die Option *Anmeldung auf diesem Gerät/in diesem Browser nicht speichern*. Mithilfe dieser Option können die Benutzer die auf dem Gerät gespeicherten Daten zur Anmeldung löschen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Danach wird die Option wieder ausgeblendet. Die Benutzer können bei der nächsten Anmeldung an SecurityGateway die Option zum Speichern und Beibehalten der Anmeldung auf diesem Gerät wieder aktivieren. Diese Option steht auch den Benutzern der Leistungsmerkmale für sichere Nachrichten[115] zur Verfügung, wenn sie ihre Anmeldung gespeichert haben.

- Mithilfe neuer Optionen auf den Seiten Benutzerkonten » Benutzer-Optionen[73] und Sichere Nachrichten » Empfänger-Optionen[115] können die Administratoren den Anmeldeseiten für SecurityGateway und dem Web-Portal für sichere Nachrichten Kontaktdaten oder eine Kontakt-Verknüpfung hinzufügen.
- Der Editor für die Datenquellen für Benutzerprüfung[66] wurde um eine Schaltfläche "Speichern und prüfen" erweitert.
- Die Anmeldeseite unterstützt jetzt CSRF-Token sowie sekundäre Session-IDs zum Schutz gegen Cross-Site-Request-Forgery.
- Das Leistungsmerkmal zum Speichern von Anmeldedaten[73] unterstützt jetzt als Prüfmethode auch Schlüsselpaare aus öffentlichen und privaten Schlüsseln.
- Die Nachrichtentexte für die Benachrichtigungen über sichere Nachrichten wurden im Erscheinungsbild und inhaltlich aktualisiert.
- Die Zahl der Datenbank-Transaktionen wurde verringert. Dies trägt dazu bei, einen übermäßigen Größenzuwachs der Datenbank zu verhindern.
- Der Host "`vbr.emailcertifcation.org`" für die Zertifizierung über VBR wurde abgeschafft und aus den Einstellungen zur Zertifizierung von Nachrichten[179] entfernt.
- Das Menü Archivierung » Einhaltung von Vorschriften[110] wurde um die Option "*Nachrichten nur aus aktiven Archiv-Speichern löschen*" erweitert. Diese Option bestimmt, ob die Einstellung "*Archivierte Nachrichten automatisch löschen nach Überschreiten eines Alters von (x) Tagen*" nur auf aktive Archiv-Speicher wirkt. Die Option ist per Voreinstellung aktiv; damit bleibt die Verhaltensweise gegenüber den bisherigen Programmversionen unverändert.
- Die SMTP-Socketverbindung wird jetzt für die SIEVE-Aktionen "Fehler" (error) und "Abweisen" (reject) getrennt, falls diese Aktionen während der Auswertung der IP-Adressen ausgelöst werden.
- Beim Programmstart werden jetzt alle gesperrten Nachrichten, die in der Eingangs-Warteschlange noch etwa vorhanden sind, in das Verzeichnis `CrashDumps\InboundQueue` verschoben. Nachrichten in der Eingangs-Warteschlange werden entsperrt, wenn im SMTP-Protokolldialog eine Antwort an den Absender gesendet wird. Gesperrte Nachrichten können irrtümlich in der Eingangs-Warteschlange verbleiben, falls SecurityGateway abstürzt oder abrupt beendet wird, bevor eine ordnungsgemäße Beendigung mit Abschluss der Verarbeitungsvorgänge möglich war. In einem solchen Fall hat der Absender keine Antwort auf den SMTP-Befehl `DATA` erhalten, sodass zu erwarten ist, dass er von sich aus die Nachricht erneut übermittelt. Wird die Nachricht dennoch aus der Eingangs-Warteschlange zugestellt, so erhält der Empfänger dann möglicherweise dieselbe Nachricht mehrfach. Der Inhalt der Nachrichten kann aber zur Fehlersuche hilfreich sein, weswegen sie nicht ohne weiteres gelöscht werden. Nachrichten, die in das genannte Verzeichnis verschoben wurden, werden nach 30 Tagen automatisch gelöscht.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- LetsEncrypt[131] - Die Funktionen für die Protokollierung wurden geändert. Sie nutzen jetzt nicht mehr das PowerShell-Cmdlet Out-File sondern Add-Content. Add-Content nutzt die Standard-Zeichensatztabelle (Codepage) des Systems. Infolge dieser Änderung sollte es möglich werden, die Protokolldatei in SecurityGateway zu betrachten. Die Zeichensatztabelle für bestehende Protokolldateien wird nicht geändert; die Änderung wird erst mit Erstellung einer neuen Protokolldatei wirksam.

Eine vollständige Liste aller weiteren Änderungen und Fehlerbehebungen ist in den Versionsinformationen für SecurityGateway enthalten. Sie können die Versionsinformationen über die Programmgruppe für SecurityGateway im Windows-Startmenü aufrufen.

Neuigkeiten in Version 8.5.0

Zur besonderen Beachtung

Die 32-Bit-Versionen (Builds) der Software und die Unterstützung für 32-Bit-Betriebssysteme wurden eingestellt. Ab SecurityGateway 8.5.0 werden nur noch 64-Bit-Versionen veröffentlicht. Hierdurch können Entwicklung und Tests rationalisiert werden. Darüber hinaus können nun auch Bibliotheken eingesetzt werden, von denen ausschließlich 64-Bit-Versionen zur Verfügung stehen. Falls Sie derzeit eine 32-Bit-Version auf einem unterstützten 64-Bit-Betriebssystem einsetzen, können Sie die 64-Bit-Version herunterladen und einfach über die bestehende Installation installieren.

Besonders wichtige neue Leistungsmerkmale

Webportal für sichere Nachrichten[112]

Mithilfe des neuen Leistungsmerkmals für sichere Nachrichten können Ihre Benutzer über SecurityGateway sichere Nachrichten an Empfänger außerhalb ihrer eigenen Domänen senden, ohne dass die sicheren Nachrichten dabei den SecurityGateway-Server verlassen. Die Nachrichten werden dabei mithilfe eines Web-Portals für sichere Nachrichten übermittelt. Wird eine Nachricht versandt, so erhält der Empfänger eine Benachrichtigung per E-Mail. Sie verständigt ihn davon, dass für ihn eine sichere Nachricht vorliegt, und sie enthält eine Verknüpfung, mit deren Hilfe er ein Benutzerkonto als Empfänger sicherer Nachrichten[113] erstellen kann. Über diese Benutzerkonten können die Empfänger sichere Nachrichten auf Ihrem SecurityGateway-Server lesen. Die Empfänger greifen dabei mithilfe ihrer Browser auf die Nachrichten zu, und für die Verbindung zwischen dem SecurityGateway-Server und dem Empfänger besteht Ende-zu-Ende-Verschlüsselung über HTTPS. Die Leistungsmerkmale für sichere Nachrichten erfordern ein gültiges SSL-Zertifikat[129], auch muss HTTPS aktiv sein[126] (siehe auch die Beschreibung im Abschnitt HTTPS-Server[132]). Die Empfänger können die Nachrichten im SecurityGateway-Portal lesen und beantworten. Sie können auch wahlweise neue sichere Nachrichten an hierfür festgelegte Benutzer verfassen[119]. Sie finden in den Abschnitten Empfänger[113] and Empfänger-Optionen[115] nähere Informationen über Benutzerkonten für die Empfänger sicherer Nachrichten.

Benutzerabhängiges Nachrichten-Routing

- Mithilfe der Optionen im neuen Abschnitt Postausgang auf der Seite Benutzer bearbeiten[57] können Sie jetzt die Nachrichten bestimmter Benutzer durch besonders festgelegte Mailserver der Domäne verarbeiten lassen. Die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nachrichten so konfigurierter Benutzer werden nicht über die Standard-Mailserver der jeweiligen Domäne übermittelt.

- Der Konfigurationsdialog für die Domänen[50] wurde eine neue Option hinzugefügt: "*Mail-Server nur für Zuweisung zu bestimmten Domänen-Benutzern verfügbar machen und nicht allgemein für Zustellung der Nachrichten der Domäne nutzen*".
- Diese Leistungsmerkmale gestatteen den Betrieb gemischter Infrastrukturen, in denen die Postfächer einiger Benutzer in Clouddiensten und die Postfächer anderer Benutzer lokal gehostet werden. Sie gestatten es auch, eine einzige Domäne und einen einzigen SecurityGateway-Server zu nutzen, um Nachrichten an physikalisch voneinander getrennte Mailserver zu senden, etwa Mailserver in einzelnen Niederlassungen eines Unternehmens.

Leistungsindikatoren (Performance Counter)[330]

SecurityGateway stellt jetzt auch verschiedene Leistungsindikatoren (sie werden auch als Performance Counter bezeichnet) zur Verfügung, die in der Windows-Leistungsüberwachung (sie wird auch als Windows Performance Monitor bezeichnet) verwendet werden können. Sie können hiermit den Status von SecurityGateway in Echtzeit überwachen. Die zur Verfügung stehenden Leistungsindikatoren sind unter anderem: Zahl der aktiven Verbindungen, Zahl der Nachrichten in den Warteschlangen, Status der Serverdienste als aktiv oder nicht aktiv, Betriebszeit seit Programmstart, Zahl der Domänen und Zahl der Benutzer.

Weitere Leistungsmerkmale und Änderungen

- Dem Konfigurationsdialog Benutzer-Optionen[73] wurde eine neue Option hinzugefügt, mit deren Hilfe die Nutzung starker Kennwörter erzwungen werden kann. Diese Option kann für jeden Benutzer einzeln auf der Seite Benutzer bearbeiten[57] deaktiviert werden.
- Auf den Seiten Dashboard und Lizenzverwaltung erscheint jetzt ein Hinweis, falls ein Lizenzschlüssel des Typs Service-Provider oder Private Cloud verwendet wird.
- Beim Filtern von Dateianlagen stehen jetzt Weiße Listen für Empfänger zur Verfügung.[263] In den E-Mail-Adressen der Empfänger werden dabei auch Jokerzeichen unterstützt. Für das Filtern von Dateianlagen und die Quarantäne für Dateianlagen können hiermit Listen von Empfänger-Adressen erfasst werden. Für diese Empfänger-Adressen werden die Leistungsmerkmale zum Filtern und zur Quarantäne für Dateianlagen übergangen.
- Lets Encrypt - Das Skript löscht die Protokolldatei nicht mehr bei jeder Ausführung.

Eine vollständige Liste aller weiteren Änderungen und Fehlerbehebungen ist in den Versionsinformationen für SecurityGateway enthalten. Sie können die Versionsinformationen über die Programmgruppe für SecurityGateway im Windows-Startmenü aufrufen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Neuigkeiten in Version 8.0.0

Besonders wichtige neue Leistungsmerkmale

- SecurityGateway unterstützt grundsätzlich die Datenbankreplikation aktiv-aktiv für Ihren Cluster-Betrieb[137]. Es ist hierfür aber ein externes Hilfsprogramm für die Replikation erforderlich. Dessen Konfiguration ist nicht in der vorliegenden Hilfedatei beschrieben. Sie finden Informationen über die Anforderungen und Hinweise zur Konfiguration Ihres Clusters für die Replikation aktiv-aktiv in folgendem, in englischer Sprache verfügbaren PDF: SecurityGateway: Configuring Active-Active Database Replication.
- Data Leak Prevention (Schutz gegen Datendiebstahl) - Suche nach medizinischen Begriffen[249]. Nachrichten können jetzt nach medizinischen Begriffen durchsucht werden. Sie können hierzu eine Liste medizinischer Begriffe definieren und jedem Begriff einen Punktwert als Bewertung zuweisen. Die Nachrichten werden nach diesen Begriffen durchsucht, und die Bewertungen aller jeweils gefundenen Begriffe werden zusammengezählt. Ergibt sich für eine Nachricht eine Bewertung über den angegebenen Schwellwerten, so werden die den Schwellwerten zugeordneten Aktionen ausgeführt.
- Sie können ab jetzt während der Verarbeitung der Nachrichten benutzerdefinierte Prozesse und Skripte ausführen und Aktionen in Abhängigkeit von den Ergebnissen dieser Prozesse und Skripte definieren.
  - Die auszuführenden Skripte müssen im Verzeichnis "*Ausführbare Dateien für Sieve-Skripte*" abgelegt werden. Dieses Verzeichnis können Sie über Einstellungen » System » Verzeichnisse[134] konfigurieren.
  - Das Sieve-Schlüsselwort "execute[296]" ("ausführen") wurde hinzugefügt. Es kann sowohl als Aktion als auch als Test verwendet werden.
  - Der erste Parameter ist der Name des Skripts. Derzeit werden .bat, .exe und PowerShell unterstützt.
  - er zweite Parameter sind die Argumente und Parameter, die an den Prozess übergeben werden. Der Parameter `message_filename` wird in den vollständigen Pfad- und Dateinamen der RFC822-Quelldatei für die gerade bearbeitete Nachricht umgesetzt.
  - Ein Beispiel hierzu: `if execute "Test.ps1" "-msg '${message_filename}'" { }`
- Alle für eine Domäne archivierten Nachrichten können jetzt exportiert werden[111].
- Änderungsprotokoll[318] - Das Änderungsprotokoll steht ab jetzt als neues Protokoll zur Verfügung. In ihm sind alle Änderungen an der Konfiguration und die Nutzer vermerkt, die diese Änderungen durchgeführt haben.
- Die Quarantäne-Berichte für die Quarantäne für Benutzer und die Administrative Quarantäne können jetzt nach einem konfigurierbaren Zeitplan versandt werden[86].
- Mithilfe einer neuen Option[86] können die per E-Mail versandten Quarantäne-Berichte angepasst werden. Diese Option bewirkt, dass nur die Nachrichten im Quarantäne-Bericht aufgeführt werden, die seit dem Versand des letzten Quarantäne-Berichts neu in den Quarantäne-Ordner eingestellt wurden. Falls

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

keine Nachrichten vorhanden sind, die in den Bericht aufgenommen werden müssten, wird kein Quarantäne-Bericht erstellt.

Weitere Leistungsmerkmale und Änderungen

- Die Vorgehensweise für das Zurücksetzen vergessener Kennwörter[73] wurde geändert. Es wird jetzt eine E-Mail-Nachricht mit einer Verknüpfung versandt, mit deren Hilfe der Benutzer sein Kennwort ändern kann.
- LetsEncrypt[126] - Das Skript wurde aktualisiert und wertet jetzt den neuen Aussteller (Issuer) aus, den LetsEncrypt verwendet.
- Das DKIM-Signaturverfahren[199] wurde aktualisiert und nutzt jetzt als Hash-Algorithmus SHA256.
- Das XMLRPC-API und das PowerShell-Modul wurden um die Methoden `GetServerSetting` und `PutServerSetting` erweitert.
- Die Seite Einstellungen » E-Mail-Konfiguration » E-Mail-Protokoll[92] wurde um Zeitüberschreitungen (Timeouts) für SMTP-Verbindungen und SMTP-Protokolldialoge erweitert.
- Auf der Seite Nachrichten-Protokoll[317] » Nachrichten-Informationen » Nachricht können jetzt die Dateianlagen heruntergeladen werden.
- Die Popups für Warnungen, Bestätigungen und Abfragen wurden aktualisiert.
- Dem Verzeichnis `docs\API\PowerShell Samples` wurden mehrere PowerShell-Beispielskripte hinzugefügt, die zu Referenzzwecken dienen.
- Im Cluster-Betrieb ist der Wert für das Feld HELO-Domänenname[92] (erreichbar über Einstellungen » E-Mail-Konfiguration » E-Mail-Protokoll) jetzt nach Servern getrennt festzulegen. Der Wert kann auf jedem Server im Cluster eindeutig und getrennt konfiguriert werden.
- Über die Weboberfläche können jetzt SQL-Statements manuell[149] auf der Datenbank ausgeführt werden. Von dieser Möglichkeit sollten Sie aber nur Gebrauch machen, wenn der technische Support Sie hierzu auffordert. Es empfiehlt sich, dass Sie eine Datensicherung der Datenbank erstellen, bevor Sie ein SQL-Statement auf der Datenbank ausführen.
- Mithilfe einer neuen Option kann die Verknüpfung "Domäne der Schwarzen Liste hinzufügen" in die per E-Mail versandten Quarantäne-Berichte[86] aufgenommen werden.

Eine vollständige Liste aller weiteren Änderungen und Fehlerbehebungen ist in den Versionsinformationen für SecurityGateway enthalten. Sie können die Versionsinformationen über die Programmgruppe für SecurityGateway im Windows-Startmenü aufrufen.

Neuigkeiten in Version 7.0.0

Zur besonderen Beachtung

- Aus der Seite E-Mail-Protokoll[92] (zu erreichen über Einstellungen » E-Mail-Konfiguration » E-Mail-Protokoll) wurden zwei Optionen entfernt, und zwar die Option, nach Möglichkeit ESMTP zu nutzen, und die Option, den ESMTP-Befehlsparameter SIZE zu unterdrücken. Beide Leistungsmerkmale werden

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

jetzt stets den Gegenstellen bekannt gegeben, und ESMTP wird stets verwendet, soweit möglich.

- In der Datei `clamd.conf` haben sich Änderungen ergeben, und viele Einstellungen werden nicht mehr unterstützt. Die Installationsroutine überschreibt daher eine bestehende Datei `clamd.conf`. Falls Sie Ihre Datei `clamd.conf` angepasst haben, müssen Sie die Datei `clamd.conf` nach der Installation überprüfen und möglicherweise anpassen.
- Die Option, nach Wochentagen getrennte Protokolldateien zu erstellen, wurde aus der Konfiguration der Protokollierung[320] entfernt. Falls diese Option bislang aktiv war, wurde während der Aktualisierung stattdessen die Option "*Jeden Tag einen neuen Satz Protokolldateien anlegen*" aktiviert.

Änderungen und neue Leistungsmerkmale

Cluster-Betrieb[137]

Die neuen Leistungsmerkmale für den Cluster-Betrieb von SecurityGateway ermöglichen die gemeinsame Nutzung Ihrer Konfiguration durch mehrere SecurityGateway-Server in Ihrem Netzwerk. Hiermit können Sie beispielsweise Lastverteilung für die Hardware- oder Software-Auslastung umsetzen und die im E-Mail-Betrieb anfallende Systemlast auf mehrere SecurityGateway-Server verteilen. Dies kann durch möglichst große Ausnutzung Ihrer E-Mail-Ressourcen Verarbeitungsgeschwindigkeit und Effizienz erhöhen, die Netzwerkauslastung senken und Überlastungen verringern. Es kann außerdem die Ausfallsicherheit Ihrer E-Mail-Systeme in den Fällen erhöhen, in denen auf einem Server ein Hardware- oder Softwareausfall eintritt. Die nachfolgende Übersicht soll Ihnen die Kriterien vermitteln, nach denen Sie entscheiden können, ob Sie in Ihrem Netzwerk den Cluster-Betrieb für SecurityGateway einführen wollen (ausführliche Informationen und eine Anleitung zur Einrichtung finden Sie im Abschnitt Cluster-Betrieb[137]):

- Der Cluster-Betrieb gestattet mehreren aktiven SecurityGateway-Instanzen oder -Servern die gemeinsame Nutzung derselben Datenbank.
- Hierzu muss ein externer Firebird-Datenbankserver der Version 3 manuell installiert und konfiguriert werden.
- Die Installationsroutine wurde um eine Option ergänzt, mit deren Hilfe die Serverdaten des externen Firebird-Datenbankservers angegeben werden können. Diese Option steht nur bei Neuinstallationen zur Verfügung. Bestehende Installationen können mithilfe des Befehlszeilenprogramms sgdbtool.exe auf die Nutzung eines externen Firebird-Datenbankservers umgestellt werden.
- Gemeinsamer Dateizugriff ist erforderlich. Es müssen freigegebene Verzeichnisse vorhanden und über einen UNC-Pfad für alle Server im Cluster zugänglich sein. Um diese Anforderung zu erfüllen, muss möglicherweise das Benutzerkonto für den Windows-Dienst SecurityGateway[143] geändert werden.
- Der Primär-Server ist für die geplanten Wartungsaufgaben verantwortlich.
- Für jeden Server im Cluster muss ein eigener, gesonderter Lizenzschlüssel vorhanden sein.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Aktualisierung der Datenbank auf Firebird 3 139

- Die Installationsroutine enthält und installiert Laufzeitversionen für Firebird 2 und 3 in SecurityGateway 7.0.
- Bei Neuinstallationen von SecurityGateway 7.0 oder einer neueren Version wird Firebird 3 genutzt.
- Bei der Aktualisierung einer bestehenden SecurityGateway-Installation auf SecurityGateway Version 7 oder eine neuere Version wird weiterhin Firebird 2 genutzt.
- Die Nutzung der neuen Leistungsmerkmale für den Cluster-Betrieb 137 erfordert eine Datenbank des Formats Firebird 3.
- Die Datenbank kann aktualisiert werden, sodass sie zu Firebird 3 kompatibel wird. Hierzu muss die Datenbank mithilfe der Laufzeitversion für die Version 2.x gesichert und mithilfe der Laufzeitversion für die Version 3.x wieder hergestellt werden. Der Administrator kann eine bestehende Datenbank von Version 2 auf Version 3 mithilfe des Befehlszeilenprogramms `sgdbtool.exe` aktualisieren. Dieses Programm befindet sich im Verzeichnis `\SecurityGateway\App`. Um die Datenbank zu aktualisieren, beenden Sie den Dienst SecurityGateway, und führen Sie in einer Windows-Befehlszeile den Befehl "**`sgdbtool.exe convertfb3`**" aus.

Zwei-Faktor-Authentifizierung 73

Die Administratoren können auf der Seite Benutzer-Optionen 73 bestimmen, ob die Zweifaktor-Authentifizierung (2FA) genutzt werden darf oder verpflichtend zu nutzen ist. Falls die Zweifaktor-Authentifizierung verpflichtend genutzt werden muss, wird den Benutzern bei der ersten Anmeldung eine Seite angezeigt, auf der er die Zweifaktor-Authentifizierung einrichten kann. Ansonsten können die Benutzer die Zweifaktor-Authentifizierung auf der Seite Hauptmenü » Mein Benutzerkonto » Zwei-Faktor-Authentifizierung 33 die Zwei-Faktor-Authentifizierung konfigurieren.

Prüfung auf kompromittierte Kennwörter 76

SecurityGateway kann die Kennwörter der Benutzer mit einer Liste als kompromittiert bekannter Kennwörter abgleichen, die durch einen Drittanbieter bereit gestellt wird. Der Abgleich findet statt, ohne dass das Kennwort an den Anbieter übermittelt wird. Ist das Kennwort eines Benutzers in der Liste vorhanden, so bedeutet dies nicht, dass das Benutzerkonto kompromittiert oder gehackt wurde. Es bedeutet vielmehr, dass das fragliche Kennwort bereits einmal auf einem anderen System durch einen Benutzer verwendet wurde, und dass dieses verwendete Kennwort von einer Datenpanne oder einem Datenleck betroffen war. Kennwörter, die als kompromittiert bekannt und veröffentlicht sind, können durch Angreifer für Wörterbuchangriffe verwendet werden. Kennwörter, die noch nie auf anderen Systemen verwendet wurden, sind demgegenüber sicherer. Nähere Informationen hierzu erhalten Sie in englischer Sprache unter Pwned Passwords.

Domänen-Administratoren können neue Domänen erstellen 61

Mithilfe einer neuen Option auf der Seite Administrator bearbeiten 61 können Sie Domänen-Administratoren die Berechtigung erteilen, neue Domänen zu erstellen. Erstellt ein Domänen-Administrator eine neue Domäne, so erhält er automatisch die Berechtigungsstufe des Domänen-Administrators auch für diese durch ihn erstellte

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Domäne. Die Anzahl der Domänen, die ein Domänen-Administrator erstellen darf, kann mithilfe einer weiteren Option begrenzt werden.

Neue SMTP-Erweiterungen

RequireTLS (RFC 8689)

Die Arbeiten der IETF an dem Verfahren RequireTLS sind abgeschlossen. Dieses Verfahren wird ab jetzt unterstützt. Mithilfe von RequireTLS können Sie festlegen, welche Nachrichten **zwingend** über TLS-geschützte Verbindungen übermittelt werden müssen. Steht TLS für die Übermittlung einer solchen Nachricht nicht zur Verfügung, oder sind die Parameter, die während des TLS-Verbindungsaufbaus und für die beteiligten Zertifikate übermittelt werden, nicht akzeptabel, so werden die Nachrichten zurückgeleitet und nicht etwa ohne TLS zugestellt. RequireTLS ist per Voreinstellung aktiv. Es wirkt jedoch nur auf solche Nachrichten, die aufgrund der neuen Aktion des Inhaltsfilters *"Nachricht für REQUIRETLS kennzeichnen"* ausdrücklich entsprechend gekennzeichnet werden, oder die an nach dem Schema `<Postfach>+requiretls@Domäne.tld` aufgebaute E-Mail-Adressen (z.B. `arvel+requiretls@mdaemon.com`) versandt werden. Alle anderen Nachrichten werden so verarbeitet, als ob das Leistungsmerkmal nicht aktiv wäre. Nachrichten, für die RequireTLS aktiv ist, können nur dann erfolgreich versandt werden, wenn bestimmte Bedingungen alle erfüllt sind. Ist auch nur eine Bedingung nicht erfüllt, so werden die Nachrichten nicht etwa über eine unverschlüsselte Verbindung übermittelt sondern an den Absender zurückgeleitet. Nähere Informationen über die Anforderungen und die Einrichtung von RequireTLS finden Sie in der Beschreibung der Option REQUIRETLS (RFC 8689) aktivieren. Eine vollständige Beschreibung für RequireTLS finden Sie in englischer Sprache in dem RFC-Dokument RFC 8689: SMTP Require TLS Option.

SMTP MTA-STS (RFC 8461) - Strict Transport Security

Die Arbeiten der IETF an dem Verfahren MTA-STS sind abgeschlossen. Dieses Verfahren wird ab jetzt unterstützt. Das Verfahren SMTP MTA Strict Transport Security (abgekürzt MTA-STS, Verfahren für erzwungene Transportverschlüsselung für SMTP-Mailserver) gestattet es Anbietern von E-Mail-Dienstleistungen, bekannt zu geben, dass sie durch Transport Layer Security (TLS) transportverschlüsselte SMTP-Verbindungen unterstützen. Darüber hinaus können sie festlegen, dass SMTP-Server, die Nachrichten an sie übermitteln wollen, die Übermittlung von Nachrichten an solche MX-Hosts ablehnen sollen, die TLS mit einem vertrauenswürdigen Server-Zertifikat nicht unterstützen. MTA-STS ist per Voreinstellung aktiv. Nähere Informationen über die Konfiguration dieses Leistungsmerkmals finden Sie in der Beschreibung der Option MTA-STS (RFC 8461) aktivieren. Eine vollständige Beschreibung für MTA-STS finden Sie in englischer Sprache in dem RFC-Dokument RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

Berichte über SMTP TLS (RFC 8460)

Mithilfe des Leistungsmerkmals zur Berichterstellung über SMTP TLS können Domänen, die MTA-STS einsetzen, Benachrichtigungen erhalten, falls der Abruf der Richtliniendatei für MTA-STS oder die Herstellung einer verschlüsselten Verbindung mittels STARTTLS fehlschlagen. Wenn dieses Leistungsmerkmal aktiv ist, sendet SecurityGateway einmal täglich einen Bericht an alle Domänen, an die SecurityGateway während des zurückliegenden Tages Nachrichten versandt oder zu versenden versucht hat, und für die MTA-STS aktiv ist. Zur Konfiguration der Information, die in den Berichten enthalten ist, stehen mehrere Optionen zur Verfügung. Die TLS-Berichte sind per Voreinstellung abgeschaltet. Eine

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

vollständige Beschreibung für die TLS-Berichte finden Sie in englischer Sprache in dem RFC-Dokument RFC 8460: SMTP TLS Reporting.

Weitere Leistungsmerkmale und Änderungen

- Die Benutzeroberfläche von SecurityGateway wurde aktualisiert und hat ein moderneres Erscheinungsbild erhalten.
- Die Komponente FusionCharts für die grafische Darstellung von Auswertungen wurde aktualisiert.
- Bestimmte Absender können jetzt von der Virenprüfung 187 ausgenommen werden.
- Mithilfe einer neuen Option kann der Weißen Liste Vorrang vor der Schwarzen Liste 274 gegeben werden.
- LetsEncrypt prüft jetzt, welche PowerShell-Version auf dem Server installiert ist. Falls die erforderliche Version nicht installiert ist, wird das Skript mit einem Fehler beendet.
- LetsEncrypt fügt jetzt der Umgebungsvariable PSModulePath für die jeweilige Sitzung den Verzeichnispfad für die SecurityGateway-Module hinzu, falls er nicht bereits in der Umgebungsvariable enthalten ist.
- LetsEncrypt löscht jetzt das Benutzerkonto und legt es neu an, wenn zwischen dem Testbetrieb ("Staging") und dem Produktivbetrieb ("Live") gewechselt wird.
- LetsEncrypt fragt jetzt die Fehlermeldungen von LetsEncrypt ab, falls eine Challenge fehlschlägt, und stellt die entsprechenden Informationen am Bildschirm dar.
- Mithilfe des neuen Befehlszeilenparameters -Staging, der an das Skript übergeben werden kann, kann das Staging-System von LetsEncrypt für den Probebetrieb einfach genutzt werden; es wird statt des Produktivsystems genutzt.
- Die Bibliothek JSTree wurde auf Version 3.3.8 aktualisiert.
- Das Benutzerkonto, unter dem der Windows-Dienst SecurityGateway 143 ausgeführt werden kann, kann jetzt angegeben werden.
- Die in RFC 5229 beschriebene Erweiterung für die SIEVE-Variablen wird ab jetzt unterstützt.
- Die Erweiterung für die SIEVE-Variablen wurde um den Befehl :eval erweitert. Hierdurch sind einfache Berechnungen möglich:

  Einige Beispiele hierzu:

```
require "securitygateway";
require "variables";
require "fileinto";

if header :matches "from" "*" {
    set :length "length" "${1}";
    set :eval "fileintovar" "${length} * 25 - 1 / 8+3";
    fileinto "${fileintovar}";
}
```

- Die Option, nach Wochentagen getrennte Protokolldateien zu erstellen, wurde entfernt. Falls diese Option bislang aktiv war, wurde während der

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Aktualisierung stattdessen die Option "Jeden Tag einen neuen Satz Protokolldateien anlegen" 320 aktiviert.

- Mithilfe einer neuen Option können sich Benutzer das Kennwort während der Eingabe anzeigen lassen. Die Seite Benutzer-Optionen 73 wurde um eine Option erweitert, mit deren Hilfe die Nutzung dieses Leistungsmerkmals unterbunden werden kann.
- Die Aktualisierungsroutine für Cyren AV wurde geändert; sie nutzt beim Abruf der Virendefinitionen jetzt TLS.
- Mithilfe einer neuen Option kann der Computername jetzt in die Dateinamen der Protokolldateien aufgenommen werden 320. Diese Option ist erforderlich, falls das Protokollverzeichnis als UNC-Pfad freigegeben ist und mehrere Server in einem Cluster ihre Protokolldateien in dasselbe Verzeichnis speichern.
- Die Installationsroutine wurde um eine Option ergänzt, mit deren Hilfe während der Erstinstallation die Serverdaten eines externen Firebird-Datenbankservers angegeben werden können.
- Die Bibliothek Chilkat wurde auf Version 9.5.0.82 aktualisiert.
- Mithilfe einer neuen Option zur Protokollierung 320 können SMTP- und HTTP-Verbindungen von bestimmten IP-Adressen von der Protokollierung ausgenommen werden. Unvollständige und abgewiesene SMTP-Nachrichten von festgelegten IP-Adressen werden auch nicht in die Datenbank eingetragen. Wird eine Nachricht zur Zustellung angenommen, so wird sie in die Datenbank eingetragen.
- Es wurde eine neue Sieve-Aktion "changesender" hinzugefügt. Mit ihrer Hilfe kann der Absender im SMTP-Umschlag geändert werden, den SecurityGateway bei der Übermittlung der Nachricht verwendet, die geändert oder bezeichnet werden soll.
- Das Modul Cyren AV wurde auf Version 6.3.0r2 aktualisiert.
- Das Modul ClamAV wurde auf Version 0.102.4 aktualisiert.

Eine vollständige Liste aller weiteren Änderungen und Fehlerbehebungen ist in den Versionsinformationen für SecurityGateway enthalten. Sie können die Versionsinformationen über die Programmgruppe für SecurityGateway im Windows-Startmenü aufrufen.

Neuigkeiten in Version 6.5.0

Zur besonderen Beachtung

Die Leistungsmerkmale für LetsEncrypt wurden aktualisiert und nutzen jetzt ACME v2. Diese Aktualisierung wurde notwendig, da LetsEncrypt die Unterstützung für ACME v1 einstellt. Für die Nutzung von LetsEncrypt sind ab jetzt PowerShell 5 und das .Net Framework 4.7.2 erforderlich.

Änderungen und neue Leistungsmerkmale

- ClamAV wurde auf Version 0.101.4 aktualisiert.
- Das Modul Cyren AV wurde auf Version 6.2.2 aktualisiert.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- Die Leistungsmerkmale zum Filtern von Dateianlagen[263] können jetzt auch RAR-Archive auswerten.
- Mithilfe eines neuen Leistungsmerkmals kann ein Journal[95] mit Kopien aller zur Zustellung angenommenen Nachrichten an eine bestimmte E-Mail-Adresse versandt werden.
- Die Kennzeichnung in der Betreffzeile, die die Verarbeitung durch RMail[235] steuert, kann jetzt auf Wunsch entfernt werden.
- Kalendereinladungen können jetzt von der Verarbeitung durch RMail[235] ausgenommen werden.
- Die Datenbank kann jetzt auch auf einem gesonderten externen Firebird-Server gehostet werden. Die Anwendung sgdbtool.exe unterstützt hierfür jetzt den neuen Parameter "-setdbconnect". Mit seiner Hilfe können Sie IP-Adresse, Datenbank-Pfad oder -Alias, Benutzername und Kennwort angegeben, die für Verbindung mit der Datenbank verwendet werden sollen.
- Die Option, den Quarantäne-Übersichten die Verknüpfung "Schwarze Liste" hinzuzufügen, wurde umbenannt in *Option "Schwarze Liste" in Quarantäne-Übersicht und -E-Mail aufnehmen*[86]". Sie wirkt jetzt auch auf die Quarantäne-Übersicht der Benutzer, die diese auf der Web-Oberfläche einsehen können.
- Es wurden XMP-API-Funktionen zur Verwaltung der Sieve-Skripte hinzugefügt.
- Es wurden XML-API-Funktionen zur Aktivierung und Verwaltung der Archiv-Speicher hinzugefügt.
- Alle Einstellungen, die sich auf DKIM ADSP bezogen, wurden abgeschafft und entfernt.
- Es können jetzt auch TNEF-Dateien (winmail.dat) nach gesperrten Dateianlagen durchsucht werden.
- Nachrichten von Mail-Servern der Domäne werden, falls diese Funktion aktiv ist, jetzt auch dann mithilfe von DKIM signiert, wenn die SMTP-Verbindung, in der sie übermittelt wurden, nicht echtheitsbestätigt war.
- Eine neue Option ermöglicht es, im Rahmen der Virenprüfung[187] auch Makros in Dokumenten zu erkennen.
- Der Reflektor für die Registrierungsdatenbank wird nicht mehr genutzt. Der 64-Bit-Teil der Systemregistrierungsdatenbank wird jetzt auch durch 32-Bit-Versionen von SecurityGateway genutzt, die auf 64-Bit-Versionen des Betriebssystems ausgeführt werden. Schlüssel und ihre Inhalte, die im Knoten Wow6432bit der Registrierungsdatenbank möglicherweise bereits bestehen, werden ohne Nutzung des Reflektors in den Knoten HKEY_LOCAL_MACHINE\SOFTWARE\ALT-N Technologies\SecurityGateway übernommen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Neuigkeiten in Version 6.1.0

Änderungen und neue Leistungsmerkmale

Einhaltung von Vorschriften bei der Archivierung 110

Mithilfe dieses neuen Konfigurationsdialogs können Sie bestimmen, wie lange archivierte Nachrichten gegen Löschung geschützt werden müssen, und wie lange sie aufbewahrt werden, bevor sie automatisch gelöscht werden. Es steht eine neue Option *Kontakt vergessen* zur Verfügung; sie löscht archivierte Nachrichten, die an bestimmte Benutzer gesandt wurden, und wahlweise auch archivierte Nachrichten, die durch diese Benutzer versandt wurden. Es steht eine weitere Option *Legal Hold* zur Verfügung, mit deren Hilfe alle archivierten Nachrichten gegen Löschung geschützt werden können. Ist diese Option aktiv, so werden alle anderen Einstellungen und Benutzerrechte übergangen, die an anderen Stellen in SecurityGateway getroffen sind und die Löschung beeinflussen würden.

Weitere neue Leistungsmerkmale für die Archivierung

- Die Seite Benutzerkonten » Benutzer-Optionen » Zugriffssteuerung 73 wurde um die Option "Benutzern das Löschen archivierter Nachrichten gestatten, die an ihre Benutzerkonten gerichtet sind oder von ihnen stammen" erweitert. Diese Option ist per Voreinstellung abgeschaltet.
- Die Seite Benutzer-Einstellungen 34 wurde um eine Option erweitert, mit deren Hilfe Sie alle archivierten Nachrichten löschen können, die durch den Benutzer versandt oder empfangen wurden. Es erscheint eine Sicherheitsabfrage, auf die Sie die Löschung bestätigen oder abbrechen können.

Benutzerprüfung über Office 365/Azure Active Directory 66

Als Datenquelle für die Benutzerprüfung 63 stehen jetzt auch Office 365 und Azure Active Directory zur Verfügung. SecurityGateway kann mithilfe der neuen Datenquellen die Benutzer direkt über Office 365 und Azure Active Directory überprüfen, die ihnen zugewiesenen Aliasnamen abrufen und die Kennwörter der Benutzer auf Gültigkeit prüfen. Um die Benutzerprüfung über Office 365 und Azure Active Directory durchzuführen, müssen Sie zunächst bestimmte Rechte einräumen. Sie finden hierzu eine Anleitung in englischer Sprache unter https://www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=1229.

Weitere Änderungen

- Weiße und Schwarze Listen können jetzt durchsucht werden.
- Der Quarantäne-Bericht kann jetzt nach Nachrichten-Bewertung sortiert werden. Die Nachrichten mit der niedrigsten Spam-Bewertung, bei denen zugleich die Wahrscheinlichkeit höher ist, dass falsch positive Treffer vorliegen, erscheinen dabei zu Beginn des Berichts.
- LetsEncrypt wurde um eine Option ergänzt, mit deren Hilfe Zertifikate gelöscht werden können, die durch LetsEncrypt ausgestellt wurden, deren Subject dem vollqualifizierten Domänennamen von SecurityGateway entspricht, und deren Ablaufdatum länger als 30 Tage zurück liegt. Um diese Option zu nutzen, übergeben Sie `-RemoveOldCertificates` als Befehlszeilenparameter.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- LetsEncrypt: PowerShell unterstützt per Voreinstellung nur SSL v3 und TLS 1.0. Mithilfe neu hinzugefügten Programmkodes können in der aktiven Sitzung jetzt aucn TLS 1.0, 1.1 und 1.2 genutzt werden. PowerShell beachtet auch die Einstellungen des Betriebssystems für die clientseitige Unterstützung der Protokolle SSL und TLS. Falls Sie daher TLS 1.0 als Clientprotokoll im Betriebssystem deaktivieren, versucht auch PowerShell nicht, dieses Protokoll zu nutzen.
- Die Bibliothek Chilkat wurde auf Version 9.5.0.78 aktualisiert.

Neuigkeiten in Version 6.0.0

Zur besonderen Beachtung

SecurityGateway erfordert ab jetzt Microsoft Windows Vista oder eine neuere Version oder Microsoft Windows Server 2008 oder eine neuere Version. Da Microsoft für Microsoft Windows XP und Microsoft Windows 2003 keine Sicherheits-Updates mehr bereit stellt, und da diese Versionen auch bestimmte erforderliche Leistungsmerkmale nicht unterstützen, werden sie nicht mehr unterstützt.

Neue Leistungsmerkmale

Archivierung von Nachrichten

Die Langzeitarchivierung von E-Mail-Nachrichten wird ab jetzt unterstützt. Die archivierten Nachrichten können in vollem Umfang durchsucht werden. Die archivierten Nachrichten werden in konfigurierbaren Archiven gespeichert.

64-Bit-Version

Es steht jetzt eine 64-Bit-Version von SecurityGateway für die Installation auf 64-Bit-Betriebssystemen zur Verfügung. Die 64-Bit-Version kann mehr aktive Verbindungen verarbeiten, ohne dass der Speicher hierdurch ausgeschöpft wird.

Verbesserter Schutz gegen Datendiebstahl

Zur Verhinderung von Datendiebstahl (sog. "Data Leakage Prevention") stehen mehr als sechzig zusätzliche Vorlagen für Regeln zur Verfügung.

Weitere Änderungen und Leistungsmerkmale

- Die Unterstützung für die Google G Suite wurde verbessert. Ist ein Mailserver einer Domäne so konfiguriert, dass er Nachrichten an die Google G Suite (aspmx.l.google.com) ausliefert, so werden Verbindungen von beliebigen Mailservern der Google G Suite wie Verbindungen von Mailservern der Domänen behandelt. Hierdurch kann SecurityGateway bei Nutzung der Google G Suite einfacher als Ausgangsgateway für E-Mails eingesetzt werden.
- Die Optionen zum Abweisen von Nachrichten wegen RFC-Verstößen oder Inkompatibilität mit DMARC führen jetzt zusätzliche Prüfungen aus, um ungültige Syntax in der Absenderkopfzeile From zu erkennen.
- Die Symbole für eingehende und abgehende Nachrichten im Nachrichten-Protokoll wurden aktualisiert.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- TLS Server Name Identification (SNI) wird jetzt unterstützt. Dieses Leistungsmerkmal gestattet die Nutzung je eines eigenen Zertifikats für jede Domäne, ohne dass die Domänen dabei an verschiedene IP-Adressen gebunden sein müssen. Es können mehrere Zertifikate zugleich aktiv sein, und SecurityGateway nutzt jeweils das Zertifikat, in dessen Feld Subject Alternative Name (SAN) der jeweils angeforderte Hostname enthalten ist.
- Eigensignierte Zertifikate können jetzt mit größeren Schlüssellängen und unter Verwendung von SHA2 statt SHA1 erstellt werden. Der erste Hostname wird automatisch in das Feld Subject Alternative Name (SAN) eingetragen.
- Das Modul Cyren AV wurde auf Version 6.2.0r2 aktualisiert. In dieser Version sind einige bisher gemeldete Fehler bei der Virenprüfung behoben.
- Die Prüfung durch SMTP-Rückruf unterstützt jetzt auch über STARTTLS verschlüsselte Verbindungen.
- ClamAV wurde auf Version 0.101.1 aktualisiert.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kapitel II

2 Hauptmenü

2.1 Mein Benutzerkonto

Die Hauptseite Mein Benutzerkonto ist die erste Seite, die Ihnen als Benutzer nach der Anmeldung an SecurityGateway angezeigt wird. Sie besteht aus zwei Abschnitten: Einstellungen zum Benutzerkonto und Statistik für das Benutzerkonto. Der Abschnitt Einstellungen zum Benutzerkonto enthält Verknüpfungen mit den Aufgaben, die Benutzer meistens ausführen wollen. Ein Klick auf diese Verknüpfungen führt direkt auf die Seite, von der aus Sie die entsprechenden Aufgaben erledigen können. Im Abschnitt Statistik für das Benutzerkonto stehen vier Berichte zur Verfügung, welche die Aktivität Ihres Benutzerkontos während der letzten 24 Stunden darstellen. Der Bericht *Normale/Spam-Nachrichten* stellt die Summen der normalen oder legitimen Nachrichten den Spam-Nachrichten gegenüber, die für Ihr Benutzerkonto verarbeitet wurden. Spam-Nachrichten sind dabei solche Nachrichten, die als Werbung, Nachrichten mit gefälschten Absendern, vireninfiziert und in ähnlicher Weise beurteilt wurden. Die *Aufschlüsselung der Spam-Nachrichten* schlüsselt die Spam-Nachrichten nach Typen auf. *Eingehende/Abgehende Nachrichten* zeigt, wie viele Nachrichten Sie empfangen und gesendet haben. *Aktivste Spam-Quellen* zeigt die Absender an, welche die meisten Spam-Nachrichten an Sie gerichtet haben.

Im Navigationsbereich auf der linken Seite erscheinen die folgenden Verknüpfungen, die sich auf Ihr Benutzerkonto beziehen:

Mein Benutzerkonto

- **Hauptmenü**—Diese Verknüpfung führt zur Leitseite Mein Benutzerkonto, auf der die meist gebrauchten Aufgaben für das Benutzerkonto aufgeführt und mehrere Statistik-Berichte verfügbar sind.
- **Zwei-Faktor-Authentifizierung** 33—Wenn Sie über eine gesicherte Verbindung angemeldet sind (Sie erkennen dies an dem Text "https://" in der Adresszeile des Browsers, den Sie für den Zugriff auf SecurityGateway nutzen), erscheint in Ihrem Menü Mein Benutzerkonto die Seite Zwei-Faktor-Authentifizierung. Die Zwei-Faktor-Authentifizierung ist ein aus zwei Schritten bestehendes Prüfverfahren, mit dessen Hilfe Sie Ihr Benutzerkonto besser sichern können. Es verlangt, dass Sie bei jeder Anmeldung an Webmail neben Ihrer E-Mail-Adresse und Ihrem Kennwort auch einen Bestätigungskode eingeben, der durch eine App auf Ihrem Smartphone erzeugt wird. **Beachte**: Die Zwei-Faktor-Authentifizierung ist unter Umständen nicht für alle Benutzer verfügbar. Dies kann auch dann der Fall sein, wenn diese eine gesicherte Verbindung nutzen.
- **Einstellungen zum Benutzerkonto** 34—Diese Verknüpfung führt zu den Einstellungen zu Ihrem Benutzerkonto. Dort können Sie Ihr Kennwort ändern, die Einstellungen für Ihre Quarantäne anpassen, die Funktionen zur automatischen Weißen Liste ein- und ausschalten und die Zahl der Elemente wählen, die auf einer Seite angezeigt werden sollen.
- **Weiße Liste** 37—Um die Liste der E-Mail-Adressen einzusehen, die in Ihrer persönlichen Weißen Liste erfasst sind, klicken Sie auf diese Verknüpfung. Um zu verhindern, dass SecurityGateway die Nachrichten eines Absenders irrtümlich als Spam erkennt oder sie insgesamt abweist, können Sie die Adresse des Absenders in Ihre Weiße Liste eintragen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **Schwarze Liste** 39—Diese Verknüpfung führt zu Ihrer Schwarzen Liste. Falls Sie von einem Absender keine Nachrichten mehr empfangen möchten, können Sie die Adresse des Absenders in Ihre Schwarze Liste eintragen.

- **Meine Quarantäne anzeigen** 42—In Ihrem Quarantäne-Ordner werden Nachrichten abgelegt, die SecurityGateway als zu verdächtig für eine direkte Zustellung an Sie bewertet hat. Von dieser Seite aus können Sie eine Übersicht über die Nachrichten in Quarantäne einsehen, die Nachrichten aus der Quarantäne freigeben (sie werden dann als legitime Nachrichten behandelt und an Sie zugestellt), die Nachrichten löschen und die Absender in Ihre Weiße Liste 37 oder Ihre Schwarze Liste 39 eintragen.

- **Mein Nachrichtenprotokoll anzeigen** 43—Diese Verknüpfung führt zu einer Übersicht über alle Nachrichten, die Ihr Benutzerkonto versandt und empfangen hat. Sie erhalten von hier aus auch nähere Informationen über alle diese Nachrichten, und sie können Nachrichten als Spam oder normale Nachrichten kennzeichnen und Adressen in die Weiße Liste und die Schwarze Liste eintragen.

Welche Optionen Ihnen im Einzelfall zur Verfügung stehen, hängt von den Berechtigungen ab, mit denen Ihr Systemverwalter Ihr Benutzerkonto in SecurityGateway versehen hat. Einige der hier beschriebenen Optionen werden Ihnen daher möglicherweise nicht angezeigt.

2.1.1 Zwei-Faktor-Authentifizierung

Wenn Sie über eine gesicherte Verbindung angemeldet sind (Sie erkennen dies an dem Text "https://" in der Adresszeile des Browsers, den Sie für den Zugriff auf SecurityGateway nutzen), erscheint in Ihrem Menü Mein Benutzerkonto die Seite Zwei-Faktor-Authentifizierung. Die Zwei-Faktor-Authentifizierung ist ein aus zwei Schritten bestehendes Prüfverfahren, mit dessen Hilfe Sie Ihr Benutzerkonto besser sichern können. Es verlangt, dass Sie bei jeder Anmeldung an Webmail neben Ihrer E-Mail-Adresse und Ihrem Kennwort auch einen Bestätigungskode eingeben, der durch eine App auf Ihrem Smartphone erzeugt wird.

Die Zwei-Faktor-Authentifizierung ist unter Umständen nicht für alle Benutzer verfügbar. Dies kann auch dann der Fall sein, wenn diese eine gesicherte Verbindung nutzen.

Einrichten der Zwei-Faktor-Authentifizierung

Um die Zwei-Faktor-Authentifizierung nutzen zu können, müssen Sie die App Google Authenticator (oder eine andere App, die zum Google Authenticator kompatibel ist) auf Ihrem Smartphone oder sonstigen mobilen Endgerät eingerichtet haben. Sie erhalten entsprechende Apps, indem Sie in Ihrem bevorzugten Appstore nach "Google Authenticator" suchen.

1. Rufen Sie in SecurityGateway im Abschnitt Mein Benutzerkonto die Seite Zwei-Faktor-Authentifizierung auf. Geben Sie dort Ihr **Derzeitiges Kennwort** ein.
2. Klicken Sie auf **Zwei-Faktor-Authentifizierung einrichten**. Es erscheinen dann auf derselben Seite ein QR-Kode und die Schaltfläche **Geheimen**

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Schlüssel anzeigen. Falls Sie den QR-Kode nicht nutzen wollen oder können, klicken Sie auf **Geheimen Schlüssel anzeigen**, um den zur Einrichtung nötigen geheimen Schlüssel einzusehen.

3. Wählen Sie in Ihrer Authenticator-App die Option **QR-Kode scannen** (oder eine vergleichbare Option; die Benennung ist nach Apps unterschiedlich), um ein neues Benutzerkonto einzurichten. Alternativ können Sie auch über die Option **Manuelle Eingabe** (oder eine vergleichbare Option) den geheimen Schlüssel eingeben, den Sie sich mithilfe der in Schritt 2 beschriebenen Schaltfläche **Geheimen Schlüssel anzeigen** anzeigen lassen können.
4. Scannen Sie den QR-Kode. Falls Sie die manuelle Eingabe nutzen, geben Sie den angezeigten geheimen Schlüssel von Hand ein, und wählen Sie als Schlüsseltyp "zeitbasiert" (oder eine vergleichbare Option). Ihre App sollte nun einen sechsstelligen Zahlenkode anzeigen.
5. Geben Sie diesen Zahlenkode in SecurityGateway in das Eingabefeld **Bestätigungskode** ein, und klicken Sie danach auf **Verbindung prüfen**.
6. Nach erfolgreicher Verbindung werden sie bei jeder künftigen Anmeldung an SecurityGateway zunächst zur Eingabe Ihres Kennworts und dann zur Eingabe des jeweils in der App angezeigten Zahlenkodes aufgefordert.

Deaktivieren der Zwei-Faktor-Authentifizierung

Um die Zwei-Faktor-Authentifizierung zu deaktivieren, geben Sie auf der Seite Zwei-Faktor-Authentifizierung Ihr Kennwort ein, und klicken Sie danach auf **Zwei-Faktor-Authentifizierung deaktivieren**.

2.1.2 Einstellungen zum Benutzerkonto

Auf der Seite Einstellungen zum Benutzerkonto können Sie Ihr Kennwort ändern, die Einstellungen für Ihre Quarantäne anpassen, die Funktionen zur automatischen Weißen Liste ein- und ausschalten und die Zahl der Elemente wählen, die auf einer Seite angezeigt werden sollen.

Welche Optionen Ihnen im Einzelfall zur Verfügung stehen, hängt von den Berechtigungen ab, mit denen Ihr Systemverwalter Ihr Benutzerkonto in SecurityGateway versehen hat. Einige der hier beschriebenen Optionen werden Ihnen daher möglicherweise nicht angezeigt.

Kennwort ändern

Kennwort
Um Ihr Kennwort zu ändern, geben Sie das neue Kennwort hier ein.

Kennwort (zur Bestätigung)
Nachdem Sie in dem Feld oben das neue Kennwort eingegeben haben, geben Sie es in dieses Feld noch einmal ein, und klicken Sie auf *Speichern*.

Quarantäne

Standard-Einstellungen meiner Domäne für die Quarantäne verwenden
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass die Quarantäne 42 den Einstellungen folgt, die der Systemverwalter für die Domäne festgelegt hat.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Besondere Quarantäne-Einstellungen für mein Benutzerkonto festlegen
Sie können auch Ihre eigenen, von der Voreinstellung abweichenden, Quarantäne-Einstellungen vornehmen. Wählen Sie dazu diese Option, und konfigurieren Sie dann die folgenden Optionen für Ihr Benutzerkonto.

Nachrichten in Quarantäne auf dem Server halten
Diese Option veranlasst SecurityGateway, eingehende Nachrichten in Quarantäne 42 zu geben, wenn sie für eine direkte Zustellung zu verdächtig erscheinen. Sie können die Nachrichten in Quarantäne dann genauer untersuchen.

Übersicht über den Inhalt meines Quarantäne-Ordners per E-Mail senden:
Falls SecurityGateway verdächtige Nachrichten für Sie in Quarantäne gibt, können Sie sich regelmäßig per E-Mail eine Übersicht über den jeweils aktuellen Inhalt Ihres Quarantäne-Ordners zusenden lassen.

Nie
Diese Option bewirkt, dass Sie keine Übersicht über die Nachrichten erhalten, die sich in Ihrem Quarantäne-Ordner befinden.

Alle [xx] Stunde(n)
Diese Option bewirkt, dass Sie die Übersicht in dem hier in Stunden angegebenen Intervall erhalten.

Täglich
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass SecurityGateway Ihnen täglich eine Übersicht über die für Sie in Quarantäne gehaltenen Nachrichten sendet.

Wöchentlich
Diese Option bewirkt, dass Sie die Übersicht einmal pro Woche erhalten.

Quarantäne-E-Mail sortieren nach: [Empfangen | Von | Betreff]
Mithilfe dieser Option können Sie die Sortierreihenfolge für die Liste der in Quarantäne befindlichen Nachrichten bestimmen. Diese Liste ist in der Übersicht über die Quarantäne enthalten, die Sie per E-Mail erhalten. Per Voreinstellung ist die Liste nach dem Datum sortiert, an dem die Nachrichten empfangen wurden. Sie können sie aber auch nach Absender oder Betreff sortieren lassen.

Option "Schwarze Liste" in Quarantäne-Übersicht und -E-Mail aufnehmen
Diese Option fügt eine Verknüpfung in die Liste der Nachrichten in Quarantäne und in die per E-Mail versandten Quarantäne-Berichte ein, mit deren Hilfe Sie die E-Mail-Adresse des Absenders in die Schwarze Liste aufnehmen können.

Option "Domäne der Schwarzen Liste hinzufügen" in Quarantäne-Übersicht und -E-Mail aufnehmen
Diese Option fügt eine Verknüpfung in die Liste der Nachrichten in Quarantäne und in die per E-Mail versandten Quarantäne-Berichte ein, mit deren Hilfe Sie die Domäne des Absenders in die Schwarze Liste aufnehmen können.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Option "Nachricht anzeigen" in Quarantäne-E-Mail aufnehmen
Diese Option fügt eine Verknüpfung in die per E-Mail versandten Quarantäne-Berichte ein, mit deren Hilfe Sie sich die Inhalt der in Quarantäne befindlichen Nachrichten anzeigen lassen können.

Meinem Mailserver oder -client das Filtern von Nachrichten in Quarantäne ermöglichen
Falls SecurityGateway für Sie eingehende Nachrichten nicht in Quarantäne geben soll, wählen Sie diese Option aus. SecurityGateway stellt Ihnen dann auch die Nachrichten normal zu, die andernfalls in Quarantäne gegeben worden wären. Diese Funktion ist hilfreich, falls Sie die Nachrichten durch Ihren E-Mail-Server oder -Client filtern lassen möchten. Um die Identifizierung solcher Nachrichten, die in Quarantäne gegeben worden wären, zu ermöglichen, fügt SecurityGateway, anhand der folgenden beiden Optionen, eine Kennzeichnung in die Betreffzeile oder eine besondere Kopfzeile in diese Nachrichten ein. Sie können dann auf Ihrem Server oder in Ihrem Mailclient Filter und Regeln anlegen, die auf die Kennzeichnung oder die Kopfzeile ansprechen.

...Betreff kennzeichnen mit [*Text*]
Diese Option bewirkt, dass SecurityGateway der Betreffzeile aller Nachrichten, die bei aktivierter Quarantäne-Option eigentlich in Quarantäne gegeben worden wären, den hier angegebenen Text hinzufügt. Per Voreinstellung lautet dieser Text "`*** SPAM ***`", Sie können den Text aber nach Ihren Wünschen beliebig ändern.

...Kopfzeile hinzufügen [*Text*]
Diese Option bewirkt, dass SecurityGateway in alle Nachrichten, die bei aktivierter Quarantäne-Option eigentlich in Quarantäne gegeben worden wären, die hier angegebene Kopfzeile einfügt. Die meisten Mailclients zeigen diese Kopfzeile zwar nur an, wenn die Eigenschaften oder der Quelltext der Nachricht aufgerufen werden, in den meisten Mailclients und Mail-Servern können Sie aber Filter einrichten, die auf diese Kopfzeile ansprechen und bestimmte Aktionen für die Nachrichten durchführen, die sie enthalten. Per Voreinstellung heißt diese Kopfzeile "`X-Spam-Flag: YES`", Sie können die Kopfzeile aber nach Ihren Wünschen beliebig ändern.

Optionen

Nachrichten für dieses Benutzerkonto nicht archivieren
Diese Option bewirkt, dass Nachrichten nicht archiviert werden, falls sie von diesem Benutzerkonto aus versandt wurden oder an dieses Benutzerkonto gerichtet sind. Diese Option gilt auch dann, wenn die Domäne, zu der das Benutzerkonto gehört, für die Archivierung von Nachrichten konfiguriert ist. Diese Option steht nur den Administratoren zur Verfügung.

Alle für dieses Benutzerkonto archivierten Daten löschen
Sie können **alle** für diesen Benutzer archivierten Nachrichten löschen, indem Sie auf diese Verknüpfung klicken. Der Löschvorgang betrifft die Nachrichten, die der Benutzer versendet und empfangen hat. Es erscheint eine Sicherheitsabfrage, auf die Sie den Löschvorgang bestätigen oder abbrechen können.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Anti-Spam-Tests für Nachrichten nicht durchführen, wenn sie an das vorliegende Benutzerkonto gerichtet sind
Diese Option bewirkt, dass der Server für die Nachrichten, die an Ihr Benutzerkonto gerichtet sind, keine Anti-Spam-Prüfungen durchführt. Es fallen dadurch einige Anti-Spam-Prüfungen weg, und dies kann das Volumen der Spam-Nachrichten, die Ihr Benutzerkonto erreichen, deutlich erhöhen.

Adressen, an die ich Nachrichten versende, automatisch in Weiße Liste eintragen
Diese Option bewirkt, dass alle Adressen, an die Sie E-Mail-Nachrichten versenden, automatisch in Ihre Weiße Liste 37 eingetragen werden. Diese Maßnahme hilft, sicherzustellen, dass Nachrichten von diesen Adressen in Zukunft nicht irrtümlich als Spam erkannt oder sonst blockiert werden.

Benutzerkonto von der "Erkennung für Hijacking" ausnehmen
Mithilfe dieser Option können Sie das Benutzerkonto von der Behandlung durch das Leistungsmerkmal Hijacking-Erkennung ausnehmen. Eine solche Ausnahme kann beispielsweise für Benutzerkonten erforderlich sein, die zulässigerweise binnen kurzer Zeit sehr viele Nachrichten versenden.

Statistik-Diagramme anzeigen: [automatisch | immer | manuell | nie]
Mithilfe dieser Option bestimmen Sie, wann die Statistik-Diagramme auf dem Dashboard und der Leitseite 32 angezeigt werden. Es stehen die Optionen automatisch, immer, manuell und nie zur Verfügung.

Sprache
Mithilfe dieses Auswahlmenüs bestimmen Sie die Sprache, in der Ihnen der Server automatisch erzeugte Systemnachrichten senden soll.

Zahl der Elemente, die auf jeder Seite angezeigt werden
Diese Option legt die Zahl der Elemente fest, die Ihnen auf jeder Bildschirmseite von SecurityGateway höchstens angezeigt werden. Sie betrifft u.a. Listen von Adressen in Ihrer Weißen Liste, Einträge in Ihrem Nachrichten-Protokoll, und anderes mehr. Falls die Zahl der Elemente, die in einer Liste enthalten sind, die Höchstzahl für eine Bildschirmseite übersteigt, finden Sie am Ende jeder Seite einige Steuerelemente, mit deren Hilfe Sie zwischen den weiteren Seiten blättern und navigieren können.

Anmeldung auf diesem Gerät/in diesem Browser nicht speichern
Diese Option wird nur angezeigt, wenn Sie bei der Anmeldung an SecurityGateway mithilfe der Option "*Anmeldung auf diesem Gerät speichern und beibehalten*" Ihre Anmeldung gespeichert haben. Durch Anklicken dieser Verknüpfung löschen Sie die zur Anmeldung gespeicherten Daten. Wenn Sie sich das nächste Mal bei SecurityGateway anmelden, können Sie die Option *Anmeldung auf diesem Gerät speichern und beibehalten* erneut nutzen.

2.1.3 Weiße Liste

Die Seite Weiße Liste zeigt Ihre persönliche Weiße Liste an. Um zu verhindern, dass SecurityGateway Nachrichten von bestimmten Absendern irrtümlich als Spam erkennt oder sonst abweist, können Sie die Adressen der Absender in Ihre Weiße Liste eintragen. Üblicherweise wird nur eine Adresse zur gleichen Zeit in die Weiße Liste eingetragen; falls Sie jedoch in einem Durchgang mehrere Adressen eintragen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Adressen aus einer Textdatei lesen und in die Weiße Liste eintragen. Die Weiße Liste

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt Ihrer Weißen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können.

Hinzufügen von Adressen zur Weißen Listet

Um eine Adresse in Ihre Weiße Liste einzutragen, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Neu.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Weißen Liste[39] aufgerufen (vgl. unten).

Bearbeiten einer Adresse in der Weißen Liste

Um eine bereits in der Weißen Liste erfasste Adresse zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie den gewünschten Eintrag aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Bearbeiten.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Weißen Liste[39] für den ausgewählten Eintrag aufgerufen (vgl. unten).

Löschen von Adressen aus der Weißen Liste

Um eine Adresse oder mehrere Adressen aus der Weißen Liste zu löschen, wählen Sie die gewünschten Einträge aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Löschen*. Um mehr als einen Eintrag auszuwählen, halten Sie die Strg-Taste gedrückt, während Sie die gewünschten Einträge durch Anklicken auswählen. Nachdem Sie auf *Löschen* geklickt haben, erscheint ein Bestätigungsdialog mit der Abfrage, ob Sie die gewünschten Einträge wirklich löschen wollen.

Import von Adressen in die Weiße Liste

Um eine Adressliste in die Weiße Liste zu importieren, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Listen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die Textdatei aus, deren Inhalt Sie in die Weiße Liste importieren wollen. Klicken Sie auf *Listen importieren*, um mit dem Import zu beginnen.

Die Textdatei darf nur eine Adresse pro Zeile enthalten, und Sie sollten die Datei mit einem reinen Texteditor (wie etwa Notepad) erstellen, damit sie nicht unbeabsichtigt Formatierungen oder sonstige Sonderzeichen enthält, die zu Störungen beim Import führen können.

Import mithilfe einer CSV-Datei

Falls Sie zu jeder importierten Adresse auch einen Kommentar importieren wollen, müssen Sie statt einer reinen Adressliste eine kommagetrennte Datei (CSV-Datei) importieren, die beide Informationen enthält. Sie können die CSV-Datei mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Jedes Datenelement muss in Anführungs- und Schlusszeichen gesetzt, und die Datenelemente in einer Zeile müssen durch ein Komma getrennt sein.

Format:

Die CSV-Datei muss zwei Spalten enthalten: *Value* ("Wert") und *Comments* ("Kommentare"). Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Die Spalte *Value* enthält die E-Mail-Adressen, die Sie in die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Weiße Liste eintragen wollen, und die Spalte *Comments* enthält den Kommentar, der für die zugehörige Adresse erfasst werden soll. Soll für eine Adresse kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Beispiele für Inhalte von CSV-Dateien:

```
"Value","Comments"
"myfriend@example.net","Ein Kommentar über meinen Freund."
"someone@example.org",""
"mister@domain.com","Ein Kommentar über Mister."
```

Export von Adressen aus der Weißen Liste

Um Adressen aus Ihrer Weißen Liste zu exportieren, gehen Sie folgendermaßen vor:

1. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
2. Klicken Sie auf *Speichern*.
3. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
4. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

Eintrag in der Weißen Liste

Dieses Dialogfenster dient dem Hinzufügen neuer Adressen zur Weißen Liste und dem Bearbeiten bestehender Einträge. Es wird immer dann aufgerufen, wenn Sie in der Symbolleiste am oberen Seitenrand auf *Neu* oder *Bearbeiten* klicken.

Listeneintrag

E-Mail-Adresse:
Tragen Sie in dieses erste Feld die E-Mail-Adresse ein, die Sie der Weißen Liste hinzufügen wollen. Um alle Adressen einer Domäne in die Weiße Liste einzutragen, setzen Sie anstatt des Postfachnamens einen Stern. Ein Beispiel hierzu: "*@example.org" erfasst alle Absender, die unter der Domäne example.org Nachrichten versenden, in der Weißen Liste.

Kommentar:
In dieses Textfeld können Sie Kommentare oder Anmerkungen eintragen, die Sie zu diesem Eintrag erfassen wollen. Der Eintrag dient nur zu Ihrer Information.

Speichern und Beenden
Sobald Sie die Bearbeitung des Eintrags abgeschlossen haben, klicken Sie auf *Speichern und Beenden,* um den Eintrag in der Weißen Liste zu speichern.

Schließen
Um das Dialogfenster zu schließen, ohne den gerade bearbeiteten Eintrag zu speichern, klicken Sie auf dieses Steuerelement.

2.1.4 Schwarze Liste

Die Seite Meine Schwarze Liste zeigt Ihre persönliche Schwarze Liste an. Um zu verhindern, dass bestimmte Absender Ihnen E-Mail-Nachrichten senden, können Sie die Adressen der Absender in Ihre Schwarze Liste eintragen. Üblicherweise wird nur

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

eine Adresse zur gleichen Zeit in die Schwarze Liste eingetragen; falls Sie jedoch in einem Durchgang mehrere Adressen eintragen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Adressen aus einer Textdatei lesen und in die Schwarze Liste eintragen. Die Schwarze Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt Ihrer Schwarzen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können.

Hinzufügen von Adressen zur Schwarzen Liste

Um eine Adresse in Ihre Schwarze Liste einzutragen, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Neu.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Schwarzen Liste 41 aufgerufen (vgl. unten).

Bearbeiten einer Adresse in der Schwarzen Liste

Um eine bereits in der Schwarzen Liste erfasste Adresse zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie den gewünschten Eintrag aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Bearbeiten.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Schwarzen Liste 41 für den ausgewählten Eintrag aufgerufen (vgl. unten).

Löschen von Adressen aus der Schwarzen Liste

Um eine Adresse oder mehrere Adressen aus der Schwarzen Liste zu löschen, wählen Sie die gewünschten Einträge aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Löschen*. Um mehr als einen Eintrag auszuwählen, halten Sie die Strg-Taste gedrückt, während Sie die gewünschten Einträge durch Anklicken auswählen. Nachdem Sie auf *Löschen* geklickt haben, erscheint ein Bestätigungsdialog mit der Abfrage, ob Sie die gewünschten Einträge wirklich löschen wollen.

Import von Adressen in die Schwarze Liste

Um eine Adressliste in die Schwarze Liste zu importieren, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Listen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die Textdatei aus, deren Inhalt Sie in die Schwarze Liste importieren wollen. Klicken Sie auf *Listen importieren*, um mit dem Import zu beginnen.

Die Textdatei darf nur eine Adresse pro Zeile enthalten, und Sie sollten die Datei mit einem reinen Texteditor (wie etwa Notepad) erstellen, damit sie nicht unbeabsichtigt Formatierungen oder sonstige Sonderzeichen enthält, die zu Störungen beim Import führen können.

Import mithilfe einer CSV-Datei

Falls Sie zu jeder importierten Adresse auch einen Kommentar importieren wollen, müssen Sie statt einer reinen Adressliste eine kommagetrennte Datei (CSV-Datei) importieren, die beide Informationen enthält. Sie können die CSV-Datei mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Jedes Datenelement muss in Anführungs- und Schlusszeichen gesetzt, und die Datenelemente in einer Zeile müssen durch ein Komma getrennt sein.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Format:
Die CSV-Datei muss zwei Spalten enthalten: *Value* ("Wert") und *Comments* ("Kommentare"). Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Die Spalte *Value* enthält die E-Mail-Adressen, die Sie in die Schwarze Liste eintragen wollen, und die Spalte *Comments* enthält den Kommentar, der für die zugehörige Adresse erfasst werden soll. Soll für eine Adresse kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Beispiele für Inhalte von CSV-Dateien:

```
"Value","Comments"
"myenemy@example.net","Ein Kommentar über meinen Feind."
"someone@example.org",""
"mister@domain.com","Ein Kommentar über Mister."
```

Export von Adressen aus der Schwarzen Liste

Um Adressen aus Ihrer Schwarzen Liste zu exportieren, gehen Sie folgendermaßen vor:

1. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
2. Klicken Sie auf *Speichern*.
3. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
4. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

Eintrag in die Schwarze Liste

Dieses Dialogfenster dient dem Hinzufügen neuer Adressen zur Schwarzen Liste und dem Bearbeiten bestehender Einträge. Es wird immer dann aufgerufen, wenn Sie in der Symbolleiste am oberen Seitenrand auf *Neu* oder *Bearbeiten* klicken.

Listeneintrag

E-Mail-Adresse:
Tragen Sie in dieses erste Feld die E-Mail-Adresse ein, die Sie der Schwarzen Liste hinzufügen wollen. Um alle Adressen einer Domäne in die Schwarze Liste einzutragen, setzen Sie anstatt des Postfachnamens einen Stern. Ein Beispiel hierzu: "*@example.org" erfasst alle Absender, die unter der Domäne example.org Nachrichten versenden, in der Schwarzen Liste.

Kommentar:
In dieses Textfeld können Sie Kommentare oder Anmerkungen eintragen, die Sie zu diesem Eintrag erfassen wollen. Der Eintrag dient nur zu Ihrer Information.

Speichern und Beenden
Sobald Sie die Bearbeitung des Eintrags abgeschlossen haben, klicken Sie auf *Speichern und Beenden,* um den Eintrag in der Schwarzen Liste zu speichern.

Schließen
Um das Dialogfenster zu schließen, ohne den gerade bearbeiteten Eintrag zu speichern, klicken Sie auf dieses Steuerelement.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

2.2 Meine Quarantäne anzeigen

In Ihrem Quarantäne-Ordner werden Nachrichten abgelegt, die SecurityGateway als zu verdächtig für eine direkte Zustellung an Sie bewertet hat. Die Quarantäne hilft, Sie vor einem Zustrom großer Mengen Spams, verdächtiger und sonst unerwünschter Nachrichten zu schützen. Ihre in Quarantäne gegebenen Nachrichten werden auf dem SecurityGateway-Server gehalten, und Sie können die Nachrichten in Quarantäne einsehen, löschen oder aus der Quarantäne freigeben (sie werden dann als legitime Nachrichten behandelt und an Sie zugestellt). SecurityGateway sendet Ihnen regelmäßig Übersichten über die Inhalte Ihres Quarantäne-Ordners per E-Mail, um Ihnen bei der Verwaltung der in Quarantäne gegebenen Nachrichten zu helfen. Sie können über die Seite Meine Einstellungen[34] die Optionen für Ihre Quarantäne konfigurieren.

Der Systemverwalter bestimmt, ob ein Benutzer auf den Quarantäne-Ordner zugreifen und die Quarantäne-Einstellungen für das eigene Benutzerkonto anpassen darf. Sie haben daher unter Umständen nicht auf alle beschriebenen Funktionen und Einstellungen Zugriff.

Jeder Eintrag in der Quarantäne enthält eine Spalte, in der Datum und Uhrzeit, vermerkt sind, zu denen die Nachricht in Quarantäne gegeben wurde, sowie Spalten für Absender und Empfänger und den Betreff der Nachricht. In weiteren Spalten sind die Gründe angegeben, warum die Nachricht in Quarantäne gegeben wurde, sowie ihre Größe und ihre Nachrichten-Bewertung, ein interner Wert, anhand dessen SecurityGateway Spam erkennt.

In der Symbolleiste am oberen Rand der Quarantäne-Übersicht stehen Ihnen mehrere Steuerelemente zur Verfügung, mit denen Sie die nachfolgend beschriebenen Aufgaben erledigen können:

- **Aktualisieren**—Klicken Sie auf dieses Steuerelement, um die Darstellung der Quarantäne-Übersicht zu aktualisieren. Es werden dann auch Einträge angezeigt, die in Quarantäne gegeben wurden, nachdem Sie die Übersicht aufgerufen haben.
- **Suche**—Über dieses Steuerelement erhalten Sie Zugriff auf umfassende Such-Funktionen, mit deren Hilfe Sie die Quarantäne-Übersicht filtern können, sodass nur bestimmte Nachrichten angezeigt werden. Sie können nach Gründen suchen, aus denen Nachrichten in Quarantäne gegeben wurden, bestimmten Text in beliebigen Kopfzeilen suchen, den Zeitrahmen für die Suche einschränken, und vieles mehr. Um die Quarantäne-Übersicht zu durchsuchen, öffnen Sie die Such-Maske durch einen Klick auf *Suche* in der Symbolleiste. Legen Sie dann die Suchkriterien fest, und klicken Sie schließlich in der Such-Maske auf das Steuerelement Suche. Die Suche wird dann durchgeführt, und die Ergebnisse erscheinen unterhalb der Such-Maske. Sie können durch erneutes Anklicken von *Suche* in der Symbolleiste die Such-Maske ausblenden und die Ergebnisse der Suche in der Quarantäne-Übersicht angezeigt lassen. Um zur vollständigen Anzeige der Quarantäne-Übersicht zurückzukehren, klicken Sie in der Such-Maske auf *Abbrechen*.
- **Anzeigen**—Wählen Sie eine Nachricht aus, und klicken Sie dann auf dieses Steuerelement, um die Nachrichten-Informationen einzublenden. Sie sind in drei Registerkarten unterteilt: Mitschnitt, Nachricht und Quelltext. Die Registerkarte Mitschnitt enthält den Mitschnitt des eigentlichen Zustellvorgangs und insbesondere als technische Information für die SMTP-

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Verbindung die Kommunikation mit dem Server oder dem Client, der die Nachricht übermittelt, sowie Daten zur internen Verarbeitung. Die Registerkarte Nachricht enthält den Inhalt der Nachricht selbst. Die Registerkarte Quelltext enthält den Quelltext der Nachricht einschließlich der Kopfzeilen, des HTML-Kodes und sonstiger Komponenten.

- **Freigeben**—Um eine Nachricht aus der Quarantäne zur Zustellung freizugeben, wählen Sie die Nachricht aus, und klicken Sie dann auf dieses Steuerelement.
- **Weiße Liste**—Um den Absender einer Nachricht in Ihre Weiße Liste[37] einzutragen, wählen Sie die Nachricht aus, und klicken Sie auf dieses Steuerelement.
- **Löschen**—Um eine Nachricht zu löschen, wählen Sie die Nachricht aus, und klicken Sie auf dieses Steuerelement.
- **Schwarze Liste**—Um den Absender einer Nachricht in Ihre Schwarze Liste[39] einzutragen, wählen Sie die Nachricht aus, und klicken Sie auf dieses Steuerelement.
- **Alle löschen**—Um alle Nachrichten aus der Quarantäne zu löschen, klicken Sie auf dieses Steuerelement.

2.3 Mein Nachrichten-Protokoll anzeigen

Das Nachrichten-Protokoll enthält zu jeder Nachricht, die Sie senden und empfangen, einen eigenen Eintrag. Darin sind Datum und Uhrzeit, zu denen die Nachricht verarbeitet wurde, Absender und Empfänger, sowie der Betreff der Nachricht vermerkt. Das Protokoll gibt außerdem Aufschluss über die Ergebnisse der Zustellversuche, insbesondere, ob die Nachricht zugestellt oder nicht zugestellt wurde. Wurde eine Nachricht nicht zugestellt, so ist auch der Grund aufgeführt, etwa, dass der Absender in einer Schwarzen Liste erfasst war, dass die Nachricht eine gesperrte Dateianlage enthielt, oder ähnliches. Auch die Größe der Nachricht und die Bewertung der Nachricht werden erfasst. Die Bewertung der Nachricht ist ein interner Wert, anhand dessen SecurityGateway Spam erkennt.

Es haben nicht alle Benutzer Zugriff auf das Nachrichten-Protokoll.

In der Symbolleiste am oberen Rand des Nachrichten-Protokolls stehen Ihnen mehrere Steuerelemente zur Verfügung, mit denen Sie die nachfolgend beschriebenen Aufgaben erledigen können:

- **Aktualisieren**—Klicken Sie auf dieses Steuerelement, um die Darstellung des Nachrichten-Protokolls zu aktualisieren. Es werden dann auch Einträge angezeigt, die in das Protokoll eingetragen wurden, nachdem Sie das Protokoll aufgerufen haben.
- **Suche**—Über dieses Steuerelement erhalten Sie Zugriff auf umfassende Such-Funktionen, mit deren Hilfe Sie das Nachrichten-Protokoll filtern können, sodass nur bestimmte Nachrichten angezeigt werden. Sie können das Protokoll nach ein- und abgehenden Nachrichten filtern, bestimmten Text in beliebigen Kopfzeilen suchen, den Zeitrahmen für die Suche einschränken, und vieles mehr. Um das Nachrichten-Protokoll zu durchsuchen, öffnen Sie die Such-Maske durch einen Klick auf *Suche* in der Symbolleiste. Legen Sie dann die Suchkriterien fest, und klicken Sie

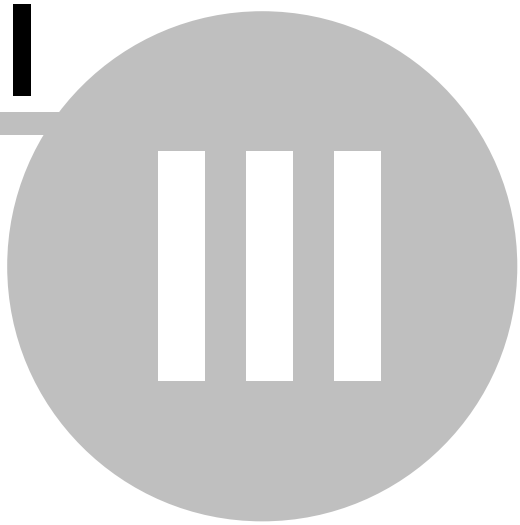
Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

schließlich in der Such-Maske auf das Steuerelement Suche. Die Suche wird dann durchgeführt, und die Ergebnisse erscheinen im Nachrichten-Protokoll. Sie können durch erneutes Anklicken von *Suche* in der Symbolleiste die Such-Maske ausblenden und die Ergebnisse der Suche im Nachrichten-Protokoll angezeigt lassen. Um zur vollständigen Anzeige des Nachrichten-Protokolls zurückzukehren, klicken Sie in der Such-Maske auf *Abbrechen*.

- **Details**—Wählen Sie eine Nachricht aus, und klicken Sie dann auf dieses Steuerelement, um die Nachrichten-Informationen einzublenden. Sie sind in drei Registerkarten unterteilt: Mitschnitt, Nachricht und Quelltext. Die Registerkarte Mitschnitt enthält den Mitschnitt des eigentlichen Zustellvorgangs und insbesondere als technische Information für die SMTP-Verbindung die Kommunikation mit dem Server oder dem Client, der die Nachricht übermittelt, sowie Daten zur internen Verarbeitung. Die Registerkarte Nachricht enthält den Inhalt der Nachricht selbst. Ob der Nachrichten-Inhalt im Einzelfall verfügbar ist, hängt vom Alter der Nachricht und davon ab, ob die Nachricht erfolgreich zugestellt wurde und ob SecurityGateway so konfiguriert ist, dass die Inhalte gespeichert werden. Die Registerkarte Quelltext enthält den Quelltext der Nachricht einschließlich der Kopfzeilen, des HTML-Kodes und sonstiger Komponenten. Der Quelltext ist unter Umständen nicht verfügbar, etwa, wenn die Nachricht alt ist oder die Optionen zur Datenhaltung von SecurityGateway eine Speicherung dieser Daten nicht vorsehen.
- **Erneut zustellen**—Um eine Nachricht oder mehrere Nachrichten erneut zuzustellen, wählen Sie sie aus der Liste aus, und klicken Sie dann auf dieses Steuerelement. Sie können mehrere Nachrichten auswählen, indem Sie die Strg- oder Hochschalttaste gedrückt halten. Die erneute Zustellung ist nur möglich, solange die Inhalte der Nachrichten noch nicht aus der Datenbank gelöscht wurden.
- **Spam**—Um eine Nachricht als Spam zu kennzeichnen, wählen Sie die Nachricht aus, und klicken Sie dann auf dieses Steuerelement. Sie können SecurityGateway dadurch helfen, Spam-Nachrichten in Zukunft noch sicherer zu erkennen. Diese Option ist nicht in allen Fällen verfügbar und steht immer dann nicht zur Verfügung, wenn SecurityGateway so konfiguriert ist, dass das zugrundeliegende Verfahren nicht unterstützt wird.
- **Kein Spam**—Um eine Nachricht als normale Nachricht zu kennzeichnen, wählen Sie die Nachricht aus, und klicken Sie dann auf dieses Steuerelement. Sie können SecurityGateway dadurch helfen, legitime Nachrichten in Zukunft nicht irrtümlich als Spam zu erkennen. Diese Option ist nicht in allen Fällen verfügbar und steht immer dann nicht zur Verfügung, wenn SecurityGateway so konfiguriert ist, dass das zugrundeliegende Verfahren nicht unterstützt wird.
- **Weiße Liste**—Um den Absender einer Nachricht in Ihre Weiße Liste 37 einzutragen, wählen Sie die Nachricht aus, und klicken Sie auf dieses Steuerelement.
- **Schwarze Liste**—Um den Absender einer Nachricht in Ihre Schwarze Liste 39 einzutragen, wählen Sie die Nachricht aus, und klicken Sie auf dieses Steuerelement.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kapitel



3 Einstellungen/Benutzer

Das Menü *Einstellungen/Benutzer* ist in sieben Abschnitte untergliedert. Sie enthalten Verknüpfungen zu den zentralen Einstellungen in der Konfiguration von SecurityGateway. Mithilfe dieser Optionen können Sie Ihre Domänen und Benutzerkonten einrichten, Einstellungen für die Zustellung der Nachrichten und die Quarantäne treffen, die Datenbank und die Konfiguration sichern, und weitere Einstellungen vornehmen. Die folgende Übersicht enthält eine kurze Beschreibung jedes Abschnitts. Nähere Informationen enthalten die Übersichten für die einzelnen Abschnitte und die Dokumentation der Optionen in jedem Abschnitt.

Benutzerkonten 47
Der Abschnitt Benutzerkonten im Menü *Einstellungen/Benutzer* enthält die Einstellungen für die Benutzerkonten und die Domänen, die SecurityGateway bedient. Der Abschnitt enthält fünf Verknüpfungen für die entsprechenden Aufgaben; hierzu gehören die Erstellung von Domänen und Benutzerkonten, die Einrichtung von Datenquellen für die Benutzerprüfung, sowie die Voreinstellungen für verschiedene Funktionen, die die Benutzer allenfalls selbst steuern dürfen.

E-Mail-Konfiguration 78
Der Abschnitt E-Mail-Konfiguration enthält Verknüpfungen mit fünf Seiten, von denen aus verschiedene Funktionen für die Behandlung der Nachrichten gesteuert werden. Sie können mithilfe der Optionen in diesem Abschnitt beispielsweise die Server festlegen, auf denen sich die Benutzerkonten Ihrer E-Mail-Benutzer befinden, die Quarantäne-Optionen und verschiedene Optionen für die Nachrichten-Zustellung konfigurieren und andere technische Einstellungen verwalten.

Disclaimer (Kopftexte / Fußtexte) 119
Disclaimer für Nachrichten sind Textbausteine, die der Server über den oder unter dem Nachrichtentext eingehender, abgehender und lokaler E-Mail-Nachrichten einfügen kann. Sie können mithilfe der Optionen auf dieser Seite die Disclaimer erstellen und verwalten.

System 125
Der Abschnitt System im Menü *Einstellungen/Benutzerkonten* enthält Verknüpfungen mit verschiedenen System-Einstellungen, wie etwa zur Verschlüsselung, zur HTTP-Schnittstelle, zu den Verzeichnissen und zur Verwaltung des Speicherplatzes.

Datenbank 143
Die Optionen, die Sie über diesen Abschnitt erreichen können, bestimmen die Art und den Umfang der Daten, die SecurityGateway speichern und vorhalten soll, die automatische Datensicherung und die Optionen für die Wiederherstellung der Server-Konfiguration und der Datenbank aus den Datensicherungen.

Software-Aktualisierung 149
Mithilfe dieser Funktion können Sie überprüfen, ob eine neuere Version von SecurityGateway verfügbar ist. Sie können manuell nach neuen Versionen suchen oder SecurityGateway mithilfe einer entsprechenden Option veranlassen, automatisch nach neuen Software-Versionen zu suchen. Ist

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

eine neue Version verfügbar, so kann die neue Version direkt über die Web-Schnittstelle heruntergeladen und installiert werden.

Lizenzverwaltung 150
In der Lizenzverwaltung können Sie die Informationen zu Ihrer Produkt-Lizenz angeben und einsehen. Dazu gehören der Name und die Firma des Lizenznehmers, der Lizenzschlüssel und der Status Ihrer Lizenz.

3.1 Benutzerkonten

Der Abschnitt Benutzerkonten im Menü Einstellungen/Benutzer 46 enthält verschiedene Optionen zur Steuerung der Benutzerkonten und Domänen, die SecurityGateway bedient. Der Abschnitt enthält fünf Verknüpfungen, mit deren Hilfe Sie die zugehörigen Aufgaben erledigen können:

Domänen 48 und **Benutzer** 54—Mithilfe der Listen der Domänen und Benutzer können Sie Ihre Domänen und Benutzer verwalten. Um die Liste der Domänen aufzurufen, klicken Sie im Navigationsbereich links auf *Einstellungen/Benutzer,* und klicken Sie dann im Abschnitt Benutzerkonten auf *Domänen und Benutzer*. Um die Liste der Benutzer aufzurufen, wählen Sie aus der Liste der Domänen eine Domäne aus, und klicken Sie dann in der Symbolleiste auf das Steuerelement *Benutzer*.

Administratoren 60—Mithilfe der Liste der Administratoren können Sie alle Globalen und Domänen-Administratoren verwalten, die in SecurityGateway eingerichtet sind. Globale Administratoren haben uneingeschränkten Zugriff auf alle Einstellungen und Optionen von SecurityGateway; sie haben auch Zugriff auf die Benutzerkonten und Einstellungen anderer Administratoren. Domänen-Administratoren haben Zugriff auf alle Einstellungen und Optionen der Domänen, für die sie zu Administratoren bestimmt sind. Sie können Einstellungen nicht ändern, die das gesamte System oder solche Domänen betreffen, für die sie nicht zuständig sind.

Datenquellen für Benutzerprüfung 63—Mithilfe dieser Seite können Sie alle Datenquellen für die Benutzerprüfung verwalten. Die Datenquellen dienen zur Prüfung, ob eine unbekannte lokale Adresse zu einem gültigen Benutzerkonto gehört. Geht eine Nachricht ein, die an einen für SecurityGateway unbekannten lokalen Benutzer gerichtet ist, so fragt SecurityGateway die Datenquellen für die Benutzerprüfung ab, die für die Zieldomäne eingerichtet sind, um festzustellen, ob die Adresse zu einem gültigen Benutzerkonto gehört. Besteht ein solches gültiges Benutzerkonto, so legt SecurityGateway einen Benutzer für die Zieladresse an und versucht dann, die Nachricht an den Mailserver der Domäne 79 zuzustellen. Ergibt die Prüfung, dass kein gültiges Benutzerkonto besteht, so wird die Nachricht abgewiesen.

Automatisches Anlegen von Domänen 72—SecurityGateway kann Domänen automatisch neu anlegen, wenn eine Nachricht an einen unbekannten Benutzer einer unbekannten Domäne eingeht und die Abfrage der Datenquellen für die Benutzerprüfung ergibt, dass sowohl der Benutzer als auch die Domäne gültig sind. Die entsprechenden Einstellungen finden Sie auf dieser Seite.

Benutzer-Optionen 73—Auf dieser Seite können Sie festlegen, welche Optionen den Benutzern von SecurityGateway zur Verfügung stehen, wenn sie auf SecurityGateway zugreifen. Die Benutzer-Optionen können sowohl systemweit als auch nach Domänen getrennt konfiguriert werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

3.1.1 Domänen und Benutzer

3.1.1.1 Liste der Domänen

MMithilfe der Listen der Domänen und Benutzer können Sie Ihre Domänen und Benutzer verwalten. Um die Liste der Domänen aufzurufen, klicken Sie im Navigationsbereich links auf *Einstellungen/Benutzer,* und klicken Sie dann im Abschnitt Benutzerkonten auf *Domänen und Benutzer*. Um die Liste der Domänen aufzurufen, klicken Sie im Navigationsbereich links auf *Einstellungen/Benutzer,* und klicken Sie dann im Abschnitt Benutzerkonten auf *Domänen und Benutzer*. Sie können die Liste der Domänen auch aus der Übersicht, die nach Anklicken der Verknüpfung Einstellungen/Benutzer rechts angezeigt wird, über die Verknüpfung *Domänen anzeigen und verwalten* im Abschnitt Domänen erreichen.

Die Liste der Domänen enthält zwei Spalten: Name und Benutzer. In der Spalte Name sind alle Domänen aufgeführt, und die Spalte Benutzer zeigt die Anzahl der Benutzerkonten an, die zu den einzelnen Domänen gehören. Um die Eigenschaften 50 einer Domäne einzusehen und zu bearbeiten, klicken Sie auf die gewünschte Domäne doppelt. Um die Liste der Benutzer 54 für eine Domäne aufzurufen, wählen Sie die gewünschte Domäne durch Einfachklick aus, und klicken Sie dann auf das Steuerelement Benutzer.

Sie können verschiedene Aufgaben, die mit der Liste der Domänen zusammenhängen, über die Symbolleiste am oberen Seitenrand erledigen. In den meisten Fällen müssen Sie zunächst eine Domäne aus der Liste auswählen, bevor Sie die zugehörigen Steuerelemente anklicken können. Die einzigen Ausnahmen von dieser Regel sind Neu, Import und Export; Sie können diese Steuerelemente anklicken, ohne zuvor eine Domäne ausgewählt zu haben. Die Symbolleiste enthält die folgenden zehn Steuerelemente:

Neu
Ein Klick auf *Neu* ruft den Dialog Eigenschaften 50 auf, mit dessen Hilfe Sie in SecurityGateway eine neue Domäne anlegen können. Im Dialog *Eigenschaften* bestimmen Sie den Namen, den Mailserver und die sonstigen Einstellungen für die Domäne.

Bearbeiten
Ein Klick auf das Steuerelement Bearbeiten in der Symbolleiste ruft den Dialog Eigenschaften 50 für die Domäne auf, die in der Liste der Domänen gerade ausgewählt ist. Sie können diesen Dialog auch durch einen Doppelklick auf die gewünschte Domäne in der Liste der Domänen aufrufen.

Löschen
Um eine oder mehrere Domänen zu löschen, wählen Sie die Domänen in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Domänen wirklich löschen wollen. Sie können mehrere Domänen auswählen, indem Sie während des Anklickens der Domänen die Strg-Taste gedrückt halten.

Suche anzeigen/ausblenden
Um die Suchfunktion für die Liste der Domänen aufzurufen, klicken Sie auf *Suche anzeigen*. Geben Sie im Eingabefeld *Domänenname* den Text ein, nach dem Sie die Liste der Domänen durchsuchen wollen, und klicken Sie dann auf *Suche*, um

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

die Liste der Domänen anhand dieses Textes zu filtern. Klicken Sie auf *X Suche abbrechen*, um sich die ungefilterte Liste der Domänen wieder anzeigen zu lassen.

Benutzer
Um die Liste der Benutzer 54 für eine Domäne aufzurufen, wählen Sie die Domäne durch Einfachklick aus, und klicken Sie dann in der Symbolleiste auf *Benutzer*. Die Liste der Benutzer erfüllt ähnliche Aufgaben wie die Liste der Domänen, sie betrifft jedoch die Benutzer von SecurityGateway.

Nachrichten
Dieses Steuerelement öffnet das Nachrichten-Protokoll 307 für die ausgewählte Domäne. Das Nachrichten-Protokoll enthält einen Eintrag für jede Nachricht, die an die Domäne oder von der Domäne aus gesendet wurde. Über das Nachrichten-Protokoll kann für jeden Eintrag eine Seite mit weiterführenden Nachrichten-Informationen aufgerufen werden; diese Seite enthält den SMTP-Verbindungsmitschnitt und, sofern verfügbar, den Inhalt und den Quelltext der Nachricht.

Quarantäne
Um die Quarantäne 308 für die ausgewählte Domäne zu öffnen, klicken Sie auf das Steuerelement *Quarantäne*. In der Übersicht, die dann angezeigt wird, sind alle Nachrichten aufgeführt, die für die Domäne in Quarantäne gegeben wurden, und sie können von der Übersicht aus geprüft und durchgesehen werden.

Weiße Liste
Mithilfe des Steuerelements Weiße Liste können Sie die Weiße Liste für Adressen 276 für die ausgewählte Domäne aufrufen.

Schwarze Liste
Mithilfe des Steuerelements Schwarze Liste können Sie die Schwarze Liste für Adressen 266 für die ausgewählte Domäne aufrufen.

Import
Sie können mithilfe einer kommagetrennten Datei (Format CSV) eine Liste von Domänen in die Liste der Domänen importieren. Klicken Sie hierzu am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Domänen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die CSV-Datei aus, deren Inhalt Sie in die Liste der Domänen importieren wollen. Klicken Sie auf *Domänen importieren*, um mit dem Import zu beginnen.

Format der CSV-Datei
Sie können die CSV-Datei für den Import in die Liste der Domänen mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen.

Die CSV-Datei kann zwei Spalten enthalten: *Domain* ("Domäne") und *MaxUsers* ("Höchstzahl der Benutzer"). Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Die Spalte *Domain* enthält den Domänennamen (z.B. example.com), und die Spalte *MaxUsers* enthält die Höchstzahl der Benutzer, die dieser Domäne angehören dürfen. Alle Domänennamen müssen in Anführungs- und Schlusszeichen gesetzt werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Falls ein Wert *MaxUsers* angegeben wird, muss er vom Domänennamen durch ein Komma getrennt sein.

Beispiele für Inhalte von CSV-Dateien:

```
"Domain","MaxUsers"
"domain.com", 50
"example.com"
"example.org", 10
```

Export
Sie können die Liste der Domänen mithilfe des Steuerelements Export in der Symbolleiste exportieren. Es wird dabei eine CSV-Datei in demselben Format erstellt, wie sie auch für den bereits dokumentierten Import benötigt wird. Um die Liste der Domänen zu exportieren, gehen Sie folgendermaßen vor:

1. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
1. Klicken Sie auf *Speichern*.
2. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
3. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

3.1.1.1.1 Eigenschaften der Domäne

Mithilfe des Dialogs Eigenschaften können in SecurityGateway neue Domänen angelegt und bestehende Domänen bearbeitet werden. Um den Dialog Eigenschaften aufzurufen, klicken Sie in der Liste der Domänen[48] auf *Neu*, oder wählen Sie eine Domäne aus der Liste aus, und klicken Sie auf *Bearbeiten*. Der Dialog *Eigenschaften* ist in vier Registerkarten unterteilt: Eigenschaften, Prüfung, Mailserver und Admins.

Domänen-Administratoren[60] haben auf die Listen der Datenquellen für die Benutzerprüfung und der Mailserver nur Lesezugriff.

Eigenschaften

Auf der Registerkarte Eigenschaften werden der Domänenname, die Höchstzahl der Benutzerkonten, die einer Domäne angehören dürfen, und das AUTH-Kennwort festgelegt. Die Höchstzahl der Benutzerkonten und das Kennwort müssen nicht zwingend festgelegt werden.

Domänenname:
Geben Sie den Domänennamen in dieses Textfeld ein, etwa "example.com", "domain.com" oder ähnliches. Dieser Domänenname erscheint in der E-Mail-Adresse aller Benutzer dieser Domäne.

Zahl der Benutzerkonten begrenzen
Falls Sie die Zahl der Benutzerkonten begrenzen wollen, die dieser Domäne angehören dürfen, aktivieren Sie dieses Feld, und geben Sie in das folgende Feld die gewünschte Höchstzahl der Benutzer ein. Diese Option ist per Voreinstellung abgeschaltet.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Höchstzahl der Benutzerkonten:
Falls Sie die Zahl der Benutzerkonten begrenzen wollen, die dieser Domäne angehören dürfen, aktivieren Sie die Option *Zahl der Benutzerkonten begrenzen*, und geben Sie die gewünschte Höchstzahl der Benutzerkonten hier ein.

Nachrichtengröße begrenzen
Mithilfe dieser Option können Sie die höchstzulässige Größe für Nachrichten für diese Domäne bestimmen; diese Größenbegrenzung wirkt auf Nachrichten, die über SMTP übermittelt werden. Per Voreinstellung ist diese Option abgeschaltet; es gilt dann die systemweit wirksame Begrenzung, die mit der Einstellung Größenbegrenzung für SMTP-Nachrichten konfigurieren 92 festgelegt wird.

Kennwort für SMTP-AUTH
Mithilfe dieser Option können Sie für die Domäne ein SMTP-AUTH-Kennwort festlegen. Ihre Benutzer und die Mailserver der Domäne 79 können dieses Kennwort zur Echtheitsbestätigung nutzen, wenn sie Nachrichten über SecurityGateway versenden. Um dieses Kennwort für die Echtheitsbestätigung zu nutzen, muss der Domänenname als Anmeldename oder Benutzername eingesetzt werden. Heißt die Domäne beispielsweise "example.com", und wird in dieses Feld "1234Kennwort" als AUTH-Kennwort eingetragen, so erfolgt die Echtheitsbestätigung mit "example.com" und "1234Kennwort". Falls Sie hier kein Kennwort eintragen, so kann sich ein Absender nicht dadurch echtheitsbestätigen, dass er den Domänennamen als Anmeldenamen und ein leeres Kennwort übermittelt; das System unterbindet entsprechende Versuche.

Das SMTP-AUTH-Kennwort kann auch nützlich sein, falls der Administrator die Echtheitsbestätigung mithilfe von CRAM-MD5 durchführt will. Diese Art der Echtheitsbestätigung setzt voraus, dass SecurityGateway das Kennwort kennt, die Datenquelle für Benutzerprüfungen kann dabei nicht eingesetzt werden.

In den meisten Fällen wird der Benutzer zur Echtheitsbestätigung die E-Mail-Adresse und das Kennwort seines eigenen Benutzerkontos als Anmeldedaten nutzen. Es sind aber auch Szenarien denkbar, in denen ein Mailserver der Domäne eigene Anmeldedaten benötigt, oder in denen sich mehrere Benutzer gemeinsame AUTH-Anmeldedaten teilen müssen. Diese Option soll auch die genannten Szenarien abdecken.

Domäne an IP-Adresse binden
Mithilfe dieser Option können Sie die Domäne an eine bestimmte IP-Adresse binden. Aktivieren Sie dazu die Option, und geben Sie eine IP-Adresse und einen Hostnamen an. Abgehende Nachrichten der Domäne werden von der angegebenen IP-Adresse aus versandt. Sie können auch eine Zeichenkette für die Meldung HELO oder einen SMTP-Hostnamen für die Domäne angeben. Dies ist der vollqualifizierte Domänenname (FQDN), der beim Versand von Nachrichten dieser Domäne in der SMTP-Meldung HELO/EHLO erscheint. Bei eingehenden Verbindungen wird dieser Wert ebenfalls genutzt, falls nicht mehrere Domänen an dieselbe IP-Adresse gebunden sind. Sind mehrere Domänen an dieselbe IP-Adresse gebunden, so wird aus den dieser Domäne zugewiesenen FQDN derjenige genutzt, der in alphabetischer Reihenfolge zuerst erscheint.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Domänen-Aliasnamen
Mithilfe dieser Option können Sie die Aliasnamen für die Domäne festlegen. Die Benutzer einer Domäne werden dann auch für alle Aliasnamen der Domäne als gültig angesehen. Diese Funktion ist beispielsweise hilfreich, wenn derselbe Domänenname unter verschiedenen Top-Level-Domänen registriert ist, etwa altn.com, altn.us, altn.biz usw.

Prüfung

Mithilfe der Registerkarte Prüfung werden die Datenquellen für die Benutzerprüfung[63] festgelegt, die für diese Domäne genutzt werden. Geht eine Nachricht ein, die an einen für SecurityGateway unbekannten lokalen Benutzer gerichtet ist, so fragt SecurityGateway die Datenquellen für die Benutzerprüfung ab, die für die Zieldomäne eingerichtet sind, um festzustellen, ob die Adresse zu einem gültigen Benutzerkonto gehört. Besteht ein solches gültiges Benutzerkonto, so legt SecurityGateway einen Benutzer für die Zieladresse an.

Datenquellen für Benutzerprüfung nicht abfragen, Benutzer werden manuell verwaltet
Diese Option bewirkt, dass für die gerade bearbeitete Domäne keine Datenquellen für die Benutzerprüfung abgefragt werden. Wenn diese Option aktiv ist, müssen alle Benutzer dieser Domäne manuell verwaltet werden.

Verfügbare Datenquellen:
In diesem Abschnitt sind alle verfügbaren Datenquellen für die Benutzerprüfung aufgeführt, die für das System konfiguriert sind. Um dieser Domäne eine Datenquelle zuzuordnen, wählen Sie die gewünschte Datenquelle aus, und klicken Sie auf den Pfeil "--->".

Ausgewählte Datenquellen:
In diesem Abschnitt sind alle Datenquellen für die Benutzerprüfung aufgeführt, die dieser Domäne zugeordnet sind. Um die Zuordnung einer Datenquelle zu dieser Domäne aufzuheben, wählen Sie die gewünschte Datenquelle aus, und klicken Sie auf den Pfeil "<---".

Voreinstellung: Aufwärts/Abwärts
Die Datenquellen werden in der Reihenfolge abgefragt, in der sie in der Liste der ausgewählten Datenquellen erscheinen. Um die Position einer Datenquelle zu verändern, klicken Sie die gewünschte Datenquelle an, und verschieben Sie sie mithilfe der Steuerelemente "Aufwärts" und "Abwärts" an die gewünschte neue Position.

Sobald entweder ein positives oder ein negatives Ergebnis eingetreten ist, nimmt SecurityGateway dieses Ergebnis an und fragt keine weiteren Datenquellen mehr ab. Sind beispielsweise drei Datenquellen der Domäne zugeordnet, und teilt die erste Datenquelle mit, dass der Benutzer nicht existiert, so nimmt SecurityGateway dieses Ergebnis an und fragt die verbleibenden beiden Datenquellen nicht mehr ab. Tritt bei der Abfrage hingehen ein vorübergehender Fehler auf, etwa, weil eine Datenquelle vorübergehend nicht verfügbar ist, so wird die Nachricht mit einem Fehlerkode

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

4xx abgewiesen; dieser Fehlerkode fordert den Absender auf, die Zustellung später erneut zu versuchen.

Neu
Falls Sie für diese Domäne eine neue Datenquelle für die Benutzerprüfung anlegen wollen, klicken Sie auf *Neu*. Es öffnet sich der Dialog Neue Datenquelle für die Benutzerprüfung 66. Nachdem die Datenquelle angelegt wurde, erscheint sie in der Liste der verfügbaren Datenquellen.

Mailserver

Mithilfe der Registerkarte Mailserver werden die Mailserver der Domäne 79 bestimmt, die dieser Domäne zugeordnet sind. Geht eine Nachricht für einen geprüften und gültigen Benutzer dieser Domäne ein, so versucht SecurityGateway, die Nachricht an die Server zuzustellen, die in der Liste der ausgewählten Server eingetragen sind. Die Zustellung erfolgt in der Reihenfolge, in der die Server in der List erscheinen.

Verfügbare Server:
In diesem Abschnitt sind alle verfügbaren Mailserver aufgeführt, die für das System konfiguriert sind. Um dieser Domäne einen Mailserver zuzuordnen, wählen Sie den gewünschten Mailserver aus, und klicken Sie auf den Pfeil "--->".

Ausgewählte Server:
In diesem Abschnitt sind alle Mailserver aufgeführt, die dieser Domäne zugeordnet sind. Um die Zuordnung eines Mailservers zu dieser Domäne aufzuheben, wählen Sie den gewünschten Mailserver aus, und klicken Sie auf den Pfeil "<---".

Voreinstellung: Aufwärts/Abwärts
SecurityGateway versucht, die Nachrichten an die Mailserver der Domäne in der Reihenfolge zuzustellen, in der die Mailserver in der Liste der ausgewählten Server erscheinen. Um die Position eines Mailservers zu verändern, klicken Sie den gewünschten Mailserver an, und verschieben Sie ihn mithilfe der Steuerelemente "Aufwärts" und "Abwärts" an die gewünschte neue Position.

Mail-Server nur für Zuweisung zu bestimmten Domänen-Benutzern verfügbar machen und nicht allgemein für Zustellung der Nachrichten der Domäne nutzen
Um diese Option zu aktivieren, wählen Sie den gewünschten Server aus, und aktivieren Sie das Kontrollkästchen. Diese Option bewirkt, dass der betreffende Server nicht für die Zustellung von Nachrichten der gesamten Domäne verwendet wird. Er wird mit "[NUR BENUTZER]" gekennzeichnet. Sie können diesen Server dann für die Zustellung von Nachrichten für bestimmte Benutzer verwenden. Die Einstellungen, die erforderlich sind, um den Server einem Benutzer zuzuweisen, finden Sie auf der Seite Benutzer bearbeiten » Eigenschaften 57 im Abschnitt Postausgang.

Neu
Falls Sie für diese Domäne einen neuen Mailserver der Domäne anlegen wollen, klicken Sie auf *Neu*. Es öffnet sich der Dialog Neuer Mailserver 80. Nachdem der Mailserver angelegt wurde, erscheint er in der Liste der verfügbaren Mailserver.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Admins

Mithilfe der Registerkarte Admins werden die Administratoren[60] bestimmt, die zur Verwaltung dieser Domäne berechtigt sind. Globale Administratoren sind hier hier nicht aufgeführt, da sie ohnehin jede Domäne verwalten dürfen.

Verfügbare Administratoren:
In diesem Abschnitt sind alle verfügbaren Domänen-Administratoren aufgeführt, die für das System konfiguriert sind, und zwar unabhängig davon, für welche Domänen sie zuständig sind.. Um einem Administrator die Verwaltung dieser Domäne zu gestatten, wählen Sie den gewünschten Administrator aus, und klicken Sie auf den Pfeil "--->".

Ausgewählte Administratoren:
In diesem Abschnitt sind alle Domänen-Administratoren aufgeführt, die diese Domäne verwalten dürfen. Um die Berechtigung eines Administrators für die Verwaltung dieser Domäne zu widerrufen, wählen Sie den gewünschten Administrator aus, und klicken Sie auf den Pfeil "<---".

Neu
Falls Sie für diese Domäne einen neuen Administrator anlegen wollen, klicken Sie auf *Neu*. Es öffnet sich der Dialog Neuer Administrator[61]. Nachdem der neue Administrator angelegt wurde, erscheint er in der Liste der ausgewählten Administratoren.

3.1.1.2 Liste der Benutzer

Mithilfe der Liste der Benutzer werden die Benutzerkonten einer Domäne verwaltet. Um diese Liste aufzurufen, klicken Sie im Navigationsbereich links auf *Einstellungen/Benutzer,* und klicken Sie dann im rechten Bereich unter Benutzer und Administratoren auf die Domäne, für die Sie die Liste der Benutzer aufrufen wollen. Sie können die Liste der Benutzer auch mithilfe des Eintrags der Domäne in der Liste der Domänen[48] aufrufen.

Die Liste der Benutzer enthält drei Spalten: Aktiviert, Name und Postfach. Die Spalte Aktiviert enthält ein Kontrollkästchen für jeden Eintrag, mit dessen Hilfe das zugehörige Benutzerkonto schnell aktiviert und gesperrt werden kann. In der Spalte Name erscheint der Vor- und Nachname des jeweiligen Benutzers (z.B. Frank Thomas), und in der Spalte Postfach erscheint das Postfach aus der E-Mail-Adresse des jeweiligen Benutzers (z.B. für "frank@example.com" nur "frank"). Um einen Benutzer zu bearbeiten, klicken Sie doppelt auf den Listeneintrag des gewünschten Benutzers, oder wählen Sie den Eintrag durch Einfachklick aus, und klicken Sie dann in der Symbolleiste am oberen Seitenrand auf Bearbeiten. In beiden Fällen wird der Dialog Benutzer bearbeiten[57] aufgerufen.

Sie können verschiedene Aufgaben, die mit der Liste der Benutzer zusammenhängen, über die Symbolleiste am oberen Seitenrand erledigen. In den meisten Fällen müssen Sie zunächst einen Benutzer aus der Liste auswählen, bevor Sie die zugehörigen Steuerelemente anklicken können. Die einzigen Ausnahmen von dieser Regel sind Neu, Import und Export; Sie können diese Steuerelemente anklicken, ohne zuvor einen Benutzer ausgewählt zu haben. Die Symbolleiste enthält die folgenden elf Steuerelemente:

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Zurück
Falls Sie die Liste der Benutzer über die Liste der Domänen[48] aufgerufen haben, können Sie mithilfe dieses Steuerelements einfach zur vorhergehenden Seite zurückkehren.

Neu
Klicken Sie auf *Neu,* um den Dialog Neuer Benutzer[57] aufzurufen und ein neues Benutzerkonto in dieser Domäne anzulegen. In dem Dialog *Neuer Benutzer* bestimmen Sie, wie auch im Dialog Benutzer bearbeiten[57], den Postfachnamen, Vor- und Nachnamen, das Kennwort und die Berechtigungen des Benutzers.

Bearbeiten
Ein Klick auf das Steuerelement Bearbeiten in der Symbolleiste ruft den Dialog Benutzer bearbeiten[57] für den Benutzer auf, der in der Liste der Benutzer gerade ausgewählt ist. Sie können diesen Dialog auch durch einen Doppelklick auf den gewünschten Benutzer in der Liste der Benutzer aufrufen.

Löschen
Um einen oder mehrere Benutzer zu löschen, wählen Sie die Benutzer in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Benutzer wirklich löschen wollen. Sie können mehrere Benutzer auswählen, indem Sie während des Anklickens der Domänen die Strg-Taste oder die Hochschalttaste gedrückt halten.

Suche anzeigen/ausblenden
Um die Suchfunktion für die Liste der Benutzer aufzurufen, klicken Sie auf *Suche anzeigen*. Geben Sie in den Eingabefeldern *Benutzername* oder *Postfach* den Text ein, nach dem Sie die Liste der Benutzer durchsuchen wollen, und klicken Sie dann auf *Suche*, um die Liste der Benutzer anhand dieses Textes zu filtern. Klicken Sie auf *X Suche abbrechen*, um sich die ungefilterte Liste der Benutzer wieder anzeigen zu lassen.

Einstellungen
Dieses Steuerelement öffnet die Seite Meine Einstellungen[34] des ausgewählten Benutzerkontos. Dort können das Kennwort des Benutzer geändert, die Einstellungen für die Quarantäne des Benutzers, die Funktionen zur automatischen Weißen Liste und die Zahl der Elemente, die dem Benutzer nach der Anmeldung an SecurityGateway auf jeder Bildschirmseite angezeigt werden sollen, konfiguriert werden.

Nachrichten
Dieses Steuerelement öffnet das Nachrichten-Protokoll[307] für den ausgewählten Benutzer. Das Nachrichten-Protokoll enthält einen Eintrag für jede Nachricht, die an den Benutzer oder durch den Benutzer gesendet wurde. Über das Nachrichten-Protokoll kann für jeden Eintrag eine Seite mit weiterführenden Nachrichten-Informationen aufgerufen werden; diese Seite enthält den SMTP-Verbindungsmitschnitt und, sofern verfügbar, den Inhalt und den Quelltext der Nachricht.

Quarantäne
Um die Quarantäne[308] für den ausgewählten Benutzer zu öffnen, klicken Sie auf das Steuerelement *Quarantäne*. In der Übersicht, die dann angezeigt wird, sind alle Nachrichten aufgeführt, die für den Benutzer in Quarantäne gegeben wurden, und sie können von der Übersicht aus geprüft und durchgesehen werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Weiße Liste
Mithilfe des Steuerelements Weiße Liste können Sie die Weiße Liste für Adressen[276] für den ausgewählten Benutzer aufrufen. Diese Weiße Liste ist die persönliche Weiße Liste des Benutzers, und sie wirkt nur für sein Benutzerkonto.

Schwarze Liste
Mithilfe des Steuerelements Schwarze Liste können Sie die Schwarze Liste für Adressen[266] für den ausgewählten Benutzer aufrufen. Diese Schwarze Liste ist die persönliche Schwarze Liste des Benutzers, und sie wirkt nur für sein Benutzerkonto.

Import
Sie können mithilfe einer kommagetrennten Datei (Format CSV) eine Liste von Benutzern in die Liste der Benutzer importieren. Klicken Sie hierzu am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Benutzer importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die CSV-Datei aus, deren Inhalt Sie in die Liste der Domänen importieren wollen. Klicken Sie auf *Benutzer importieren*, um mit dem Import zu beginnen.

Im unteren Teil des Dialogs Benutzer importieren befindet sich die Option *"Nicht existierende Domänen automatisch anlegen"*. Ist diese Option aktiv, so werden neue Domänen automatisch angelegt, falls die zu importierende Liste der Benutzer E-Mail-Adressen aus Domänen enthält, die in SecurityGateway noch nicht angelegt sind. Ist diese Option abgeschaltet, so werden Adressen aus der zu importierenden Liste ignoriert und nicht importiert, falls sie Domänen enthalten, die in SecurityGateway noch nicht angelegt sind.

Format der CSV-Datei
Sie können die CSV-Datei für den Import in die Liste der Benutzer mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv.

Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Die folgenden Felder können im Feldraster enthalten sein, wobei die Namen der Felder jeweils in englischer Sprache erscheinen müssen:

- **Email** - E-Mail, die E-Mail-Adresse des Benutzers, z.B. "frank@example.com".
- **MailBox** - Postfach, der Postfachname aus der E-Mail-Adresse (im Beispiel "frank" aus "frank@example.com").
- **Domain** - Domäne, die Domäne aus der E-Mail-Adresse (im Beispiel "example.com").
- **FullName** - Vor- und Nachname, der Vor- und Nachname des Benutzers, z.B. "Frank Thomas".
- **Password** - Kennwort, das Kennwort des Benutzers, das er im Rahmen der Echtheitsbestätigung bei der Anmeldung an SecurityGateway und beim Versand von Nachrichten über SecurityGateway verwendet.
- **Enabled** - Aktiviert, bestimmt, ob das Benutzerkonto aktiv oder gesperrt ist. Um anzuzeigen, dass das Benutzerkonto aktiv ist, können Sie "1", "yes" (ja) oder "true" (wahr) in dieses Feld eintragen. Um anzuzeigen,

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

dass das Benutzerkonto gesperrt ist, können Sie "0", "no" (nein) oder "false" (unwahr) eintragen.

Die Felder Email, Mailbox und Domain werden in der jeweils angegebenen Reihenfolge verarbeitet. Widerspricht der Inhalt eines Feldes dem eines für denselben Eintrag bereits bearbeiteten Feldes, so wird der Inhalt des letzten für den Eintrag bearbeiteten Feldes verwendet. Lautet die Adresse im Feld Email beispielsweise "frank@example.com", erscheint dann aber "domain.com" im später verarbeiteten Feld Domain desselben Eintrags, so ergibt sich die Adresse "frank@domain.com", und diese Adresse wird in die Liste der Benutzer eingetragen.

Die Einträge für alle Felder müssen in Anführungs- und Schlusszeichen gesetzt und durch Kommata getrennt sein.

Beispiele für Inhalte von CSV-Dateien:

```
"Email", "MailBox", "Domain", "FullName", "Password",
"Enabled"
"frank@example.com", "frank", "example.com", "Frank Thomas",
"1234Kennwort", "1"
"rip@example.com", "rip", "example.com", "Rip Collector",
"FoundAPenny", "yes"
"big@domain.com", "big", "domain.com", "Mister Big",
"NumeroUno", "1"
```

Export
Sie können die Liste der Benutzer mithilfe des Steuerelements Export in der Symbolleiste exportieren. Es wird dabei eine CSV-Datei in demselben Format erstellt, wie sie auch für den bereits dokumentierten Import benötigt wird. Um die Liste der Benutzer zu exportieren, gehen Sie folgendermaßen vor:

1. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
1. Klicken Sie auf *Speichern*.
2. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
3. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

3.1.1.2.1 Benutzer bearbeiten

Mithilfe des Dialogs Benutzer bearbeiten können Sie für die Domänen von SecurityGateway neue Benutzerkonten anlegen und bestehende Benutzerkonten bearbeiten. Sie erreichen diesen Dialog, indem Sie in der Liste der Benutzer 54 auf *Neu* klicken, oder indem Sie einen Eintrag auswählen und *Bearbeiten* anklicken. Im Dialog *Benutzer bearbeiten* tragen Sie den Postfachnamen sowie den Vor- und Zunamen des Benutzers und sein Kennwort ein. Hier bestimmen Sie auch, ob der Benutzer ein Administrator 60 ist. Sie können auch Aliasnamen angeben, die Sie mit dem Benutzerkonto verknüpfen wollen.

Eigenschaften

Dieses Benutzerkonto ist gesperrt.
Um das Benutzerkonto zu sperren, klicken Sie dieses Kontrollkästchen an. SecurityGateway nimmt von dem Benutzer keine Nachrichten mehr an, sobald sein Konto gesperrt ist.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Postfachname:
Diese Option bestimmt den Postfachnamen und den Domänennamen des Benutzers (z.B. frank@example.com). Aus der Kombination beider Daten ergibt sich die E-Mail-Adresse des Benutzers, die er bei der Anmeldung in SecurityGateway verwendet. Die Adresse dient im Mailclient des Benutzers gleichzeitig als *Anmeldename* oder *Benutzername* für die SMTP-Echtheitsbestätigung.

Vor- und Nachname:
Hier werden Vor- und Nachname des Benutzers eingetragen (z.B. "Frank Thomas").

Kennwort:
Hier wird das Kennwort eingetragen, das der Benutzer zur Anmeldung und im Rahmen der SMTP-Echtheitsbestätigung verwendet.

Kennwort (zur Bestätigung):
Wird ein neues Kennwort eingetragen, so muss das Kennwort in dieses Feld erneut eingetragen werden. So wird bestätigt, dass das Kennwort richtig eingegeben wurde.

Starkes Kennwort für dieses Benutzerkonto nicht erzwingen
Diese Option bewirkt, dass das Benutzerkonto vom Erfordernis ausgenommen ist, starke Kennwörter 76 zu verwenden.

Administrator-Einstellungen

Benutzerkonto ist ein Administratorkonto
Um einen Benutzer zum Globalen oder zum Domänen-Administrator 60 zu bestimmen, aktivieren Sie dieses Kontrollkästchen, und wählen Sie eine der folgenden Optionen aus.

Globaler Administrator
Globale Administratoren 60 haben uneingeschränkten Zugriff auf alle Einstellungen und Optionen von SecurityGateway; sie haben auch Zugriff auf die Benutzerkonten und Einstellungen anderer Administratoren. Sie sollten daher bei der Bestimmung eines Benutzerkontos zum Globalen Administrator sehr bedachtsam vorgehen.

Domänen-Administrator
Domänen-Administratoren haben Zugriff auf alle Einstellungen und Optionen der Domänen, für die sie zu Administratoren bestimmt sind. Sie können Einstellungen nicht ändern, die das gesamte System oder solche Domänen betreffen, für die sie nicht zuständig sind. Falls Sie ein Benutzerkonto zum Domänen-Administrator bestimmen, müssen Sie zugleich wenigstens eine Domäne aus der Liste der *Verfügbaren Domänen* auswählen, für die der Domänen-Administrator zuständig ist.

Verfügbare Domänen:
In diesem Abschnitt sind alle in SecurityGateway angelegten Domänen aufgeführt, für die der Benutzer zum Domänen-Administrator bestimmt werden kann. Um den Benutzer zum Domänen-Administrator für eine oder mehrere dieser Domänen zu bestimmen, wählen Sie die Domäne aus der Liste aus, und klicken Sie auf den Pfeil "--->".

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausgewählte Domänen:
In diesem Abschnitt sind alle in SecurityGateway angelegten Domänen aufgeführt, für die der Benutzer zum Domänen-Administrator bestimmt ist. Um eine Domäne aus dieser Liste zu entfernen, wählen Sie die Domäne aus der Liste aus, und klicken Sie auf den Pfeil "<---".

Darf Domänen erstellen
Diese Option gestattet dem Domänen-Administrator das Erstellen neuer Domänen. Er wird für diese neu erstellten Domänen ebenfalls als Domänen-Administrator eingetragen.

Höchstzahl der Domänen, die erstellt werden dürfen: [xx] Domänen
Wenn Sie den Domänen-Administratoren das Erstellen neuer Domänen gestatten, können Sie mit Hilfe dieser Option die Anzahl der neuen Domänen beschränken, die die Domänen-Administratoren erstellen dürfen.

Postausgang

Mailserver der Domäne verwenden
Per Voreinstellung werden die Nachrichten der Benutzer durch die Mailserver der Domäne verarbeitet, die der Domäne des Benutzers zugewiesen sind 50. Falls Sie für die Nachrichten eines Benutzers nicht die allgemeinen Mailserver der Domäne sondern einen besonderen, von den Mailservern der Domäne abweichenden Mailserver verwenden wollen, aktivieren Sie die nachfolgend beschrieben Option.

Nachrichten mithilfe des angegebenen Mailservers/der angegebenen Mailserver zustellen
Diese Option bewirkt, dass Nachrichten für den gerade bearbeiteten Benutzer nicht über die allgemeinen Mailserver der Domäne geleitet werden, die der Domäne des Benutzers zugewiesen sind. Stattdessen werden die Nachrichten für den Benutzer über den oder die hier angegebenen Mail-Server geleitet.

Verfügbare/Ausgewählte Server
Um die Nachrichten des gerade bearbeiteten Benutzers durch einen oder mehrere besondere Mail-Server verarbeiten zu lassen, wählen Sie den oder die gewünschten Mail-Server aus der Liste der verfügbaren Server aus, und verschieben Sie sie mithilfe des Pfeils in die Liste der ausgewählten Server.

Aliasnamen

Auf der Registerkarte Aliasnamen können Sie die Aliasnamen angeben, die Sie mit dem Benutzerkonto verknüpfen wollen. Sie können auch in SecurityGateway bestehende Benutzerkonten verschmelzen und dabei Benutzerkonten, die Sie nicht mehr als eigenständige Benutzer fortführen wollen, in Aliasnamen für andere Benutzerkonten umwandeln.

Aliasnamen:
Um dem Benutzerkonto einen Aliasnamen zuzuordnen, tragen Sie die entsprechende E-Mail-Adresse in dieses Feld ein, und klicken Sie dann auf **Hinzufügen**. Um einen Aliasnamen aus der Liste zu löschen, wählen Sie den gewünschten Eintrag aus, und klicken Sie dann auf **Entfernen**.

Benutzer verschmelzen:
Mithilfe der Option Benutzer verschmelzen können Sie ein anderes eigenständiges Benutzerkonto in einen Aliasnamen für den Benutzer umwandeln, den Sie gerade

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

bearbeiten. Diese Funktion hilft insbesondere in den Fällen weiter, in denen SecurityGateway aufgrund der Informationen einer Datenquelle für Benutzerprüfung irrtümlich einen zusätzlichen Benutzer in SecurityGateway angelegt hat, obwohl die fragliche Adresse eigentlich ein Aliasname für einen bereits bestehenden Benutzer ist.

Sie können die gewünschte Adresse, die Sie verschmelzen wollen, einfach aufsuchen. Geben Sie dazu die Adresse im Feld Benutzer verschmelzen ein; die Liste der Benutzer wird dann direkt während der Eingabe gefiltert und zeigt nur die Einträge an, die mit Ihren Angaben übereinstimmen.

Verknüpfung "Benutzer verschmelzen"
Um ein Benutzerkonto in einen Aliasnamen umzuwandeln, klicken Sie in der Liste Benutzer verschmelzen auf die Verknüpfung "Benutzer verschmelzen", die zu dem gewünschten Benutzerkonto gehört. Die zugehörige Adresse wird dann in die Liste der Aliasnamen verschoben.

3.1.2 Administratoren

Mithilfe der Liste der Administratoren werden alle Globalen und Domänen-Administratoren verwaltet, die in SecurityGateway eingerichtet sind.

Globale Administratoren haben uneingeschränkten Zugriff auf alle Einstellungen und Optionen von SecurityGateway; sie haben auch Zugriff auf die Benutzerkonten und Einstellungen anderer Administratoren. Sie sollten daher bei der Bestimmung eines Benutzerkontos zum Globalen Administrator sehr bedachtsam vorgehen.

Domänen-Administratoren haben Zugriff auf alle Einstellungen und Optionen der Domänen, für die sie zu Administratoren bestimmt sind. Sie können Einstellungen nicht ändern, die das gesamte System oder solche Domänen betreffen, für die sie nicht zuständig sind. Falls Sie ein Benutzerkonto zum Domänen-Administrator bestimmen, müssen Sie zugleich wenigstens eine Domäne auswählen, für die der Domänen-Administrator zuständig ist.

Die Liste der Administratoren enthält drei Spalten: Aktiviert, E-Mail und Vor- und Nachname. Die Spalte Aktiviert enthält ein Kontrollkästchen für jeden Eintrag, mit dessen Hilfe das zugehörige Administratorkonto schnell aktiviert und gesperrt werden kann. In der Spalte E-Mail erscheint die E-Mail-Adresse des jeweiligen Administrators, die er für die Anmeldung an SecurityGateway nutzt; Benutzerkonten von Administratoren müssen keine lokalen Benutzerkonten sein und müssen auch nicht zu einer durch SecurityGateway verwalteten Domäne gehören. In der Spalte Vor- und Nachname erscheint der Name des Administrators (z.B. Frank Thomas). Um einen Administrator zu bearbeiten, klicken Sie doppelt auf den Listeneintrag des gewünschten Administrators, oder wählen Sie den Eintrag durch Einfachklick aus, und klicken Sie dann in der Symbolleiste am oberen Seitenrand auf Bearbeiten. In beiden Fällen wird der Dialog Administrator bearbeiten 61 aufgerufen.

Die Symbolleiste am oberen Seitenrand enthält die folgenden vier Optionen:

Neu
Klicken Sie auf *Neu,* um den Dialog Neuer Administrator aufzurufen und ein neues Administratorkonto anzulegen. Dieser Dialog entspricht dem Dialog Administrator bearbeiten 61.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Bearbeiten
Ein Klick auf das Steuerelement Bearbeiten in der Symbolleiste ruft den Dialog Administrator bearbeiten 61 für den Administrator auf, der in der Liste gerade ausgewählt ist. Sie können diesen Dialog auch durch einen Doppelklick auf den gewünschten Administrator in der Liste aufrufen.

Löschen
Um einen oder mehrere Administratoren zu löschen, wählen Sie die Administratoren in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Administratoren wirklich löschen wollen. Sie können mehrere Administratoren auswählen, indem Sie während des Anklickens der Domänen die Strg-Taste oder die Hochschalttaste gedrückt halten.

Für Domäne:
Mithilfe des Auswahlfeldes *Für Domäne:* können Sie die Domäne auswählen, deren Administratoren in der Liste angezeigt werden sollen. Per Voreinstellung werden alle Administratoren angezeigt. Sie können stattdessen "-- Global --" auswählen, um nur Globale Administratoren anzuzeigen, oder eine Domäne auswählen, um nur die Domänen-Administratoren dieser Domäne anzuzeigen.

3.1.2.1 Administrator bearbeiten

Mithilfe des Dialogs Administrator bearbeiten können Sie bestehende Globale und Domänen-Administratoren bearbeiten und neue Administratoren erstellen. Sie erreichen diesen Dialog, indem Sie auf der Seite Administratoren 60 auf *Neu* klicken, oder indem Sie einen Eintrag auswählen und *Bearbeiten* anklicken. Im Dialog *Administrator bearbeiten* geben Sie an, ob der Administrator ein lokales Benutzerkonto hat oder ein externer Benutzer ist, Sie geben weiter das lokale Postfach oder die externe E-Mail-Adresse des Administrators und seinen Vor- und Nachnamen an. Hier bestimmen Sie auch, ob der Benutzer ein Globaler oder Domänen-Administrator ist.

Eigenschaften

Lokaler Benutzer - Mitglied einer lokalen Domäne
Wählen Sie diese Option, falls das Administrator-Konto einem lokalen Benutzerkonto entsprechen soll, das zu einer durch SecurityGateway verwalteten Domäne gehört.

Extern - kein Mitglied einer lokalen Domäne
Administratoren müssen nicht zwingend lokale Benutzerkonten gaben. Sie können auch externe Benutzer mit externen E-Mail-Adressen sein. Falls der Administrator ein solcher externer Benutzer ist, wählen Sie diese Option aus.

Postfach oder E-Mail-Adresse
Falls Sie weiter oben die Option *Lokaler Benutzer* ausgewählt haben, geben Sie hier den Namen des Postfachs für den Administrator an, und wählen Sie dann aus dem Menü eine lokale Domäne aus. Falls Sie *Extern* gewählt haben, geben Sie hier nur die externe E-Mail-Adresse des Administrators ein. In beiden Fällen nutzen die Administratoren ihre E-Mail-Adressen für die Anmeldung an SecurityGateway.

Vor- und Nachname:
Hier werden Vor- und Nachname des Administrators eingetragen (z.B. "Frank Thomas").

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kennwort:
Hier wird das Kennwort eingetragen, das der Administrator zur Anmeldung an SecurityGateway verwendet.

Kennwort (zur Bestätigung):
Wird ein neues Kennwort eingetragen, so muss das Kennwort in dieses Feld erneut eingetragen werden. So wird bestätigt, dass das Kennwort richtig eingegeben wurde.

Dieses Benutzerkonto ist gesperrt.
Um das Benutzerkonto des Administrators zu sperren, klicken Sie dieses Kontrollkästchen an. SecurityGateway nimmt von dem Benutzer keine Nachrichten mehr an, sobald sein Konto gesperrt ist.

Typ

Mithilfe der folgenden Optionen bestimmen Sie, ob der Administrator die Berechtigung eines Globalen oder eines Domänen-Administrators erhält.

Globaler Administrator
Globale Administratoren[60] haben uneingeschränkten Zugriff auf alle Einstellungen und Optionen von SecurityGateway; sie haben auch Zugriff auf die Benutzerkonten und Einstellungen anderer Administratoren. Sie sollten daher bei der Bestimmung eines Benutzerkontos sehr bedachtsam vorgehen.

Domänen-Administrator
Domänen-Administratoren haben Zugriff auf alle Einstellungen und Optionen der Domänen, für die sie zu Administratoren bestimmt sind. Sie können Einstellungen nicht ändern, die das gesamte System oder solche Domänen betreffen, für die sie nicht zuständig sind. Falls Sie ein Benutzerkonto zum Domänen-Administrator bestimmen, müssen Sie zugleich wenigstens eine Domäne aus der Liste der *Verfügbaren Domänen* auswählen, für die der Domänen-Administrator zuständig ist.

Verfügbare Domänen:
In diesem Abschnitt sind alle in SecurityGateway angelegten Domänen aufgeführt, für die der Benutzer zum Domänen-Administrator bestimmt werden kann. Um den Benutzer zum Domänen-Administrator für eine oder mehrere dieser Domänen zu bestimmen, wählen Sie die Domäne aus der Liste aus, und klicken Sie auf den Pfeil "--->".

Ausgewählte Domänen:
In diesem Abschnitt sind alle in SecurityGateway angelegten Domänen aufgeführt, für die der Benutzer zum Domänen-Administrator bestimmt ist. Um eine Domäne aus dieser Liste zu entfernen, wählen Sie die Domäne aus der Liste aus, und klicken Sie auf den Pfeil "<---".

Darf Domänen erstellen
Diese Option berechtigt den Domänen-Administrator, neue Domänen zu erstellen. Erstellt der Domänen-Administrator eine Domäne, so wird er ihr automatisch als Domänen-Administrator hinzugefügt. Diese Option ist per Voreinstellung abgeschaltet.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Höchstzahl der Domänen, die erstellt werden dürfen: [xx]
Mithilfe dieser Option können Sie die Anzahl der Domänen beschränken, die ein Domänen-Administrator erstellen darf, falls er die entsprechende Berechtigung hat. Die Voreinstellung für diese Option ist die Begrenzung auf 5 Domänen. Sie können eine abweichende Begrenzung festlegen. Wenn Sie diese Option deaktivieren, darf der Domänen-Administrator eine unbegrenzte Anzahl Domänen erstellen.

3.1.3 Datenquellen für Benutzerprüfung

Mithilfe dieser Seite können Sie alle Datenquellen für die Benutzerprüfung verwalten. Diese Datenquellen dienen der Gültigkeitsprüfung für unbekannte lokale Adressen. Um diese Seite aufzurufen, klicken Sie im Navigationsbereich links auf *Einstellungen/Benutzer*, und klicken Sie dann im Abschnitt Benutzerkonten auf *Datenquellen für Benutzerprüfung*.

Geht eine Nachricht ein, die an einen für SecurityGateway unbekannten lokalen Benutzer gerichtet ist, so fragt SecurityGateway die Datenquellen für die Benutzerprüfung ab, die für die Zieldomäne eingerichtet sind, um festzustellen, ob die Adresse zu einem gültigen Benutzerkonto gehört. Besteht ein solches gültiges Benutzerkonto, so legt SecurityGateway ein Benutzerkonto für die Zieladresse an und versucht dann, die Nachricht an den Mailserver der Domäne 79 zuzustellen. Ergibt die Prüfung, dass die Adresse nicht gültig ist, so wird die Nachricht abgewiesen. Nachdem auf diese Weise ein neues Benutzerkonto angelegt wurde, kann dem Benutzer eine Begrüßungsnachricht 73 übermittelt werden, die auch eine Verknüpfung für die Anmeldung an SecurityGateway enthält.

Versendet ein lokaler Benutzer, der SecurityGateway noch nicht bekannt ist, abgehend eine Nachricht, so fragt SecurityGateway die Datenquellen für die Benutzerprüfung in gleicher Weise ab, wie es bei eingehenden Nachrichten geschieht. Versucht ein Benutzer, mithilfe seiner E-Mail-Adresse und seines Kennworts eine Echtheitsbestätigung durchzuführen, so leitet SecurityGateway diese Anmeldedaten an die Datenquellen für die Benutzerprüfung weiter. Schlägt die Echtheitsbestätigung fehl, so wird die Nachricht abgewiesen. Ist die Echtheitsbestätigung erfolgreich, so wird die Nachricht zur Zustellung entgegengenommen, und es wird in SecurityGateway für den Benutzer ein Benutzerkonto angelegt. Ist ein solches Benutzerkonto bereits vorhanden, so prüft SecurityGateway die Anmeldedaten des Benutzers erst anhand der lokalen Benutzerdatenbank. Ergibt sich nach dieser Prüfung keine Übereinstimmung, so werden die Datenquellen für die Benutzerprüfung abgefragt.

Die Datenquellen für die Benutzerprüfung werden in der Reihenfolge abgefragt, in der Sie auf der Registerkarte Prüfung im Dialog Eigenschaften 50 der Domäne erscheinen. Sobald entweder ein positives oder ein negatives Ergebnis eingetreten ist, nimmt SecurityGateway dieses Ergebnis an und fragt keine weiteren Datenquellen mehr ab. Sind beispielsweise drei Datenquellen der Domäne zugeordnet, und teilt die erste Datenquelle mit, dass der Benutzer nicht existiert, so nimmt SecurityGateway dieses Ergebnis an und fragt die verbleibenden beiden Datenquellen nicht mehr ab. Tritt bei der Abfrage hingehen ein vorübergehender Fehler auf, etwa, weil eine Datenquelle vorübergehend nicht

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

verfügbar ist, so wird die Nachricht mit einem Fehlerkode *4xx* abgewiesen; dieser Fehlerkode fordert den Absender auf, die Zustellung später erneut zu versuchen.

Es ist äußerst wichtig, dass die Datenquellen für die Benutzerprüfung richtig konfiguriert sind und **ausschließlich** wirklich gültige Benutzer als solche bestätigen. Handelt es sich etwa bei einer Datenquelle um ein offenes Relais, oder besteht bei der Datenquelle ein "Catch-all-Alias" für eine durch SecurityGateway verwaltete Domäne, so bestätigt diese Datenquelle jede beliebige Nachricht, die für einen unbekannten Benutzer eingeht. Da die meisten eingehenden Spam-Nachrichten an ungültige und nicht bestehende Benutzer gerichtet sind, diese Benutzer aber durch die falsch konfigurierte Datenquelle als echt bestätigt werden, führt dieses Vorgehen mit Sicherheit dazu, dass zahlreiche Benutzer irrtümlich angelegt werden. Die Höchstzahl der Benutzer, die nach der jeweiligen Lizenz zulässig sind, würde dann sehr schnell erreicht werden.

In der Übersicht über die Datenquellen für die Benutzerprüfung wird ein Eintrag pro Zeile angezeigt, und jede Zeile ist in vier Spalten unterteilt: Beschreibung, Server, Port und Typ. In der Spalte Beschreibung erscheint eine Beschreibung der Datenquelle (z.B. "*Server X bei example.com*"). In der Spalte Server erscheinen der Hostname oder die IP-Adresse der Datenquelle, und in der Spalte Port erscheint die Portnummer, die die jeweilige Datenquelle nutzt. In der Spalte Typ wird die Art der Datenquelle angezeigt: SMTP-Prüfung (vorwärtsgerichtet)[68], Active Directory/Exchange[68], MDaemon (Minger)[69], LDAP[69] oder Office 365[70]. Um eine Datenquelle zu bearbeiten, klicken Sie doppelt auf ihren Eintrag, oder wählen Sie die Datenquelle durch Einfachklick aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf Bearbeiten. In beiden Fällen öffnet sich der Dialog Datenquelle für Benutzerprüfung bearbeiten[66].

Alle Datenquellen außer LDAP unterstützen die dynamische Echtheitsbestätigung. Versuchen Benutzer, die Echtheitsbestätigung durchzuführen oder sich an SecurityGateway anzumelden, werden ihre Anmeldedaten zunächst lokal durch SecurityGateway geprüft; falls SecurityGateway keine Übereinstimmung feststellt, werden die Anmeldedaten zur Echtheitsbestätigung an die Datenquellen weitergeleitet. Die Benutzer können somit die Echtheitsbestätigung durchführen und sich an SecurityGateway anmelden, ohne dass sie sich gesonderte Anmeldedaten nur für SecurityGateway merken müssen.

AUTH-Kennwörter können nicht dynamisch geprüft werden, falls das Verfahren CRAM-MD5[92] zur Echtheitsbestätigung eingesetzt wird.

Die Symbolleiste am oberen Seitenrand enthält die folgenden fünf Optionen:

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Neu
Um eine neue Datenquelle für Benutzerprüfung zu erstellen, klicken Sie auf *Neu.* Es öffnet sich der Dialog Neue Datenquelle für Benutzerprüfung, der dem Dialog Datenquelle für Benutzerprüfung bearbeiten 66 entspricht.

Bearbeiten
Um die gerade in der Liste ausgewählte Datenquelle zu bearbeiten, klicken Sie in der Symbolleiste auf Bearbeiten. Es öffnet sich der Dialog Datenquelle für Benutzerprüfung bearbeiten 66. Sie können diesen Dialog auch durch einen Doppelklick auf den gewünschten Eintrag aufrufen.

Löschen
Um einen oder mehrere Datenquellen für Benutzerprüfung zu löschen, wählen Sie die Einträge in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Datenquellen wirklich löschen wollen. Sie können mehrere Einträge auswählen, indem Sie während des Anklickens der Einträge die Strg-Taste oder die Hochschalttaste gedrückt halten.

Benutzer prüfen
Ist im Auswahlfeld *Für Domäne:* der Eintrag "-- Alle --" aktiv, so versucht SecurityGateway nach einem Klick auf dieses Steuerelement sofort, alle Benutzer zu prüfen — und zwar auch jene, die in der Vergangenheit bereits einmal geprüft wurden. Alle Benutzer, die über die Datenquelle nicht erfolgreich geprüft werden können, einschließlich der manuell angelegten Benutzer, werden dann gelöscht. Wird in dem Auswahlmenü *Für Domäne:* eine bestimmte Domäne ausgewählt, so prüft SecurityGateway nur die Benutzer dieser Domäne.

Optionen
Durch Anklicken dieses Steuerelements wird die Seite Optionen zur Datenquelle für Benutzerprüfung aufgerufen. Sie können hier Optionen für das Zwischenspeichern von Antworten und für die turnusgemäße Überprüfung von Benutzern in bestimmten Zeitabständen festlegen.

Benutzer vormerken zur erneuten Prüfung nach [xx] Stunden
Diese Option erleichtert die Pflege der Benutzerliste. Sie fragt bei der Datenquelle für Benutzerprüfung in regelmäßigen Abständen ab, ob die Benutzer noch existieren. Sobald die hier in Stunden angegebene Zeit abgelaufen ist, werden die früher schon geprüften Benutzer für eine erneute Prüfung vorgemerkt. Sobald sie dann E-Mail-Nachrichten versenden oder empfangen, werden sie erneut überprüft. Deaktivierte Benutzer werden nicht gelöscht.

Negative Antworten zwischenspeichern für [xx] Minuten
Meldet eine Datenquelle für Benutzerprüfung auf die Abfrage hin, dass ein Benutzerkonto nicht existiert, so wird diese Antwort für die hier in Minuten angegebene Zeit im Cache gespeichert. Dies verringert die Zahl der redundanten Abfragen bei der Datenquelle.

Standard-Datenquellen für Benutzerprüfung stets nach externen Aliasnamen abfragen
Ist diese Option aktiv, so werden alle unbekannten Adressen durch Abfrage bei den Standard-Datenquellen für Benutzerprüfung geprüft. Meldet eine Datenquelle für Benutzerprüfung, dass es sich bei der Adresse um einen externen Alias eines Benutzers in einer lokalen Domäne handelt, so wird der lokale Benutzer nötigenfalls angelegt, und der Alias wird mit dem Benutzer verknüpft. Diese Option ist nur verfügbar, wenn mindestens eine Datenquelle für Benutzerprüfung konfiguriert ist.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

> Da alle unbekannten Adressen in dieser Weise geprüft werden, kann sich eine hohe Anzahl von Abfragen ergeben.

Für Domäne:
Mithilfe des Auswahlfeldes *Für Domäne:* können Sie die Domäne auswählen, deren Datenquellen für Benutzerprüfung in der Liste angezeigt werden sollen. Per Voreinstellung werden alle Datenquellen angezeigt. Sie können stattdessen "--Standard --" auswählen, um nur die Datenquellen anzuzeigen, die Sie im Dialog Datenquelle für Benutzerprüfung bearbeiten 66 als Standard-Datenquellen bestimmt haben, und Sie können eine Domäne auswählen, um nur die Datenquellen für diese Domäne anzuzeigen.

3.1.3.1 Optionen zur Datenquelle für Benutzerprüfung

Benutzer vormerken zur erneuten Prüfung nach [xx] Stunden
Diese Option erleichtert die Pflege der Benutzerliste. Sie fragt bei der Datenquelle für Benutzerprüfung in regelmäßigen Abständen ab, ob die Benutzer noch existieren. Sobald die hier in Stunden angegebene Zeit abgelaufen ist, werden die früher schon geprüften Benutzer für eine erneute Prüfung vorgemerkt. Sobald sie dann E-Mail-Nachrichten versenden oder empfangen, werden sie erneut überprüft. Deaktivierte Benutzer werden nicht gelöscht.

Negative Antworten zwischenspeichern für [xx] Minuten
Meldet eine Datenquelle für Benutzerprüfung auf die Abfrage hin, dass ein Benutzerkonto nicht existiert, so wird diese Antwort für die hier in Minuten angegebene Zeit im Cache gespeichert. Dies verringert die Zahl der redundanten Abfragen bei der Datenquelle.

Standard-Datenquellen für Benutzerprüfung stets nach externen Aliasnamen abfragen
Ist diese Option aktiv, so werden alle unbekannten Adressen durch Abfrage bei den Standard-Datenquellen für Benutzerprüfung geprüft. Meldet eine Datenquelle für Benutzerprüfung, dass es sich bei der Adresse um einen externen Alias eines Benutzers in einer lokalen Domäne handelt, so wird der lokale Benutzer nötigenfalls angelegt, und der Alias wird mit dem Benutzer verknüpft. Diese Option ist nur verfügbar, wenn mindestens eine Datenquelle für Benutzerprüfung konfiguriert ist.

> Da alle unbekannten Adressen in dieser Weise geprüft werden, kann sich eine hohe Anzahl von Abfragen ergeben.

Siehe auch:

Datenquellen für Benutzerprüfung 63

3.1.3.2 Datenquelle für Benutzerprüfung bearbeiten

Mithilfe des Dialogs Datenquellen für Benutzerprüfung bearbeiten können Sie bestehende Datenquellen für Benutzerprüfung 63 bearbeiten und neue Datenquellen erstellen. Sie erreichen diesen Dialog, indem Sie auf der Seite Datenquellen für Benutzerprüfung auf *Neu* klicken, oder indem Sie einen Eintrag auswählen und *Bearbeiten* anklicken. In diesem Dialog bestimmen Sie den Typ der Datenquelle, ihren Standort, den Port, über den eine Verbindung zur Datenquelle hergestellt wird, die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Anmeldedaten, falls solche benötigt werden, und die Domänen für die SecurityGateway diese Datenquelle nutzen soll.

Eigenschaften

Typ:
In diesem Auswahlfeld geben Sie an, welche Art der Benutzerprüfung die Datenquelle durchführt: SMTP-Prüfung (vorwärtsgerichtet)[68], Active Directory/Exchange[68], MDaemon (Minger)[69], LDAP[69] oder Office 365[70]. Die Optionen *Beschreibung*, *Hostname oder IP* und *Port,* die weiter unten beschrieben werden, betreffen alle vier Typen der Datenquellen für Benutzerprüfung gleichermaßen. Die anderen Optionen ändern sich in Abhängigkeit von dem ausgewählten Typ der Datenquelle. Allen Typen der Datenquellen ist gemeinsam, dass SecurityGateway nach erfolgreicher Prüfung eines noch unbekannten lokalen Benutzers ein Benutzerkonto anlegt, und dass dem Benutzer eine Begrüßungsnachricht[73] übermittelt werden kann, die auch eine Verknüpfung für die Anmeldung an SecurityGateway enthält. Der Benutzer kann sich dann mithilfe seiner E-Mail-Adresse und seines Kennworts bei SecurityGateway anmelden und sein Nachrichten-Protokoll, seinen Quarantäne-Ordner und anderes einsehen. Da eine dynamische Echtheitsbestätigung über LDAP nicht möglich ist, muss den Benutzern bei Nutzung einer Datenquelle dieses Typs ein Kennwort für SecurityGateway zugewiesen werden, bevor sie sich an SecurityGateway anmelden können.

Alle Datenquellen außer LDAP unterstützen die dynamische Echtheitsbestätigung. Versuchen Benutzer, die Echtheitsbestätigung durchzuführen oder sich an SecurityGateway anzumelden, werden ihre Anmeldedaten zunächst lokal durch SecurityGateway geprüft; falls SecurityGateway keine Übereinstimmung feststellt, werden die Anmeldedaten zur Echtheitsbestätigung an die Datenquellen weitergeleitet. Die Benutzer können somit die Echtheitsbestätigung durchführen und sich an SecurityGateway anmelden, ohne dass sie sich gesonderte Anmeldedaten nur für SecurityGateway merken müssen.

AUTH-Kennwörter können nicht dynamisch geprüft werden, falls das Verfahren CRAM-MD5[92] zur Echtheitsbestätigung eingesetzt wird.

Beschreibung:
Tragen Sie in dieses Feld eine Beschreibung der Datenquelle ein (z.B. "*Server X bei example.com*"). Der Inhalt dieses Feldes entspricht der Spalte *Beschreibung* auf der Seite Datenquellen für Benutzerprüfung[63].

Hostname oder IP:
Tragen Sie in dieses Feld den Hostnamen oder die IP-Adresse der Datenquelle ein. SecurityGateway stellt die Verbindung zu dieser Datenquelle mithilfe der hier angegebenen Daten her. Die Option entspricht der Spalte *Host* auf der Seite Datenquellen für Benutzerprüfung.

Port:
SecurityGateway stellt die Verbindung zur Datenquelle über diesen Port her; die Option entspricht der Spalte *Port* auf der Seite Datenquellen für Benutzerprüfung.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

SMTP-Prüfung (vorwärtsgerichtet)

Falls Sie unbekannte lokale Empfänger eingehender Nachrichten und unbekannte Absender abgehender Nachrichten über SMTP prüfen wollen, wählen Sie diesen Typ aus. SecurityGateway versucht dann, ähnlich wie bei der Prüfung durch Rückruf 217, den Benutzer über das SMTP-Protokoll zu prüfen. Versuchen unbekannte lokale Absender die Echtheitsbestätigung, so gibt SecurityGateway die Anmeldedaten des Benutzers an die SMTP-Datenquelle zur Echtheitsbestätigung weiter. Ist die Echtheitsbestätigung erfolgreich, so wird die Nachricht durch SecurityGateway zur Zustellung angenommen, und für den Benutzer wird ein Benutzerkonto erstellt. Besteht ein Benutzerkonto bereits, so prüft SecurityGateway die Anmeldedaten zunächst anhand der lokalen Benutzerdatenbank. Ergibt diese Prüfung keine Übereinstimmung, so wird die SMTP-Datenquelle abgefragt.

Erfordert Echtheitsbestätigung
Falls für den Zugang zur SMTP-Datenquelle eine Echtheitsbestätigung erforderlich ist, aktivieren Sie dieses Kontrollkästchen, und geben Sie Benutzernamen und Kennwort in die folgenden Felder ein.

Benutzername:
Falls für den Zugang zur SMTP-Datenquelle eine Echtheitsbestätigung erforderlich ist, geben Sie den Benutzernamen hier ein.

Kennwort:
Geben Sie hier das Kennwort für die SMTP-Datenquelle ein.

Active Directory/Exchange

Falls Sie unbekannte lokale Benutzer anhand eines Active Directorys oder eines Exchange-Servers prüfen wollen, wählen Sie dieses Typ aus. Dieser Typ unterstützt, ebenso wie die oben beschriebene SMTP-Prüfung, die dynamische Echtheitsbestätigung. Versuchen unbekannte lokale Absender die Echtheitsbestätigung, so gibt SecurityGateway die Anmeldedaten des Benutzers an das Active Directory oder den Exchange-Server zur Echtheitsbestätigung weiter. Ist die Echtheitsbestätigung erfolgreich, so wird die Nachricht durch SecurityGateway zur Zustellung angenommen, und für den Benutzer wird ein Benutzerkonto erstellt. Besteht ein Benutzerkonto bereits, so prüft SecurityGateway die Anmeldedaten zunächst anhand der lokalen Benutzerdatenbank. Ergibt diese Prüfung keine Übereinstimmung, so werden das Active Directory oder der Exchange-Server abgefragt.

Benutzername:
In dieses Feld muss der Benutzername eingetragen werden, der für den Zugang zum Active Directory oder Exchange-Server erforderlich ist.

Kennwort:
In dieses Feld muss das Kennwort eingetragen werden, das zu dem eben angegebenen Benutzernamen gehört.

Suchfilter:
Bei der Abfrage des Active Directorys oder Exchange-Servers wird der hier angegebene Suchfilter genutzt. Der voreingestellte Suchfilter sollte in den meisten Fällen ausreichen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Suchumfang:
Diese Option bestimmt den Umfang und den Bereich der Suche im Active Directory.

nur Base-DN
Um die Suche auf den Base-DN zu beschränken, wählen Sie diese Option. Die Suche erstreckt sich dann nicht auf dieser Ebene untergeordnete Ebenen im Verzeichnisbaum (Directory Information Tree, kurz DIT).

1 Ebene unter Base-DN
Um die Suche im Active Directory auf eine Ebene im DIT unterhalb des Base-DN zu erstrecken, wählen Sie diese Option.

Base-DN und alle untergeordneten Einträge
Diese Option erstreckt die Suche vom Base-DN auf alle untergeordneten Child-Einträge bis zur untersten Ebene des DIT. Diese Option ist per Voreinstellung aktiv.

MDaemon (Minger)

Falls Sie einen MDaemon-Server mit Minger als Datenquelle für die Benutzerprüfung einsetzen wollen, wählen Sie diese Option aus. Es kommt eine erweiterte Version des Minger-Protokolls zum Einsatz, das nur MDaemon-Servern zur Verfügung steht; diese Option kann daher nicht mit anderen Server-Typen verwendet werden. Wie auch die beiden schon beschriebenen Verfahren, unterstützt auch dieses Verfahren die dynamische Echtheitsbestätigung. Ihre Benutzer können daher mithilfe ihrer Anmeldedaten für den Mailserver die Echtheitsbestätigung durchführen und sich an Ihren SecurityGateway-Benutzerkonten anmelden.

Erfordert Echtheitsbestätigung
Aktivieren Sie dieses Kontrollkästchen, falls der MDaemon-Server für die Nutzung von Minger eine Echtheitsbestätigung verlangt.

Kennwort:
Geben Sie hier das Minger-Kennwort für den verwendeten MDaemon-Server ein.

LDAP

Falls Sie einen LDAP-Server als Datenquelle für die Benutzerprüfung einsetzen wollen, wählen Sie diese Option aus. Anders, als die anderen Prüfverfahren, unterstützt LDAP die Echtheitsbestätigung der Anmeldedaten des Benutzers nicht. Die dynamische Echtheitsbestätigung wird daher bei diesem Verfahren nicht unterstützt. Falls auf Ihrem System die Benutzer eine Echtheitsbestätigung durchführen müssen, können sie sich nur dann bei SecurityGateway anmelden und Nachrichten über SecurityGateway verwenden, wenn sie das Kennwort verwenden, das dem Benutzerkonto in SecurityGateway selbst zugeordnet ist.

Bind-DN:
Geben Sie hier den Distinguished Name (DN), der Zugang zum LDAP-Server hat. SecurityGateway nutzt diesen Namen im Rahmen der LDAP-Abfrage. Der DN wird im Rahmen des Bind-Vorgangs zur Echtheitsbestätigung verwendet.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kennwort:
Dieses Kennwort wird zusammen mit dem *Bind-DN* zur Echtheitsbestätigung an den LDAP-Server übermittelt.

Base-DN:
Hier wird der Wurzel-DN eingetragen. Er dient als Ausgangspunkt im Verzeichnisbaum (Directory Information Tree, kurz DIT), von dem aus SecurityGateway das Active Directory nach Benutzern durchsucht.

Suchfilter:
Bei der Abfrage des LDAP-Servers wird der hier angegebene Suchfilter genutzt. Der voreingestellte Suchfilter sollte in den meisten Fällen ausreichen.

Suchumfang:
Diese Option bestimmt den Umfang und den Bereich der LDAP-Suche.

nur Base-DN
Um die Suche auf den oben angegebenen *Base-DN* zu beschränken, wählen Sie diese Option. Die Suche erstreckt sich dann nicht auf dieser Ebene untergeordnete Ebenen im Verzeichnisbaum (Directory Information Tree, kurz DIT).

1 Ebene unter Base-DN
Um die Suche auf eine Ebene im DIT unterhalb des *Base-DN* zu erstrecken, wählen Sie diese Option.

Base-DN und alle untergeordneten Einträge
Diese Option erstreckt die Suche vom *Base-DN* auf alle untergeordneten Child-Einträge bis zur untersten Ebene des DIT. Diese Option ist per Voreinstellung aktiv.

Office 365

Um Office 365 als Datenquelle für die Benutzerprüfung zu verwenden, aktivieren Sie diese Option, und richten Sie die Datenquelle nach der folgenden Anleitung ein.

SecurityGateway kann nur dann auf den Office-365-Mandanten zugreifen, wenn für das Abonnement des Mandanten der Plan Exchange Online aktiv ist. Bitte stellen Sie sicher, dass dieser Plan in Ihrem Office-365-Mandanten enthalten ist, wenn Sie diese Datenquelle für Benutzerprüfung einsetzen wollen.

Um Office 365 als Datenquelle für Benutzerprüfung verwenden zu können, benötigt SecurityGateway einen Dienstprinzipal mit Berechtigung zum Zugriff auf den Office-365-Mandanten. Office 365 setzt das Azure Active Directory als Verzeichnisdienst ein. Führen Sie die nachfolgend beschriebenen Schritte aus, um Office 365 als Datenquelle für Benutzerprüfung in SecurityGateway zu konfigurieren.

Im Azure Active Directory:

1. Rufen Sie im Abschnitt Azure Active Directory die Seite **App-Registrierungen** auf.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

2. Klicken Sie auf **Neue Registrierung**.
3. Tragen Sie im Feld Name den Namen der App ein.
4. Klicken Sie auf **Registrieren**.
5. Notieren Sie sich die Anwendungs-ID.
6. Klicken Sie auf **API-Berechtigungen**.
7. Klicken Sie auf **+ Eine Berechtigung hinzufügen**.
8. Wählen Sie Microsoft Graph.
9. Klicken Sie auf **Anwendungs-Berechtigungen**.
10. Wählen Sie **Group.Read.All** und **User.Read.All**
11. Klicken Sie auf **Berechtigungen hinzufügen**.
12. Klicken Sie auf **Administratoreinwilligung erteilen für...**
13. Klicken Sie auf **Ja**.
14. Klicken Sie auf **Zertifikate & Geheimnisse**.
15. Klicken Sie auf **+ Neues Anwendungsgeheimnis**.
16. Tragen Sie eine Beschreibung in das Feld Beschreibung ein.
17. Wählen Sie aus, wie lange das Kennwort gültig sein soll.
18. Notieren Sie sich das erzeugte Kennwort.

In SecurityGateway:

1. Melden Sie sich als globaler Administrator an SecurityGateway an.
2. Klicken Sie auf **Einstellungen / Benutzer**.
3. Klicken Sie auf Select **Benutzerkonten**.
4. Klicken Sie auf **Datenquellen für Benutzerprüfung**.
5. Klicken Sie auf **Neu**.
6. Wählen Sie **Office 365** aus.
7. Tragen Sie eine Beschreibung ein.
8. Tragen Sie den Domänennamen von Office 365 in das Feld **Domänename** ein.
9. Wählen Sie den Typ aus.

   Die hier zutreffende Option wird in den meisten Fällen "Global" sein.
10. Tragen Sie die Anwendungs-ID aus dem Azure Active Directory in das Feld **Dienstprinzipal** ein.

    Sie finden die Anwendungs-ID in der Übersichtsseite für die App-Registrierungen im Azure Active Directory.
11. Tragen Sie das im Azure Active Directory erstellte Kennwort in das Feld **Kennwort** ein.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Typ

Dieser Server ist eine Standard-Datenquelle für die Benutzerprüfung
Falls Sie diese Datenquelle als eine der Standard-Datenquellen für die Benutzerprüfung festlegen wollen, aktivieren Sie dieses Kontrollkästchen. Die Standard-Datenquellen werden für alle SecurityGateway-Domänen verwendet, denen nicht bestimmte Datenquellen zur Nutzung zugeordnet sind. Sie kommen auch für die Funktion Automatisches Anlegen von Domänen[72] zum Einsatz.

Geben Sie im Folgenden an, welche Domänen diese Datenquelle für die Benutzerprüfung nutzen sollen...
Mithilfe der folgenden Optionen können Sie diese Datenquelle einer SecurityGateway-Domäne oder mehreren SecurityGateway-Domänen zuordnen. Sind einer Domäne mehrere Datenquellen zugeordnet, so können Sie die Reihenfolge, in der diese abgefragt werden, auf der Registerkarte Prüfung[50] in Dialog Eigenschaften der Domäne festlegen.

Verfügbare Domänen:
In diesem Abschnitt sind alle in SecurityGateway angelegten Domänen aufgeführt. Um die Domänen festzulegen, denen diese Datenquelle zugeordnet werden soll, wählen Sie die Domänen aus der Liste aus, und klicken Sie auf den Pfeil "--->".

Ausgewählte Domänen:
In diesem Abschnitt sind alle in SecurityGateway angelegten Domänen aufgeführt, denen diese Datenquelle zugeordnet ist. Um eine Domäne aus dieser Liste zu entfernen, wählen Sie die Domäne aus der Liste aus, und klicken Sie auf den Pfeil "<---".

3.1.4 Automatisches Anlegen von Domänen

Mithilfe dieser Seite können Sie bestimmen, ob SecurityGateway eine Domäne automatisch anlegen soll, falls eine eingehende Nachricht an einen unbekannten Benutzer einer unbekannten Domäne eingeht und der Empfänger durch eine Datenquelle für Benutzerprüfung[63] erfolgreich geprüft wird. Um diese Seite aufzurufen, klicken Sie im Navigationsbereich links auf *Einstellungen/Benutzer,* und klicken Sie dann im Abschnitt Benutzerkonten auf *Automatisches Anlegen von Domänen*.

Konfiguration

Automatisches Anlegen von Domänen aktivieren
Ist diese Option aktiv, so fragt SecurityGateway die Standard-Datenquellen für Benutzerprüfung ab, sobald eine Nachricht für einen unbekannten Benutzer einer unbekannten Domäne eingeht. Ist die Adresse gültig, so legt SecurityGateway die Domäne und den Benutzer an. Das automatische Anlegen von Domänen funktioniert nur, falls wenigstens eine Standard-Datenquelle für Benutzerprüfung[66] eingerichtet ist. Da jede unbekannte Adresse eine Abfrage auslöst, muss mit einer großen Anzahl von Abfragen gerechnet werden. Diese Funktion ist per Voreinstellung abgeschaltet.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Für die Nutzung dieser Funktion ist es äußerst wichtig, dass die Datenquellen für die Benutzerprüfung richtig konfiguriert sind und AUSSCHLIESSLICH wirklich gültige Benutzer als solche bestätigen. Handelt es sich etwa bei einer Datenquelle um ein offenes Relais, so bestätigt diese Datenquelle jede beliebige Nachricht, die für einen unbekannten Benutzer eingeht. Durch eingehende Spam-Nachrichten, die an ungültige Adressen gerichtet sind, würden dann zahlreiche ungültige Domänen und Benutzer angelegt werden.

3.1.5 Benutzer-Optionen

Mithilfe dieser Seite können Sie bestimmen, auf welche Optionen Ihre Benutzer nach der Anmeldung an SecurityGateway mithilfe ihrer Benutzerkonten zugreifen können. Die Benutzer-Optionen können sowohl systemweit als auch nach Domänen getrennt geändert werden.

Zugriffssteuerung

Benutzern das Ändern ihrer Kennwörter gestatten
Diese Option gestattet es den Benutzern, ihre Kennwörter für SecurityGateway über die Seite Einstellungen zum Benutzerkonto 34 zu ändern.

Symbol "Kennwort anzeigen" in Kennwortfeldern aktivieren
In jedem Kennwortfeld erscheint ein Symbol, das ein Auge darstellt. Klickt der Benutzer auf dieses Symbol, so kann er das Kennwort im Klartext sehen, das er soeben eingegeben hat. Falls Sie nicht wünschen, dass sich die Benutzer die eingegebenen Kennwörter im Klartext anzeigen lassen können, deaktivieren Sie diese Option.

Benutzern gestatten, ihre eigenen Quarantäne-Ordner einzusehen und zu verwalten
Ist diese Option aktiv, so können die Benutzer eingehende Nachrichten einsehen und verwalten, die für sie in Quarantäne gegeben wurden. Die Benutzer erhalten dann Zugriff auf die Seite Meine Quarantäne anzeigen 42, von der aus sie Nachrichten freigeben und löschen und weitere Aufgaben erledigen können.

Benutzern das Bearbeiten ihrer eigenen Quarantäne-Einstellungen gestatten
Um den Benutzern zu gestatten, ihre Quarantäne-Einstellungen über die Seite Meine Einstellungen 34 zu bearbeiten, aktivieren Sie dieses Kontrollkästchen.

Benutzern das Betrachten eines Protokolls der für sie ein- und abgehenden Nachrichten gestatten
Diese Option gestattet es den Benutzern, die Nachrichten-Protokolle für ihre Benutzerkonten über die Verknüpfung Mein Nachrichten-Protokoll anzeigen 43 in SecurityGateway aufzurufen. In dem Protokoll erscheinen alle Nachrichten, die über die E-Mail-Adresse des Benutzers versendet oder unter ihr empfangen wurden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Benutzern das Durchsuchen und Anzeigen archivierter Nachrichten gestatten, die an ihre Benutzerkonten gerichtet sind oder von ihnen stammen
Per Voreinstellung können die Benutzer archivierte Nachrichten durchsuchen und einsehen, die an ihre Benutzerkonten gerichtet sind oder von ihnen aus versandt wurden. Falls Sie verhindern wollen, dass die Benutzer diese Suchfunktion nutzen, deaktivieren Sie diese Option.

Benutzern das Löschen archivierter Nachrichten gestatten, die an ihre Benutzerkonten gerichtet sind oder von ihnen stammen
Diese Option gestattet den Benutzern das Löschen archivierter Nachrichten, die an ihre Benutzerkonten gerichtet sind oder von ihnen aus versandt wurden. Diese Option ist per Voreinstellung abgeschaltet.

Benutzern gestatten, die Anti-Spam-Prüfungen für Nachrichten an ihre eigenen Benutzerkonten abzuschalten
Um den Benutzern zu gestatten, die Anti-Spam-Prüfungen für Nachrichten abzuschalten, die für ihre Benutzerkonten eingehen, aktivieren Sie dieses Kontrollkästchen. Schaltet ein Benutzer die Anti-Spam-Prüfungen für sein Benutzerkonto über die Seite Einstellungen zum Benutzerkonto 34 ab, so werden die Prüfungen DNSBL 169, URIBL 172, Heuristik und Bayes 162 sowie Outbreak Protection 157 nicht mehr durchgeführt.

Benutzer dürfen Erkennung für Hijacking für eigene Benutzerkonten deaktivieren
Per Voreinstellung können die Benutzer nicht selbst bestimmen, ob ihre Benutzerkonten von der Erkennung für Hijacking von Benutzerkonten 234 ausgenommen sein sollen. Falls Sie den Benutzern gestatten wollen, diese Einstellung zu ändern, aktivieren Sie diese Option.

Benutzern das Aktivieren der Zwei-Faktor-Authentifizierung gestatten
Diese Option gestattet es den Benutzern, für ihre Benutzerkonten die Zwei-Faktor-Authentifizierung zu aktivieren, um hierdurch die Anmeldung an ihren SecurityGateway-Benutzerkonten zusätzlich zu sichern. Ist diese Option aktiv, und meldet sich der Benutzer im Browser über eine sichere HTTPS-Verbindung an, so erscheint im Abschnitt Mein Benutzerkonto die Seite Zwei-Faktor-Authentifizierung 33. Die Zwei-Faktor-Authentifizierung stellt eine zusätzliche Sicherheitsmaßnahme dar, und sie verlangt bei der Anmeldung sowohl die Eingabe des Kennworts als auch eines besonderen Sicherheitskodes, der mithilfe einer Authenticator-App auf dem Smartphone des Benutzers erzeugt wird.

Aktivieren der Zwei-Faktor-Authentifizierung durch die Benutzer erzwingen
Diese Option macht die Nutzung der Zwei-Faktor-Authentifizierung bei der Anmeldung für alle Benutzer verpflichtend. Ist diese Option aktiv, so wird jeder Benutzer bei der ersten Anmeldung auf eine Seite zum Einrichten der Zwei-Faktor-Authentifizierung geleitet.

Speichern von Anmeldedaten durch Benutzer auf Endgeräten zulassen (erfordert HTTPS)
Ist diese Option aktiv, und stellt ein Benutzer eine durch HTTPS gesicherte Verbindung her, so erscheint auf der Anmeldeseite die Option "*Anmeldung auf diesem Gerät speichern und beibehalten*". Aktiviert der Benutzer diese Option, so wird er automatisch angemeldet, wenn er von demselben Gerät aus wiederum eine Verbindung zu SecurityGateway herstellt. Dies gilt jedoch nur, wenn der Benutzer sein Browserfenster schließt, ohne auf die Schaltfläche *Abmelden* zu klicken. Klickt der Benutzer auf die Schaltfläche *Abmelden*, so muss er sich beim nächsten Verbindungsaufbau erneut anmelden. Die Anmeldedaten werden für den Zeitraum

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

gespeichert, der mithilfe der folgenden Option "*Benutzer für folgende Anzahl Tage speichern (1 bis 365)*" bestimmt wird. Nach Ablauf dieses Zeitraums muss er sich erneut anmelden. Diese Option ist per Voreinstellung abgeschaltet. **Beachte:** Bei Benutzern, auf deren Geräten oder in deren Browsern mithilfe der Option *Anmeldung auf diesem Gerät speichern und beibehalten* die Anmeldedaten gespeichert wurden, erscheint auf der Seite Mein Benutzerkonto » Einstellungen 34 die Option *Anmeldung auf diesem Gerät/in diesem Browser nicht speichern*. Die Benutzer können mit dieser Option die gespeicherten Anmeldedaten löschen.

Benutzer für folgende Anzahl Tage speichern (1 bis 365)
Ist die Option *Speichern von Anmeldedaten durch Benutzer auf Endgeräten zulassen* aktiv, so steuert diese Option, für welchen Zeitraum die Anmeldung des Benutzers gespeichert wird, bevor er sich erneut anmelden muss. Die Voreinstellung für diesen Zeitraum beträgt 30 Tage.

Optionen zur Anmeldung

Verknüpfung "Kennwort vergessen" im Anmeldedialog anzeigen
Per Voreinstellung erscheint im Anmeldedialog eine Verknüpfung "Kennwort vergessen", mit deren Hilfe sich die Benutzer eine Verknüpfung zum Ändern ihres Kennworts an die E-Mail-Adresse senden lassen können, die ihrem Benutzerkonto in SecurityGateway zugeordnet ist. Falls Sie diese Verknüpfung ausblenden wollen, deaktivieren Sie diese Option.

Folgende Kontaktdaten für den Administrator auf der Anmeldeseite anzeigen
Mithilfe dieser Option können Sie Kontaktinformationen für den Administrator oder auch Verknüpfungen konfigurieren. Diese Inhalte werden auf der Anmeldeseite angezeigt. Der Text, den Sie in das Eingabefeld eintragen, kann auch HTML-Kode in bestimmtem Umfang enthalten, etwa Anker und Grafiken.

Voreinstellungen

Anti-Spam-Tests für Nachrichten nicht durchführen, wenn sie an das vorliegende Benutzerkonto gerichtet sind
Diese Option ist die Voreinstellung zur gleichnamigen Option auf der Seite Einstellungen zum Benutzerkonto 34 der einzelnen Benutzer. Ist die Option aktiv, so führt der Server per Voreinstellung die Prüfungen DNSBL 169, URIBL 172, Heuristik und Bayes 162 sowie Outbreak Protection 157 für Nachrichten, die an das Benutzerkonto gerichtet sind, nicht durch.

"Erkennung des Hijackings von Benutzerkonten" für dieses Benutzerkonto deaktivieren
Diese Option bewirkt, dass die Benutzerkonten per Voreinstellung von dem Leistungsmerkmale Erkennung des Hijackings von Benutzerkonten 234 ausgenommen sind. Diese Ausnahme kann beispielsweise für Benutzerkonten erforderlich sein, die in kurzer Zeit viele Nachrichten versenden müssen. Sie können diese Option für einzelne Benutzerkonten getrennt auf der Seite Einstellungen zum Benutzerkonto 34 konfigurieren.

Adressen, an die der Benutzer Nachrichten versendet, automatisch in Weiße Liste eintragen
Diese Option ist die Voreinstellung zur Option *Adressen, an die ich Nachrichten versende, automatisch in Weiße Liste eintragen* auf der Seite Einstellungen zum Benutzerkonto 34 der einzelnen Benutzer. Ist diese Option für einen Benutzer

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

aktiv, so wird jede Adresse, an die der Benutzer eine Nachricht sendet, in seine Weiße Liste eingetragen. Der Benutzer erreicht diese über die Verknüpfung Meine Weiße Liste[37]. Dadurch wird sichergestellt, dass künftige von diesen Adressen aus eingehende Nachrichten nicht irrtümlich als Spam gekennzeichnet werden.

Starke Kennwörter erzwingen
Per Voreinstellung müssen alle neuen Kennwörter mindestens acht Zeichen lang sein und jedes der folgenden Elemente enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen (z.B. ;,_.?/-=)

Auf der Seite Benutzer bearbeiten[57] steht die Option *Starkes Kennwort für dieses Benutzerkonto nicht erzwingen* zur Verfügung. Mithilfe dieser Option können Sie das Benutzerkonto von dem Erfordernis ausnehmen, starke Kennwörter zu verwenden.

Statistik-Diagramme anzeigen
Mit dieser Option können Sie festlegen, wann die Statistik-Diagramme auf dem Dashboard[9] und den Leitseiten[32] erscheinen. Sie können bestimmen, dass die Diagramme automatisch, immer, manuell oder nie erscheinen.

Sprache
Mithilfe dieses Auswahlmenüs bestimmen Sie die Sprache, in welcher der Server automatisch erzeugte Systemnachrichten senden soll. Die Benutzer können mithilfe einer gleich lautenden Option diese Spracheinstellung für ihre Benutzerkonten übergehen.

Kennwörter mit Liste kompromittierter Kennwörter eines Drittanbieters abgleichen
SecurityGateway kann die Kennwörter der Benutzer mit einer Liste als kompromittiert bekannter Kennwörter abgleichen, die durch einen Drittanbieter bereit gestellt wird. Der Abgleich findet statt, ohne dass das Kennwort an den Anbieter übermittelt wird. Ist das Kennwort eines Benutzers in der Liste vorhanden, so bedeutet dies nicht, dass das Benutzerkonto kompromittiert oder gehackt wurde. Es bedeutet vielmehr, dass das fragliche Kennwort bereits einmal auf einem anderen System durch einen Benutzer verwendet wurde, und dass dieses verwendete Kennwort von einer Datenpanne oder einem Datenleck betroffen war. Kennwörter, die als kompromittiert bekannt und veröffentlicht sind, können durch Angreifer für Wörterbuchangriffe verwendet werden. Kennwörter, die noch nie auf anderen Systemen verwendet wurden, sind demgegenüber sicherer. Nähere Informationen hierzu erhalten Sie in englischer Sprache unter Pwned Passwords.

Mithilfe des Dropdown-Menüs können Sie bestimmen, in welchem Intervall die Kennwörter mit der Liste abgeglichen werden sollen. Es stehen folgende Einstellungen zur Auswahl; sie bezeichnen jeweils den Zeitraum, der seit der letzten Prüfung vergangen sein muss, bevor eine neue Prüfung ausgeführt wird:

- Nie (Die Kennwörter werden nicht mit der Liste abgeglichen. Dies ist die Voreinstellung.)
- Ein Tag seit der letzten Prüfung

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- Eine Woche seit der letzten Prüfung
- Ein Monat seit der letzten Prüfung

Zahl der Elemente, die auf jeder Seite angezeigt werden:
Diese Option legt die Zahl der Elemente fest, die dem Benutzer auf jeder Bildschirmseite von SecurityGateway höchstens angezeigt werden. Sie betrifft u.a. Listen von Adressen in der Weißen Liste, dem Nachrichten-Protokoll, und anderes mehr. Falls die Zahl der Elemente, die in einer Liste enthalten sind, die Höchstzahl für eine Bildschirmseite übersteigt, findet der Benutzer am Ende jeder Seite einige Steuerelemente, mit deren Hilfe er zwischen den weiteren Seiten blättern und navigieren kann. Die Voreinstellung für diese Option beträgt 50.

Nutzungsbedingungen

Anmeldung durch Benutzer erst zulassen, wenn sie die folgenden Nutzungsbedingungen als verbindlich anerkannt haben
Diese Option bewirkt, dass Benutzer bei jeder Anmeldung bestimmte Nutzungsbedingungen oder andere Bedingungen anerkennen müssen. Sie können diese Nutzungsbedingungen in das Textfeld weiter unten eintragen. Die Benutzer können die Nutzungsbedingungen durch Aktivieren eines Kontrollkästchens während der Anmeldung anerkennen.

Neue Benutzer

Begrüßungsnachricht an neue Benutzer senden
Falls Sie nach dem Anlegen eines neuen Benutzerkontos dem Benutzer eine Begrüßungsnachricht senden wollen, aktivieren Sie dieses Kontrollkästchen. Die Nachricht enthält eine Verknüpfung mit SecurityGateway, mit deren Hilfe die Benutzer sich anmelden und ihre Einstellungen sowie den Quarantäne-Ordner verwalten können. Diese Option ist per Voreinstellung abgeschaltet.

Warnmeldung an Globale Administratoren senden, sobald ein neuer Benutzer angelegt wird
Diese Option bewirkt, dass die globalen Administratoren 60 immer dann per E-Mail benachrichtigt werden, wenn neue Benutzerkonten erstellt wurden.

Kennwort des neuen Benutzers mit Liste kompromittierter Kennwörter eines Drittanbieters abgleichen
Diese Option bewirkt, dass die Option *Kennwörter mit Liste kompromittierter Kennwörter eines Drittanbieters abgleichen* weiter oben auch auf die Kennwörter neuer Benutzer angewendet wird.

Pluszeichen (+) in Postfachnamen der Benutzer zulassen
Enable this option if you need to create users for which the mailbox name contains a plus (+) character. If enabled, those mailboxes will not be considered sub-address aliases. For example, `frank.thomas+billing@example.com` will be considered its own user rather than an alias of `frank.thomas@example.com` (see Subaddressing 77 below).

Subadressierung

Die *Subadressierung* (sie ist auch als "*Plus-Adressierung*" bekannt) gestattet das Einbinden von Ordnernamen oder Tags in E-Mail-Adressen ist. Mithilfe dieser Funktion können Nachrichten, die an *Postfach+Tag@Domäne* adressiert sind (z.B.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

frank.thomas+rechnungen@example.com), automatisch in dem Ordner des Benutzerkontos abgelegt werden, der in der Adresse bezeichnet ist. Manche E-Mail-Server führen diesen Vorgang automatisch aus, andere behandeln die Adresse einfach als Alias, und wieder andere unterstützen die Subadressierung möglicherweise gar nicht; diese behandeln die gesamte Adresse als normale E-Mail-Adresse und nicht als eine Adresse, die einen Tag enthält.

Einige Beispiele hierzu: Verfügt `frank.thomas@example.com` auf einem E-Mail-Server, der die Subadressierung unterstützt, über einen IMAP-Ordner namens "`Rechnungen`", so werden Nachrichten, die an "`frank.thomas+Rechnungen@example.com`" gerichtet sind, an Frank Thomas zugestellt und automatisch in diesen Ordner geleitet. Falls der Server die Subadressierung wie einen Alias behandelt, dann würde die Nachricht einfach in den Posteingang von Frank Thomas zugestellt werden (er könnte dann aber einen E-Mail-Filter erstellen, der diese Nachricht automatisch in den Ordner "`Rechnungen`" verschiebt). Falls der Server keine Subadressierung unterstützt, würde die Nachricht als Nachricht an den unbekannten Benutzer "`frank.thomas+Rechnungen`" behandelt und daher abgewiesen werden.

SecurityGateway prüft bei eingehenden Nachrichten mit einer Empfängeradresse nach dem oben dargestellten Muster, ob ein Benutzer mit dem Postfachnamen einschließlich des Zeichens "+" besteht, oder ob es sich um einen als Alias zu behandelnden subadressierten Benutzer handelt. Werden kein Benutzer und kein Alias gefunden, oder wird der Benutzer gefunden, muss aber erneut überprüft werden[66], so wird die betreffende Datenquelle für Benutzerprüfung[63] abgefragt. Bei dieser Abfrage wird die vollständige durch SecurityGateway empfangene Adresse verwendet. Hierdurch wird sichergestellt, dass der Mailserver die Adresse auch wirklich akzeptiert. Falls die Adresse erfolgreich geprüft wird, erstellt SecurityGateway je nach Bedarf einen neuen Benutzer oder einen Alias für den Benutzer.

Wird die Nachricht an einen Mailserver der Domäne[79] übermittelt, so verwendet SecurityGateway hierfür immer die vollständige E-Mail-Adresse, die in der Ursprungsnachricht enthalten war, also z.B. "`frank.thomas+rechnungen@example.com`".

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Benutzer-Optionen dieser Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

3.2 E-Mail-Konfiguration

Der Abschnitt E-Mail im Menü *Einstellungen/Benutzer* enthält die folgenden fünf Seiten, mit denen sich verschiedene Nachrichten-bezogene Funktionen steuern lassen:

Mailserver der Domäne[79]—Auf dieser Seite können Sie alle Mailserver Ihrer Domänen verwalten. Mailserver der Domänen sind die Mailserver, für die SecurityGateway als Netzübergang oder Gateway arbeitet. Üblicherweise sind dies

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

die Server, die die E-Mail-Konten Ihrer Benutzer bedienen, und auf denen auch die Nachrichten der Benutzer gespeichert sind. Empfängt SecurityGateway eine Nachricht für einen geprüften Benutzer einer Ihrer Domänen, so versucht SecurityGateway, die Nachricht an die Mailserver zuzustellen, die der Empfängerdomäne zugeordnet sind.

Externe POP-Benutzerkonten 82—Mithilfe der Optionen für externe POP-Benutzerkonten können Sie SecurityGateway veranlassen, Nachrichten aus einem externen POP-Postfächern abzurufen. Dabei kommt das Übertragungsprotokoll POP3 zum Einsatz; die Nachrichten werden dann automatisch an die Benutzer der Domäne weitergeleitet, die dem POP-Postfach zugeordnet ist. Sie werden dazu nach dem Abruf anhand der Einstellungen ausgewertet, die Sie im Konfigurationsdialog POP-Benutzerkonto bearbeiten 83 festlegen können, und an alle gültigen Benutzer weitergeleitet, die dabei als Empfänger erkannt werden. Die Zustellung erfolgt dabei so, wie wenn die Nachrichten über herkömmliche SMTP-Verbindungen übermittelt worden wären.

Quarantäne-Konfiguration 86—Auf dieser Seite können Sie Einstellungen treffen, die von den Optionen "*...Nachricht in Quarantäne geben*" abweichen, die für zahlreiche Sicherheits-Funktionen 154 zur Verfügung stehen. Sie können außerdem wählen, ob Ihre Benutzer für ihre Benutzerkonten eigene, von den Standard-Einstellungen für die Quarantäne der jeweiligen Domänen abweichende Einstellungen festlegen dürfen, und ob sie den Inhalt ihrer Quarantäne-Ordner einsehen und verwalten dürfen. Schließlich können Sie auch bestimmen, wie oft die Benutzer eine Übersicht über die Inhalte ihrer Quarantäne-Ordner erhalten sollen: nie, täglich oder wöchentlich.

Postausgang 90—Die Optionen auf der Seite Postausgang bestimmen, ob SecurityGateway abgehende Nachrichten selbst zustellt oder durch einen anderen Mailserver zustellen lässt. Auf dieser Seite wird auch festgelegt, wie lange SecurityGateway versuchen soll, eingehende und abgehende Nachrichten nach vorübergehenden Zustellfehlern erneut zuzustellen, bevor die Nachrichten als unzustellbar an den Absender zurückgeleitet werden. Diese Optionen wirken systemweit auf alle Domänen, die SecurityGateway verwaltet.

E-Mail-Protokoll 92—Die Seite E-Mail-Protokoll enthält verschiedene Optionen, die die technische Verarbeitung von E-Mail durch SecurityGateway beeinflussen. Sie können auf dieser Seite die Ports festlegen, die zum Empfang von Nachrichten dienen, die Höchstzahl gleichzeitiger SMTP-Verbindungen begrenzen und unter anderem bestimmen, ob SecurityGateway VRFY-Anfragen beantwortet und ob Kennwörter im Klartext zugelassen sind. Daneben enthält die Seite zahlreiche weiter gehende Optionen.

3.2.1 Mailserver der Domäne

Auf dieser Seite können Sie alle Mailserver Ihrer Domänen verwalten. Mailserver der Domänen sind die Mailserver, für die SecurityGateway als Netzübergang oder Gateway arbeitet. Üblicherweise sind dies die Server, die die E-Mail-Konten Ihrer Benutzer bedienen, und auf denen auch die Nachrichten der Benutzer gespeichert sind. Empfängt SecurityGateway eine Nachricht für einen geprüften Benutzer einer Ihrer Domänen, so versucht SecurityGateway, die Nachricht an die Mailserver zuzustellen, die der Empfängerdomäne zugeordnet sind. Jeder Domäne, die SecurityGateway verwaltet 48, können ein oder mehrere Mailserver besonders zugeordnet werden. Sind keine Server zugeordnet, so werden die Standard-Mailserver 80 genutzt. Um die Liste der Mailserver der Domäne

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

aufzurufen, klicken Sie im Navigationsbereich links auf *Einstellungen/Benutzer*, und klicken Sie dann im Abschnitt E-Mail auf *Mailserver der Domäne*.

In der Übersicht über die Mailserver der Domäne wird ein Eintrag pro Zeile angezeigt. Er enthält die drei Spalten Beschreibung, Server und Port. Die Spalte Beschreibung enthält eine Beschreibung des Mailservers (z.B. "*Server X bei example.com*"). Die Spalte Server enthält den Hostnamen oder die IP-Adresse des Mailservers. Die Spalte Port enthält den Port, der beim Versand von Nachrichten über den Mailserver verwendet wird. Um einen Mailserver der Domäne zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie einen Eintrag aus und klicken Sie dann in der Symbolleiste am oberen Seitenrand auf Bearbeiten. In beiden Fällen öffnet sich der Dialog Mailserver bearbeiten 80.

Die Symbolleiste am oberen Seitenrand enthält die folgenden vier Optionen:

Neu
Um einen neuen Mailserver anzulegen, klicken Sie auf *Neu*. Es öffnet sich der Dialog Neuer Mailserver, der dem Dialog Mailserver bearbeiten 80 entspricht.

Bearbeiten
Um den gerade in der Liste ausgewählten Mailserver zu bearbeiten, klicken Sie in der Symbolleiste auf Bearbeiten. Es öffnet sich der Dialog Mailserver bearbeiten 80 . Sie können diesen Dialog auch durch Doppelklick auf einen Eintrag aufrufen.

Löschen
Um einen oder mehrere Mailserver der Domäne zu löschen, wählen Sie die Einträge in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Server wirklich löschen wollen. Sie können mehrere Einträge auswählen, indem Sie während des Anklickens der Einträge die Strg-Taste oder die Hochschalttaste gedrückt halten.

Für Domäne:
Mithilfe des Auswahlfeldes *Für Domäne:* können Sie die Domäne auswählen, deren Mailserver in der Liste angezeigt werden sollen. Per Voreinstellung werden alle Server angezeigt. Sie können stattdessen "-- Standard --" auswählen, um nur die Mailserver anzuzeigen, die Sie im Dialog Mailserver bearbeiten 80 als Standard-Mailserver bestimmt haben, und Sie können eine Domäne auswählen, um nur die Mailserver für diese Domäne anzuzeigen.

3.2.1.1 Mailserver bearbeiten

Mithilfe des Dialogs Mailserver bearbeiten können Sie bestehende Mailserver der Domäne 79 bearbeiten und neue Mailserver erstellen. Sie erreichen diesen Dialog, indem Sie auf der Seite Mailserver der Domäne auf *Neu* klicken, oder indem Sie einen Eintrag auswählen und *Bearbeiten* anklicken. In diesem Dialog geben Sie eine Beschreibung für den Server an, außerdem seine Adresse als Standort und den Port, auf dem der Server erreichbar ist, sowie, falls erforderlich, die Anmeldedaten und die SecurityGateway-Domänen, die den Server benutzen sollen. Hier bestimmen Sie auch, ob der Server ein Standard-Mailserver ist.

Eigenschaften

Beschreibung:
Tragen Sie in dieses Feld eine Beschreibung des Servers ein (z.B. "*Server X bei example.com*"). Der Inhalt dieses Feldes entspricht der Spalte *Beschreibung* auf der Seite Mailserver der Domäne 79.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Hostname oder IP:
Tragen Sie in dieses Feld den Hostnamen oder die IP-Adresse des Mailservers ein. SecurityGateway stellt die Verbindung zu diesem Mailserver mithilfe der hier angegebenen Daten her. Die Option entspricht der Spalte *Server* auf der Seite Mailserver der Domäne.

Port:
SecurityGateway stellt die Verbindung zu dem Server über diesen Port her; die Option entspricht der Spalte *Port* auf der Seite Mailserver der Domäne.

Erfordert SMTP-Echtheitsbestätigung
Falls Nachrichten über den Mailserver der Domäne nur nach Echtheitsbestätigung gesendet werden können, aktivieren Sie dieses Kontrollkästchen, und geben Sie Benutzernamen und Kennwort in die folgenden Felder ein.

Benutzername:
Falls der Mailserver der Domäne eine Echtheitsbestätigung erfordert, geben Sie den Benutzernamen hier ein.

Kennwort:
Geben Sie hier das Kennwort für den Mailserver der Domäne hier ein.

Typ

Dieser Server ist ein Standard-Mailserver
Falls Sie diesen Mailserver als einen der Standard-Mailserver der Domäne festlegen wollen, aktivieren Sie dieses Kontrollkästchen. Die Standard-Mailserver werden für alle SecurityGateway-Domänen verwendet, denen nicht bestimmte Mailserver zur Nutzung zugeordnet sind.

Geben Sie im Folgenden an, welche Domänen diesen Mailserver nutzen sollen...
Mithilfe der folgenden Optionen können Sie diesen Server einer SecurityGateway-Domäne oder mehreren SecurityGateway-Domänen zuordnen. Sind einer Domäne mehrere Server zugeordnet, so können Sie die Reihenfolge, in der die Zustellung über die Server versucht wird, auf der Registerkarte Mailserver 50 im Konfigurationsdialog für die Domäne festlegen

Verfügbare Domänen:
In diesem Abschnitt sind alle in SecurityGateway angelegten Domänen aufgeführt. Um die Domänen festzulegen, denen dieser Mailserver zugeordnet werden soll, wählen Sie die Domänen aus der Liste aus, und klicken Sie auf den Pfeil "--->".

Ausgewählte Domänen:
In diesem Abschnitt sind alle in SecurityGateway angelegten Domänen aufgeführt, denen dieser Mailserver zugeordnet ist. Um eine Domäne aus dieser Liste zu entfernen, wählen Sie die Domäne aus der Liste aus, und klicken Sie auf den Pfeil "<---".

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

3.2.2 Externe POP-Benutzerkonten

Mithilfe der Optionen für externe POP-Benutzerkonten können Sie SecurityGateway veranlassen, Nachrichten aus einem externen POP-Postfächern abzurufen. Dabei kommt das Übertragungsprotokoll POP3 zum Einsatz; die Nachrichten werden dann automatisch an die Benutzer der Domäne weitergeleitet, die dem POP-Postfach zugeordnet ist. Sie werden dazu nach dem Abruf anhand der Einstellungen ausgewertet, die Sie im Konfigurationsdialog POP-Benutzerkonto bearbeiten 83 festlegen können, und an alle gültigen Benutzer weitergeleitet, die dabei als Empfänger erkannt werden. Die Zustellung erfolgt dabei so, wie wenn die Nachrichten über herkömmliche SMTP-Verbindungen übermittelt worden wären.

Dabei ist es jedoch wichtig, eine Einschränkung zu berücksichtigen. Nachrichten, die in Postfächern abgelegt sind und von dort über das Protokoll POP3 abgerufen werden, enthalten die wichtigen Routingdaten (manchmal auch als "Umschlag" der Nachrichten bezeichnet) nicht mehr, die während der Übermittlung von Nachrichten mithilfe des Protokolls SMTP üblicherweise übertragen werden. Dieser Umstand erklärt sich dadurch, dass POP-Postfächer gemäß ihrer Zweckbestimmung einem einzelnen Empfänger, nicht aber einer ganzen Domäne oder mehreren Empfängern zugeordnet sein sollen. Es wird davon ausgegangen, dass alle Nachrichten im Postfach an denselben Empfänger gerichtet sind und daher die Routingdaten aus der Zustellung an das Postfach nicht mehr benötigt werden. Ohne diese Routingdaten muss SecurityGateway auf die Funktionen eines Parsers 85 zurückgreifen und mit ihrer Hilfe anhand der Inhalte der Kopfzeilen versuchen, den Empfänger zu bestimmen. Erkennt SecurityGateway in den Kopfzeilen gültige Empfänger in der Domäne, der das POP-Postfach zugeordnet ist, so werden die Nachrichten an diese Empfänger zugestellt. Nachrichten, aus denen sich ein gültiger Empfänger nicht entnehmen lässt, werden aus dem POP-Postach entfernt und von SecurityGateway gelöscht.

In der Übersicht über die externen POP-Benutzerkonten wird ein Eintrag pro Zeile angezeigt. Er enthält die fünf Spalten Aktiviert, Beschreibung, Host, Port und Domäne. Nähere Informationen über diese Spalten und über das Erstellen und Bearbeiten von POP-Benutzerkonten finden Sie in der Beschreibung des Konfigurationsdialogs POP-Benutzerkonto bearbeiten 83.

Die Symbolleiste am oberen Seitenrand enthält die folgenden fünf Optionen:

Neu
Um ein neues POP-Benutzerkonto anzulegen, klicken Sie auf *Neu*. Es öffnet sich der Dialog POP-Benutzerkonto hinzufügen, der dem Dialog POP-Benutzerkonto bearbeiten entspricht.

Bearbeiten
Um den gerade in der Liste ausgewählten Eintrag zu bearbeiten, klicken Sie in der Symbolleiste auf Bearbeiten. Es öffnet sich der Dialog POP-Benutzerkonto bearbeiten 83. Sie können diesen Dialog auch durch Doppelklick auf einen Eintrag aufrufen.

Löschen
Um ein POP-Benutzerkonto oder mehrere POP-Benutzerkonten zu löschen, wählen Sie die Einträge in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Einträge wirklich löschen wollen. Sie können mehrere Einträge auswählen, indem Sie

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

während des Anklickens der Einträge die Strg-Taste oder die Hochschalttaste gedrückt halten.

Jetzt abfragen
Durch Anklicken dieses Steuerelements veranlassen Sie, dass alle ausgewählten POP-Benutzerkonten sofort auf neue Nachrichten abgefragt werden.

Für Domäne:
Mithilfe des Auswahlfeldes *Für Domäne:* können Sie die Domäne auswählen, deren POP-Benutzerkonten in der Liste angezeigt werden sollen. Per Voreinstellung werden alle Benutzerkonten angezeigt. Sie können stattdessen eine Domäne auswählen, um nur die POP-Benutzerkonten für diese Domäne anzuzeigen.

3.2.2.1 POP-Benutzerkonto bearbeiten

Mithilfe des Dialogs POP-Benutzerkonto bearbeiten können Sie bestehende Externe POP-Benutzerkonten 82 bearbeiten und neue POP-Benutzerkonten erstellen. Sie erreichen diesen Dialog, indem Sie auf der Seite Externe POP-Benutzerkonten auf *Neu* klicken, oder indem Sie einen Eintrag auswählen und *Bearbeiten* anklicken. Der Dialog POP-Benutzerkonto bearbeiten ist in zwei Registerkarten unterteilt: *Host und Optionen* und *Parser*. Auf der Registerkarte Host und Optionen geben Sie den Host und die Anmeldedaten für das POP-Benutzerkonto an, Sie legen fest, ob eine zu dem POP-Host eine sichere Verbindung aufgebaut wird und welcher Verschlüsselungstyp zum Einsatz kommt, und Sie bestimmen, wie oft SecurityGateway das POP-Benutzerkonto auf neue Nachrichten abfragt. Auf der Registerkarte Parser bestimmen Sie die Kopfzeilen, die SecurityGateway nach Empfängeradressen und IP-Adressen der Absender durchsucht und auswertet.

Host und Optionen

Dieses Benutzerkonto ist gesperrt.
Durch Aktivieren dieses Kontrollkästchens können Sie das POP-Benutzerkonto deaktivieren. Das Benutzerkonto erscheint dann zwar noch in der Liste Externe POP-Benutzerkonten 82, SecurityGateway ruft aus ihm aber keine Nachrichten mehr ab. Um den Abruf der Nachrichten wieder aufzunehmen, deaktivieren Sie das Kontrollkästchen.

Nachrichten für folgende Domäne abrufen
Mithilfe dieses Auswahlmenüs ordnen Sie das POP-Benutzerkonto einer Domäne zu. Bei der Auswertung der Kopfzeilen der abgerufenen Nachrichten nach Empfängeradressen sucht SecurityGateway nach gültigen Empfängern der hier angegebenen Domäne.

Postfach

Beschreibung
In dieses Textfeld können Sie eine Beschreibung für das POP-Benutzerkonto eintragen. Die Beschreibung dient nur zu Ihrer Information und erscheint in der Liste der POP-Benutzerkonten.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Hostname oder IP
Geben Sie hier den Domänennamen oder die IP-Adresse für das POP-Benutzerkonto an (etwa `pop.example.com`).

Port
Geben Sie hier den Port an, auf dem SecurityGateway die Verbindung herstellt, um Nachrichten aus dem Benutzerkonto abzurufen. Per Voreinstellung verwendet SecurityGateway den POP-Port 110.

Benutzername
Geben Sie hier den Anmelde- oder Benutzernamen für das POP-Benutzerkonto ein.

Kennwort
Geben Sie hier das Kennwort für das POP-Benutzerkonto ein.

Sicherheit

Sichere Verbindung verwenden
SecurityGateway für E-Mail-Server unterstützt die neueste Verschlüsselungstechnologie, um Ihre Daten zu schützen und die Verbindung zu sichern. Wählen Sie nachfolgend die Option aus, die Sie für den Abruf der Nachrichten aus diesem POP-Konto einsetzen wollen.

Nie—Wählen Sie diese Option, falls der POP-Host verschlüsselte Verbindungen nicht unterstützt, oder falls Sie keine Verschlüsselung verwenden wollen.

TLS, falls verfügbar—Diese Option bewirkt, dass die Verschlüsselungsmethode Transport Layer Security (TLS) für den Abruf der Nachrichten aus diesem POP-Benutzerkonto immer eingesetzt wird, soweit dies möglich ist. Unterstützt der POP-Host die Methode TLS nicht, so ruft SecurityGateway die Nachrichten über eine unverschlüsselte Verbindung ab. Diese Option ist per Voreinstellung aktiv.

TLS—Diese Option bewirkt, dass die Verschlüsselungsmethode TLS für den Abruf von Nachrichten aus diesem POP-Benutzerkonto zwingend verlangt wird.

SSL—Diese Option bewirkt, dass die Verschlüsselungsmethode SSL für den Abruf von Nachrichten aus diesem POP-Benutzerkonto zwingend verlangt wird.

Sichere Echtheitsbestätigung (APOP) erzwingen
Diese Option bewirkt, dass für die Echtheitsbestätigung im Rahmen des Abrufs von Nachrichten aus diesem Benutzerkonto der Befehl APOP und das Echtheitsbestätigungsverfahren CRAM-MD5 verwendet werden. Sie können damit die Echtheitsbestätigung durchführen lassen, ohne dass das Kennwort im Klartext übermittelt wird.

Abruf von Nachrichten

Nachrichten auf dem Server belassen
Diese Option bewirkt, dass SecurityGateway die Nachrichten aus dem Postfach abruft, danach aber nicht von dem externen POP-Host löscht.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

...bis sie das folgende Alter in Tagen erreicht haben
Hier können Sie angeben, nach welcher Haltezeit in Tagen SecurityGateway die Nachrichten aus dem POP-Benutzerkonto löschen soll.

Manche Hosts begrenzen selbst die Speicherdauer für Nachrichten in ihren Postfächern.

Anruf-Intervall: [xx] Minuten
Diese Option bestimmt, wie oft SecurityGateway neue Nachrichten von dem POP-Host abrufen soll. Es empfiehlt sich, etwa alle fünf Minuten einen Abruf ausführen zu lassen.

Zeitüberschreitung: [xx] Sekunden
Hier wird die Zeit in Sekunden angegeben, für die SecurityGateway auf eine Antwort des POP-Hosts warten soll, bevor die Verbindung wegen Zeitüberschreitung getrennt wird. Ein Wert von 60 Sekunden empfiehlt sich für die meisten Anwendungsfälle.

Parser

Empfänger (RCPT)

Folgende Kopfzeilen nach Empfängern (RCPT) durchsuchen
Mithilfe dieser Option bestimmen Sie, welche Kopfzeilen SecurityGateway nach den E-Mail-Adressen der Empfänger durchsucht und auswertet. Alle hier aufgeführten Kopfzeilen werden nach Adressen durchsucht.

"Received"-Kopfzeilen nach Empfängern (RCPT) durchsuchen
Empfänger-Daten aus den SMTP-Umschlägen sind manchmal auch in den "Received"-Kopfzeilen zu finden; daher kann es sinnvoll sein, auch diese Kopfzeilen daraufhin auszuwerten, ob sie gültige Empfänger-Adressen enthalten. Diese Option bewirkt, dass gültige E-Mail-Adressen auch aus den "Received"-Kopfzeilen der abgerufenen Nachrichten entnommen werden können.

Überspringen der ersten [xx] "Received"-Kopfzeilen
Für bestimmte Server-Konfigurationen kann es sinnvoll sein, die "Received"-Kopfzeilen zwar auszuwerten, eine gewisse Anzahl dieser Kopfzeilen aber zu überspringen. Mithilfe dieser Option legen Sie die Zahl der "Received"-Kopfzeilen fest, die SecurityGateway in der Auswertung überspringen und nicht auswerten soll.

IP-Adresse

"Received"-Kopfzeilen nach IP-Adresse des Absenders durchsuchen
Diese Option bewirkt, dass alle "Received"-Kopfzeilen der abgerufenen Nachrichten daraufhin ausgewertet werden, ob sie die IP-Adresse des Absenders enthalten. Die IP-Adresse des Absenders kann für verschiedene Sicherheitsprüfungen und für die Abwehr von Spam sehr hilfreich sein.

Überspringen der ersten [xx] "Received"-Kopfzeilen
Für bestimmte Server-Konfigurationen kann es sinnvoll sein, die "Received"-Kopfzeilen zwar auszuwerten, eine gewisse Anzahl dieser Kopfzeilen aber zu

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

überspringen. Mithilfe dieser Option legen Sie die Zahl der "Received"-Kopfzeilen fest, die SecurityGateway in der Auswertung überspringen und nicht auswerten soll.

Folgende Kopfzeile nach IP-Adresse des Absenders durchsuchen:
Mithilfe dieser Option können Sie eine bestimmte Kopfzeile festlegen, die SecurityGateway nach der IP-Adresse des Absenders auswerten soll. Per Voreinstellung ist dies die Kopfzeile `X-ORIGINATING-IP`.

3.2.3 Quarantäne-Konfiguration

Auf der Seite können Sie Einstellungen treffen, die von den Optionen "*...Nachricht in Quarantäne geben*" abweichen, die für zahlreiche Sicherheits-Funktionen[154] zur Verfügung stehen. Die Einstellungen können systemweit oder für bestimmte Domänen getroffen werden. Sie können außerdem wählen, ob Ihre Benutzer für ihre Benutzerkonten eigene, von den Standard-Einstellungen für die Quarantäne der jeweiligen Domänen abweichende Einstellungen festlegen dürfen, und ob sie den Inhalt ihrer Quarantäne-Ordner einsehen und verwalten dürfen. Schließlich können Sie auch bestimmen, wie oft die Benutzer eine Übersicht über die Inhalte ihrer Quarantäne-Ordner erhalten sollen: nie, täglich oder wöchentlich.

Nachrichten

Nachrichten in Quarantäne auf dem Server halten
Diese Option veranlasst SecurityGateway, eingehende Nachrichten in Quarantäne[42] zu geben, wenn sie eines der Kriterien aus einer Sicherheits-Funktion[154] erfüllen. Diese Option ist per Voreinstellung aktiv.

Benutzern eine Übersicht über den Inhalt ihrer Quarantäne-Ordner per E-Mail senden:
Falls SecurityGateway verdächtige Nachrichten in Quarantäne gibt, können die Benutzer regelmäßig per E-Mail eine Übersicht über den jeweils aktuellen Inhalt ihrer Quarantäne-Ordners erhalten. Diese Option bestimmt, wie oft die Übersicht versandt wird.

Nie
Diese Option bewirkt, dass die Benutzer keine Übersicht über die Nachrichten erhalten, die sich in ihren Quarantäne-Ordnern befinden.

Alle [xx] Stunde(n)
Diese Option bewirkt, dass die Benutzer die Übersicht in dem hier in Stunden angegebenen Intervall erhalten.

Täglich
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass SecurityGateway jedem Benutzerkonto täglich eine Übersicht über die für den betreffenden Benutzer in Quarantäne gehaltenen Nachrichten sendet.

Wöchentlich
Diese Option bewirkt, dass die Benutzer die Übersicht einmal pro Woche erhalten.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nach dem unten angegebenen Zeitplan
Klicken Sie auf **Hinzufügen**, um den Zeitplan für Quarantäne-Berichte aufzurufen. Sie können dort einen benutzerdefinierten Zeitplan erstellen, nach dem die Berichte über die Inhalte der Quarantäne-Ordner versandt werden sollen.

Zeitplan

Tag(e)
Beim Erstellen eines neuen Eintrags für den Zeitplan wählen Sie zunächst den Tag oder die Tage aus, an dem oder an denen Sie die E-Mail-Nachrichten versenden wollen. Es stehe folgende Möglichkeiten zur Verfügung: Täglich, Wochentage (Montag bis Freitag einschließlich), Wochenenden (Samstag und Sonntag), sowie bestimmte Tage. Falls Sie mehrere einzeln bestimmte Tage angeben wollen, müssen Sie für jeden dieser Tage einen eigenen Eintrag im Zeitplan erstellen.

Beginn um...
Geben Sie hier die Uhrzeit an, zu der der Quarantäne-Bericht versandt oder der Versand im Intervall begonnen werden soll. Sie müssen die Uhrzeit im 24-Stunden-Format (00:00 bis 23:59 Uhr) angeben. Falls Sie den Bericht während des Tages in gleichmäßigen Intervallen versenden lassen wollen, müssen Sie außerdem die Optionen *Ende um...* sowie *Im Intervall von...* weiter unten konfigurieren. Falls Sie pro Tag nur einen Bericht versenden lassen wollen, lassen Sie die Optionen *Ende um...* sowie *Im Intervall von...* leer.

Ende um...
Geben Sie hier die Uhrzeit an, zu der der Versand der Quarantäne-Berichte im angegebenen Intervall beendet werden soll. Sie müssen die Uhrzeit im 24-Stunden-Format (00:01 bis 23:59 Uhr) angeben. Die hier angegebene Uhrzeit muss nach der Uhrzeit liegen, die Sie im Feld *Beginn um...* angegeben haben. Ein Beispiel hierzu: Falls die Uhrzeit im Feld *Beginn um...* "10:00" lautet, dann reichen die zulässigen Uhrzeiten für das Feld *Ende um...* von "10:01" bis "23:59". Falls Sie nur einen Quarantäne-Bericht pro Tag versenden lassen wollen, dann lassen Sie dieses Feld leer.

Im Intervall von [xx] Minuten
Geben Sie hier das Intervall an, in dem die E-Mail-Nachrichten mit den Quarantäne-Berichten im Zeitraum versandt werden sollen, der durch die Felder *Beginn um...* und *Ende um...* bestimmt ist. Falls Sie nur einen Quarantäne-Bericht pro Tag versenden lassen wollen, dann lassen Sie dieses Feld leer.

Nur Nachrichten aufnehmen, die seit Versand der letzten E-Mail-Nachricht in Quarantäne gegeben wurden
Per Voreinstellung enthält jeder Quarantäne-Bericht eine Liste aller Nachrichten im Quarantäne-Ordner. Diese Option bewirkt, dass nur die Nachrichten im Quarantäne-Bericht aufgeführt werden, die seit dem Versand des letzten Quarantäne-Berichts neu in den Quarantäne-Ordner eingestellt wurden. Falls keine Nachrichten vorhanden sind, die in den Bericht aufgenommen werden müssten, wird kein Quarantäne-Bericht erstellt.

Nachdem Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf **Speichern und Beenden**, um den Eintrag zu erstellen und der Seite Quarantäne-Konfiguration hinzuzufügen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Quarantäne-E-Mail sortieren nach: [Empfangen | Von | Betreff | Bewertung]
Mithilfe dieser Option bestimmen Sie die Sortierreihenfolge für die E-Mail-Nachrichten für den Quarantäne-Bericht. Per Voreinstellung werden die Berichte nach Empfangsdatum sortiert; sie können wahlweise stattdessen nach Absender, Betreff oder Spam-Bewertung sortiert werden.

Option "Schwarze Liste" in Quarantäne-Übersicht und -E-Mail aufnehmen
Diese Option fügt eine Verknüpfung in die für die Benutzer erstellte Liste der Nachrichten in Quarantäne und in die per E-Mail an die Benutzer versandten Quarantäne-Berichte ein, mit deren Hilfe sie die E-Mail-Adresse des Absenders in die Schwarze Liste aufnehmen können.

Option "Domäne der Schwarzen Liste hinzufügen" in Quarantäne-Übersicht und -E-Mail aufnehmen
Diese Option fügt eine Verknüpfung in die für die Benutzer erstellte Liste der Nachrichten in Quarantäne und in die per E-Mail an die Benutzer versandten Quarantäne-Berichte ein, mit deren Hilfe sie die Domäne des Absenders in die Schwarze Liste aufnehmen können.

Option "Nachricht anzeigen" in Quarantäne-E-Mail aufnehmen
Diese Option fügt eine Verknüpfung in die für die Benutzer erstellte per E-Mail an die Benutzer versandten Quarantäne-Berichte ein, mit deren Hilfe sie sich die Inhalt der in Quarantäne befindlichen Nachrichten anzeigen lassen können. Diese Option ist auch verfügbar auf der Seite Hauptmenü » Mein Benutzerkonto » Einstellungen 34.

Mailserver oder -client das Filtern von Nachrichten in Quarantäne ermöglichen
Ist diese Option aktiv, so geht sie allen Optionen "... Nachricht in Quarantäne geben" in den verschiedenen Sicherheits-Funktionen 154 vor. SecurityGateway stellt den Empfängern dann auch die Nachrichten normal zu, die andernfalls in Quarantäne gegeben worden wären. Diese Funktion ist hilfreich, falls die Empfänger die Nachrichten durch ihren E-Mail-Server oder -Client filtern oder in Quarantäne geben lassen möchten. Mithilfe des Auswahlmenüs "*Für Domäne:*" am oberen Seitenrand können Sie diese Option systemweit oder nur für bestimmte Domänen ändern.

...Betreff kennzeichnen mit [*Text*]
Diese Option bewirkt, dass SecurityGateway der Betreffzeile aller Nachrichten, die bei aktivierter Quarantäne-Option eigentlich in Quarantäne gegeben worden wären, den hier angegebenen Text hinzufügt. Der Client oder der Server des Empfängers können diese Kennzeichnung verwenden, um Nachrichten zu filtern.

...Kopfzeile hinzufügen [*Text*]
Diese Option bewirkt, dass SecurityGateway in alle Nachrichten, die bei aktivierter Quarantäne-Option eigentlich in Quarantäne gegeben worden wären, die hier angegebene Kopfzeile einfügt. Der Client oder der Server des Empfängers können diese Kopfzeile verwenden, um Nachrichten zu filtern. Per Voreinstellung heißt diese Kopfzeile "`X-Spam-Flag: YES`".

Benutzer

Die beiden folgenden Benutzer-Optionen entsprechen den gleichnamigen Optionen auf der Seite Benutzer-Optionen 73. Änderungen an diesen Optionen, die Sie auf

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

einer Seite durchführen, werden auf der jeweils anderen Seite gespiegelt. Die Optionen sind lediglich aus Gründen der einfacheren Nutzung doppelt vorhanden.

Benutzern gestatten, ihre eigenen Quarantäne-Ordner einzusehen und zu verwalten
Ist diese Option aktiv, so können die Benutzer eingehende Nachrichten einsehen und verwalten, die für sie in Quarantäne gegeben wurden. Die Benutzer erhalten dann Zugriff auf die Seite Meine Quarantäne anzeigen 42, von der aus sie Nachrichten freigeben und löschen und weitere Aufgaben erledigen können.

Benutzern das Bearbeiten ihrer eigenen Quarantäne-Einstellungen gestatten
Um den Benutzern zu gestatten, ihre Quarantäne-Einstellungen über die Seite Meine Einstellungen 34 zu bearbeiten, aktivieren Sie dieses Kontrollkästchen.

Administrative Quarantäne (Alle Domänen)

Mithilfe dieser Optionen können Sie festlegen, ob und wann die Administratoren Berichte über die Inhalte der administrativen Quarantäne per E-Mail erhalten. Die Optionen entsprechen inhaltlich den weiter oben beschriebenen Optionen zu den Quarantäne-Berichten für die Benutzer.

Use these options to specify when or if administrators will be sent an email that lists the contents of the administrative quarantine. These options are identical to the user quarantine report options outlined above.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Quarantäne-Optionen dieser Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

3.2.3.1 Zeitplan für Quarantäne-Berichte

Klicken Sie auf der Seite Quarantäne-Konfiguration 86 im Abschnitt "*Nach dem unten angegebenen Zeitplan*" auf die Schaltfläche **Hinzufügen**, um den Zeitplan für Quarantäne-Berichte aufzurufen. Sie können hier einen benutzerdefinierten Zeitplan erstellen, nach dem die Berichte über die Inhalte der Quarantäne-Ordner versandt werden sollen.

Zeitplan

Tag(e)
Beim Erstellen eines neuen Eintrags für den Zeitplan wählen Sie zunächst den Tag oder die Tage aus, an dem oder an denen Sie die E-Mail-Nachrichten versenden wollen. Es stehe folgende Möglichkeiten zur Verfügung: Täglich, Wochentage (Montag bis Freitag einschließlich), Wochenenden (Samstag und Sonntag), sowie bestimmte Tage. Falls Sie mehrere einzeln bestimmte Tage angeben wollen, müssen Sie für jeden dieser Tage einen eigenen Eintrag im Zeitplan erstellen.

Beginn um...
Geben Sie hier die Uhrzeit an, zu der der Quarantäne-Bericht versandt oder der Versand im Intervall begonnen werden soll. Sie müssen die Uhrzeit im 24-Stunden-Format (00:00 bis 23:59 Uhr) angeben. Falls Sie den Bericht während des Tages in gleichmäßigen Intervallen versenden lassen wollen, müssen Sie außerdem die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Optionen *Ende um...* sowie *Im Intervall von...* weiter unten konfigurieren. Falls Sie pro Tag nur einen Bericht versenden lassen wollen, lassen Sie die Optionen *Ende um...* sowie *Im Intervall von...* leer.

Ende um...
Geben Sie hier die Uhrzeit an, zu der der Versand der Quarantäne-Berichte im angegebenen Intervall beendet werden soll. Sie müssen die Uhrzeit im 24-Stunden-Format (00:01 bis 23:59 Uhr) angeben. Die hier angegebene Uhrzeit muss nach der Uhrzeit liegen, die Sie im Feld *Beginn um...* angegeben haben. Ein Beispiel hierzu: Falls die Uhrzeit im Feld *Beginn um...* "10:00" lautet, dann reichen die zulässigen Uhrzeiten für das Feld *Ende um...* von "10:01" bis "23:59". Falls Sie nur einen Quarantäne-Bericht pro Tag versenden lassen wollen, dann lassen Sie dieses Feld leer.

Im Intervall von [xx] Minuten
Geben Sie hier das Intervall an, in dem die E-Mail-Nachrichten mit den Quarantäne-Berichten im Zeitraum versandt werden sollen, der durch die Felder *Beginn um...* und *Ende um...* bestimmt ist. Falls Sie nur einen Quarantäne-Bericht pro Tag versenden lassen wollen, dann lassen Sie dieses Feld leer.

Nur Nachrichten aufnehmen, die seit Versand der letzten E-Mail-Nachricht in Quarantäne gegeben wurden
Per Voreinstellung enthält jeder Quarantäne-Bericht eine Liste aller Nachrichten im Quarantäne-Ordner. Diese Option bewirkt, dass nur die Nachrichten im Quarantäne-Bericht aufgeführt werden, die seit dem Versand des letzten Quarantäne-Berichts neu in den Quarantäne-Ordner eingestellt wurden. Falls keine Nachrichten vorhanden sind, die in den Bericht aufgenommen werden müssten, wird kein Quarantäne-Bericht erstellt.

Nachdem Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf **Speichern und Beenden**, um den Eintrag zu erstellen und der Seite Quarantäne-Konfiguration hinzuzufügen.

3.2.4 Postausgang

Die Optionen auf der Seite Postausgang bestimmen, ob SecurityGateway abgehende Nachrichten selbst zustellt oder durch einen anderen Mailserver zustellen lässt. Auf dieser Seite wird auch festgelegt, wie lange SecurityGateway versuchen soll, eingehende und abgehende Nachrichten nach vorübergehenden Zustellfehlern erneut zuzustellen 91, bevor die Nachrichten als unzustellbar 92 an den Absender zurückgeleitet werden. Diese Optionen wirken systemweit auf alle Domänen, die SecurityGateway verwaltet.

Zustellung externer Nachrichten

Abgehende Nachrichten immer direkt an Mailserver des Empfängers senden
Ist diese Option aktiv, so versucht SecurityGateway, jede abgehende Nachricht direkt an den Mailserver des Empfängers zuzustellen und nutzt dabei den normalen SMTP-Zustellvorgang. Dabei werden u.a. normale DNS-Abfragen durchgeführt und MX-Einträge geprüft. Diese Option ist per Voreinstellung aktiv.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Abgehende Nachrichten immer an nachfolgend angegebenen Server senden
Um alle abgehenden Nachrichten an einen anderen Server zu übermitteln und die Zustellung der Nachrichten diesem Server zu überlassen, wählen Sie diese Option.

Mailserver:
Geben Sie hier den Mailserver an, an den SecurityGateway alle abgehenden Nachrichten übermitteln soll. Dieser Server muss die Zustellung der Nachrichten übernehmen. Sie können einen Hostnamen oder eine IP-Adresse eintragen, wie etwa `mail.example.com` oder `192.168.0.1`.

Port
SecurityGateway benutzt zur Übermittlung der Nachrichten an den oben angegebenen Server den hier eingetragenen Port.

Zugriff auf den oben angegebenen Mailserver erfordert Echtheitsbestätigung
Falls der oben angegebene Mailserver den Zugriff nur nach Echtheitsbestätigung gestattet, aktivieren Sie dieses Kontrollkästchen, und tragen Sie die Anmeldedaten in die folgenden Felder ein.

Benutzername:
Falls eine Echtheitsbestätigung erforderlich ist, tragen Sie hier den Benutzernamen oder Anmeldenamen ein.

Kennwort:
Tragen Sie hier das Kennwort ein, das zu dem oben angegebenen Benutzernamen gehört.

Wiederholungs-Warteschlange

Die Optionen zur Wiederholungs-Warteschlange bestimmen, wie SecurityGateway solche Nachrichten behandelt, die wegen eines vorübergehenden Fehlers nicht zugestellt werden können - etwa, weil der Mailserver des Empfängers vorübergehend nicht erreichbar ist.

Während der ersten Stunde Zustellung versuchen alle [xx] Minuten (empfohlen: 5)
Nachdem eine Nachricht erstmals nicht zugestellt werden konnte, unternimmt SecurityGateway eine Stunde lang weitere Zustellversuche in dem hier angegebenen Intervall. Die Voreinstellung beträgt 5 Minuten.

Absender informieren, falls die Nachricht während dieses Zeitraums nicht zugestellt wurde
Kann eine Nachricht eine Stunde lang nicht zugestellt werden, so benachrichtigt SecurityGateway per Voreinstellung den Absender per E-Mail darüber, dass die Zustellung eine Stunde lang erfolglos versucht wurde, und dass die Zustellversuche fortgesetzt werden. Falls Sie diese Benachrichtigungen nicht wünschen, deaktivieren Sie diese Option.

... Ursprungsnachricht in die Information an den Absender einbinden
Wenn SecurityGateway nach Ablauf der ersten Stunde über die bislang fehlgeschlagene Zustellung benachrichtigt, so ist per Voreinstellung in dieser Benachrichtigung eine Kopie der Ursprungsnachricht enthalten. Falls Sie nicht wünschen, dass die Benachrichtigung auch die Ursprungsnachricht enthält, deaktivieren Sie diese Option.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Zustellung danach versuchen alle [xx] Minuten (empfohlen: 240)
Konnte eine Nachricht eine Stunde lang nicht zugestellt werden, so ändert SecurityGateway das Intervall für weitere Zustellversuche in den hier angegebenen Wert. Die Voreinstellung beträgt 240 Minuten. SecurityGateway versucht die Zustellung in diesem Intervall weiter, bis die im Abschnitt Unzustellbare Nachrichten unten angegebene Höchstdauer abgelaufen ist.

SMTP-Verbindungsfehler cachen
Schlägt die SMTP-Verbindung mit dem Host einer Gegenstelle fehl, so versucht SecurityGateway für einen bestimmten Zeitraum keine weiteren Verbindungen zu diesem Host. Dieser Zeitraum ist eine Minute kürzer als der in der Option *Während der ersten Stunde Zustellung versuchen alle [xx] Minuten* weiter oben angegebene Zeitraum. Hierdurch kann verhindert werden, dass SecurityGateway unnötig immer wieder versucht, Verbindungen zu einem gerade nicht erreichbaren Host herzustellen. Ein solcher Fall kann etwa eintreten, wenn für denselben Host mehrere Nachrichten vorliegen und sich beim Versuch, die erste Nachricht zuzustellen, zeigt, dass der Host nicht erreichbar ist. Falls Sie die fehlgeschlagenen SMTP-Verbindungsversuche nicht im Cache speichern wollen, deaktivieren Sie diese Option.

Unzustellbare Nachrichten

Kann eine eingehende oder abgehende Nachricht wegen eines vorübergehenden Fehlers nicht zugestellt werden (etwa, weil der Mailserver des Empfängers vorübergehend nicht erreichbar ist), so bestimmen die folgenden Optionen, wie lange SecurityGateway versuchen soll, die Nachricht zuzustellen. Nach Ablauf der angegebenen Fristen versucht SecurityGateway keine weitere Zustellung und leitet die Nachricht an den Absender zurück.

Falls eine Nachricht nach [xx] Tagen immer noch unzustellbar ist, dann weitere Zustellversuche einstellen (empfohlen: 5)
Hier wird die Höchstdauer in Tagen festgelegt, während der SecurityGateway weiterhin versucht, die Nachricht zuzustellen. Nach Ablauf dieser Frist unternimmt SecurityGateway keine Zustellversuche mehr.

Absender informieren, dass die Nachricht nicht zugestellt werden konnte
Bricht SecurityGateway die Zustellversuche ab, so benachrichtigt SecurityGateway per Voreinstellung den Absender per E-Mail darüber, dass die Zustellung endgültig fehlgeschlagen ist. Falls Sie diese Benachrichtigungen nicht wünschen, deaktivieren Sie diese Option.

... Ursprungsnachricht in die Information an den Absender einbinden
Wenn SecurityGateway den Absender darüber benachrichtigt, dass die Zustellung endgültig fehlgeschlagen ist, so ist per Voreinstellung in dieser Benachrichtigung eine Kopie der Ursprungsnachricht enthalten. Falls Sie nicht wünschen, dass die Benachrichtigung auch die Ursprungsnachricht enthält, deaktivieren Sie diese Option.

3.2.5 E-Mail-Protokoll


Die Seite E-Mail-Protokoll enthält verschiedene Optionen, die die technische Verarbeitung von E-Mail durch SecurityGateway beeinflussen. Sie können auf dieser Seite die Ports festlegen, die zum Empfang von Nachrichten dienen, die Höchstzahl

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

gleichzeitiger SMTP-Verbindungen begrenzen und unter anderem bestimmen, ob SecurityGateway VRFY-Anfragen beantwortet und ob Kennwörter im Klartext zugelassen sind. Daneben enthält die Seite zahlreiche weiter gehende Optionen.

Server

HELO-Domänenname:
Hier wird der Domänenname eingetragen, mit dem sich SecurityGateway während des SMTP-Protokolldialogs identifiziert (z.B. mail.example.com, smtp.domain.com u.ä.). Der Eintrag wird auch für die Received-Kopfzeilen und die Kopfzeilen über die Ergebnisse der Echtheitsbestätigung ("Authentication Results") sowie an den Stellen genutzt, an denen es erforderlich ist, genau zu bestimmen, welcher Server eine Nachricht verarbeitet hat. **Beachte:** Falls Sie SecurityGateway im Cluster-Betrieb 137 einsetzen, können Sie diese Option für jeden einzelnen Server im Cluster auf einen eigenen Wert setzen.

SMTP-Ports (kommagetrennt):
Hier werden die Ports eingetragen, auf denen SecurityGateway Nachrichten über SMTP empfängt. Falls Sie mehrere Ports eintragen wollen, müssen Sie die Ports durch Kommata trennen. Der Standard-SMTP-Port ist 25.

Besondere SSL-Ports (kommagetrennt):
Tragen Sie hier die besonderen SSL-Ports ein, auf denen Sie Nachrichten empfangen wollen. Falls Sie mehrere Ports eintragen wollen, müssen Sie die Ports durch Kommata trennen. Der Standard-SSL-Port ist 465.

MSA-Ports (kommagetrennt):
Tragen Sie in dieses Feld Ihre MSA-Ports ein, und trennen Sie mehrere Einträge durch Kommata. Der Standard-MSA-Port ist 465.

Sockets an diese IPs binden (kommagetrennt):
Falls Sie SecurityGateway an bestimmte IP-Adressen binden wollen, tragen Sie diese IPs hier ein, und trennen Sie mehrere Einträge durch Kommata.

Höchstzahl gleichzeitig eingehender SMTP-Verbindungen:
Dieser Eintrag bestimmt, wie viele gleichzeitig eingehende SMTP-Verbindungen SecurityGateway annimmt, bevor weitere Verbindungen mit der Meldung "Server überlastet" abgewiesen werden. Die Voreinstellung beträgt 100.

Höchstzahl gleichzeitig abgehender SMTP-Verbindungen:
Dieser Eintrag bestimmt, wie viele abgehende SMTP-Verbindungen gleichzeitig aufgebaut werden, wenn Nachrichten versandt werden. In jeder Verbindung werden so lange Nachrichten übermittelt, bis alle auf die Zustellung wartenden Nachrichten versandt sind. Ist in diesem Feld beispielsweise der Wert 30 eingetragen, dann können bis zu 30 Verbindungen gleichzeitig aufgebaut werden, und SecurityGateway kann versuchen, 30 verschiedene Nachrichten gleichzeitig zuzustellen.

Höchstzahl gleichzeitiger POP-Verbindungen zum Nachrichtenabruf:
Dieser Eintrag bestimmt, wie viele Verbindungen zum Abruf von Nachrichten über POP der Server gleichzeitig zulässt, bevor er weitere Verbindungsversuche mit dem Hinweis darauf abweist, dass der Server überlastet ist.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Standard-Domäne:
Wählen Sie aus dem folgenden Auswahlmenü eine Domäne aus. SecurityGateway setzt diese Domäne ein, wenn ein Benutzer sich anmeldet, ohne einen Domänennamen anzugeben. SecurityGateway setzt diese Domäne auch für die Befehle MAIL, RCPT und VRFY ein, falls für diese Befehle keine Domäne angegeben wird. SecurityGateway nutzt diese Domäne schließlich für den Versand von Warnmeldungen und Mitteilungen an externe Administratoren[60].

SMTP-Protokolleinstellungen

Befehl VRFY befolgen
Falls Sie VRFY[217]-Befehle befolgen wollen, aktivieren Sie diese Option. Die Option ist per Voreinstellung abgeschaltet.

Unverschlüsselte Kennwörter zulassen (SSL oder CRAM-MD5 nicht erforderlich)
Per Voreinstellung akzeptiert SecurityGateway auch Kennwörter im Klartext, die während der SMTP-Echtheitsbestätigung übermittelt werden. Falls Sie diese Option aktivieren, ist eine Echtheitsbestätigung nur noch bei Nutzung von SSL oder CRAM-MD5 möglich.

Echtheitsbestätigung über CRAM-MD5 unterstützen
Ist diese Option aktiv, so unterstützt SecurityGateway die Echtheitsbestätigung über CRAM-MD5. Die Option ist per Voreinstellung abgeschaltet.

Software-Versionsinformationen nicht in Antworten und Kopfzeilen "Received:" aufnehmen
Diese Option verhindert, dass in den Antworten des Servers und in den Kopfzeilen "Received:" Informationen zur Software-Version von SecurityGateway erscheinen. Diese Option ist per Voreinstellung abgeschaltet.

Befehle und Kopfzeilen auf RFC-Verstöße prüfen
Falls Sie Nachrichten abweisen wollen, die nicht den RFC-Internet-Standards entsprechen, aktivieren Sie diese Option. SecurityGateway weist bei aktivierter Option Nachrichten ab, deren Parameter Kontroll- oder 8-Bit-Zeichen enthalten, sowie Nachrichten, denen Datum, Absender oder die Kopfzeile From fehlen. Diese erforderlichen Kopfzeilen müssen auch Inhalte enthalten; sie dürfen nicht leer sein, sonst werden die Nachrichten ebenfalls als nicht standardkonform abgewiesen. Falls Sie nicht standardkonforme Nachrichten zulassen wollen, deaktivieren Sie diese Option.

Höchstzahl der RCPT-Befehle pro Nachricht: [xx] (RFC empfiehlt 100)
Hier wird festgelegt, wie viele RCPT-Befehle (und damit, wie viele Empfänger) je Nachricht zugelassen sind. Die Voreinstellung beträgt 100.

Größenbegrenzung für durch SMTP übermittelte Nachrichten: [xx] KB (0 = keine Begrenzung)
Wird hier ein Wert eingetragen, so nimmt SecurityGateway Nachrichten nicht an, deren Größe diesen Wert überschreitet. Ist diese Option aktiv, so versucht SecurityGateway, den ESMTP-Befehl SIZE zu nutzen, der in RFC-1870 definiert ist. Unterstützt die übermittelnde Gegenstelle diese SMTP-Erweiterung, so kann SecurityGateway die Größe der Nachricht feststellen, bevor die Zustellung beginnt. SecurityGateway kann die Nachricht dann gegebenenfalls sofort abweisen. Unterstützt die übermittelnde Gegenstelle diese SMTP-Erweiterung nicht, so muss SecurityGateway zulassen, dass die übermittelnde Gegenstelle mit der Übertragung der Nachricht beginnt. Die Nachricht kann dann erst abgewiesen

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

werden, wenn die Größenbegrenzung während der Übertragung erreicht wird. Die Voreinstellung "0" bewirkt, dass Nachrichten keiner Größenbegrenzung unterliegen.

Verbindung trennen, falls Übertragungsvolumen folgenden Wert überschreitet: [xx] KB (0 = nie)
Falls das Datenvolumen während einer SMTP-Verbindung den hier angegebenen Schwellwert überschreitet, trennt SecurityGateway die Verbindung. Die Voreinstellung für diese Option beträgt "0"; dies bewirkt, dass das Datenvolumen nicht begrenzt ist.

Zeitüberschreitung für Verbindungen: [xx] Sekunden (Empfohlen: 30)
Diese Option bestimmt, wie lange SecurityGateway auf eine SMTP-Verbindung wartet, bevor der Verbindungsversuch abgebrochen wird.

Zeitüberschreitung für Protokolldialoge: [xx] Sekunden (Empfohlen: 300)
Diese Option bestimmt, wie lange SecurityGateway auf den Beginn des SMTP-Protokolldialogs durch den Host der Gegenstelle wartet, nachdem die SMTP-Verbindung hergestellt ist.

Schleifenerkennung und -Kontrolle

Höchstzahl der Zwischenstationen (1-100):
Nach den RFC-Standards muss jeder Mailserver jede Nachricht immer dann kennzeichnen, wenn er sie verarbeitet. Die entsprechenden Stempel können gezählt werden und lassen sich als Hilfslösung verwenden, um Endlosschleifen in der Nachrichtenzustellung zu ermitteln und zu unterbinden. Solche Endlosschleifen können aufgrund fehlerhafter Konfigurationen entstehen. Falls sie nicht entdeckt werden, belegen sie unnötig Ressourcen. Die Endlosschleifen können dadurch ermittelt werden, dass geprüft wird, wie oft eine Nachricht bereits verarbeitet wurde. Nach Erreichen des Schwellwerts kann die Nachricht in die Defekt 312-Warteschlange verschoben werden, wodurch die Endlosschleife unterbrochen wird. Die Voreinstellung beträgt 20.

3.3 Archivierung

3.3.1 Konfiguration

Die Archivierung von E-Mail-Nachrichten erfasst und speichert alle Nachrichten, die durch SecurityGateway hindurch geleitet werden. Administratoren und Benutzer können die archivierten Nachrichten einfach durchsuchen 109.

Konfiguration

E-Mail-Archivierung aktivieren
Diese Option bewirkt, dass Kopien jeder eingehenden und abgehenden Nachricht, die von Ihren Domänen stammen oder an sie gerichtet sind, gespeichert werden. Die Nachrichten werden dabei in Archiv-Speichern abgelegt. Die Archiv-Speicher 105 sind durchsuchbar 109. Jeder Archiv-Speicher ist einer einzigen Domäne zugeordnet. Sie können diese Einstellungen mithilfe der Dropdown-Liste "Für Domäne" in der rechten oberen Bildschirmecke für einzelne Domänen abweichend konfigurieren.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

"Journal-Berichte" und weitergeleitete Nachrichten akzeptieren, die an folgendes Postfach gesandt werden:
Mithilfe dieser Option können Sie ein Postfach oder mehrere Postfächer so konfigurieren, dass diese Journal-Berichte und andere weitergeleitete Nachrichten von Microsoft Office 365 zur Archivierung annehmen. SecurityGateway nimmt die Nachrichten für alle Domänen an, für die die Archivierung von Nachrichten aktiv ist. SecurityGateway wertet anschließend die Kopfzeilen aus, um den eigentlich gewünschten Empfänger zu bestimmen. Hiernach prüft SecurityGateway, ob der Absender oder Empfänger ein gültiger lokaler Benutzer ist; falls nötig, fragt SecurityGateway hierzu die entsprechenden Datenquellen für Benutzerprüfung ab. SecurityGateway prüft schließlich, ob für die betroffene Domäne die Archivierung von Nachrichten aktiv ist. Sind alle diese Voraussetzungen erfüllt, so fügt SecurityGateway die Nachricht dem Archiv-Speicher der Domäne hinzu. **Beachte:** Die eingehenden Nachrichten müssen hierbei von einem Mailserver der Domäne 79 empfangen worden sein.

E-Mail-Journal aktivieren
Mithilfe dieser Option können Sie ein Journale für den E-Mail-Verkehr erstellen. Diese Journale werden für die Nachrichten erstellt, die mithilfe der Option **Journal über folgende Nachrichten führen** weiter unten bestimmt werden. Sie werden an die **E-Mail-Adresse für Journal** versandt. Die Ursprungsnachrichten werden dabei unverändert als Dateianlagen an die Journale angefügt. Der Nachrichtentext des Journals enthält Informationen aus der Ursprungsnachricht, insbesondere Absender, E-Mail-Adresse, Betreffzeile, Nachrichten-ID und E-Mail-Adressen der Empfänger. Sie können ein Journal nur über *interne Nachrichten* (dies ist die Voreinstellung), nur über *externe Nachrichten*, oder über *alle Nachrichten* führen.

Archiv-Speicher

Archiv-Speicher sind die Container, in denen archivierte E-Mail-Nachrichten gespeichert werden. Jeder Archiv-Speicher ist einer einzigen Domäne zugeordnet.

Archiv-Speicher automatisch erstellen
Diese Option bewirkt, dass SecurityGateway die Erstellung Ihrer Archiv-Speicher selbst steuert. Es wird empfohlen, diese Option zu aktivieren.

Klicken Sie hier, um die automatische Erstellung der Archiv-Speicher zu konfigurieren

Automatische Erstellung von Archiv-Speichern

Mithilfe dieses Konfigurationsdialogs können Sie bestimmen, wie oft SecurityGateway neue Archiv-Speicher automatisch erstellen soll, wenn bestehende Archiv-Speicher das festgelegte Alter oder die festgelegte Größe erreichen, oder wenn die Zahl der in ihnen gespeicherten Nachrichten den festgelegten Wert erreicht.

Neuen Archiv-Speicher erstellen...

Jährlich/Vierteljährlich/Monatlich
Mithilfe dieser Optionen können Sie für die Domäne einen neuen Archiv-Speicher automatisch jedes Jahr, jedes Vierteljahr oder jeden Monat erstellen lassen.

Falls der aktuelle Archiv-Speicher entweder
Mithilfe dieser Option können Sie für die Domänen einen neuen Archiv-

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Speicher automatisch erstellen lassen, sobald der bestehende Archiv-Speicher eine bestimmte Größe erreicht oder in ihm eine bestimmte Anzahl von Nachrichten gespeichert ist. Sie können wahlweise eine Option oder beide Optionen zugleich aktivieren. Sind beide Optionen aktiv, so wird immer dann ein neuer Archiv-Speicher erstellt, wenn die Bedingungen einer Option erfüllt sind.

[xx] oder mehr Nachrichten enthält
Diese Option bewirkt, dass für die Domäne ein neuer Archiv-Speicher erstellt wird, sobald der bestehende Archiv-Speicher die hier angegebene Anzahl von Nachrichten enthält. Die Voreinstellung lautet 5 Millionen Nachrichten.

[xx] oder mehr Gigabyte Daten enthält
Diese Option bewirkt, dass für die Domäne ein neuer Archiv-Speicher erstellt wird, sobald der bestehende Archiv-Speicher das hier in Gigabyte angegebene Datenvolumen enthält.

SecurityGateway prüft im Abstand von einigen Minuten, ob neue Archiv-Speicher erstellt werden müssen. Ein Archiv-Speicher kann daher die oben angegebenen Grenzen geringfügig überschreiten, bevor ein neuer Archiv-Speicher erstellt wird.

Datenbank

Lokale Firebird-Datenbankdatei nutzen
Diese Option bewirkt, dass SecurityGateway eine lokale Firebird-Datenbankdatei für die Archivierung nutzt. Diese Option ist per Voreinstellung aktiv.

Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen
Sie können diese Option nutzen, um eine Verbindung mit einem externen Firebird-Datenbankserver herzustellen und diesen zur Archivierung zu nutzen. Falls Sie den **Cluster-Betrieb** 137 nutzen, müssen Sie diese Option aktivieren.

Denselben Server nutzen, der als Datenbankserver für SecurityGateway genutzt wird
Diese Option ist per Voreinstellung aktiv, wenn Sie die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" aktivieren. Zum Zweck der Archivierung stellt SecurityGateway dann eine Verbindung mit demselben Firebird-Datenbankserver her, den Sie auch für die SecurityGateway-Datenbank konfiguriert haben. Für diese Verbindung werden die bestehenden Zugangsdaten genutzt. Die einzigen Daten, die Sie zusätzlich angeben müssen, sind *Datenbank-Pfad/Aliasname* weiter unten. Hiermit bezeichnen Sie die Datenbank, die für die automatisch erstellten Archiv-Speicher genutzt werden.

Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen
Mithilfe dieser Option können Sie einen gesonderten Firebird-

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Datenbankserver für die Archiv-Speicher nutzen. Sie müssen hierzu den *Server-Namen* oder die *IP-Adresse*, *Port, Benutzernamen* und *Kennwort* angeben, die für die Verbindung mit dem Datenbankserver erforderlich sind. Sie müssen außerdem *Datenbank-Pfad/Aliasnamen* für die automatisch erstellten Archiv-Speicher angeben.

Datenbank-Pfad/Aliasname:
Geben Sie hier den Pfad für die Datenbankdateien der automatisch erstellten Archiv-Speicher ein. **Beachte:** Dieser Pfad bezieht sich auf den Firebird-Datenbankserver, nicht zwingend auf einen Netzwerkpfad. Ein Beispiel hierzu: `C:\Datenbanken\Archive\$DOMAIN$.fbd`.

Makros für Archiv-Namen
Sie können in den Dateinamen Ihrer Archive die Makros $DOMAIN$ (Domäne), $YEAR$ (Jahr), $MONTH$ (Monat) und $QUARTER$ (Quartal) nutzen. Mithilfe dieser Makros können Sie den automatisch erstellten Archiven jeweils eindeutige Namen zuweisen. Ein Beispiel hierzu: Der Eintrag "`C:\Datenbanken\Archive\$DOMAIN$-$MONTH$.fbd`" im Feld *Datenbank-Pfad* erstellt für die Domäne example.com eine Datenbankdatei "`Example.com-September.fbd`". Sie müssen sicherstellen, dass der Verzeichnispfad zu der Datenbankdatei, der im Beispiel "`C:\Datenbanken\Archive\`" lautet, auf dem Firebird-Server tatsächlich existiert; der Firebird-Server legt den Pfad nicht automatisch an.

Der Firebird-Server erstellt beim Erstellen neuer Datenbanken neue Verzeichnisse nicht automatisch. Falls Sie im *Datenbank-Pfad* Makros in Verzeichnisnamen nutzen wollen, müssen Sie daher zunächst alle diesen Makros möglicherweise entsprechenden Verzeichnisse von Hand auf dem Firebird-Server anlegen. Ein Beispiel hierzu: Wenn Sie den *Datenbank-Pfad* auf "C:\Datenbanken\Archive\$Domain$\archiv.fbd" konfigurieren, dann müssen Sie auf dem Firebird-Server im Verzeichnis "C:\Datenbanken\Archive" Unterverzeichnisse für alle in Frage kommenden Domänen von Hand erstellen. Aus diesem Grund empfiehlt es sich, Makros nur in den Dateinamen der Archiv-Datenbanken zu nutzen und von ihrer Nutzung im Verzeichnispfad abzusehen.

Speicherorte

Für Datenbanken, Nachrichten-Inhalte und Indizes für die Suche unterschiedliche Verzeichnisse verwenden
Per Voreinstellung sind die Daten eines Archiv-Speichers in dem Verzeichnis abgelegt, durch die Option *Verzeichnis* weiter unten bezeichnet ist. Dieses Verzeichnis enthält zwei Unterverzeichnisse, `\data\` und `\index\`. Um den Speicherort aller drei Verzeichnisse benutzerdefiniert festzulegen, aktivieren Sie diese Option.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Falls Sie die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" weiter oben aktivieren, dann bestimmt diese Option nur, wo die Nachrichteninhalte und der Suchindex gespeichert werden. Der Speicherort für die Datenbank wird mithilfe der Option *Datenbank-Pfad/Aliasname* weiter oben festgelegt.

Verzeichnis:

Per Voreinstellung lautet der Verzeichnispfad für die Datenbank bei automatisch erstellten Archiv-Speichern wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\
```

Das Makro `$DOMAIN$` im Pfad wird ersetzt durch den Namen der Domäne, der der Archiv-Speicher zugeordnet ist. Dieses Verzeichnis enthält die Firebird-Datenbankdatei `ARCHIVE.FBD`. Diese Datenbank enthält die Metadaten (Domäne, Benutzer, Datum usw.) der archivierten Nachrichten. Archivierte Nachrichten können nur dann wieder hergestellt werden, wenn diese Datei vorhanden und intakt ist. Per Voreinstellung enthält dieses Verzeichnis auch die Unterverzeichnisse "`..\data`" und "`..\index`", in denen die Inhalte archivierter Nachrichten und die Indizes gespeichert werden.

Falls Sie den Cluster-Betrieb 137 nutzen und die Option "*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" weiter oben aktiviert haben, dann steuert die vorliegende Option lediglich den Speicherort für die Unterverzeichnisse "`..\data`" und "`..\index`", nicht aber den Speicherort der Datenbankdatei. Der Speicherort der Datenbank wird durch die Option *Datenbank-Pfad/Alias* weiter oben bestimmt. Das hier angegebene *Verzeichnis* muss dann außerdem an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben.

For example: `\\share01\databases\Archive\$Domain$\`

Die folgenden Speicherorte werden verwendet, wenn Sie die Option "*Für Datenbanken, Nachrichten-Inhalte und Indizes für die Suche unterschiedliche Verzeichnisse verwenden*" weiter oben aktivieren:

Verzeichnis für Datenbank:
Dies ist der Speicherort für die Datenbankdatei des Archiv-Speichers. **Beachte:** Diese Option ist nicht verfügbar, wenn die Option "*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" weiter oben aktiv ist; dann wird der

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Speicherort der Datenbankdatei durch die Option *Datenbank-Pfad/Aliasname* weiter oben bestimmt.

Per Voreinstellung lautet der Verzeichnispfad für die Datenbank wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\
```

Das Makro `$DOMAIN$` im Pfad wird ersetzt durch den Namen der Domäne, der der Archiv-Speicher zugeordnet ist. Dieses Verzeichnis enthält die Datendatei `archive.sgd`, in der die archivierten Daten in komprimierter Form gespeichert sind. Archivierte Nachrichten können nur dann wieder hergestellt werden, wenn diese Datei vorhanden und intakt ist. Per Voreinstellung lautet der Verzeichnisname für dieses Verzeichnis "`..\data`", und es ist ein Unterverzeichnis des Verzeichnisses für die Datenbank.

Verzeichnis für Inhalte:
Per Voreinstellung lautet der Verzeichnispfad für die Inhaltsdaten bei automatisch erstellten Archiv-Speichern wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\data
```

Das Makro `$DOMAIN$` im Pfad wird ersetzt durch den Namen der Domäne, der der Archiv-Speicher zugeordnet ist. Dieses Verzeichnis enthält die Datendatei `archive.sgd`, in der die archivierten Daten in komprimierter Form gespeichert sind. Archivierte Nachrichten können nur dann wieder hergestellt werden, wenn diese Datei vorhanden und intakt ist. Per Voreinstellung lautet der Verzeichnisname für dieses Verzeichnis "`..\data`", und es ist ein Unterverzeichnis des Verzeichnisses für die Datenbank.

Beachte: Falls Sie den Cluster-Betrieb[137] nutzen, oder falls die Option "*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" aktiv ist, muss dieses Verzeichnis an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben (z.B. `\\Freigabe01\Datenbanken\Archive\$Domain$\Daten`).

Verzeichnis für Index:
Per Voreinstellung lautet der Verzeichnispfad für die Indexdaten bei automatisch erstellten Archiv-Speichern wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\index
```

Das Makro `$DOMAIN$` im Pfad wird ersetzt durch den Namen der Domäne, der der Archiv-Speicher zugeordnet ist. Dieses Verzeichnis enthält den Volltext-Index, der durch das Modul CLucene Full Text Indexing erstellt wird. Dieser Index kann neu erstellt werden, falls er beschädigt werden sollte. Sie können den Volltext-Index mithilfe der Option Wartung im Konfigurationsdialog Archiv-Speicher[105] neu erstellen. Per Voreinstellung lautet der Verzeichnisname für dieses Verzeichnis "`..\index`", und es ist ein Unterverzeichnis des Verzeichnisses für die Datenbank.

Beachte: Falls Sie den Cluster-Betrieb[137] nutzen, oder falls die Option

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

"*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" aktiv ist, muss dieses Verzeichnis an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben (z.B. `\\Freigabe01\Datenbanken\Archive\$Domain$\Index`).

Klicken Sie hier, um die Archiv-Speicher zu verwalten
Durch Anklicken dieser Verknüpfung rufen Sie den Konfigurationsdialog Archiv-Speicher 105 auf. Sie können von dort aus Ihre Archiv-Speicher verwalten.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Quarantäne-Optionen dieser Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

3.3.1.1 Automatische Erstellung von Archiv-Speichern

Mithilfe dieses Konfigurationsdialogs können Sie bestimmen, wie oft SecurityGateway neue Archiv-Speicher automatisch erstellen soll, wenn bestehende Archiv-Speicher das festgelegte Alter oder die festgelegte Größe erreichen, oder wenn die Zahl der in ihnen gespeicherten Nachrichten den festgelegten Wert erreicht. Sie erreichen diesen Konfigurationsdialog, indem Sie auf der Seite Archivierung - Konfiguration 95 die Verknüpfung "*Klicken Sie hier, um die automatische Erstellung der Archiv-Speicher zu konfigurieren*" anklicken.

Neuen Archiv-Speicher erstellen...

Jährlich/Vierteljährlich/Monatlich
Mithilfe dieser Optionen können Sie für die Domäne einen neuen Archiv-Speicher automatisch jedes Jahr, jedes Vierteljahr oder jeden Monat erstellen lassen.

Falls der aktuelle Archiv-Speicher entweder
Mithilfe dieser Option können Sie für die Domänen einen neuen Archiv-Speicher automatisch erstellen lassen, sobald der bestehende Archiv-Speicher eine bestimmte Größe erreicht oder in ihm eine bestimmte Anzahl von Nachrichten gespeichert ist. Sie können wahlweise eine Option oder beide Optionen zugleich aktivieren. Sind beide Optionen aktiv, so wird immer dann ein neuer Archiv-Speicher erstellt, wenn die Bedingungen einer Option erfüllt sind.

[xx] oder mehr Nachrichten enthält
Diese Option bewirkt, dass für die Domäne ein neuer Archiv-Speicher erstellt wird, sobald der bestehende Archiv-Speicher die hier angegebene Anzahl von Nachrichten enthält. Die Voreinstellung lautet 5 Millionen Nachrichten.

[xx] oder mehr Gigabyte Daten enthält
Diese Option bewirkt, dass für die Domäne ein neuer Archiv-Speicher erstellt wird, sobald der bestehende Archiv-Speicher das hier in Gigabyte angegebene Datenvolumen enthält.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

SecurityGateway prüft im Abstand von einigen Minuten, ob neue Archiv-Speicher erstellt werden müssen. Ein Archiv-Speicher kann daher die oben angegebenen Grenzen geringfügig überschreiten, bevor ein neuer Archiv-Speicher erstellt wird.

Datenbank

Lokale Firebird-Datenbankdatei nutzen
Diese Option bewirkt, dass SecurityGateway eine lokale Firebird-Datenbankdatei für die Archivierung nutzt. Diese Option ist per Voreinstellung aktiv.

Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen
Sie können diese Option nutzen, um eine Verbindung mit einem externen Firebird-Datenbankserver herzustellen und diesen zur Archivierung zu nutzen. Falls Sie den **Cluster-Betrieb** 137 nutzen, müssen Sie diese Option aktivieren.

Denselben Server nutzen, der als Datenbankserver für SecurityGateway genutzt wird
Diese Option ist per Voreinstellung aktiv, wenn Sie die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" aktivieren. Zum Zweck der Archivierung stellt SecurityGateway dann eine Verbindung mit demselben Firebird-Datenbankserver her, den Sie auch für die SecurityGateway-Datenbank konfiguriert haben. Für diese Verbindung werden die bestehenden Zugangsdaten genutzt. Die einzigen Daten, die Sie zusätzlich angeben müssen, sind *Datenbank-Pfad/Aliasname* weiter unten. Hiermit bezeichnen Sie die Datenbank, die für die automatisch erstellten Archiv-Speicher genutzt werden.

Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen
Mithilfe dieser Option können Sie einen gesonderten Firebird-Datenbankserver für die Archiv-Speicher nutzen. Sie müssen hierzu den *Server-Namen* oder die *IP-Adresse*, *Port, Benutzernamen* und *Kennwort* angeben, die für die Verbindung mit dem Datenbankserver erforderlich sind. Sie müssen außerdem *Datenbank-Pfad/Aliasnamen* für die automatisch erstellten Archiv-Speicher angeben.

Datenbank-Pfad/Aliasname:
Geben Sie hier den Pfad für die Datenbankdateien der automatisch erstellten Archiv-Speicher ein. **Beachte:** Dieser Pfad bezieht sich auf den Firebird-Datenbankserver, nicht zwingend auf einen Netzwerkpfad. Ein Beispiel hierzu: `C:\Datenbanken\Archive\$DOMAIN$.fbd`.

Makros für Archiv-Namen
Sie können in den Dateinamen Ihrer Archive die Makros $DOMAIN$ (Domäne), $YEAR$ (Jahr), $MONTH$ (Monat) und $QUARTER$ (Quartal) nutzen. Mithilfe dieser Makros können Sie den automatisch erstellten Archiven jeweils eindeutige Namen zuweisen. Ein Beispiel hierzu: Der Eintrag "`C:\Datenbanken\Archive\$DOMAIN$-$MONTH$.fbd`" im Feld *Datenbank-Pfad* erstellt für die Domäne example.com eine Datenbankdatei "`Example.com-September.fbd`". Sie müssen sicherstellen, dass der Verzeichnispfad zu der Datenbankdatei, der im Beispiel "`C:\Datenbanken\Archive\`" lautet, auf dem

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Firebird-Server tatsächlich existiert; der Firebird-Server legt den Pfad nicht automatisch an.

Der Firebird-Server erstellt beim Erstellen neuer Datenbanken neue Verzeichnisse nicht automatisch. Falls Sie im *Datenbank-Pfad* Makros in Verzeichnisnamen nutzen wollen, müssen Sie daher zunächst alle diesen Makros möglicherweise entsprechenden Verzeichnisse von Hand auf dem Firebird-Server anlegen. Ein Beispiel hierzu: Wenn Sie den *Datenbank-Pfad* auf "C:\Datenbanken\Archive\$Domain$\archiv.fbd" konfigurieren, dann müssen Sie auf dem Firebird-Server im Verzeichnis "C:\Datenbanken\Archive" Unterverzeichnisse für alle in Frage kommenden Domänen von Hand erstellen. Aus diesem Grund empfiehlt es sich, Makros nur in den Dateinamen der Archiv-Datenbanken zu nutzen und von ihrer Nutzung im Verzeichnispfad abzusehen.

Speicherorte

Für Datenbanken, Nachrichten-Inhalte und Indizes für die Suche unterschiedliche Verzeichnisse verwenden
Per Voreinstellung sind die Daten eines Archiv-Speichers in dem Verzeichnis abgelegt, durch die Option *Verzeichnis* weiter unten bezeichnet ist. Dieses Verzeichnis enthält zwei Unterverzeichnisse, `\data\` und `\index\`. Um den Speicherort aller drei Verzeichnisse benutzerdefiniert festzulegen, aktivieren Sie diese Option.

Falls Sie die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" weiter oben aktivieren, dann bestimmt diese Option nur, wo die Nachrichteninhalte und der Suchindex gespeichert werden. Der Speicherort für die Datenbank wird mithilfe der Option *Datenbank-Pfad/Aliasname* weiter oben festgelegt.

Verzeichnis:

Per Voreinstellung lautet der Verzeichnispfad für die Datenbank bei automatisch erstellten Archiv-Speichern wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\
```

Das Makro `$DOMAIN$` im Pfad wird ersetzt durch den Namen der Domäne, der der Archiv-Speicher zugeordnet ist. Dieses Verzeichnis enthält die Firebird-Datenbankdatei `ARCHIVE.FBD`. Diese Datenbank enthält die Metadaten (Domäne, Benutzer, Datum usw.) der archivierten Nachrichten. Archivierte Nachrichten können nur dann wieder hergestellt werden, wenn diese Datei vorhanden und intakt ist. Per Voreinstellung enthält dieses Verzeichnis auch die Unterverzeichnisse "`..\data`" und "`..\index`", in denen die Inhalte archivierter Nachrichten und die Indizes gespeichert werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Falls Sie den Cluster-Betrieb[137] nutzen und die Option "*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" weiter oben aktiviert haben, dann steuert die vorliegende Option lediglich den Speicherort für die Unterverzeichnisse "..\data" und "..\index", nicht aber den Speicherort der Datenbankdatei. Der Speicherort der Datenbank wird durch die Option *Datenbank-Pfad/Alias* weiter oben bestimmt. Das hier angegebene *Verzeichnis* muss dann außerdem an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben.

For example: \\share01\databases\Archive\$Domain$\

Die folgenden Speicherorte werden verwendet, wenn Sie die Option "*Für Datenbanken, Nachrichten-Inhalte und Indizes für die Suche unterschiedliche Verzeichnisse verwenden*" weiter oben aktivieren:

Verzeichnis für Datenbank:
Dies ist der Speicherort für die Datenbankdatei des Archiv-Speichers.
Beachte: Diese Option ist nicht verfügbar, wenn die Option "*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" weiter oben aktiv ist; dann wird der Speicherort der Datenbankdatei durch die Option *Datenbank-Pfad/Aliasname* weiter oben bestimmt.

Per Voreinstellung lautet der Verzeichnispfad für die Datenbank wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\
```

Das Makro `$DOMAIN$` im Pfad wird ersetzt durch den Namen der Domäne, der der Archiv-Speicher zugeordnet ist. Dieses Verzeichnis enthält die Datendatei `archive.sgd`, in der die archivierten Daten in komprimierter Form gespeichert sind. Archivierte Nachrichten können nur dann wieder hergestellt werden, wenn diese Datei vorhanden und intakt ist. Per Voreinstellung lautet der Verzeichnisname für dieses Verzeichnis "..\data", und es ist ein Unterverzeichnis des Verzeichnisses für die Datenbank.

Verzeichnis für Inhalte:
Per Voreinstellung lautet der Verzeichnispfad für die Inhaltsdaten bei automatisch erstellten Archiv-Speichern wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\data
```

Das Makro `$DOMAIN$` im Pfad wird ersetzt durch den Namen der Domäne, der der Archiv-Speicher zugeordnet ist. Dieses Verzeichnis enthält die Datendatei `archive.sgd`, in der die archivierten Daten in komprimierter Form gespeichert sind. Archivierte Nachrichten können nur dann wieder hergestellt werden, wenn diese Datei vorhanden und intakt ist. Per Voreinstellung lautet der Verzeichnisname für dieses Verzeichnis "..\data", und es ist ein Unterverzeichnis des Verzeichnisses für die Datenbank.

Beachte: Falls Sie den Cluster-Betrieb[137] nutzen, oder falls die Option

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

"*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" aktiv ist, muss dieses Verzeichnis an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben (z.B. `\\Freigabe01\Datenbanken\Archive\$Domain$\Daten`).

Verzeichnis für Index:
Per Voreinstellung lautet der Verzeichnispfad für die Indexdaten bei automatisch erstellten Archiv-Speichern wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\index
```

Das Makro `$DOMAIN$` im Pfad wird ersetzt durch den Namen der Domäne, der der Archiv-Speicher zugeordnet ist. Dieses Verzeichnis enthält den Volltext-Index, der durch das Modul CLucene Full Text Indexing erstellt wird. Dieser Index kann neu erstellt werden, falls er beschädigt werden sollte. Sie können den Volltext-Index mithilfe der Option Wartung im Konfigurationsdialog Archiv-Speicher 105 neu erstellen. Per Voreinstellung lautet der Verzeichnisname für dieses Verzeichnis "`..\index`", und es ist ein Unterverzeichnis des Verzeichnisses für die Datenbank.

Beachte: Falls Sie den Cluster-Betrieb 137 nutzen, oder falls die Option "*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" aktiv ist, muss dieses Verzeichnis an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben (z.B. `\\Freigabe01\Datenbanken\Archive\$Domain$\Index`).

3.3.2 Archiv-Speicher

Mithilfe dieses Konfigurationsdialogs können Sie Ihre Archiv-Speicher verwalten. Ihre Archiv-Speicher enthalten die archivierten Nachrichten. Jeder Archiv-Speicher kann nur mit einer bestimmten Domäne verknüpft sein. Sie können mehrere Archiv-Speicher derselben Domäne zuordnen, aber es kann dann jeweils nur ein Archiv-Speicher zur selben Zeit *aktiv* sein. Sie können die Archiv-Speicher mithilfe der Optionen auf dieser Seite von Hand erstellen, oder Sie können die Archiv-Speicher mithilfe der Optionen im Konfigurationsdialog Archivierung - Konfiguration 95 automatisch erstellen lassen.

In der Übersicht über die Archiv-Speicher erscheint ein Eintrag pro Zeile. Es stehen verschiedene Spalten zur Verfügung, die Sie durch Anklicken der zugehörigen Schaltflächen am oberen Ende der Übersicht ein- und ausblenden können.

Die Symbolleiste am oberen Seitenrand enthält folgende Optionen:

Neu
Um einen neuen Archiv-Speicher von Hand zu erstellen, klicken Sie auf *Neu*. Es öffnet sich der Konfigurationsdialog für die Erstellung eines neuen Archiv-Speichers. Inhaltlich gleicht dieser Konfigurationsdialog dem Konfigurationsdialog Archiv-Speicher bearbeiten 106.

Bearbeiten
Um einen Archiv-Speicher zu bearbeiten, wählen Sie den gewünschten Archiv-Speicher aus, und klicken Sie dann in der Symbolleiste auf *Bearbeiten*. Es öffnet sich der Konfigurationsdialog Archiv-Speicher bearbeiten 106. Sie können diesen Konfigurationsdialog wahlweise auch aufrufen, indem Sie auf den Eintrag des gewünschten Archiv-Speichers in der Übersicht doppelt klicken.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Löschen
Um einen oder mehrere Archiv-Speicher zu löschen, wählen Sie die gewünschten Archiv-Speicher aus der Übersicht aus, und klicken Sie danach auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie den Löschvorgang bestätigen oder abbrechen können. Sie können mehrere Einträge in der Übersicht mithilfe der Tasten Strg und Umschalt auswählen.

Wartung
Der Volltext-Index des Archiv-Speichers wird zum Durchsuchen archivierter Nachrichten[109] benötigt. Sie können diesen Volltext-Index für einen oder mehrere Archiv-Speicher neu erstellen lassen. Wählen Sie hierzu die gewünschten Archiv-Speicher aus der Übersicht aus, klicken Sie danach auf **Wartung** und schließlich auf **Volltext-Index neu erstellen**. Es erscheint eine Sicherheitsabfrage, auf die Sie den Vorgang bestätigen oder abbrechen können. Botte beachten Sie, dass Sie den Archiv-Speicher nicht durchsuchen können, so lange der Volltext-Index neu erstellt wird.

Für Domäne:
Mithilfe des Dropdown-Menüs *Für Domäne:* können Sie die Domäne auswählen, deren Archiv-Speicher in der Übersicht erscheinen sollen. Um die Archiv-Speicher für alle Domänen anzuzeigen, wählen Sie den Eintrag "-- Alle --" aus. Per Voreinstellung werden die Archiv-Speicher für alle Domänen angezeigt.

3.3.2.1 Archiv-Speicher bearbeiten

Archiv-Speicher

Abfragen für diesen Archiv-Speicher zulassen
Diese Option bewirkt, dass der gerade bearbeitete Archiv-Speicher mithilfe der Optionen auf der Seite Archivierte Nachrichten durchsuchen[109] durchsucht werden kann. Ist diese Option nicht aktiv, so werden die Nachrichten in diesem Archiv-Speicher nicht in die Suche einbezogen. Diese Option ist per Voreinstellung aktiv.

Neue Nachrichten für diese Domäne hier archivieren
Diese Option bestimmt, ob der gerade bearbeitete Archiv-Speicher der *aktive* Archiv-Speicher für die Domäne ist. Der aktive Archiv-Speicher ist der Archiv-Speicher, in dem neu hinzugekommene Nachrichten für die Domäne archiviert werden. Den Domänen können mehrere Archiv-Speicher zugeordnet sein, aber es kann hiervon jeweils nur ein Archiv-Speicher zur selben Zeit aktiv sein. Sie können beispielsweise einen neuen Archiv-Speicher für eine Domäne erstellen lassen, wenn der bestehende Archiv-Speicher eine bestimmte Größe erreicht. Danach bleibt der bisherige Archiv-Speicher in der Übersicht über die Archiv-Speicher[105] verfügbar und kann auch weiterhin durchsucht werden. Diese Option bestimmt, in welchem Archiv-Speicher neu hinzugekommene Nachrichten abgelegt werden. Besteht für eine Domäne ein aktiver Archiv-Speicher, und bearbeiten Sie einen anderen Archiv-Speicher für dieselbe Domäne, der nicht aktiv ist, so können Sie diesen Archiv-Speicher durch Aktivieren dieser Option als aktiv kennzeichnen. Der zuvor aktive Archiv-Speicher ist danach nicht mehr aktiv.

Falls Sie für eine Domäne die Automatische Erstellung von Archiv-Speichern[101] nutzen und diese Option für den gerade aktiven Archiv-Speicher deaktivieren, erstellt

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

SecurityGateway automatisch einen neuen Archiv-Speicher für die Domäne, sobald dies erforderlich ist. Falls Sie die Funktionen zur automatischen Erstellung von Archiv-Speichern nicht nutzen und den für eine Domäne aktiven Archiv-Speicher deaktivieren, so wird für diese Domäne keine Archivierung mehr durchgeführt.

Domäne
Dies ist die Domäne, der der Archiv-Speicher zugeordnet ist. Einem Archiv-Speicher kann nur eine Domäne zugeordnet sein. Sie können diese Option nur dann bearbeiten, wenn Sie einen neuen Archiv-Speicher von Hand anlegen. Sie können die Zuordnung bereits bestehender Archiv-Speicher zu den Domänen nicht ändern.

Name
Mithilfe dieser Option können Sie einen Namen für den Archiv-Speicher vergeben, der Ihren eigenen Verwaltungszwecken dient.

Datenbank

Lokale Firebird-Datenbankdatei nutzen
Diese Option bewirkt, dass SecurityGateway eine lokale Firebird-Datenbankdatei für die Archivierung nutzt. Diese Option ist per Voreinstellung aktiv.

Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen
Sie können diese Option nutzen, um eine Verbindung mit einem externen Firebird-Datenbankserver herzustellen und diesen zur Archivierung zu nutzen. Falls Sie den **Cluster-Betrieb** 137 nutzen, müssen Sie diese Option aktivieren.

Denselben Server nutzen, der als Datenbankserver für SecurityGateway genutzt wird
Diese Option ist per Voreinstellung aktiv, wenn Sie die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" aktivieren. Zum Zweck der Archivierung stellt SecurityGateway dann eine Verbindung mit demselben Firebird-Datenbankserver her, den Sie auch für die SecurityGateway-Datenbank konfiguriert haben. Für diese Verbindung werden die bestehenden Zugangsdaten genutzt. Die einzigen Daten, die Sie zusätzlich angeben müssen, sind *Datenbank-Pfad/Aliasname* weiter unten. Hiermit bezeichnen Sie die Datenbank, die für die automatisch erstellten Archiv-Speicher genutzt werden.

Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen
Mithilfe dieser Option können Sie einen gesonderten Firebird-Datenbankserver für die Archiv-Speicher nutzen. Sie müssen hierzu den *Server-Namen* oder die *IP-Adresse*, *Port, Benutzernamen* und *Kennwort* angeben, die für die Verbindung mit dem Datenbankserver erforderlich sind. Sie müssen außerdem *Datenbank-Pfad/Aliasnamen* für die automatisch erstellten Archiv-Speicher angeben.

Datenbank-Pfad/Aliasname:
Geben Sie hier den Pfad für die Datenbankdateien der automatisch erstellten Archiv-Speicher ein. **Beachte:** Dieser Pfad bezieht sich auf den Firebird-

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Datenbankserver, nicht zwingend auf einen Netzwerkpfad. Ein Beispiel hierzu: `C:\Datenbanken\Archive\$DOMAIN$.fbd`. Sie können hier statt eines Datenbank-Pfads auch auch einen *Aliasnamen* festlegen, um einen Aliasnamen für die Datenbank zu definieren. Hierzu müssen Sie die Datei Aliases.conf bearbeiten. Die Datei `Aliases.conf` befindet sich im Hauptverzeichnis Ihrer Datenbankserver-Installation für Firebird.

Speicherorte

Für Datenbanken, Nachrichten-Inhalte und Indizes für die Suche unterschiedliche Verzeichnisse verwenden
Per Voreinstellung sind die Daten eines Archiv-Speichers in dem Verzeichnis abgelegt, durch die Option *Verzeichnis* weiter unten bezeichnet ist. Dieses Verzeichnis enthält zwei Unterverzeichnisse, `\data\` und `\index\`. Um den Speicherort aller drei Verzeichnisse benutzerdefiniert festzulegen, aktivieren Sie diese Option.

Falls Sie die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" weiter oben aktivieren, dann bestimmt diese Option nur, wo die Nachrichteninhalte und der Suchindex gespeichert werden. Der Speicherort für die Datenbank wird mithilfe der Option *Datenbank-Pfad/Aliasname* weiter oben festgelegt

Verzeichnis:
Dieses Verzeichnis enthält die Firebird-Datenbankdatei `ARCHIVE.FBD`. Diese Datenbank enthält die Metadaten (Domäne, Benutzer, Datum usw.) der archivierten Nachrichten. Archivierte Nachrichten können nur dann wieder hergestellt werden, wenn diese Datei vorhanden und intakt ist. Per Voreinstellung enthält dieses Verzeichnis auch die Unterverzeichnisse "`..\data`" und "`..\index`", in denen die Inhalte archivierter Nachrichten und die Indizes gespeichert werden.

Falls Sie den Cluster-Betrieb 137 nutzen und die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" weiter oben aktiviert haben, dann steuert die vorliegende Option lediglich den Speicherort für die Unterverzeichnisse "`..\data`" und "`..\index`", nicht aber den Speicherort der Datenbankdatei. Der Speicherort der Datenbankdatei wird durch die Option *Datenbank-Pfad/Alias* weiter oben bestimmt. Das hier angegebene *Verzeichnis* muss dann außerdem an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben.

Ein Beispiel hierzu: `\\Freigabe01\Datenbanken\Archive\$Domain$\`

Die folgenden Speicherorte werden verwendet, wenn Sie die Option "*Für Datenbanken, Nachrichten-Inhalte und Indizes für die Suche unterschiedliche Verzeichnisse verwenden*" weiter oben aktivieren:

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Verzeichnis für Datenbank:
Dies ist der Speicherort für die Datenbankdatei des Archiv-Speichers. **Beachte:** Diese Option ist nicht verfügbar, wenn die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" weiter oben aktiv ist; dann wird der Speicherort der Datenbankdatei durch die Option *Datenbank-Pfad/Aliasname* weiter oben bestimmt.

Per Voreinstellung lautet der Verzeichnispfad für die Datenbank wie folgt:

```
..\SecurityGateway\Archive\$DOMAIN$\
```

Verzeichnis für Inhalte:
Dieses Verzeichnis enthält die Datendatei `archive.sgd`, in der die archivierten Daten in komprimierter Form gespeichert sind. Archivierte Nachrichten können nur dann wieder hergestellt werden, wenn diese Datei vorhanden und intakt ist. Per Voreinstellung lautet der Verzeichnisname für dieses Verzeichnis "`..\data`", und es ist ein Unterverzeichnis des Verzeichnisses für die Datenbank.

Beachte: Falls Sie den Cluster-Betrieb[137] nutzen, oder falls die Option "*Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*" aktiv ist, muss dieses Verzeichnis an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben (z.B. `\\Freigabe01\Datenbanken\Archive\$Domain$\Daten`).

Verzeichnis für Index:
Per Voreinstellung lautet der Verzeichnisname für die Indexdaten "`..\index`", und das Verzeichnis wird als Unterverzeichnis des Datenbankverzeichnisses angelegt. Dieses Verzeichnis enthält den Volltext-Index, der durch das Modul CLucene Full Text Indexing erstellt wird. Dieser Index kann neu erstellt werden, falls er beschädigt werden sollte. Sie können den Volltext-Index mithilfe der Option Wartung im Konfigurationsdialog Archiv-Speicher[105] neu erstellen.

Beachte: Falls Sie den Cluster-Betrieb[137] nutzen, oder falls die Option "*Verbindung mit folgender Firebird-Instanz auf folgendem Datenbankserver herstellen*" aktiv ist, muss dieses Verzeichnis an einem über das Netzwerk erreichbaren Speicherort abgelegt sein, und Sie müssen UNC-Pfadnamen angeben (z.B. `\\Freigabe01\Datenbanken\Archive\$Domain$\Index`).

3.3.3 Archivierte Nachrichten durchsuchen

Mithilfe dieser Seite können Sie die archivierten Nachrichten durchsuchen. Die Suche erstreckt sich dabei auf alle Archiv-Speicher, für die Abfragen zugelassen sind[106]. SecurityGateway durchsucht die Nachrichten anhand der Parameter, die Sie für die Suche bestimmen. Mithilfe der Option *Für Domäne:* am oberen Fensterrand können Sie die Suche auf eine Domäne einschränken oder, durch Auswahl der Option *Alle Domänen* auf alle Domänen erstrecken. Mithilfe der erweiterten Optionen können Sie die Suche nach Betreffzeile, Nachrichtentext, Datumsbereich, Dateianlagen, Größe und verschiedenen anderen Eigenschaften konkretisieren.

Auf dieser Seite finden Sie auch Werkzeuge zum Betrachten der Nachrichten, die die Suche aufgefunden hat. Sie können diese Nachrichten außerdem herunterladen und in dem Postfach wieder herstellen, aus dem sie archiviert wurden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Hinweise zur Suche

Die Suche unterstützt die Jokerzeichen ? und *.

Sie können das Jokerzeichen * mit Zeichenketten verwenden, um Nachrichten zu finden, die diese Zeichenketten enthalten. Einige Beispiele hierzu: Eine Suche nach `send*` findet Nachrichten, die die Zeichenketten `send`, `sender`, `sending` und weitere vergleichbare enthalten. and so on. Eine Suche nach `*example.com` findet Nachrichten, die beliebige E-Mail-Adressen @example.com oder in der Domäne example.com enthalten, wie etwa `mail.example.com`, `sg.example.com` und weitere vergleichbare.

Für eine strikte Suche nach Zeichenketten setzen Sie diese in Anführungs- und Schlusszeichen. Einige Beispiele hierzu: Eine Suche nach `"Frank Thomas"` findet nur Nachrichten, die den Namen `Frank Thomas` enthalten. Lassen Sie hingegen die Anführungs- und Schlusszeichen weg, so findet die Suche alle Nachrichten, die die Zeichenketten "Frank," "Thomas," "Frank Thomas" oder "Thomas Frank" enthalten.

Sie können einzelne Zeichenketten aus der Suche ausschließen, indem Sie den Zeichenketten ein Minuszeichen ("-") voranstellen. Einige Beispiele hierzu: Eine Suche nach `-John Smith` findet alle Nachrichten, die "`Smith`" enthalten und schließt alle Nachrichten aus, die außerdem die Zeichenkette "`John`" enthalten.

Sie können, falls erforderlich, den Volltext-Index mithilfe der Option Wartung im Konfigurationsdialog Archiv-Speicher 105 neu erstellen.

3.3.4 Einhaltung von Vorschriften bei der Archivierung

Mithilfe dieses Konfigurationsdialogs können Sie bestimmen, wie lange archivierte Nachrichten gegen Löschung geschützt werden müssen, und wie lange sie aufbewahrt werden, bevor sie automatisch gelöscht werden. Es steht eine neue Option *Kontakt vergessen* zur Verfügung; sie löscht archivierte Nachrichten, die an bestimmte Benutzer gesandt wurden, und wahlweise auch archivierte Nachrichten, die durch diese Benutzer versandt wurden. Es steht eine weitere Option *Legal Hold* zur Verfügung, mit deren Hilfe alle archivierten Nachrichten gegen Löschung geschützt werden können. Ist diese Option aktiv, so werden alle anderen Einstellungen und Benutzerrechte übergangen, die an anderen Stellen in SecurityGateway getroffen sind und die Löschung beeinflussen würden.

Datenhaltung

Archivierte Nachrichten für mindestens folgende Dauer aufbewahren
Diese Option bewirkt, dass archivierte Nachrichten mindestens für die hier in Tagen angegebene Zeitdauer gespeichert bleiben. Diese Option geht den anderen Einstellungen zur Archivierung und den entsprechenden Benutzerrechten vor.

Archivierte Nachrichten automatisch löschen nach Überschreiten eines Alters von [xx] Tagen
Diese Option bewirkt, dass archivierte Nachrichten automatisch gelöscht werden, sobald sie das hier in Tagen angegebene Alter überschritten haben. Diese Option wirkt nicht auf Nachrichten, für die eine andere Option die Löschung verhindert, insbesondere die Option *Legal Hold*, die weiter unten beschrieben ist.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nachrichten nur aus aktiven Archiv-Speichern löschen
Per Voreinstellung wirkt die Option *Archivierte Nachrichten automatisch löschen...* weiter oben nur auf aktive Archiv-Speicher. Falls Sie alle alten Nachrichten auch aus nicht mehr aktiven Archiv-Speichern löschen lassen wollen, deaktivieren Sie diese Option.

Legal Hold

Legal Hold aktivieren
So lange diese Option aktiv ist, können keine Nachrichten aus dem Archiv gelöscht werden. Die in anderen Konfigurationsdialogen festgelegten Benutzerrechte und Aufbewahrungsfristen werden dabei übergangen. Der Begriff "Legal Hold" ist vor allem in englischsprachigen Ländern gebräuchlich und bezeichnet dort ein Verfahren, mit dem bestimmte Unterlagen, insbesondere, wenn sie einer Offenlegungspflicht unterfallen, vor dem Verlust geschützt werden müssen, und daher ihre Löschung unterbunden werden muss.

Kontakt vergessen

Mithilfe der folgenden Optionen können alle archivierten Nachrichten gelöscht werden, die von einer bestimmten E-Mail-Adresse aus empfangen wurden. Wahlweise können auch solche archivierten Nachrichten gelöscht werden, die an diese E-Mail-Adresse versandt wurden.

E-Mail-Adresse
Geben Sie hier die E-Mail-Adresse an, deren archivierte Nachrichten Sie löschen wollen. Per Voreinstellung löscht die Option Kontakt vergessen nur solche archivierte Nachrichten, die **von** dieser Adresse aus versandt wurden. Falls Sie außerdem archivierte Nachrichten löschen wollen, die **an** diese E-Mail-Adresse versandt wurden, aktivieren Sie die Option "*... auch alle an den Kontakt versandten Nachrichten löschen*" weiter unten.

...auch alle an den Kontakt versandten Nachrichten löschen
Diese Option bewirkt, dass nicht nur archivierte Nachrichten gelöscht werden, die **von** der angegebenen E-Mail-Adresse aus versandt wurden, sondern auch solche archivierten Nachrichten, die **an** diese E-Mail-Adresse versandt wurden.

Bestätigungsnachricht senden, dass alle Nachrichten gelöscht wurden
Mithilfe der folgenden Bestätigungsoptionen können Sie SecurityGateway veranlassen, per E-Mail eine Bestätigungsnachricht zu versenden, sobald alle Nachrichten gelöscht wurden. Diese Bestätigungsnachricht kann gerichtet sein an Sie selbst, an den Kontakt, dessen archivierte Nachrichten gelöscht wurden, oder an eine andere E-Mail-Adresse.

Klicken Sie hier, um alle Nachrichten von dem und an den Kontakt zu löschen
Nachdem Sie die Optionen zum Vergessen des Kontakts wunschgemäß konfiguriert haben, können Sie durch Anklicken dieser Verknüpfung die Löschung durchführen.

3.3.5 Export

Mithilfe der Optionen auf dieser Seite können sie alle für eine Domäne archivierten Nachrichten exportieren. Die Nachrichten werden in ein ZIP-Archiv gepackt; dieses Archiv kann heruntergeladen werden. Sobald das ZIP-Archiv zum Herunterladen bereit gestellt ist, wird an die hier angegebene E-Mail-Adresse eine entsprechende

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Benachrichtigung versandt. Diese Benachrichtigung enthält die Verknüpfung zum Abruf der ZIP-Datei.

Um die archivierten Nachrichten zu archivieren, wählen Sie eine Domäne aus, geben Sie die E-Mail-Adresse an, an die die Nachricht mit der Verknüpfung zum Abruf des Archivs versandt werden soll, und klicken Sie dann auf **Export**.

3.4 Sichere Nachrichten

3.4.1 Konfiguration

Mithilfe des Leistungsmerkmals für sichere Nachrichten können Ihre Benutzer über SecurityGateway sichere Nachrichten an Empfänger außerhalb ihrer eigenen Domänen senden, ohne dass die sicheren Nachrichten dabei den SecurityGateway-Server verlassen. Die Nachrichten werden dabei mithilfe eines Web-Portals für sichere Nachrichten übermittelt. Wird eine Nachricht versandt, so erhält der Empfänger eine Benachrichtigung per E-Mail. Sie verständigt ihn davon, dass für ihn eine sichere Nachricht vorliegt, und sie enthält eine Verknüpfung, mit deren Hilfe er ein Benutzerkonto als Empfänger sicherer Nachrichten 113 erstellen kann. Über diese Benutzerkonten können die Empfänger sichere Nachrichten auf Ihrem SecurityGateway-Server lesen. Die Empfänger greifen dabei mithilfe ihrer Browser auf die Nachrichten zu, und für die Verbindung zwischen dem SecurityGateway-Server und dem Empfänger besteht Ende-zu-Ende-Verschlüsselung über HTTPS. Die Leistungsmerkmale für sichere Nachrichten erfordern ein gültiges SSL-Zertifikat 129, auch muss HTTPS aktiv sein 126 (siehe auch die Beschreibung im Abschnitt HTTPS-Server 132). Die Empfänger können die Nachrichten im SecurityGateway-Portal lesen und beantworten. Sie können auch wahlweise neue sichere Nachrichten an hierfür festgelegte Benutzer verfassen 119. Sie finden in den Abschnitten Empfänger 113 and Empfänger-Optionen 115 nähere Informationen über Benutzerkonten für die Empfänger sicherer Nachrichten.

Versand sicherer Nachrichten

Um eine Nachricht als sichere Nachricht und nicht über den herkömmlichen Zustellweg für E-Mail-Nachrichten zu versenden, erstellen Sie eine Regel für den Inhaltsfilter 258 oder die Verhinderung von Datendiebstahl 244, und nehmen Sie die Aktion "*Als sichere Web-Nachricht senden*" in die Regel auf. Ein Beispiel hierzu: Sie können eine Regel erstellen, die eine Nachricht immer dann als sichere Nachricht versendet, wenn ihr Betreff mit "[Sichere Nachricht]" beginnt. Sie können für den Versand sicherer Nachrichten auch ein Sieve-Skript manuell erstellen. Hierfür steht die Sieve-Aktion 294 `vnd.mdaemon.securewebmsg` zur Verfügung.

Sichere Nachrichten aktivieren

Diese Option aktiviert die Leistungsmerkmale für sichere Nachrichten.

Empfänger sicherer Nachrichten automatisch erstellen
Per Voreinstellung werden Benutzerkonten für alle Empfänger sicherer Nachrichten 113 automatisch erstellt, an die sichere Nachrichten versandt werden. Diese Empfänger erhalten auch eine Verknüpfung, über die sie auf das Benutzerkonto zugreifen und die Nachrichten lesen können. Falls Sie alle Benutzerkonten für die Empfänger manuell erstellen wollen, deaktivieren Sie diese Option.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Wenn diese Option deaktiviert ist, müssen die Empfänger sicherer Nachrichten erst manuell auf der Seite Empfänger 113 erstellt werden, bevor sie sichere Nachrichten empfangen können. Bewirkt eine Regel oder ein Skript, dass eine Nachricht als sichere Nachricht versandt wird, und hat ein Empfänger noch kein entsprechendes Benutzerkonto, so wird die Nachricht an den Absender zurückgeleitet.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Optionen dieser Domäne für sichere Nachrichten anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

3.4.2 Empfänger

Diese Seite enthält einen Eintrag für jedes Benutzerkonto eines Empfängers sicherer Nachrichten, das automatisch 112 oder manuell erstellt wurde. Um ein neues Benutzerkonto für einen Empfänger manuell zu erstellen, klicken Sie in der Symbolleiste auf **Neu**. Sie können bestehende Benutzerkonten schnell aktivieren und deaktivieren, indem Sie das zugehörige Kontrollkästchen in der Spalte *Aktiviert* ein- und ausschalten. Um die Eigenschaften eines Benutzerkontos einzusehen und zu bearbeiten, klicken Sie doppelt auf das Benutzerkonto, oder klicken Sie das Benutzerkonto einmal an, und klicken Sie dann auf **Bearbeiten**. Zu den Eigenschaften des Benutzerkontos gehören beispielsweise E-Mail-Adresse, Name und Kennwort. Um die Einstellungen zur Archivierung, Sprache der Benutzeroberfläche und Zahl der pro Seite angezeigten Elemente zu bearbeiten, wählen Sie das Benutzerkonto aus, und klicken Sie dann auf **Einstellungen** 115. Um das Nachrichten-Protokoll 43 für ein Benutzerkonto einzusehen, wählen Sie das Benutzerkonto aus, und klicken Sie dann auf **Nachrichten**.

Benutzerkonten für Empfänger erstellen und bearbeiten

Um ein neues Benutzerkonto für einen Empfänger manuell zu erstellen, klicken Sie in der Symbolleiste auf **Neu**. Um ein bestehendes Benutzerkonto zu bearbeiten, wählen Sie das Benutzerkonto aus, und klicken Sie dann auf **Bearbeiten**.

Eigenschaften

Dieses Benutzerkonto ist gesperrt
Um das Benutzerkonto des Empfängers zu deaktivieren, aktivieren Sie dieses Kontrollkästchen.

Zugeordnete lokale Domäne:
Wählen Sie hier die Domäne aus, der Sie das Benutzerkonto zuordnen wollen. Benutzerkonten für Empfänger, die automatisch erstellt werden, werden der Domäne des Absenders der sicheren Nachricht zugeordnet. Falls Sie mithilfe der Dropdown-Liste "*Für Domäne:*" auf der Seite Empfänger- Optionen 115

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

benutzerdefinierte Optionen für die Domäne konfiguriert haben, dann werden diese Optionen auch auf das Benutzerkonto des Empfängers angewendet. Sie ersetzen die systemweiten Optionen. Das Web-Portal für sichere Nachrichten nutzt Branding und benutzerdefinierte Grafiken[136] der jeweiligen Domäne; diese werden den Empfängern beim Lesen der sicheren Nachrichten angezeigt. Domänen-Administratoren sehen nur die Benutzerkonten für Empfänger, die den Domänen zugeordnet sind, für die sie selbst Administratorrechte haben. Beachte: Wenn Benutzer unterschiedlicher lokaler Domänen sichere Nachrichten an denselben Empfänger senden, so hat der Empfänger für jede Domäne, der die Absender angehören, ein gesondertes Benutzerkonto.

E-Mail-Adresse
Dies ist die E-Mail-Adresse des Benutzerkontos für Empfänger. Sie wird zur Anmeldung am Web-Portal für sichere Nachrichten von SecurityGateway verwendet.

Vor- und Nachname
In dieses Feld tragen Sie den vollständigen Namen des Empfängers ein. Bei automatisch erstellten Benutzerkonten wird dieses Feld automatisch ausgefüllt, falls der Namen in der Empfängerkopfzeile To (An) der versandten sicheren Nachricht enthalten war.

Der Empfänger erhält eine Einladung und kann das Kennwort selbst festlegen
Sie können diese Option beim Erstellen eines Benutzerkontos für Empfänger sicherer Nachrichten verwenden. Der Empfänger erhält dann eine E-Mail-Nachricht mit einer Verknüpfung zum Web-Portal für die zugeordnete Domäne. Folgt er dieser Verknüpfung, so wird er dort aufgefordert, ein Kennwort für das Benutzerkonto zu erstellen. Wenn Sie diese Option für ein Benutzerkonto genutzt haben, wechselt sie automatisch zur weiter unten beschriebenen Option *Kennwort für Empfänger angeben*. Aktivieren Sie diese Option danach erneut, so wird die E-Mail-Nachricht erneut versandt.

Zum Einrichten des Benutzerkontos PIN verlangen
Diese Option bewirkt, dass der Empfänger bei Erstellung seines Kennworts die hier angegebene sechsstellige numerische PIN eingeben muss.

Diese PIN wird nicht in die Einladungsnachricht an den Empfänger aufgenommen. Sie muss dem Empfänger auf anderem Weg mitgeteilt werden. Sie sollte nicht per E-Mail sondern beispielsweise per Telefon übermittelt werden.

Kennwort für den Empfänger angeben
Mithilfe dieser Option können Sie das Kennwort für das Benutzerkonto angeben. Alle neuen Kennwörter müssen mindestens acht Zeichen lang sein und jedes der folgenden Elemente enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen (z.B. ;,_.?/-=)

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Einstellungen

Sie können die nachfolgend beschriebenen Optionen für das Benutzerkonto für Empfänger bearbeiten. Wählen Sie dazu den Empfänger aus, und klicken Sie dann in der Symbolleiste auf **Einstellungen**.

Optionen

Nachrichten für dieses Benutzerkonto nicht archivieren
Diese Option verhindert die Archivierung sicherer Nachrichten, die durch oder an dieses Benutzerkonto versandt werden.

Alle für dieses Benutzerkonto archivierten Nachrichten löschen
Durch Anklicken dieser Verknüpfung werden alle Nachrichten gelöscht, die für dieses Benutzerkonto für Empfänger archiviert sind.

Sprache:
Diese Option bestimmt die Sprache, in der durch das System erzeugte E-Mail-Nachrichten abgefasst sind. Die Benutzer können diese Einstellung über das Web-Portal für sichere Nachrichten selbst ändern. Eine Option gleichen Namens steht auf der Seite Empfänger-Optionen 115 zur Verfügung; mit dieser Option wird die Voreinstellung festgelegt.

Zahl der Elemente, die auf jeder Seite angezeigt werden:
Diese Option legt die Zahl der Nachrichten fest, die dem Empfänger jeder Bildschirmseite des Web-Portals höchstens angezeigt werden. Die Benutzer können diese Einstellung über das Web-Portal für sichere Nachrichten selbst ändern. Eine Option gleichen Namens steht auf der Seite Empfänger-Optionen 115 zur Verfügung; mit dieser Option wird die Voreinstellung festgelegt.

3.4.3 Empfänger-Optionen

Auf dieser Seite können Sie verschiedene Optionen und Voreinstellungen für die Benutzerkonten für Empfänger sicherer Nachrichten konfigurieren. Sie können außerdem bestimmen, welche Optionen die Empfänger über das Wen-Portal selbst konfigurieren dürfen.

Die weiter unten beschriebenen Optionen zum Anzeigen der Kennwörter, für vergessene Kennwörter und zur Speicherung der Anmeldung auf den Endgeräten bestimmen, ob die zugehörigen Steuerelemente auf der Anmeldeseite des Web-Portals für sichere Nachrichten angezeigt werden. Diese Optionen setzen jedoch voraus, dass die Empfänger das Portal über den richtigen URL aufrufen: `<SG-BASIS-URL>/SecurityGateway.dll?view=login_ex`. Ein Beispiel hierzu: "https://sg.firma.test:4443/securitygateway.dll?view=login_ex". Dieser URL wird für die Erstellung der Verknüpfung verwendet, die den Empfängern zum Einrichten ihrer Benutzerkonten übermittelt wird. Bei der Anmeldung als Empfänger sicherer Nachrichten wird ein Cookie gesetzt. Dieser Cookie bewirkt, dass Benutzer, die nur den Basis-URL von SecurityGateway (also den URL ohne den Zusatz "`view=login_ex`") aufrufen, dennoch auf das Web-Portal

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

für sichere Nachrichten umgeleitet werden. Benutzer, die den Basis-URL von Rechnern aus aufrufen, auf denen dieser Cookie nicht existiert, können sich zwar anmelden, es werden dann aber diese Elemente auf der Anmeldeseite durch die entsprechenden Optionen auf der Seite Einstellungen » Benutzerkonten » Benutzer-Optionen[73] gesteuert. Aus diesem Grund müssen Sie sicherstellen, dass alle etwa veröffentlichten URLs für die Empfänger sicherer Nachrichten den Teil "`/SecurityGateway.dll?view=login_ex`" enthalten.

Zugriffssteuerung

Empfänger dürfen ihre Kennwörter ändern
Per Voreinstellung dürfen die Benutzer des Web-Portals für sichere Nachrichten ihre Kennwörter über das Web-Portal ändern. Falls Sie den Benutzern diese Berechtigung entziehen wollen, deaktivieren Sie diese Option.

Symbol "Kennwort anzeigen" in Kennwortfeldern aktivieren
In jedem Kennwortfeld erscheint ein Symbol, das ein Auge darstellt. Klickt der Empfänger auf dieses Symbol, so kann er das Kennwort im Klartext sehen, das er soeben eingegeben hat. Falls Sie nicht wünschen, dass sich die Empfänger sicherer Nachrichten die eingegebenen Kennwörter im Klartext anzeigen lassen können, deaktivieren Sie diese Option.

Empfängern das Aktivieren der Zwei-Faktor-Authentifizierung gestatten
Die Zwei-Faktor-Authentifizierung stellt eine zusätzliche Sicherheitsmaßnahme dar, und sie verlangt bei der Anmeldung sowohl die Eingabe des Kennworts als auch eines besonderen Sicherheitskodes, der mithilfe einer Authenticator-App auf dem Smartphone des Benutzers erzeugt wird. Diese Option gestattet es den Empfängern, für ihre Benutzerkonten im Web-Portal die Zwei-Faktor-Authentifizierung zu aktivieren, um hierdurch die Anmeldung an ihren SecurityGateway-Benutzerkonten zusätzlich zu sichern. Ist diese Option aktiv, und meldet sich der Empfänger im Browser über eine sichere HTTPS-Verbindung an, so erscheinen die Optionen zur Zwei-Faktor-Authentifizierung[33]. Der Empfänger kann sie dann einrichten, falls er dies wünscht.

Aktivieren der Zwei-Faktor-Authentifizierung durch die Empfänger erzwingen
Diese Option macht die Nutzung der Zwei-Faktor-Authentifizierung bei der Anmeldung für alle Empfänger verpflichtend. Ist diese Option aktiv, so wird jeder Empfänger bei der ersten Anmeldung auf eine Seite zum Einrichten der Zwei-Faktor-Authentifizierung geleitet.

Speichern von Anmeldedaten durch Empfänger auf Endgeräten zulassen (erfordert HTTPS)
Ist diese Option aktiv, und stellt ein Empfänger eine durch HTTPS gesicherte Verbindung her, so erscheint auf der Anmeldeseite des Web-Portals für sichere Nachrichten die Option "*Anmeldung auf diesem Gerät speichern und beibehalten*". Aktiviert der Empfänger diese Option, so wird er automatisch angemeldet, wenn er von demselben Gerät aus wiederum eine Verbindung zum Web-Portal herstellt. Dies gilt jedoch nur, wenn der Empfänger sein Browserfenster schließt, ohne auf die Schaltfläche *Abmelden* zu klicken. Klickt der Empfänger auf die Schaltfläche *Abmelden*, so muss er sich beim nächsten Verbindungsaufbau erneut anmelden. Die Anmeldedaten werden für den Zeitraum gespeichert, der mithilfe der folgenden

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Option "*Empfänger für folgende Anzahl Tage speichern (1 bis 365)*" bestimmt wird. Nach Ablauf dieses Zeitraums muss er sich erneut anmelden. Diese Option ist per Voreinstellung abgeschaltet. **Beachte:** Bei Empfängern sicherer Nachrichten, auf deren Geräten oder in deren Browsern mithilfe der Option *Anmeldung auf diesem Gerät speichern und beibehalten* die Anmeldedaten gespeichert wurden, auf der Anmeldeseite des Web-Portals die Option "*Anmeldung auf diesem Gerät/in diesem Browser nicht speichern*". Sie können durch Anklicken dieser Option die Anmeldedaten von ihrem Endgerät löschen.

Empfänger für folgende Anzahl Tage speichern (1 bis 365)
Ist die Option *Speichern von Anmeldedaten durch Empfänger auf Endgeräten zulassen* aktiv, so steuert diese Option, für welchen Zeitraum die Anmeldung des Empfängers gespeichert wird, bevor er sich erneut anmelden muss. Die Voreinstellung für diesen Zeitraum beträgt 30 Tage.

Optionen zur Anmeldung

Verknüpfung "Kennwort vergessen" im Anmeldedialog anzeigen
Per Voreinstellung erscheint im Anmeldedialog des Web-Portals für sichere Nachrichten eine Verknüpfung "Kennwort vergessen", mit deren Hilfe sich die Empfänger eine Verknüpfung zum Ändern ihres Kennworts an die E-Mail-Adresse senden lassen können, die ihrem Benutzerkonto im Web-Portal zugeordnet ist. Falls Sie diese Verknüpfung ausblenden wollen, deaktivieren Sie diese Option.

Folgende Kontaktdaten für den Administrator auf der Anmeldeseite anzeigen
Mithilfe dieser Option können Sie Kontaktinformationen für den Administrator oder auch Verknüpfungen konfigurieren. Diese Inhalte werden auf der Anmeldeseite angezeigt. Der Text, den Sie in das Eingabefeld eintragen, kann auch HTML-Kode in bestimmtem Umfang enthalten, etwa Anker und Grafiken.

Voreinstellungen

Sprache:
Mithilfe dieser Dropdown-Liste können Sie die Sprache festlegen, in der der Server per Voreinstellung die durch das System erzeugten E-Mail-Nachrichten an Empfänger sicherer Nachrichten abfasst. Eine Option gleichen Namens steht auf der Seite Empfänger 113 zur Verfügung; mit dieser Option können Sie die Einstellung für einzelne Benutzer ändern. Sie erreichen diese Option, indem Sie auf der Seite Empfänger 113 den gewünschten Empfänger auswählen, und dann in der Symbolleiste auf **Einstellungen** klicken. Die Empfänger können diese Einstellungen über die Seite Einstellungen zum Benutzerkonto im Web-Portal auch selbst ändern.

Kennwörter mit Liste kompromittierter Kennwörter eines Drittanbieters abgleichen
SecurityGateway kann die Kennwörter der Empfänger mit einer Liste als kompromittiert bekannter Kennwörter abgleichen, die durch einen Drittanbieter bereit gestellt wird. Der Abgleich findet statt, ohne dass das Kennwort an den Anbieter übermittelt wird. Ist das Kennwort eines Empfängers in der Liste vorhanden, so bedeutet dies nicht, dass das Benutzerkonto kompromittiert oder gehackt wurde. Es bedeutet vielmehr, dass das fragliche Kennwort bereits einmal auf einem anderen System durch einen Benutzer verwendet wurde, und dass dieses verwendete Kennwort von einer Datenpanne oder einem Datenleck betroffen war. Kennwörter, die als kompromittiert bekannt und veröffentlicht sind, können durch Angreifer für Wörterbuchangriffe verwendet werden. Kennwörter, die noch nie auf anderen Systemen verwendet wurden, sind demgegenüber

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

sicherer. Nähere Informationen hierzu erhalten Sie in englischer Sprache unter Pwned Passwords.

Mithilfe des Dropdown-Menüs können Sie bestimmen, in welchem Intervall die Kennwörter mit der Liste abgeglichen werden sollen. Es stehen folgende Einstellungen zur Auswahl; sie bezeichnen jeweils den Zeitraum, der seit der letzten Prüfung vergangen sein muss, bevor eine neue Prüfung ausgeführt wird:

- Nie (Die Kennwörter werden nicht mit der Liste abgeglichen. Dies ist die Voreinstellung.)
- Ein Tag seit der letzten Prüfung
- Eine Woche seit der letzten Prüfung
- Ein Monat seit der letzten Prüfung

Zahl der Elemente, die auf jeder Seite angezeigt werden:
Diese Option legt die Voreinstellung für die Zahl der Nachrichten fest, die dem Empfänger jeder Bildschirmseite des Web-Portals höchstens angezeigt werden. Eine Option gleichen Namens steht auf der Seite Empfänger 113 zur Verfügung; mit dieser Option können Sie die Einstellung für einzelne Benutzer ändern. Sie erreichen diese Option, indem Sie auf der Seite Empfänger 113 den gewünschten Empfänger auswählen, und dann in der Symbolleiste auf **Einstellungen** klicken. Die Empfänger können diese Einstellungen über die Seite Einstellungen zum Benutzerkonto im Web-Portal auch selbst ändern.

Nutzungsbedingungen

Anmeldung durch Empfänger erst zulassen, wenn sie die folgenden Nutzungsbedingungen als verbindlich anerkannt haben
Diese Option bewirkt, dass Empfänger bei jeder Anmeldung bestimmte Nutzungsbedingungen oder andere Bedingungen anerkennen müssen. Sie können diese Nutzungsbedingungen in das Textfeld weiter unten eintragen. Die Empfänger können die Nutzungsbedingungen durch Aktivieren eines Kontrollkästchens während der Anmeldung anerkennen.

New Recipients

Warnmeldung an Globale Administratoren senden, sobald ein neuer Empfänger angelegt wird
Diese Option bewirkt, dass die globalen Administratoren 60 immer dann per E-Mail benachrichtigt werden, wenn ein neue Benutzerkonten für Empfänger sicherer Nachrichten erstellt wurden.

Kennwort des neuen Empfängers mit Liste kompromittierter Kennwörter eines Drittanbieters abgleichen
Per Voreinstellung werden alle neuen Kennwörter für neue Empfänger mit der Liste kompromittierter Kennwörter abgeglichen, die weiter oben unter *Kennwörter mit Liste kompromittierter Kennwörter eines Drittanbieters abgleichen* beschrieben ist. Falls Sie neue Kennwörter nicht mit dieser Liste abgleichen wollen, deaktivieren Sie diese Option.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Optionen dieser Domäne für die sicheren Nachrichten anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

3.4.4 Verfassen von Nachrichten

Diese Einstellung wird nach Domänen getrennt getroffen. Sie gestattet es den Empfängern sicherer Nachrichten der jeweiligen Domäne, neue Nachrichten an lokale Benutzer zu verfassen, die in einer besonderen Liste erfasst sind. Die Empfänger verfassen die Nachrichten dabei im Web-Portal für sichere Nachrichten und wählen die **Empfänger** aus einer Dropdown-Liste aus. **Beachte:** Empfänger sicherer Nachrichten können stets auf sichere Nachrichten antworten, die sie selbst erhalten haben.

Verfassen neuer Nachrichten

Empfänger sicherer Nachrichten dürfen neue Nachrichten an bestimmte lokale Empfänger verfassen
Mithilfe dieser Option können Sie den Empfängern, die einer Domäne zugeordnet sind 113, das Verfassen neuer Nachrichten gestatten. Wählen Sie hierzu die Domäne aus der Liste *Für Domäne:* aus, und aktivieren Sie diese Option. Die Benutzerkonten können dann Nachrichten an alle lokalen Adressen versenden, die Sie der Liste *Ausgewählte Adressen* weiter unten hinzugefügt haben. Falls Sie den Benutzerkonten einer Domäne das Verfassen neuer Nachrichten nicht gestatten wollen, deaktivieren Sie diese Option für die betroffene Domäne. In diesem Fall können die Empfänger nur auf sichere Nachrichten antworten, die sie selbst erhalten haben.

Verfügbare Adressen:
In dieser Liste sind die Benutzer der ausgewählten Domäne aufgeführt. Um einen Benutzer in die Liste der ausgewählten Adressen aufzunehmen, wählen Sie seine Adresse aus, und klicken Sie dann auf den Rechtspfeil.

Ausgewählte Adressen:
In dieser Liste sind die lokalen Adressen aufgeführt, an die die Empfänger sicherer Nachrichten in der ausgewählten Domäne neue Nachrichten senden dürfen.

3.5 Disclaimer (Kopftexte/Fußtexte)

Mithilfe der Optionen auf dieser Seite können Sie Ihre Disclaimer für Nachrichten verwalten. Disclaimer für Nachrichten sind Textbausteine, die der Server über den oder unter dem Nachrichtentext eingehender, abgehender und lokaler E-Mail-Nachrichten einfügen kann. Administratoren können mithilfe des Dialogs Disclaimer bearbeiten 120 Vorlagen für Disclaimer erstellen, die sowohl reinen Text als auch Standard-HTML und benutzerdefinierte Tags für SecurityGateway enthalten können. Die jeweilige Vorlage wird auf den Nachrichtentext sowohl des HTML- als auch des Nur-Text-Teils der E-Mail-Nachrichten angewendet, und die Vorlagen

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

können auf eine Domäne beschränkt oder systemweit angewandt werden. Für jeden Disclaimer wird ein Sieve-Skript[284] erstellt, das die Vorlage in der gewünschten Form in die Verarbeitung der Nachrichten einbezieht. Die Sieve-Skripte können auch direkt über den Konfigurationsdialog für Sieve-Skripte erstellt werden.

In der Übersicht über die Disclaimer wird ein Eintrag pro Zeile angezeigt. Er enthält die sieben Spalten Aktiviert, Beschreibung, Typ, eingehend, abgehend, lokal und Domäne. Nähere Informationen über diese Spalten und über das Erstellen und Bearbeiten von Disclaimern finden Sie in der Beschreibung des Konfigurationsdialogs Disclaimer bearbeiten[120].

Die Symbolleiste am oberen Seitenrand enthält die folgenden vier Optionen:

Neu
Um einen neuen Disclaimer anzulegen, klicken Sie auf *Neu*. Es öffnet sich der Dialog Disclaimer hinzufügen, der dem Dialog Disclaimer bearbeiten entspricht.

Bearbeiten
Um den gerade in der Liste ausgewählten Eintrag zu bearbeiten, klicken Sie in der Symbolleiste auf Bearbeiten. Es öffnet sich der Dialog Disclaimer bearbeiten[120]. Sie können diesen Dialog auch durch Doppelklick auf einen Eintrag aufrufen.

Löschen
Um einen oder mehrere Disclaimer zu löschen, wählen Sie die Einträge in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Disclaimer wirklich löschen wollen. Sie können mehrere Einträge auswählen, indem Sie während des Anklickens der Einträge die Strg-Taste oder die Hochschalttaste gedrückt halten.

Für Domäne
Mithilfe des Auswahlfeldes *Für Domäne:* können Sie die Domäne auswählen, deren Disclaimer in der Liste angezeigt werden sollen. Per Voreinstellung werden alle Disclaimer angezeigt. Sie können stattdessen "-- Global --" auswählen, um nur die systemweit gültigen Disclaimer anzuzeigen, oder Sie können eine Domäne auswählen, um nur die Disclaimer für diese Domäne anzuzeigen. Per Voreinstellung werden alle Disclaimer angezeigt, unabhängig davon, ob sie sich auf eine Domäne beziehen oder systemweit gültig sind.

3.5.1 Disclaimer bearbeiten

Mithilfe des Dialogs Disclaimer bearbeiten, den Sie auf der Seite Disclaimer für Nachrichten[119] durch Anklicken von *Neu* oder *Bearbeiten* erreichen, können Sie Vorlagen für Ihre Disclaimer für Nachrichten erstellen und bearbeiten. In diesem Dialog können Sie Disclaimer aktivieren und deaktivieren, einer bestimmten Domäne zuordnen, den Typ der Disclaimer bestimmen (Kopfzeile, Fußtext oder Benutzerdefiniert) und festlegen, auf welche Arten von Nachrichten der Disclaimer angewendet wird - eingehende, abgehende oder lokale Nachrichten.

Dieser Disclaimer ist deaktiviert.
Mithilfe dieses Kontrollkästchens können Sie den Disclaimer deaktivieren. Der Disclaimer erscheint dann zwar noch in der Liste derDisclaimer für Nachrichten[119], SecurityGateway fügt ihn aber nicht mehr in Nachrichten ein. Um den Disclaimer wieder nutzen zu können, deaktivieren Sie das Kontrollkästchen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Dieser Disclaimer gehört zu folgender Domäne:
Mithilfe dieses Auswahlmenüs können Sie den Disclaimer einer bestimmten SecurityGateway-Domäne zuordnen. Falls Sie ihn auf alle Domänen anwenden wollen, wählen Sie den Eintrag *Global*.

Beschreibung

Beschreibung
In dieses Textfeld können Sie einen Namen oder eine Beschreibung für den Disclaimer eintragen. Dieser Eintrag dient nur zu Ihrer Information und erscheint in der Liste der Disclaimer für Nachrichten.

Typ

Hier legen Sie den Typ des Disclaimers fest: Kopfzeile, Fußtext oder Benutzerdefiniert.

Kopfzeile
Wählen Sie die Option *Kopfzeile* aus, falls Sie den Disclaimer am Beginn der Nachricht über dem Nachrichtentext einfügen wollen.

Fußtext
Wählen Sie die Option *Fußtext* aus, falls Sie den Disclaimer am Ende der Nachricht unterhalb des Nachrichtentexts einfügen wollen.

Benutzerdefiniert
Wählen Sie die Option *Benutzerdefiniert* aus, falls Sie einen benutzerdefinierten Disclaimer erstellen und dabei die besonderen Tags von SecurityGateway nutzen wollen, die weiter unten erläutert werden. Durch einen benutzerdefinierten Disclaimer können Sie Text sowohl über als auch unter dem Nachrichtentext einfügen. Alle benutzerdefinierten Disclaimer müssen den Tag "`<sg:ORIGINAL_BODY>`" enthalten.

Regeln

Mithilfe der folgenden Optionen bestimmen Sie, in welche Arten von Nachrichten der Disclaimer eingefügt werden soll.

Disclaimer in eingehende Nachrichten einfügen
Diese Option bewirkt, dass der Disclaimer in alle eingehenden Nachrichten eingefügt wird, die an die oben ausgewählte Domäne gerichtet sind. Falls Sie für diesen Disclaimer den Eintrag Global ausgewählt haben, wird der Disclaimer in alle eingehenden Nachrichten unabhängig davon eingefügt, an welche Domäne sie gerichtet sind.

Disclaimer in abgehende Nachrichten einfügen
Diese Option bewirkt, dass der Disclaimer in alle abgehenden Nachrichten eingefügt wird, die aus der oben ausgewählten Domäne versandt werden. Falls Sie für diesen Disclaimer den Eintrag Global ausgewählt haben, wird der Disclaimer in alle abgehenden Nachrichten unabhängig davon eingefügt, aus welcher Domäne sie versandt werden.

Disclaimer in lokale Nachrichten einfügen
Diese Option bewirkt, dass der Disclaimer in Nachrichten eingefügt wird, die aus der oben ausgewählten Domäne versandt werden und gleichzeitig an sie gerichtet

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

sind. Der Disclaimer würde beispielsweise in eine Nachricht von `frank@example.com` eingefügt werden, falls sie an `hmudd@example.com` gerichtet wäre, nicht jedoch würde er in eine Nachricht von `frank@example.com` an `biff@example.net` eingefügt werden. Falls Sie für diesen Disclaimer den Eintrag Global ausgewählt haben, wird der Disclaimer in die lokalen Nachrichten aller Domänen eingefügt.

Text

In diesem Eingabefeld können Sie den Inhalt der Vorlage für Ihren Disclaimer eintragen und den Disclaimer als Nur-Text- oder HTML-Disclaimer konfigurieren. Vorlagen im Nur-Text-Format dürfen nur Text enthalten; HTML-Vorlagen dürfen hingegen HTML-Kode und die besonderen Tags von SecurityGateway enthalten, die weiter unten erläutert werden.

Nur-Text (HTML-Zeichen werden wörtlich übernommen)
Per Voreinstellung wird der Disclaimer im Format Nur-Text gebildet. Ist diese Option aktiv, so wird in die Nachrichten nur reiner Text eingefügt, und zwar auch dann, wenn dieser Text HTML-Kode enthält. Alle HTML-Tags und -Steuerzeichen werden direkt als reiner Text umgesetzt und in diesem Format in die Nachrichten eingefügt. So wird beispielsweise der Text "`<b>Mein Disclaimer</b>`" in genau diesem Format eingefügt; die HTML-Tags werden nicht etwa in Fettschrift umgesetzt oder aus dem Text entfernt. Falls Sie einen Disclaimer im Format Nur-Text erstellen, dürfen Sie daher HTML-Kode nicht verwenden.

Disclaimer, für die Sie den Typ *Benutzerdefiniert* ausgewählt haben, dürfen den Tag "`<sg:ORIGINAL_BODY>`" auch dann enthalten, wenn sie im Format Nur-Text verfasst wurden. Der Tag gestattet es, den Nachrichtentext der jeweiligen Nachricht an einer beliebigen Stelle in die Vorlage einzufügen. Alle anderen Tags und alle HTML-Kodes erscheinen als reiner Text und werden nicht ausgewertet oder umgesetzt.

Ein Beispiel für einen Fußtext im Format Nur-Text:

```
-------------------------------------------
Die Ansichten, die in dieser Nachricht ge-
äußert werden, entsprechen nicht unbedingt
denen von example.com und den verbundenen
Unternehmen.
-------------------------------------------
```

Ein Beispiel für eine benutzerdefinierte Vorlage im Format Nur-Text:

```
Die folgende Nachricht wurde durch einen
Mitarbeiter von example.com versandt.
--
<sg:ORIGINAL_BODY Field="body:all">{Original Email}
</sg:ORIGINAL_BODY>
-------------------------------------------
Die Ansichten, die in dieser Nachricht ge-
äußert werden, entsprechen nicht unbedingt
denen von example.com und den verbundenen
Unternehmen.
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

```
-----------------------------------------
```

HTML-Vorlagen

Falls Sie für den Disclaimer eine Vorlage auf HTML-Basis erstellen wollen, deaktivieren Sie die Option *Nur Text*. HTML-Vorlagen dürfen HTML-Kode und die besonderen Tags von SecurityGateway enthalten, die weiter unten erläutert sind.

Ein Beispiel für eine HTML-Vorlage für einen Kopftext:

```
<HTML><HEAD>
<style type="text/css">
.blueboldtext { font-family: Geneva, fixed-width; font-size: 13;
color: #114477; font-weight: bold; }
</style></HEAD>
<BODY>
<DIV>Dies ist mein Kopftext!</DIV>
<sg:HTML_ONLY><span class="blueboldtext">Dieser Text wird nur im
HTML-Body angezeigt!</span></sg:HTML_ONLY>
<sg:TEXT_ONLY>Dieser Text wird nur im Nur-Text-Body
angezeigt!</sg:TEXT_ONLY>
<BR>
-------------<br />
</BODY></HTML>
```

Ein beispiel für eine benutzerdefinierte HTML-Vorlage:

```
<DIV> </DIV>
<DIV>Dies ist mein Kopftext!</DIV>
<br />---------</DIV>
<sg:ORIGINAL_BODY Field="body:all">{Original Email}
</sg:ORIGINAL_BODY>
<br />---------</DIV>
<DIV>Dies ist mein Fußtext!</DIV>
<DIV> </DIV>
<DIV>Dieser Text wird im HTML- und Nur-Text-Body angezeigt!<br />
<sg:HTML_ONLY>Dieser Text wird nur im HTML-Body
angezeigt!</sg:HTML_ONLY>
<sg:TEXT_ONLY>Dieser Text wird nur im Nur-Text-Body
angezeigt!</sg:TEXT_ONLY></DIV>
```

Sie müssen die Tags HTML, HEAD oder BODY nicht unbedingt in die Vorlage für den Disclaimer einfügen. Falls Sie sie einfügen, werden sie mit den entsprechenden Tags in jeder einzelnen E-Mail-Nachricht verschmolzen.

Tags von SecurityGateway

SecurityGateway unterstützt drei benutzerdefinierte Tags für die Verwendung in den Vorlagen für Disclaimer. Alle drei Tags können, unabhängig von dem Typ der Vorlage, in HTML-Vorlagen verwendet werden. In benutzerdefinierten Vorlagen des Formats Nur-Text ist nur der Tag "`<sg:ORIGINAL_BODY>`" zugelassen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

<sg:ORIGINAL_BODY></sg:ORIGINAL_BODY>
Dieser Tag bestimmt die Stelle in der Vorlage, an der der ursprüngliche Nachrichtentext eingefügt wird. Der Tag wird automatisch an der richtigen Stelle eingefügt, falls Sie für einen Disclaimer den Typ Kopfzeile oder Fußtext auswählen. Bei Verwendung des Typs Benutzerdefiniert müssen Sie den Tag von Hand an der Stelle einfügen, an der der Nachrichtentext erscheinen soll. Bei Verwendung benutzerdefinierter Sieve-Skripte 284 kann der Tag an einer beliebigen Stelle eingefügt werden, er muss aber vorhanden sein.

Dieser Tag ist in allen Typen der HTML-Vorlagen für Disclaimer zugelassen: Kopfzeile, Fußtext und Benutzerdefiniert. Der Nachrichtentext erscheint, unabhängig von dem gewählten Typ, immer an der Stelle, die dieser Tag bestimmt. Bei Verwendung von Vorlagen im Format Nur-Text ist dieser Tag nur für Vorlagen des Typs Benutzerdefiniert zugelassen.

<sg:HTML_ONLY></sg:HTML_ONLY>
Inhalte, die in diesen Tag gefasst werden, erscheinen im HTML-Teil der Nachricht (dem sog. HTML-Body), nicht aber im Nur-Text-Teil (dem sog. Text-Body). Dieser Tag darf in Vorlagen für Disclaimer im Format *Nur-Text* nicht verwendet werden.

<sg:TEXT_ONLY></sg:TEXT_ONLY>
Inhalte, die in diesen Tag gefasst werden, erscheinen nur im Nur-Text-Teil der Nachricht (dem sog. Text-Body), nicht aber im HTML-Teil (dem sog. HTML-Body). Dieser Tag darf in Vorlagen für Disclaimer im Format *Nur-Text* nicht verwendet werden.

Sieve-Skript

Mithilfe des Editors für Sieve-Skripte 284 können Sie einen benutzerdefinierte Disclaimer selbst erstellen. Die Bedingungen, unter denen ein solcher Disclaimer aktiviert und damit wirksam wird, entsprechen denen für alle anderen Sieve-Skripte. Bei Nutzung des Sieve-Editors müssen einige Zeichen mit sog. Escape-Sequenzen versehen werden. Das nachfolgende Sieve-Skript ist ein Beispiel für einen benutzerdefinierten Disclaimer:

```
require ["securitygateway","body"];

if allof(body :text :contains "Jetzt Geld verdienen!")
{
disclaimer "text:
<HTML xmlns:sg = \"http://www.altn.com/Products/SecurityGateway-
Email-Firewall/\">
<HEAD><META http-equiv=\"Content-Type\" content=\"text/html;
charset=UTF-8\" />
</HEAD>
<BODY>
<DIV>Dies ist mein Kopftext!</DIV>
<DIV>Dies ist eine weitere Zeile meines Kopftextes!</DIV>
<DIV> </DIV>
<DIV>---------<br />
<sg:ORIGINAL_BODY Field=\"body:all\">{Original Email}
</sg:ORIGINAL_BODY>
<br />---------</DIV>
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

```
<DIV> </DIV>
<DIV>Dies ist mein Fußtext!</DIV>
<DIV>Dies ist eine weitere Zeile meines Fußtextes!</DIV>
<DIV> </DIV>
<DIV>Dieser Text wird im HTML- und Nur-Text-Body angezeigt!<br />
<sg:HTML_ONLY>Dieser Text wird nur im HTML-Body
angezeigt!</sg:HTML_ONLY>
<sg:TEXT_ONLY>Dieser Text wird nur im Nur-Text-Body
angezeigt!</sg:TEXT_ONLY></DIV>
</BODY></HTML> ."
; }
```

3.6 System

Der Abschnitt System im Menü *Einstellungen/Benutzer* enthält Verknüpfungen mit den folgenden System-bezogenen Funktionen:

Verschlüsselung 126—Auf dieser Seite werden die verschiedenen Einstellungen zur Verschlüsselung konfiguriert. SecurityGateway unterstützt das Protokoll Secure Sockets Layer (SSL) mit der SMTP-Erweiterung STARTTLS. Hierdurch wird verhindert, dass Dritte Ihren Mailverkehr abfangen und mitlesen. SecurityGateway unterstützt auch HTTPS und stellt damit einen entsprechenden Schutz für die Web-Schnittstelle bereit.

HTTP-Server 132—Auf der Seite HTTP-Server werden verschiedene Einstellungen für die Web-Schnittstelle von SecurityGateway vorgenommen. Sie können den Hostnamen bestimmen, der für die Verknüpfungen mit der Anmeldeseite verwendet wird, die SecurityGateway erstellt; außerdem können Sie die HTTP- und HTTPS-Ports festlegen und weitere HTTP-bezogene Einstellungen vornehmen.

Branding/Benutzerdefinierte Grafiken 136—Auf dieser Seite finden Sie Optionen für die Anpassung der Banner-Grafiken, die im Anmeldedialog und im Navigationsbereich erscheinen.

Verzeichnisse 134—Auf dieser Seite sind die Verzeichnisse aufgeführt, in denen SecurityGateway verschiedene Arten von Dateien ablegt. Sie können die Verzeichnisse und Speicherorte anpassen, indem Sie die entsprechenden Einträge auf dieser Seite bearbeiten.

Speicherplatz 135—Auf der Seite Speicherplatz wird die Überwachung des freien Festplatten-Speicherplatzes durch SecurityGateway konfiguriert. Sie enthält Optionen, mit deren Hilfe eine Warnmeldung an die Administratoren gesandt sowie Empfang und Versand von Nachrichten eingestellt werden können, falls der freie Speicherplatz zur Neige geht.

Konfiguration anzeigen 137—Auf dieser Seite werden alle Einstellungen Ihrer aktuellen SecurityGateway-Konfiguration gesammelt angezeigt. Diese Funktion ist besonders für die Diagnose von Konfigurationsproblemen in Ihrer SecurityGateway-Installation hilfreich, und sie kann beim Kontakt mit dem technischen Support weiterhelfen. Von dieser Seite aus kann die Konfiguration auch in eine XML-Datei gespeichert werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

3.6.1 Verschlüsselung

SecurityGateway enthält die neueste Verschlüsselungstechnik, um Ihre Daten zu schützen. Das Protokoll Secure Sockets Layer (SSL) — auch bekannt unter Transport Layer Security (TLS) — mit der SMTP-Erweiterung STARTTLS verhindert, dass Dritte Ihren E-Mail-Verkehr abfangen und mitlesen. Durch HTTPS bietet SecurityGateway einen vergleichbaren Schutz für die Web-Schnittstelle.

Das SSL-Protokoll wurde durch die Netscape Communications Corporation entwickelt und ist die Standard-Methode zur Sicherung der Kommunikation zwischen Servern und Clients über das Internet. Es bietet in TCP/IP-Verbindungen die Echtheitsbestätigung für den Server, Datenverschlüsselung und, wahlweise, die Echtheitsbestätigung für den Client. Da SSL bereits in alle aktuellen und gängigen Browser eingebunden ist, genügt es, ein gültiges digitales Zertifikat auf dem Server zu installieren, um die SSL-Funktionen im Browser beim Verbindungsaufbau mit SecurityGateway zu aktivieren. Für Verbindungen von Mailclients unterstützt SecurityGateway die SMTP-Erweiterung STARTTLS über SSL/TLS. In diesem Fall müssen Sie aber zunächst Ihren Client für die Nutzung von SSL konfigurieren, und der Client muss diese Erweiterung unterstützen. Die meisten Mailclients, jedoch nicht alle, unterstützen diese Erweiterung.

E-Mail- und HTTPS-Verschlüsselung

Unterstützung für SSL und STARTTLS für SMTP und HTTPS aktivieren
Um die Unterstützung für das Protokoll SSL/TLS mit der Erweiterung STARTTLS zu aktivieren, aktivieren Sie dieses Kontrollkästchen. Es wird dann das Zertifikat genutzt, das im Abschnitt Zertifikat auswählen weiter unten als "Aktiv" gekennzeichnet ist. Eine Anmeldung an SecurityGateway durch HTTPS über die verschlüsselte Web-Schnittstelle ist nur möglich, wenn diese Option und ein gültiges Zertifikat aktiv sind. Die Option ist per Voreinstellung abgeschaltet.

Nachrichten mit STARTTLS versenden, soweit möglich
Diese Option bewirkt, dass SecurityGateway bei jeder Nachricht, die über SMTP versendet wird, versucht, die Erweiterung STARTTLS zu nutzen. Unterstützt der Server der Gegenstelle STARTTLS nicht, so wird die Nachricht ohne SSL normal zugestellt. Diese Option ist per Voreinstellung abgeschaltet.

Nach Fehlern in der SSL-Protokollaushandlung Übermittlung bis zu eine Stunde lang ohne SSL versuchen
Diese Option bewirkt, dass Gegenstellen, bei denen während der SMTP-Verbindung ein SSL-Fehler auftritt, vorübergehend in die Weiße Liste aufgenommen werden. Die Weiße Liste wird jede Stunde zurückgesetzt.

REQUIRETLS (RFC 8689) aktivieren
Mithilfe von RequireTLS können Sie festlegen, welche Nachrichten **zwingend** über TLS-geschützte Verbindungen übermittelt werden müssen. Steht TLS für die Übermittlung einer solchen Nachricht nicht zur Verfügung, oder sind die Parameter, die während des TLS-Verbindungsaufbaus und für die beteiligten Zertifikate übermittelt werden, nicht akzeptabel, so werden die Nachrichten zurückgeleitet und nicht etwa ohne TLS zugestellt. Eine vollständige Beschreibung für RequireTLS finden Sie in englischer Sprache in dem RFC-Dokument RFC 8689: SMTP Require TLS Option.

RequireTLS ist per Voreinstellung aktiv. Es wirkt jedoch nur auf solche Nachrichten, die aufgrund der neuen Aktion des Inhaltsfilters 258 *"Nachricht für REQUIRETLS kennzeichnen"* ausdrücklich entsprechend gekennzeichnet werden,

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

oder die an nach dem Schema `<Postfach>+requiretls@Domäne.tld` aufgebaute E-Mail-Adressen (z.B. `arvel+requiretls@mdaemon.com`) versandt werden. Alle anderen Nachrichten werden so verarbeitet, als ob das Leistungsmerkmal nicht aktiv wäre. Nachrichten, für die RequireTLS aktiv ist, können nur dann erfolgreich versandt werden, wenn bestimmte Bedingungen alle erfüllt sind. Ist auch nur eine Bedingung nicht erfüllt, so werden die Nachrichten nicht etwa über eine unverschlüsselte Verbindung übermittelt sondern an den Absender zurückgeleitet. Folgende Bedingungen sind zu erfüllen:

- RequireTLS muss aktiv sein.
- Die Nachricht muss so gekennzeichnet sein, dass für sie die RequireTLS-Anforderungen einschlägig sind. Dies kann entweder über eine Aktion des Inhaltsfilters oder über den Versand an eine Empfängeradresse nach dem Schema "`<Postfach>+requiretls@...`" geschehen.
- Der MX-Eintrag der Domäne des Empfängers muss mithilfe von MTA-STS versehen sein.
- Die Verbindung mit dem Mailserver des Empfängers muss mithilfe von SSL (STARTTLS) gesichert sein.
- Das SSL-Zertifikat des empfangenden Hosts muss mit dem MX-Hostnamen übereinstimmen und eine Vertrauenskette zu einer vertrauenswürdigen Stammzertifizierungsstelle (CA) aufweisen.
- Der Mailserver des Empfängers muss REQUIRETLS unterstützen und dies in der Antwort auf den Befehl EHLO bekannt geben.
- Alle vorstehenden Bedingungen müssen erfüllt sein, da sonst die Nachricht nicht zugestellt sondern an den Absender zurückgeleitet wird.

MTA-STA (RFC 8461) aktivieren
Das Leistungsmerkmal MTA-STS ist per Voreinstellung aktiv. Eine vollständige Beschreibung für MTA-STS finden Sie in englischer Sprache in dem RFC-Dokument RFC 8461: SMTP MTA Strict Transport Security (MTA-STS).

Das Verfahren SMTP MTA Strict Transport Security (abgekürzt MTA-STS, Verfahren für erzwungene Transportverschlüsselung für SMTP-Mailserver) gestattet es Anbietern von E-Mail-Dienstleistungen, bekannt zu geben, dass sie durch Transport Layer Security (TLS) transportverschlüsselte SMTP-Verbindungen unterstützen. Darüber hinaus können sie festlegen, ob SMTP-Server, die Nachrichten an sie übermitteln wollen, die Übermittlung von Nachrichten an solche MX-Hosts ablehnen sollen, die TLS mit einem vertrauenswürdigen Server-Zertifikat nicht unterstützen.

Um MTA-STS für Ihre eigene Domäne zu konfigurieren, ist zunächst eine Richtliniendatei erforderlich. Diese Richtliniendatei muss über HTTPS von einem URL abrufbar sein, der nach dem Schema https://mta-sts.Domäne.TLD/.well-known/mta-sts.txt gebildet ist. An die Stelle "Domäne.TLD" ist dabei Ihr eigener Domänenname zu setzen. Der Inhalt der Richtliniendatei muss Einträge des folgenden Formats enthalten:

```
version: STSv1
mode: testing
mx: mail.domain.tld
max_age: 86400
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Als "mode" (Modus) können Sie "none" (kein MTA-STS), "testing" (MTA-STS im Versuchsbetrieb) und "enforce" (Richtlinie ist verpflichtend) einsetzen. Für jeden Ihrer MX-Hostnamen soll eine eigene Zeile "mx" enthalten sein. Subdomänen können Sie durch Jokerzeichen erfassen, etwa "*.Domäne.TLD". Der Gültigkeitszeitraum für den Eintrag (max_age) wird in Sekunden angegeben. Häufig verwendete Werte hierfür sind 86400 (dies entspricht einem Kalendertag) und 604800 (dies entspricht einer Woche).

Weiter ist ein DNS-Eintrag des Typs TXT erforderlich. Dieser Eintrag muss unter _mta-sts.Domäne. TLD abrufbar sein. An die Stelle "Domäne.TLD" ist dabei Ihr eigener Domänenname zu setzen. Der Eintrag muss dem folgenden Format entsprechen:

```
v=STSv1; id=20200206T010101;
```

Der Wert der "id" muss immer dann geändert werden, wenn sich der Inhalt der Richtliniendatei ändert. Es ist üblich, als "id" einen Zeitstempel zu verwenden.

TLS-Berichte (RFC 8460) aktivieren
Die Erstellung der TLS-Berichte ist per Voreinstellung abgeschaltet. Eine vollständige Beschreibung für die TLS-Berichte finden Sie in englischer Sprache in dem RFC-Dokument RFC 8460: SMTP TLS Reporting.

Mithilfe des Leistungsmerkmals zur Berichterstellung über SMTP TLS ("TLS-Berichte") können Domänen, die MTA-STS einsetzen, Benachrichtigungen erhalten, falls der Abruf der Richtliniendatei für MTA-STS oder die Herstellung einer verschlüsselten Verbindung mittels STARTTLS fehlschlagen. Wenn dieses Leistungsmerkmal aktiv ist, sendet SecurityGateway einmal täglich einen Bericht an alle Domänen, an die SecurityGateway während des zurückliegenden Tages Nachrichten versandt oder zu versenden versucht hat, und für die MTA-STS aktiv ist. Die Informationen, die in diese Berichte aufgenommen werden sollen, können mithilfe mehrerer Optionen bestimmt werden.

Wenn Sie dieses Leistungsmerkmal aktivieren, müssen Sie sicherstellen, dass auch die Signatur abgehender Nachrichten über DKIM 199 aktiv ist, und Sie müssen einen DNS-Eintrag des Typs TXT erstellen. Dieser Eintrag muss unter `_smtp._tls.Domäne.tld` abrufbar sein. An die Stelle "Domäne.TLD" ist dabei Ihr eigener Domänenname zu setzen. Der Eintrag muss dem folgenden Format entsprechen:

```
v=TLSRPTv1; rua=mailto:Postfach@Domäne.tld
```

An die Stelle "Postfach@Domäne.TLD" müssen Sie die E-Mail-Adresse setzen, an die die Berichte für Ihre Domäne gesandt werden sollen.

Zertifikat auswählen

In diesem Abschnitt sind alle SSL-Zertifikate aufgeführt, die Sie angelegt haben. SecurityGateway erstellt Zertifikate mit einer Eigensignatur. Dies bedeutet, dass der Ersteller des Zertifikats, auch Certificate Authority (CA) genannt, dem Eigentümer des Zertifikats entspricht. Diese Vorgehensweise ist zulässig, es ist aber möglich, dass manche Benutzer beim Verbindungsaufbau über den HTTPS-URL von SecurityGateway gefragt werden, ob sie die Verbindung mit der Ziel-Site aufbauen und/oder das Zertifikat installieren wollen. Diese Abfrage erscheint, weil die CA, die das Zertifikat erstellt hat, bei den Benutzern noch nicht in die Liste der vertrauten CAs eingetragen ist. Installiert ein Benutzer das Zertifikat, und stuft er die SecurityGateway-Domäne als eine vertrauenswürdige CA ein, so

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

erscheinen die Warnmeldungen beim Verbindungsaufbau nicht mehr. Ob die Warnmeldungen überhaupt angezeigt werden, und ob die Benutzer überhaupt besondere Maßnahmen treffen müssen, hängt unter anderem von dem verwendeten Browser und seinen Sicherheitseinstellungen ab.

SSL-Zertifikate erstellen
Um ein neues Zertifikat zu erstellen, klicken Sie am oberen Rand des Abschnitts Zertifikat auswählen auf Neu. Hierdurch öffnet sich das Dialogfenster SSL-Zertifikat 129. Um ein bestehendes Zertifikat zu löschen, wählen Sie das Zertifikat, und klicken Sie auf *Löschen*.

SSL-Zertifikat aktivieren
Um ein SSL-Zertifikat zu aktivieren, klicken Sie auf die Verknüpfung "Aktivieren", die zu dem gewünschten Eintrag gehört.

Weiße Liste für STARTTLS

Mithilfe dieser Option können Sie IP-Adressen, Hosts und Domänennamen erfassen, die von der Nutzung von STARTTLS ausgenommen sind. STARTTLS wird beim Versand an eine hier erfasste Gegenstelle nicht genutzt. STARTTLS wird auch bei eingehenden Verbindungen von Hosts und IP-Adressen auf dieser Liste nicht als verfügbares Protokoll gemeldet.

Pflichtliste für STARTTLS

Mithilfe dieser Option können Sie Hosts und IP-Adressen erfassen, für die die Nutzung von STARTTLS zwingend erforderlich ist. Ist STARTTLS nicht verfügbar, oder tritt ein Fehler auf, so wird die jeweilige Nachricht nicht an die Gegenstelle übermittelt.

SSL-Zertifikat

Dieses Dialogfenster wird für die Erstellung neuer SSL-Zertifikate genutzt. Um ein neues Zertifikat anzulegen, klicken Sie auf der Seite Verschlüsselung 126 in der Symbolleiste des Abschnitts Zertifikat auswählen auf *Neu*, und geben Sie dann die Daten für das Zertifikat ein. Nachdem Sie die Eingabe beendet haben, klicken Sie auf *Speichern und Beenden*, um das Zertifikat zu erzeugen.

Zertifikat erstellen

Host-Name
Tragen Sie hier den Hostnamen ein, zu dem Ihre Benutzer eine Verbindung herstellen (z.B. "mail.example.com").

Name der Organisation/Firma
Tragen Sie hier den Namen oder Organisation oder die Firma des "Eigentümers" des Zertifikats ein.

Alternative Hostnamen (mehrere Einträge durch Kommata trennen)
SecurityGateway unterstützt keine getrennten Zertifikate für jede Domäne — vielmehr müssen sich alle Domänen ein Zertifikat teilen. Falls die Benutzer auch zu anderen Hostnamen Verbindungen herstellen, und falls das Zertifikat auch für diese Hostnamen gültig sein soll, so müssen diese Domänennamen hier eingetragen und durch Kommata von einander getrennt werden. Jokerzeichen, wie etwa "`*.example.com`", sind zulässig.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Schlüssellänge
Wählen Sie hier die gewünschte Schlüssellänge aus, die der Schlüssel für das Zertifikat erhalten soll. Je länger der Schlüssel ist, desto sicherer sind die übermittelten Daten. Bitte beachten Sie aber, dass manche Anwendungen Schlüssel mit einer Länge über 512 nicht unterstützen.

Land/Region
Wählen Sie das Land oder die Region aus, in der sich Ihr Server befindet.

Nutzung eines Zertifikats eines anderen Ausstellers

Auch ein gekauftes oder sonst von einer anderen Stelle als SecurityGateway ausgestelltes Zertifikat kann verwendet werden. Es muss dazu mithilfe der Microsoft-Management-Konsole in den Zertifikatsspeicher eingelesen werden, den SecurityGateway verwendet. Sobald das Zertifikat in den Windows-Zertifikatsspeicher importiert wurde, sollte es in SecuritGateway sichtbar sein und damit genutzt werden können. Um ein Zertifikat zu importieren, gehen Sie folgendermaßen vor:

1. Klicken Sie in der Windows-Taskleiste auf **Start** » **Ausführen...,** und geben Sie in das Textfeld "**mmc /a**" ein.

2. Klicken Sie auf **OK,** oder drücken Sie die **Eingabetaste**.

3. Klicken Sie in der Microsoft Management Console in der Menüleiste auf **Datei** » **Snap-In hinzufügen/entfernen...** (oder drücken Sie **Strg+M**).

4. Klicken Sie auf der Registerkarte Eigenständig auf **Hinzufügen...**

5. Klicken Sie im Konfigurationsdialog *Eigenständiges Snap-In hinzufügen* auf **Zertifikate** und dann auf **Hinzufügen**.

6. Im Konfigurationsdialog *Zertifikat Snap-In* wählen Sie **Computerkonto**, und klicken Sie dann auf **Weiter**.

7. Im Konfigurationsdialog *Computer auswählen* wählen Sie **Lokalen Computer**, und klicken Sie dann auf **Fertig stellen**.

8. Klicken Sie auf **Schließen**, und klicken Sie auf **OK**.

9. Ist das Zertifikat, das Sie importieren, eigensigniert, so klicken Sie unter *Zertifikate (Lokaler Computer)* im rechten Bereich des Fensters auf **Vertrauenswürdige Stammzertifizierungsstellen** und dann auf **Zertifikate**. Falls es nicht eigensigniert ist, klicken Sie auf **Eigene Zertifikate**.

10. Klicken Sie in der Menüleiste auf **Aktion** » **Alle Aufgaben** » **Importieren...** und dann auf **Weiter**.

11. Geben Sie Pfad und Dateinamen zu dem Zertifikat an, das Sie importieren wollen (navigieren Sie nötigenfalls mithilfe von Durchsuchen), und klicken Sie auf **Weiter**.

12. Klicken Sie erneut auf **Weiter,** dann klicken Sie auf **Fertig stellen**.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nutzung von Let's Encrypt zur Verwaltung Ihres Zertifikats

Um SSL/TLS und HTTPS[126] für SecurityGateway nutzen zu können, benötigen Sie ein SSL/TLS-Zertifikat[129]. Diese Zertifikate sind kleine Dateien, die durch Zertifizierungsstellen, die auch als Certificate Authority (kurz CA) bezeichnet werden[130], ausgestellt werden. Sie dienen dem Client oder Browser dazu, zu prüfen, ob er wirklich mit dem gewünschten Server verbunden ist, und zur Verschlüsselung der Verbindung mit diesem Server über SSL, TLS oder HTTPS. Let's Encrypt ist eine Zertifizierungsstelle, die mithilfe eines automatischen Verfahrens unentgeltliche Zertifikate für die Transportverschlüsselung Transport Layer Security (TLS) zur Verfügung stellt. Dieses Verfahren soll die derzeit erforderlichen umfangreichen Arbeiten ersetzen, die zur manuellen Erstellung, Prüfung, Signatur, Installation und Erneuerung von Zertifikaten für sichere Websites erforderlich sind.

SecurityGateway enthält Leistungsmerkmale, um die automatische Verwaltung von LetsEncrypt-Zertifikaten zu ermöglichen. Im Verzeichnis "`SecurityGateway\LetsEncrypt`" ist jetzt ein PowerShell-Skript abgelegt, das LetsEncrypt unterstützt. Das Skript benötigt als dependency das Modul ACMESharp. Dieses Modul benötigt PowerShell ab Version 3.0, weswegen das Skript nicht auf dem Microsoft Windows Server 2003 eingesetzt werden kann. Damit das Skript erfolgreich eingesetzt werden und insbesondere die HTTP-Anforderung abgeschlossen werden kann, muss der HTTP-Dienst von SecurityGateway auf Port 80 arbeiten. Das Skript kann erst ausgeführt werden, wenn die PowerShell-Ausführungsrichtlinie richtig konfiguriert ist. Das Skript bereitet die Nutzung von Let's Encrypt vor. Hierzu gehört, dass die erforderlichen Dateien in das HTTP-Verzeichnis (templates) von SecurityGateway kopiert werden, die für die Ausführung der http-01-Anforderung (challenge) von LetsEncrypt erforderlich sind. Das Skript nutzt den FQDN der Standard-Domäne[92] von SecurityGateway als Domänennamen für das Zertifikat, ruft das Zertifikat ab, importiert es in Windows, und konfiguriert SecurityGateway mithilfe des XMLRPC-API von SecurityGateway so, dass das Zertifikat genutzt wird.

Falls Sie für Ihre Standard-Domäne einen FQDN eingerichtet haben, der nicht auf den SecurityGateway-Server verweist, funktioniert dieses Skript nicht. Sie können in das Zertifikat weitere Hostnamen aufnehmen, indem Sie die gewünschten Hostnamen auf der Befehlszeile nach dem Parameter -AlternateHostNames übergeben.

Ein Beispiel hierzu:

```
.\SGLetsEncrypt.ps1 -UserName admin@domain.com -Password Password1
-AlternateHostNames mail.domain.com,imap.domain.com,wc.domain.com
-ErrorEmailTo admin@domain.com
```

Sie brauchen in der Liste `AlternateHostNames` den FQDN der Standard-Domäne nicht aufzuführen. Ein Beispiel hierzu: Für die Standard-Domäne, "`example.com`", ist der FQDN "`mail.example.com`" konfiguriert. Ein weiterer Hostname, der genutzt werden soll, ist "`imap.example.com`". Beim Ausführen des Skripts wird nur "`imap.example.com`" als weiterer Hostname übergeben. Für alle weiteren Hostnamen müssen die HTTP-Anforderungen erfolgreich abgeschlossen werden. Falls auch nur bei einem Teil der Anforderungen Fehler auftreten, schlägt der Prozess insgesamt fehl.

Falls Sie keine weiteren Hostnamen angeben wollen, lassen Sie den Parameter `-AlternateHostNames` auf der Befehlszeile weg. Falls Sie im Fehlerfall keine E-Mail-Benachrichtigungen empfangen wollen, lassen Sie den Parameter `-ErrorEmailTo` auf der Befehlszeile weg.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

3.6.2 HTTP-Server

Auf der Seite HTTP-Server werden verschiedene Einstellungen für die Web-Schnittstelle von SecurityGateway vorgenommen. Sie können den Hostnamen bestimmen, der für die Verknüpfungen mit der Anmeldeseite verwendet wird, die SecurityGateway erstellt; außerdem können Sie die HTTP- und HTTPS-Ports festlegen und weitere HTTP-bezogene Einstellungen vornehmen.

Server

Host-Name (für Verknüpfungen zur Anmeldung):
SecurityGateway verwendet den hier angegebenen Hostnamen bei der Erstellung von Verknüpfungen mit der Anmeldeseite. Solche Verknüpfungen werden in Nachrichten an Benutzer und Administratoren eingefügt. Lautet der URL, den Ihre Nutzer zur Anmeldung an SecurityGateway aufrufen müssen, beispielsweise "`http://sg.example.com:...`", so müssen Sie in dieses Feld "sg.example.com" eintragen. Sollen diese Verknüpfungen das HTTPS-Protokoll nutzen, so müssen Sie den vollständigen URL einschließlich "https" eintragen (z.B. "`https://sg.example.com:4443`").

HTTP-Ports (kommagetrennt):
Hier wird der HTTP-Port eingetragen, den die Web-Schnittstelle von SecurityGateway verwendet. Beim Verbindungsaufbau mit SecurityGateway über einen Web-Browser müssen Ihre Benutzer diesen Port, durch einen Doppelpunkt getrennt, in den URL einfügen. Ein Beispiel hierzu: "`http://sg.example.com:4000`". Sie können mehrere Ports eintragen, müssen diese Einträge aber durch Kommata trennen. Die Voreinstellung für diesen Port ist 4000.

HTTPS-Ports (kommagetrennt):
Hier wird der HTTPS-Port eingetragen, den die Web-Schnittstelle von SecurityGateway auf eingehende HTTPS-Verbindungen überwacht. Beim Verbindungsaufbau mit SecurityGateway über einen Web-Browser müssen Ihre Benutzer "https" im URL für SecurityGateway nutzen und diesen Port, durch einen Doppelpunkt getrennt, in den URL einfügen. Ein Beispiel hierzu: "`https://sg.example.com:4443`". Sie können mehrere Ports eintragen, müssen diese Einträge aber durch Kommata trennen. Die Voreinstellung für diesen Port ist 4443.

Sockets an diese IPs binden (kommagetrennt):
Falls SecurityGateway nur auf Verbindungen reagieren soll, die auf bestimmten IP-Adressen eingehen, geben Sie diese IP-Adressen hier ein, und trennen Sie mehrere Einträge durch Kommata.

Zahl der Threads für HTTP-Anforderungen:
Hier wird die Höchstzahl der Threads festgelegt, die SecurityGateway für HTTP-Anforderungen verwendet. Die Voreinstellung beträgt 5.

HTTP-Anforderungen nach HTTPS umleiten
Check this box if you wish to redirect all HTTP requests to HTTPS. If you choose to use this option then you must ensure that you have a valid SSL/TLS Certificate 129 installed for the domain.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

HSTS-Header in HTTPS-Anforderungen aufnehmen
Per Voreinstellung wird in die HTTPS-Antworten der Header HTTP Strict Transport Security (HSTS) aufgenommen. Empfängt ein Browser, der HSTS unterstützt, einen HSTS-Header, und ist das SSL-Zertifikat gültig, so werden alle weitere HTTP-Anforderungen an dieselbe Domäne automatisch auf HTTPS umgestellt.

Höchstalter [xx] Sekunden
Dieser Einstellung bestimmt den Wert des Parameters "`max-age=`", der in den HSTS-Header aufgenommen wird. Die Einstellung bestimmt, wie lange der Browser die HSTS-Richtlinie zwischenspeichern soll. Die Voreinstellung beträgt 63072000 Sekunden; dies entspricht zwei Jahren.

... Subdomänen einschließen
Diese Option bewirkt, dass auch die Anweisung "`includeSubDomains`" in den Header aufgenommen wird. Sie weist den Browser an, die Richtlinie auch als für alle Subdomänen der Website gültig zu betrachten.

... Domäne zur HSTS-Preload-Liste hinzufügent
Diese Option bewirkt, dass auch die Anweisung "`preload`" in den HSTS-Header aufgenommen wird.

Sie sollten die Anweisung `preload` nur dann verwenden, wenn Sie sich sicher sind, dass Sie die Domäne zu den HSTS-Preload-Listen hinzufügen wollen, die in allen wichtigen Browsern enthalten sind. Wird eine Domäne der HSTS-Preload-Liste hinzugefügt, so führt dies dazu, dass die Browser bei Verbindungen mit der Domäne oder ihren Subdomänen immer HTTPS verwenden müssen. Hierdurch können an sich zulässige Verbindungen mit Subdomänen verhindert werden, falls es nicht beabsichtigt war, die Richtlinie auf sie zu erstrecken (etwa, weil sie die Voraussetzungen nicht erfüllen). Darüber hinaus ist zu beachten, dass es schwierig und zeitaufwändig sein kann, eine einmal in die HSTS-Preload-Liste aufgenommene Domäne von dort wieder entfernen zu lassen.

Nähere Informationen über die HSTS-Preload-Liste erhalten Sie unter https://hstspreload.org/

Konfiguration

Abbruch bei Zeitüberschreitung in Verbindungen aktivieren
Ist diese Option aktiv, so werden Benutzer und Administratoren automatisch von der Web-Schnittstelle abgemeldet, falls sie über den hier in Minuten angegebenen Zeitraum keine Aktionen durchführen. Diese Option ist per Voreinstellung aktiv.

Benutzer abmelden nach [xx] Minuten
Hier wird die Zeit in Minuten angeben, nach deren Ablauf Benutzer und Administratoren automatisch von der Web-Schnittstelle abgemeldet werden, wenn sie keine Aktionen durchführen. Die Voreinstellung für diese Option beträgt 15 Minuten.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

3.6.3 DNS-Server

Konfiguration

DNS-Server aus der Windows-Konfiguration nutzen
Diese Option bewirkt, dass SecurityGateway alle DNS-Server nutzt, die in Ihrer TCP/IP-Konfiguration in Microsoft Windows eingetragen sind. SecurityGateway versucht dann bei jeder Abfrage der Reihe nach, jeden eingetragenen DNS-Server zu erreichen, bis entweder ein DNS-Server geantwortet hat oder das Ende der Liste erreicht ist.

Manuell konfigurierte DNS-Server nutzen
Mithilfe dieser Option können Sie festlegen, dass SecurityGateway bestimmte DNS-Server nutzen soll. SecurityGateway versucht dann bei jeder Abfrage der Reihe nach, jeden hier aufgeführten DNS-Server zu erreichen, bis entweder ein DNS-Server geantwortet hat oder das Ende der Liste erreicht ist.

3.6.4 IPv6

SecurityGateway stellt automatisch fest, welche IPv6-Leistungsmerkmale Ihr Betriebssystem unterstützt, und nutzt, soweit möglich, den Dual-Stack-Betrieb. Ist der Dual-Stack-Betrieb nicht verfügbar, so überwacht SecurityGateway beide Netzwerke getrennt.

Konfiguration

...nur IPv4-Verbindungen annehmen
Diese Option bewirkt, dass SecurityGateway Verbindungen nur über IPv4 annimmt.

...nur IPv6-Verbindungen annehmen
Diese Option bewirkt, dass SecurityGateway Verbindungen nur über IPv6 annimmt.

...IPv4- und IPv6-Verbindungen annehmen
Diese Option bewirkt, dass SecurityGateway Verbindungen über IPv4 und IPv6 annimmt. Diese Option ist per Voreinstellung aktiv. SecurityGateway bevorzugt, soweit möglich, IPv6-Verbindungen gegenüber IPv4-Verbindungen.

Abgehende Verbindungen zu IPv6-Hosts aufbauen, soweit möglich
Diese Option bewirkt, dass SecurityGateway abgehende Verbindungen, soweit möglich, über IPv6 herstellt.

3.6.5 Verzeichnisse

Auf dieser Seite sind die Verzeichnisse aufgeführt, in denen SecurityGateway verschiedene Arten von Dateien ablegt. Sie können die Verzeichnisse und Speicherorte anpassen, indem Sie die entsprechenden Einträge auf dieser Seite bearbeiten. Klicken Sie zum Abschluss in der Symbolleiste auf Speichern.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Konfiguration der Verzeichnisse

Dateianlagen:
In diesem Ordner legt SecurityGateway die Dateianlagen ab, die in Nachrichten eingebunden sind. Die Dateianlagen verbleiben in diesem Verzeichnis, so lange sich die zugehörigen Nachrichten auf dem SecurityGateway-Server befinden.

Der Inhalt dieses Verzeichnisses ist nicht Bestandteil der internen Datensicherung[146] und Wiederherstellung[148] von SecurityGateway. Um die Dateianlagen zu sichern, müssen Sie eine Datensicherungs-Software eines Drittanbieters oder eine sonstige externe Sicherungslösung einsetzen.

Datensicherung:
In diesem Verzeichnis werden die Dateien für die Datensicherung[146] abgelegt. Um größtmögliche Leistung zu erzielen, empfiehlt es sich, dieses Verzeichnis auf einem physikalisch getrennten Laufwerk anzulegen.

Protokolle:
In diesem Verzeichnis werden die Protokolldateien von SecurityGateway abgelegt.

Eingangs-Warteschlange:
SecurityGateway nutzt dieses Verzeichnis als Warteschlange für eingehende Nachrichten.

Temp:
In diesem Verzeichnis werden temporäre Dateien abgelegt, die während der Verarbeitung anfallen.

Bayes'scher Lernvorgang (kein Spam):
Bei Nutzung des Bayes'schen Lernverfahrens[162] werden normale Nachrichten, die kein Spam sind, in diesem Verzeichnis abgelegt.

Bayes'scher Lernvorgang (Spam):
Bei Nutzung des Bayes'schen Lernverfahrens[162] werden Spam-Nachrichten in diesem Verzeichnis abgelegt.

Dateien für Speicherabbilder nach Absturz:
Hier wird der Speicherort festgelegt, an dem die Speicherabbilder abgelegt werden. Diese Speicherabbilder werden nach Abstürzen des Prozesses `securitygateway.exe` automatisch erstellt.

3.6.6 Speicherplatz

Auf der Seite Speicherplatz wird die Überwachung des freien Festplatten-Speicherplatzes durch SecurityGateway konfiguriert. Sie enthält Optionen, mit deren Hilfe eine Warnmeldung an die Administratoren gesandt sowie Empfang und Versand von Nachrichten eingestellt werden können, falls der freie Speicherplatz zur Neige geht.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Freien Speicherplatz überwachen
Ist diese Option aktiv, so überwacht SecurityGateway den freien Speicherplatz auf allen Datenträgern, auf die sich die Einträge auf der Seite Verzeichnisse 134 beziehen. Diese Option ist per Voreinstellung abgeschaltet.

Warnung an globale Administratoren senden, sobald freier Speicherplatz unter [xx] KB
Ist diese Option aktiv, so wird eine Warnmeldung an die globalen Administratoren 60 gesendet, sobald der freie Speicherplatz unter den hier in Megabyte (MB) angegebenen Wert fällt. Die Voreinstellung ist 1000 MB, und die Option ist per Voreinstellung aktiv.

SMTP-Dienst deaktivieren, sobald freier Speicherplatz unter [xx] KB
Diese Option bewirkt, dass SecurityGateway den SMTP-Dienst deaktiviert und somit keinerlei Nachrichten mehr annimmt, sobald der freie Speicherplatz unter den hier angegebenen Wert fällt. Die Voreinstellung ist 100 MB, und die Option ist per Voreinstellung aktiv.

3.6.7 Branding/Benutzerdefinierte Grafiken

Auf dieser Seite finden Sie Optionen für die Anpassung der Banner-Grafiken, die im Anmeldedialog und im Navigationsbereich erscheinen.

Anpassung

Standard-Grafiken verwenden
Diese Option bewirkt, dass die mit SecurityGateway ausgelieferten Standard-Grafiken angezeigt werden.

Benutzerdefinierte Grafiken verwenden
Falls Sie eigene benutzerdefinierte Grafiken anzeigen lassen wollen, aktivieren Sie diese Option.

Grafik für den Anmeldedialog

Diese Grafik ist die Haupt-Grafik, die SecurityGateway im Anmeldedialog anzeigt. In diesem Abschnitt finden Sie nähere Informationen zu den Abmessungen der Standard-Grafik sowie Steuerelemente, mit deren Hilfe Sie Ihre eigene Grafik hochladen können.

Grafik für die seitliche Navigationsleiste

Diese Grafik wird am oberen Rand der seitlichen Navigationsleiste angezeigt, nachdem Sie sich in SecurityGateway angemeldet haben. In diesem Abschnitt finden Sie nähere Informationen zu den Abmessungen der Standard-Grafik sowie Steuerelemente, mit deren Hilfe Sie Ihre eigene Grafik hochladen können.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für Branding und benutzerdefinierte Grafiken für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

3.6.8 Konfiguration anzeigen

Um alle Einstellungen Ihrer aktuellen SecurityGateway-Konfiguration gesammelt anzuzeigen, klicken Sie im Navigationsmenü unter *Einstellungen/Benutzer»System* auf *Konfiguration anzeigen*. Diese Funktion ist besonders für die Diagnose von Konfigurationsproblemen in Ihrer SecurityGateway-Installation hilfreich, und sie kann beim Kontakt mit dem technischen Support weiterhelfen. Von dieser Seite aus kann die Konfiguration auch in eine XML-Datei gespeichert werden. Klicken Sie hierzu in der Symbolleiste auf "*XML-Datei herunterladen*". Klicken Sie in dem Dialogfenster, das sich dann öffnet, auf *Speichern*, wählen Sie einen Speicherort für die Datei, und klicken Sie erneut auf *Speichern*.

Bitte beachten Sie, dass die Schlüsselwörter der einzelnen Einstellungen aus technischen Gründen in englischer Sprache angezeigt werden.

3.6.9 Cluster-Betrieb

Die Leistungsmerkmale für den Cluster-Betrieb von SecurityGateway ermöglichen die gemeinsame Nutzung Ihrer Konfiguration durch mehrere SecurityGateway-Server in Ihrem Netzwerk. Hiermit können Sie beispielsweise Lastverteilung für die Hardware- oder Software-Auslastung umsetzen und die im E-Mail-Betrieb anfallende Systemlast auf mehrere SecurityGateway-Server verteilen. Dies kann durch möglichst große Ausnutzung Ihrer E-Mail-Ressourcen Verarbeitungsgeschwindigkeit und Effizienz erhöhen, die Netzwerkauslastung senken und Überlastungen verringern. Es kann außerdem die Ausfallsicherheit Ihrer E-Mail-Systeme in den Fällen erhöhen, in denen auf einem Server ein Hardware- oder Softwareausfall eintritt.

Die nachfolgende Übersicht soll Ihnen die Kriterien vermitteln, nach denen Sie entscheiden können, ob Sie in Ihrem Netzwerk den Cluster-Betrieb für SecurityGateway einführen wollen:

Knoten

SecurityGateway-Cluster bestehen aus Primär- und Sekundärknoten, die auch als Primär- und Sekundär-Server bezeichnet werden. In jedem Cluster müssen ein SecurityGateway-Server zum Primär-Knoten und alle anderen SecurityGateway-Server zu Sekundärknoten bestimmt werden.

- Alle Knoten eines Clusters müssen denselben Versionsstand von SecurityGateway aufweisen.
- Für jeden Knoten eines Clusters ist ein eigener Lizenzschlüssel für SecurityGateway erforderlich. Sie können denselben Lizenzschlüssel nicht auf mehreren Knoten verwenden.
- Alle Knoten eines Clusters sollen sich im selben Netzwerk befinden. Der Cluster-Betrieb ist nicht auf den Betrieb von Knoten ausgelegt, die geografisch voneinander getrennt sind.
- Alle Knoten eines Clusters sollen auf dieselbe Zeitzone konfiguriert sein, und ihre Systemzeit soll genau übereinstimmen. Wesentliche Abweichungen zwischen den Systemzeiten der einzelnen Knoten können Probleme verursachen.
- Sie können Konfigurationsänderungen von jedem Knoten eines Clusters aus durchführen. Die anderen Knoten werden von der Konfigurationsänderung benachrichtigt, sobald diese abgeschlossen ist. Beachte: Der HELO-Domänenname 92 kann für jeden Server getrennt konfiguriert werden. Sie

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

können hierfür daher für jeden Server im Cluster einen eindeutigen Wert festlegen.

- Der Primärknoten ist für die Wartungsaufgaben, wie etwa das Bayes'sche Lernverfahren, zuständig.

Routing

SecurityGateway steuert nicht das Routing des Datenverkehrs von und zu einzelnen Knoten. Es empfiehlt sich daher, einen Lastverteiler (Load Balancer) eines Drittanbieters zu verwenden, um das Routing des Datenverkehrs und die Verkehrslenkung zu steuern.

Der Load Balancer muss sog. sticky sessions (das Nachhalten ausgehandelter Verbindungen) unterstützen, damit sichergestellt ist, dass der gesamte Datenverkehr, der von derselben IP-Adresse ausgeht, auch jeweils an denselben Host geroutet wird. Sticky sessions sind besonders für die Anmeldung an der Web-Schnittstelle von SecurityGateway wichtig. Es muss sichergestellt sein, dass der gesamte Datenverkehr für eine angemeldete Sitzung stets an denselben Server geroutet wird, an dem sich der Benutzer auch angemeldet hat.

Speicherorte für gemeinsam genutzte Datenbank und Verzeichnisse

Alle Knoten eines SecurityGateway-Clusters nutzen dieselbe Datenbank und bestimmte Verzeichnisse gemeinsam. Es müssen sich daher alle Knoten in demselben Netzwerk befinden, und die freigegebenen Speicherorte müssen für alle Knoten zugänglich sein. Per Voreinstellung wird der Windows-Dienst von SecurityGateway im Sicherheitskontext des Benutzerkontos Lokales System (Local System) ausgeführt; dieses Benutzerkonto hat auf Netzwerkressourcen keinen Zugriff. Sie müssen daher den Windows-Dienst 143 so konfigurieren, dass er unter einem Benutzerkonto ausgeführt wird, das Zugriff auf die benötigten Netzwerkressourcen hat. Nähere Informationen hierzu finden Sie im Abschnitt "Konfiguration von SecurityGateway für die Nutzung von Datenverzeichnissen in Netzwerkfreigaben 139" unten.

Archivierung

Wenn Sie die Leistungsmerkmale zur Archivierung 95 im Cluster-Betrieb nutzen wollen, müssen Sie die Archivierung so konfigurieren, dass ein Firebird-Datenbankserver genutzt wird, und Sie müssen Netzwerkfreigaben für die Archiv-Speicher verwenden, die für alle Knoten zugänglich sind.

Zertifikate

- Die HTTPS-Konfiguration (einschließlich der Zertifikate) wird nach Knoten getrennt vorgenommen. Sie müssen HTTPS für jeden Knoten separat konfigurieren, den Sie in den Cluster aufnehmen. Die Zertifikate werden auf den einzelnen Knoten gespeichert; sie werden nicht in der Datenbank gespeichert. Falls Sie dasselbe Zertifikat auf mehreren Knoten verwenden wollen, müssen Sie daher dieses Zertifikat auf jedem Knoten manuell importieren und SecurityGateway auf jedem Knoten für die Nutzung des Zertifikats konfigurieren.
- Die Konfiguration für die Weiße Liste für STARTTLS und die Pflichtliste für STARTTLS 126 wird knotenübergreifend gemeinsam genutzt.
- Die Optionen zu LetsEncrypt in SecurityGateway unterstützen derzeit keine Sekundärknoten.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Die Einrichtung des Cluster-Betriebs

Aktualisierung Ihrer Datenbank

Falls Sie den Cluster-Betrieb nutzen wollen und SecurityGateway von einer bestehenden Version auf Version 7.0 oder auf eine neuere Version aktualisiert haben, müssen Sie zunächst Ihre SecurityGateway-Datenbankdatei mithilfe des Programms `SGDBTool.exe` von dem Format Firebird 2.x auf das Format Firebird 3.x umstellen. Dieses Programm ist in SecurityGateway enthalten. Bei Neuinstallationen von SecurityGateway 7.0 entfällt dieser Schritt, da in Neuinstallationen bereits eine Datenbank des Formats Firebird 3.x verwendet wird.

Um Ihre Datenbank umzustellen, gehen Sie folgendermaßen vor:

1. Beenden Sie den Windows-Dienst SecurityGateway (klicken Sie hierzu im Startmenü-Ordner SecurityGateway auf **SecurityGateway beenden**, oder nutzen Sie das Windows-Verwaltungswerkzeug Dienste).
2. Öffnen Sie eine Windows-**Befehlszeile**.
3. Wechseln Sie in das Verzeichnis `\SecurityGateway\app\` Ihrer SecurityGateway-Installation.
4. Geben Sie folgenden Befehl ein: **`sgdbtool.exe -convertfb3`**. Drücken Sie die **Eingabetaste**, um den Befehl auszuführen.

Hierdurch wird zunächst eine Sicherheitskopie Ihrer bestehenden Datenbankdatei im Format Firebird 2.x unter dem Namen `SecurityGateway.fb2` gespeichert. Anschließend wird Ihre Datenbank mithilfe der Laufzeitversion von Firebird 3.x wieder hergestellt und unter dem Namen `SECURITYGATEWAY.FBD` gespeichert. Falls Sie die Archivierung 95 nutzen, müssen Sie diese Umstellung auch für alle Datenbankdateien der Archive durchführen.

Konfiguration von SecurityGateway für die Nutzung von Datenverzeichnissen in Netzwerkfreigaben

Alle Knoten eines SecurityGateway-Clusters nutzen dieselbe Datenbank und bestimmte Verzeichnisse gemeinsam. Alle Knoten müssen sich daher im selben Netzwerk befinden. Sie müssen außerdem sicherstellen, dass der Windows-Dienst 143 für jeden Knoten auf die Nutzung eines Benutzerkontos konfiguriert ist, das auf die Netzwerkfreigaben zugreifen kann, die Datenbank und Verzeichnisse enthalten. Sie müssen weiter sicherstellen, dass alle Knoten auf die Nutzung der richtigen Netzwerkfreigaben konfiguriert sind. Falls Sie die Inhalte freigegebener Verzeichnisse an andere Speicherorte verschieben müssen, um sie für alle Knoten freigeben zu können, müssen Sie diese Inhalte manuell verschieben. SecurityGateway verschiebt keine Dateien an andere Speicherorte. Mit Ausnahme des Verzeichnisses *Bayes'sche Replizierung* können die nachfolgenden freigegebenen Verzeichnisse und Speicherorte sowohl auf der Seite Verzeichnisse 134 als auch auf der Seite Cluster-Betrieb konfiguriert werden. Das Verzeichnis für *Bayes'sche Replizierung* kann nur auf der Seite Cluster-Betrieb konfiguriert werden.

- **Nachrichten-Daten** (z.B. `\\Freigabe01\SecurityGateway\Nachrichten\`)
- **Nachrichten-Protokolle/SMTP-Verbindungsmitschnitte** (z.B. `\\Freigabe01\SecurityGateway\Mitschnitte\`)
- **Dateianlagen** (z.B. `\\Freigabe01\SecurityGateway\Dateianlagen\`)

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **Bayes'scher Lernvorgang (kein Spam)** (z.B. `\\Freigabe01\SecurityGateway\BayeskeinSpam\`)
- **Bayes'scher Lernvorgang (Spam)** (z.B. `\\Freigabe01\SecurityGateway\BayesSpam\`)
- **Bayes'sche Replizierung** (e.g. `\\Freigabe01\SecurityGateway\BayesReplizierung`) **Beachte:** Dieses Verzeichnis wird nur für den Cluster-Betrieb verwendet. Der Primärknoten kopiert seine Bayes-Datenbank in dieses Verzeichnis, und die anderen Knoten übernehmen die durch den Primärknoten bereit gestellte Datenbank.

Beachte: Speicherort und Zugangsdaten für die Datenbank werden während der Installation festgelegt. Bei bestehenden Installationen können diese Daten mithilfe des Programms `SGDBTool.exe` festgelegt werden (siehe auch "Konfiguration von SecurityGateway zur Nutzung eines externen Datenbankservers 141" weiter unten).

Archiv-Speicher

Falls Sie die Leistungsmerkmale zur Archivierung 95 nutzen, müssen Sie auch Ihre Archiv-Speicher in eine Netzwerkfreigabe verschieben, und die Datenbankdateien aller Archiv-Speicher müssen auf einen Firebird-Datenbankserver verschoben werden. Nähere Informationen hierzu finden Sie im Abschnitt "Archivierung im Cluster-Betrieb 142" weiter unten.

Konfiguration des Datenbankservers Firebird 3

Zur Nutzung des Cluster-Betriebs müssen Sie den Datenbankserver Firebird 3 in einer Netzwerkfreigabe installieren, die für jeden Knoten des Clusters zugänglich ist.

Um Ihren Datenbankserver Firebird 3 einzurichten, gehen Sie folgendermaßen vor:

1. Laden Sie den Datenbankserver Firebird 3 herunter.
2. Führen Sie die Installationsroutine auf einem System aus, das für alle Knoten zugänglich ist.
3. **Akzeptieren Sie** die Lizenzbedingungen, und klicken Sie danach auf **Next ("Weiter")**.
4. Nehmen Sie die angezeigten Informationen zur Kenntnis, und klicken Sie danach auf **Next ("Weiter")**.
5. Wählen Sie ein Verzeichnis aus, und klicken Sie danach auf **Next ("Weiter")**.
6. Im Konfigurationsdialog Select Components ("Komponenten auswählen") klicken Sie auf **Next ("Weiter")**.
7. Bestimmen Sie einen Namen für den Ordner im Startmenü (oder klicken Sie auf **Don't create a Start Menu folder ["Keinen Ordner im Startmenü anlegen"]**), und klicken Sie danach auf **Next ("Weiter")**.
8. Belassen Sie die Optionen im Konfigurationsdialog Select Additional Tasks ("Weitere Aufgaben auswählen") auf den Voreinstellungen (das sind SuperServer mode ["SuperServer-Modus"], Run as a Service ["Als Dienst ausführen"] und Copy client library ["Client-Bibliothek kopieren"]), und klicken Sie danach auf **Next ("Weiter")**.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

9. Legen Sie das Kennwort für den Benutzer SYSDBA fest, und geben Sie es zweimal gleichlautend ein (der Benutzername "SYSDBA" und das zugehörige Kennwort werden später benötigt werden), und klicken Sie danach auf **Next ("Weiter")**.
10. Klicken Sie auf **Install ("Installieren")**.
11. Klicken Sie auf **Next ("Weiter")**.
12. Klicken Sie auf **Finish ("Fertig stellen")**.

Konfiguration von SecurityGateway zur Nutzung eines externen Datenbankservers

Alle Knoten eines SecurityGateway-Clusters müssen so konfiguriert werden, dass sie eine Verbindung mit derselben Datenbankdatei herstellen, und diese Datenbankdatei muss sich auf dem Datenbankserver Firebird 3 befinden, den Sie nach der vorstehenden Anleitung eingerichtet haben. Um SecurityGateway zur Nutzung des externen Datenbankservers zu konfigurieren, gehen Sie folgendermaßen vor:

1. Legen Sie auf dem Firebird-Server ein Verzeichnis für Ihre Datenbankdatei an (z.B. `C:\Datenbanken`).
2. Kopieren Sie die Datenbankdatei Ihres primären SecurityGateway.Servers (also `\SecurityGateway\App\SECURITYGATEWAY.FBD`) in dieses Verzeichnis.
3. Öffnen Sie auf Ihrem SecurityGateway-Server eine **Windows-Befehlszeile**.
4. Wechseln Sie in Ihr Verzeichnis `\SecurityGateway\app\`.
5. Geben Sie folgenden Befehl ein: **`sgdbtool.exe -setdbconnect`**. Drücken Sie danach die **Eingabetaste**.
6. Es erscheint die Abfrage "Use embedded Firebird database Y/N?" ("Integrierte Firebird-Datenbank nutzen Ja/Nein?") in englischer Sprache. Geben Sie **N** ein, und drücken Sie danach die **Eingabetaste**.
7. Es erscheint die Abfrage "Enter Firebird Server IP" ("Geben Sie die IP-Adresse des Firebird-Servers ein") in englischer Sprache. Geben Sie die IP-Adresse des Firebird-Server ein (z.B. 10.10.0.1), und drücken Sie danach die **Eingabetaste**.
8. Es erscheint die Abfragen "Enter Firebird Server Port (default 3050)" ("Geben Sie den Port des Firebird-Servers ein [Voreinstellung 3050]") in englischer Sprache. Drücken Sie hier die **Eingabetaste**.
9. Es erscheint die Abfrage "Enter Firebird Database Path or Alias" ("Geben Sie den Firebird-Datenbankpfad oder -Alias ein") in englischer Sprache. Geben Sie hier den vollständigen Pfad zu der Datenbankdatei ein, die Sie auf den Firebird-Server kopiert haben (z.B. `C:\Datenbanken\SECURITYGATEWAY.FBD`), und drücken Sie danach die **Eingabetaste**.
10. Es erscheint die Abfrage "Enter Firebird Database Username (default SYSDBA)" ("Geben Sie den Benutzernamen für die Firebird-Datenbank ein [Voreinstellung SYSDBA]") in englischer Sprache. Drücken Sie hier die **Eingabetaste**.
11. Es erscheint die Abfrage "Enter Firebird Database Password (default masterkey)" ("Geben Sie das Kennwort für die Firebird-Datenbank ein

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

[Voreinstellung masterkey]"). Geben Sie hier das Kennwort ein, das Sie während der Installation des Datenbankservers Firebird 3 festgelegt haben, und drücken Sie danach die **Eingabetaste**.

Ihr primärer SecurityGateway-Knoten sollte jetzt mit dem externen Datenbankserver verbunden sein.

Archivierung im Cluster-Betrieb

Um die Archivierung[95] im Cluster-Betrieb zu nutzen, gehen Sie folgendermaßen vor:

1. Erstellen Sie auf Ihrem Firebird-Server ein Verzeichnis oder mehrere Verzeichnisse, die die Datenbankdateien Ihrer Archiv-Speicher aufnehmen werden (z.B. "c:\Datenbanken\Archive\Example.com," "..\Archive\company.com" usw.).
2. Erstellen Sie für alle Speicherorte[108] Ihrer Archiv-Speicher Verzeichnisse, und richten Sie Verzeichnisfreigaben für diese Verzeichnisse ein.
3. Kopieren Sie alle Dateien Ihrer Archiv-Speicher an die neuen Speicherorte.
4. Bearbeiten Sie alle Speicherorte Ihrer Archiv-Speicher[108], und konfigurieren Sie sie auf die Nutzung der Verzeichnisfreigaben, die Sie als UNC-Pfade angeben. Die UNC-Pfade müssen auf die soeben angelegten Verzeichnisfreigaben verweisen.
5. Bearbeiten Sie alle Archiv-Speicher, aktivieren Sie die Option *Verbindung mit einer Firebird-Instanz auf einem Datenbankserver herstellen*, und geben Sie für jede Datenbankdatei *Datenbank-Pfad/Aliasnamen* ein.
6. Bearbeiten Sie die Einstellungen zur Automatischen Erstellung von Archiv-Speichern[101], und passen Sie diese bedarfsgemäß an; geben Sie die UNC-Pfade an, und passen Sie etwa verwendete Makros an den Cluster-Betrieb an.

Hinzufügen von Knoten zu Ihrem Cluster

Um Ihrem Cluster eine neue SecurityGateway-Installation hinzuzufügen, gehen Sie folgendermaßen vor:

1. Führen Sie auf dem System, das als neuer Knoten dienen soll, die Installationsroutine von SecurityGateway aus.
2. Wählen Sie während der Installation die Option *Verbindung zu einem bestehenden Firebird-3-Datenbankserver herstellen* aus, und geben Sie die Informationen zur Konfiguration des Datenbankservers ein, die Sie bereits oben eingegeben haben.
3. Führend Sie die Installation im Übrigen normal durch.
4. Stellen Sie sicher, dass für den Windows-Dienst[143] ein Benutzerkonto mit Zugriff auf die Netzwerkfreigaben konfiguriert ist, und dass Sie für die gemeinsam genutzten Datenverzeichnisse die erforderlichen Netzwerkfreigabe als UNC-Pfade eingetragen haben.
5. Kopieren Sie etwa erforderliche SSL-Zertifikate auf das neue System.

Datenbankreplikation aktiv-aktiv

SecurityGateway unterstützt grundsätzlich die Datenbankreplikation aktiv-aktiv für Ihren Cluster. Es ist hierfür aber ein externes Hilfsprogramm für die Replikation

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

erforderlich. Dessen Konfiguration ist nicht in der vorliegenden Hilfedatei beschrieben. Sie finden Informationen über die Anforderungen und Hinweise zur Konfiguration Ihres Clusters für die Replikation aktiv-aktiv in folgendem, in englischer Sprache verfügbaren PDF: SecurityGateway: Configuring Active-Active Database Replication (Konfiguration der Datenbankreplikation aktiv-aktiv).

3.6.10 Windows-Dienst

Der Windows-Dienst von SecurityGateway wird per Voreinstellung im Sicherheitskontext des Benutzerkontos Lokales System (Local System) ausgeführt. Dieses Benutzerkonto hat jedoch keinen Zugriff auf Netzwerkverzeichnisse und Netzwerklaufwerke. Sie müssen daher SecurityGateway unter einem anderen Benutzerkonto ausführen, falls SecurityGateway auf solche Netzwerkverzeichnisse und Netzwerklaufwerke zugreifen muss. Dies ist beispielsweise im Cluster-Betrieb 137 der Fall. Mithilfe der Optionen auf dieser Seite können Sie das Benutzerkonto mit seinen Anmeldedaten festlegen, unter dem SecurityGateway ausgeführt wird.

Benutzerkonto Lokales System
Per Voreinstellung wird der Windows-Dienst von SecurityGateway im Sicherheitskontext des Benutzerkontos SYSTEM ausgeführt.

Dieses Benutzerkonto
Falls Sie den Windows-Dienst unter einem anderen Benutzerkonto ausführen wollen, geben Sie *Anmeldenamen*, *Kennwort* und *Domäne* für dieses Benutzerkonto hier ein.

3.7 Datenbank

Der Abschnitt Datenbank im Menü *Einstellungen/Benutzer* enthält Verknüpfungen mit den folgenden vier Seiten, mit denen sich festlegen lässt, welche und wie viele Daten SecurityGateway speichert, und wie die Datenbank von SecurityGateway gesichert und wieder hergestellt wird:

Konfiguration 146—Mithilfe dieser Seite legen Sie das Verfahren für Schreibzugriffe auf die Datenbank fest. Sie können bestimmen, dass die Schreibzugriffe synchron oder asynchron erfolgen.

Datenhaltung 144—Mithilfe dieser Seite legen Sie fest, wie lange SecurityGateway die Einträge über Nachrichten, den Nachrichteninhalt und die SMTP-Verbindungsmitschnitte für die einzelnen Nachrichten in der Datenbank hält. Sie können auch festlegen, unter welchen Umständen Nachrichteninhalte gespeichert und gelöscht werden. Die Datenbank-Wartung wird jeden Tag um Mitternacht durchgeführt, und alle Werte auf dieser Seite sind in Tagen anzugeben.

Datensicherung 146—Mithilfe der Seite Datensicherung können Sie die automatische Sicherung Ihrer SecurityGateway-Datenbank planen. Sie können vollständige Sicherungen der gesamten Datenbank und Sicherungen nur der Konfigurationsdaten planen. Sie können auch festlegen, wie viele alte Sicherungsdateien gespeichert werden sollen.

Wiederherstellung 148—Auf der Seite Wiederherstellung sind alle Sicherungsdateien für Konfiguration und Datenbank aufgeführt, die mithilfe der Seite Datensicherung angelegt wurden und auf dem System gespeichert sind. Von dieser Seite aus können

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Sie die Dateien herunterladen und löschen sowie die Konfiguration oder die gesamte Datenbank aus ihnen wieder herstellen.

3.7.1 Konfiguration

 Mithilfe dieser Seite legen Sie das Verfahren für Schreibzugriffe auf die Datenbank fest. Sie können bestimmen, dass die Schreibzugriffe synchron oder asynchron erfolgen.

Verfahren für Datenbank-Schreibzugriffe

Daten synchron schreiben
Diese Option bewirkt, dass Daten sofort auf den Datenträger geschrieben werden. Datenbank-Transaktionen, die Schreibzugriffe beinhalten, werden erst abgeschlossen, wenn die Daten physikalisch auf den Datenträger geschrieben wurden. Diese Option ist per Voreinstellung aktiv. Sie bietet die größte Sicherheit für Ihre Daten.

Daten asynchron schreiben
Diese Option überlässt dem Betriebssystem die Entscheidung, wann Daten physikalisch auf den Datenträger geschrieben werden. Diese Option bietet erhöhte Leistung, sie erhöht aber auch das Risiko für eine Beschädigung der Datenbank bei Stromausfall oder unkontrolliertem Herunterfahren des Servers oder der Datenbank. Die asynchrone Betriebsart für die Schreibzugriffe wird nur empfohlen, wenn die Leistung in der synchronen Betriebsart nicht ausreicht. Es ist von entscheidender Bedeutung, dass das System durch eine zuverlässige unterbrechungsfreie Stromversorgung geschützt wird, und dass Datensicherungen der Datenbank hergestellt werden.

3.7.2 Datenhaltung

 Mithilfe dieser Seite legen Sie fest, wie lange SecurityGateway die Einträge über Nachrichten, den Nachrichteninhalt und die SMTP-Verbindungsmitschnitte für die einzelnen Nachrichten in der Datenbank hält. Sie können auch festlegen, unter welchen Umständen Nachrichteninhalte gespeichert und gelöscht werden. Die Datenbank-Wartung wird jeden Tag um Mitternacht durchgeführt, und alle Werte auf dieser Seite sind in Tagen anzugeben.

Einträge in der Nachrichten-Datenbank

Geben Sie nachfolgend an, wie lange Sie die Einträge über Nachrichten in der Datenbank halten wollen. Berichte sind auf diesen Zeitraum begrenzt. Je länger der Zeitraum dauert, desto größer wird die Datenbank.

Keine Aktion ausführen
Um die Nachrichten-Einträge überhaupt nicht aus der Datenbank zu löschen, wählen Sie diese Option aus.

Einträge löschen nach [xx] Tag(e/n)
Falls Sie jeden Tag um Mitternacht veraltete Datenbank-Einträge löschen wollen, aktivieren Sie diese Option, und geben Sie die Anzahl der Tage ein, für die Sie die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

einzelnen Einträge in der Datenbank halten wollen. Diese Option ist per Voreinstellung aktiv, und die Einträge werden per Voreinstellung nach 30 Tagen gelöscht.

Inhalte der Nachrichten

Per Voreinstellung werden die Inhalte der einzelnen Nachrichten gelöscht, sobald sie nicht mehr gebraucht werden. Dies ist etwa dann der Fall, wenn eine Nachricht dem Empfänger erfolgreich zugestellt oder aus der Quarantäne gelöscht wurde. Da es aber zu Zwecken der Fehlersuche hilfreich sein kann, auf die Nachrichten-Inhalte auch später noch zuzugreifen, stehen weiter unten auch Optionen zur Verfügung, die das automatische Löschen von Nachrichten-Inhalten unter bestimmten Umständen verhindern. Diese Optionen sind per Voreinstellung alle abgeschaltet.

Falls Sie diese Optionen aktivieren, kann dies zu einer Verringerung der Leistung und einer Vergrößerung der Datenbank führen.

Nachrichteninhalt nach erfolgreicher Zustellung nicht löschen
Um die Nachrichten-Inhalte auch dann zu erhalten, wenn eine Nachricht erfolgreich an den Server des Empfängers übermittelt wurde, aktivieren Sie diese Option.

Nachrichteninhalt nicht löschen, wenn Nachrichten aus Quarantäne gelöscht werden
Um die Nachrichten-Inhalte von Nachrichten in Quarantäne nicht zu löschen, nachdem die Nachrichten aus der Quarantäne gelöscht wurden, aktivieren Sie diese Option.

Nachrichteninhalt nicht löschen, wenn Nachrichten abgewiesen werden
Um Nachrichten-Inhalte auch dann nicht zu löschen, wenn die Nachricht nach dem Empfang abgewiesen wurde, aktivieren Sie diese Option.

Nachrichteninhalt nach endgültig fehlgeschlagener Zustellung nicht löschen
Um Nachrichten-Inhalte von Nachrichten nach endgültig fehlgeschlagener Zustellung (etwa wegen eines ungültigen Empfängers) nicht zu löschen, aktivieren Sie diese Option.

Nachrichteninhalt unvollständiger Nachrichten nicht löschen
Um Nachrichten-Inhalte unvollständiger Nachrichten nicht zu löschen, aktivieren Sie diese Option.

Nachrichten-Mitschnitte

Für jede Nachricht wird ein umfassendes Protokoll über die SMTP-Verbindung und die Verarbeitung der SIEVE-Regeln erstellt, das zusammengefasst als Mitschnitt bezeichnet wird. Die Nachrichten-Mitschnitte können bei Fehlersuche und Fehlerbehebung sehr hilfreich sein, sie vergrößern aber die Datenbank.

Nachrichten-Mitschnitt folgt Nachrichten-Eintrag in der Datenbank (oben)
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass Nachrichten-Mitschnitte ebenso behandelt werden wie die Nachrichten-Inhalte in der Datenbank. Werden alte Nachrichten-Einträge aus der Datenbank gelöscht, so werden die Nachrichten-Mitschnitte ebenfalls gelöscht.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nachrichten-Mitschnitte löschen nach [xx] Tag(e/n)
Falls Sie die Nachrichten-Mitschnitte für einen bestimmten Zeitraum aufbewahren wollen, aktivieren Sie diese Option und geben Sie den Zeitraum in Tagen ein.

Nachrichten-Mitschnitte nicht speichern
Um die Nachrichten-Mitschnitte nicht zu speichern, aktivieren Sie diese Option.

Informationen zur Bandbreite

Bandbreiten-Informationen löschen nach [xx] Tag(e/n)
Um veraltete Informationen über die Bandbreiten-Nutzung jeden Tag um Mitternacht zu löschen, aktivieren Sie diese Option, und geben Sie den Zeitraum in Tagen ein, für den die Informationen aufbewahrt werden sollen.

3.7.3 Datensicherung

Mithilfe der Seite Datensicherung können Sie die automatische Sicherung Ihrer SecurityGateway-Datenbank planen. Sie können vollständige Sicherungen der gesamten Datenbank und Sicherungen nur der Konfigurationsdaten planen. Sie können auch festlegen, wie viele alte Sicherungsdateien gespeichert werden soll. Die im Rahmen der Datensicherung erstellten Sicherungsdateien sind auf der Seite Wiederherstellung 148 aufgeführt.

Um größtmögliche Leistung zu erzielen, empfiehlt es sich, das Verzeichnis für die Sicherungsdateien (es wird auf der Seite Verzeichnisse 134 festgelegt) auf einem physikalisch getrennten Laufwerk anzulegen. Es wird nicht empfohlen, die Datenbank von SecurityGateway mithilfe einer Datensicherungs-Software eines Drittanbieters oder einer sonstigen externen Sicherungslösung zu sichern, während der Dienst SecurityGateway ausgeführt wird. Die internen Sicherungsfunktionen auf dieser Seite können ohne weiteres verwendet werden, um die Datenbank zu sichern, während der Dienst ausgeführt wird. Falls Sie eine externe Sicherungslösung einsetzen wollen, soll der Dienst vor Beginn der Sicherung beendet werden. Alternativ kann die externe Sicherungslösung auch die Sicherungsdateien sichern, die SecurityGateway selbst im Rahmen der Datensicherung angelegt hat. Schließlich umfassen die internen Sicherungsfunktionen von SecurityGateway nicht den Inhalt des Verzeichnisses Dateianlagen 134. Um die Dateianlagen zu sichern, müssen Sie eine Datensicherungs-Software eines Drittanbieters oder eine sonstige externe Sicherungslösung einsetzen.

Automatische Datensicherung

Datensicherung nicht automatisch durchführen
Diese Option ist per Voreinstellung aktiv. SecurityGateway sichert die Datenbank und die Konfiguration des Servers nicht automatisch.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Konfigurationsdaten automatisch sichern alle [xx] Tag(e/n) um [xx:xx]
Um nur die Konfiguration von SecurityGateway, nicht aber die gesamte Datenbank, zu sichern oder zu exportieren, aktivieren Sie diese Option. Geben Sie das Intervall zwischen den automatischen Sicherungen in Tagen ein, und legen Sie die Uhrzeit fest, zu der die Sicherung jeweils durchgeführt werden soll. Die während der Sicherung erzeugten Dateien sind auf der Seite Wiederherstellung 148 aufgeführt; ihre Dateinamen beginnen mit "Export".

Dieses Sicherungsverfahren umfasst nur die Konfigurationsdaten von SecurityGateway; hierzu gehören auch die Daten über Benutzer und Domänen, jedoch nicht die gesamte Datenbank. Falls Sie das System aus einer solchen Datensicherung wieder herstellen, werden daher alle Nachrichten, Nachrichten-Mitschnitte, Berichte, das Nachrichten-Protokoll und alle sonstigen Daten außer den Konfigurationsdaten gelöscht. Nur die Konfigurationsdaten selbst werden wieder hergestellt.

Gesamte Datenbank automatisch sichern alle [xx] Tag(e/n) um [xx:xx]
Um die vollständige Datenbank von SecurityGateway, einschließlich der Konfigurationsdaten, des Nachrichten-Protokolls 307, der Berichte 324, der Mitschnitte und aller sonstigen in ihr enthaltenen Daten, zu sichern, aktivieren Sie diese Option. Geben Sie das Intervall zwischen den automatischen Sicherungen in Tagen ein, und legen Sie die Uhrzeit fest, zu der die Sicherung jeweils durchgeführt werden soll. Die während der Sicherung erzeugten Dateien sind auf der Seite Wiederherstellung 148 aufgeführt; ihre Dateinamen beginnen mit "Backup".

Der Inhalt des Verzeichnisses Dateianlagen 134 wird von der Datensicherung nicht umfasst und nicht in die Sicherungsdateien übernommen. Um die Dateianlagen zu sichern, müssen Sie eine Datensicherungs-Software eines Drittanbieters oder eine sonstige externe Sicherungslösung einsetzen. Auch die Protokolldateien 318 sind nicht von der Datensicherung umfasst, obwohl das Nachrichten-Protokoll 317 im Rahmen der Sicherung der gesamten Datenbank gesichert wird. Falls Sie die Protokolldateien sichern wollen, müssen Sie hierfür ebenfalls eine Datensicherungs-Software oder eine sonstige externe Sicherungslösung einsetzen.

Höchstens [xx] Sicherungsdatei(en) speichern. Die älteste(n) Sicherungsdatei(en) werden gelöscht.
Um die Anzahl der Datensicherungen zu begrenzen, die auf dem System gespeichert werden, aktivieren Sie dieses Kontrollkästchen. Geben Sie außerdem die Anzahl der zu speichernden Sicherungsdateien an. Wird diese Anzahl erreicht, so wird bei Erstellung einer neuen Datensicherung jeweils die älteste gespeicherte Sicherungsdatei gelöscht. Diese Option ist per Voreinstellung abgeschaltet.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Manuelle Datensicherung

Klicken Sie hier, um die Konfigurationsdaten jetzt zu sichern/exportieren.
Um die Konfiguration von SecurityGateway manuell zu exportieren, klicken Sie auf diese Verknüpfung. In der Funktion entspricht diese Sicherungsmethode der Option "*Konfigurationsdaten automatisch sichern...*" weiter oben; sie wird nur nicht automatisch sondern von Hand ausgelöst und zusätzlich zu etwa geplanten automatischen Datensicherungen ausgeführt.

Klicken Sie hier, um die gesamte Datenbank jetzt zu sichern.
Um die gesamte Datenbank von SecurityGateway manuell zu sichern, klicken Sie auf diese Verknüpfung. In der Funktion entspricht diese Sicherungsmethode der Option "*Gesamte Datenbank automatisch sichern...*" weiter oben; sie wird nur nicht automatisch sondern von Hand ausgelöst und zusätzlich zu etwa geplanten automatischen Datensicherungen ausgeführt.

3.7.4 Wiederherstellung

Auf der Seite Wiederherstellung sind alle Sicherungsdateien für Konfiguration und Datenbank aufgeführt, die mithilfe der Seite Datensicherung 146 angelegt wurden und auf dem System gespeichert sind. Von dieser Seite aus können Sie die Dateien herunterladen und löschen sowie die Konfiguration oder die gesamte Datenbank aus ihnen wieder herstellen.

Datensicherung hochladen

Mithilfe der Optionen zum Durchsuchen und Hochladen können Sie eine früher heruntergeladene Datensicherung hochladen und zur Liste Wiederherstellung weiter unten hinzuzufügen. Sie können dann, in Abhängigkeit von der Art der Datensicherung, Ihre Konfigurationsdaten oder Ihre gesamte Datenbank aus der Datensicherung wieder herstellen.

Durchsuchen
Klicken Sie auf dieses Steuerelement, um die Sicherungsdatei auszuwählen, die Sie hochladen und der Liste Wiederherstellung weiter unten hinzufügen wollen. Die Sicherungsdatei sollte früher auf diesem System mithilfe der Optionen auf der Seite Datensicherung 146 erstellt und über diese Seite heruntergeladen worden sein.

Datensicherung hochladen
Nachdem Sie die Sicherungsdatei über Durchsuchen ausgewählt haben, klicken Sie auf dieses Steuerelement, um die Datei hochzuladen und der Liste Wiederherstellung unten hinzuzufügen.

Wiederherstellung

In dieser Liste sind alle Dateien aufgeführt, die über die Seite Datensicherung 146 erstellt oder über die Funktion Datensicherung hochladen weiter oben hochgeladen wurden. Für jeden Eintrag erscheinen der Dateiname, Datum und Uhrzeit, zu denen die Datei erstellt wurde, die Größe der Datei, und Verknüpfungen, mit deren Hilfe die Datei heruntergeladen und gelöscht und das System aus ihr wiederhergestellt werden kann. Dateien, deren Namen mit "Export" beginnen, enthalten nur die Konfigurationsdaten. Dateien, deren Namen mit "Backup" beginnen, sind Sicherungsdateien der gesamten Datenbank.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Weitere Informationen über die Unterschiede zwischen den einzelnen Typen von Sicherungsdateien erhalten Sie auf der Seite Datensicherung 146.

Herunterladen
Um eine Sicherungsdatei herunterzuladen, klicken Sie in dem zugehörigen Eintrag auf die Verknüpfung Herunterladen. Heruntergeladene Dateien können später wieder hochgeladen und der Liste Wiederherstellung hinzugefügt werden; hierzu dienen die Funktionen unter Datensicherung hochladen weiter oben. Durch das Herunterladen einer Datei wird sie nicht aus der Liste gelöscht.

Löschen
Um eine Sicherungsdatei zu löschen, klicken Sie in dem zugehörigen Eintrag auf diese Verknüpfung. Falls Sie die Datei aus SecurityGateway entfernen, sie aber an anderer Stelle speichern wollen, laden Sie die Datei erst mithilfe der Verknüpfung Herunterladen herunter, und löschen Sie sie aus der Liste.

Wiederherstellen
Um die Konfigurationsdaten oder die gesamte Datenbank von SecurityGateway aus einer Sicherungsdatei wieder herzustellen, klicken Sie in dem zugehörigen Eintrag auf diese Verknüpfung. Alle Änderungen, die seit der Erstellung der Sicherungsdatei vorgenommen wurden, gehen dabei verloren, und SecurityGateway ist nicht betriebsbereit, so lange die Wiederherstellung läuft. Nach Abschluss der Wiederherstellung müssen Sie sich erneut anmelden. Bevor die Wiederherstellung durchgeführt wird, erscheint eine Sicherheitsabfrage.

3.7.5 Erweitert

Falls Sie durch den technischen Support hierzu aufgefordert werden, können Sie mithilfe dieser Seite ein SQL-Statement auf der Datenbank ausführen. Es empfiehlt sich, dass Sie eine Datensicherung 146 Ihrer Datenbank erstellen, bevor Sie diesen Vorgang durchführen.

SQL-Statement ausführen

SQL-Statement:
Falls Sie durch den technischen Support hierzu aufgefordert werden, tragen Sie in dieses Eingabefeld ein SQL-Statement ein, und klicken Sie danach auf **Ausführen**. Die Ergebnisse dieses Vorgangs erscheinen im Abschnitt Ergebnis weiter unten.

3.8 Software-Aktualisierung

Mithilfe dieser Funktion können Sie überprüfen, ob eine Version von SecurityGateway verfügbar ist. Sie können manuell nach neuen Versionen suchen oder SecurityGateway mithilfe einer entsprechenden Option veranlassen, automatisch nach neuen Software-Versionen zu suchen. Ist eine neue Version verfügbar, so kann die neue Version direkt über die Web-Schnittstelle heruntergeladen und installiert werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Konfiguration

Regelmäßig nach neuen Software-Versionen suchen
Ist diese Option aktiv, so sucht SecurityGateway jeden Tag um Mitternacht automatisch nach neuen Software-Versionen.

Klicken Sie hier, um jetzt nach neuen Software-Versionen zu suchen
Um sofort nach neuen Software-Versionen zu suchen, klicken Sie auf diese Verknüpfung. Die Ergebnisse der Suche erscheinen im Abschnitt Aktualisierungen weiter unten.

Aktualisierungen

In diesem Abschnitt werden die Ergebnisse der Suche nach neuen Software-Versionen angezeigt. Ist eine neue Software-Version verfügbar, so werden alle globalen Administratoren[60] hiervon verständigt. Es erscheint dann eine Verknüpfung, mit deren Hilfe Sie den Dialog Einzelheiten zu den neuen Software-Versionen aufrufen können. Von dort aus können sie die neue Version laden und installieren.

Einzelheiten zu den neuen Software-Versionen

Ergibt die Suche nach neuen Versionen, dass eine aktualisierte Version der Software verfügbar ist, so wird je eine Verknüpfung mit der Seite Einzelheiten zu den neuen Software-Versionen in das Dashboard[9] und in den Abschnitt Aktualisierungen der Seite Software-Aktualisierung eingeblendet. Diese Seite zeigt die gerade installierte Version der Software an, die neue Version, die verfügbar ist, und die Größe der neuen Version. Sie stellt auch eine Verknüpfung bereit, über die eine Liste der Änderungen für die neue Version angezeigt werden kann, sowie Verknüpfungen, um die neue Version herunterzuladen und zu installieren.

3.9 Lizenzverwaltung

Auf dieser Seite werden Informationen zur Lizenz der Produkte angezeigt. Hierzu gehören der Name der natürlichen Person oder die Firma, der die Lizenz erteilt ist, der Lizenzschlüssel und der Status der Lizenz. Statusinformationen sind der Umfang der Lizenz und andere hierzu relevante Daten.

SecurityGateway

In diesem Abschnitt erscheinen die Lizenzinformationen für SecurityGateway.

Name des Lizenznehmers:
Hier wird der Name eingetragen auf den die Lizenz registriert ist.

Firma oder Distributor:
Hier wird die Firma des Lizenznehmers oder des Distributors eingetragen.

Lizenzschlüssel für SecurityGateway:
In dieses Feld wird der Lizenzschlüssel eingetragen. Klicken Sie auf *Speichern,* nachdem Sie den Schlüssel eingetragen haben.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Status der Lizenz
In diesem Abschnitt wird der Status der Lizenz angezeigt. Statusinformationen sind der Umfang der Lizenz und andere hierzu relevante Daten.

Konfiguration
SecurityGateway übermittelt während der Anforderung einer aktualisierten Lizenzdatei von MDaemon Technologies die Betriebssystemversion, unter der SecurityGateway ausgeführt wird. Diese Information hilft MDaemon Technologies bei der Entscheidung, welche Betriebssystemversionen unterstützt werden sollen. Mithilfe dieser Option können Sie die Übermittlung dieser Daten verhindern.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kapitel

4 Sicherheit

Das Menü *Sicherheit* ist in acht Abschnitte untergliedert und gestattet den Zugriff auf verschiedene Werkzeuge, mit deren Hilfe Sie Ihre Domänen und Benutzer gegen Spam, Viren, missbräuchliche Nutzung des E-Mail-Systems und andere Sicherheitsrisiken schützen können. Es folgt ein kurzer Überblick über die einzelnen Abschnitte. Weitere Informationen können Sie den Hilfeseiten der einzelnen Abschnitte entnehmen.

Anti-Spam 155
Der Abschnitt Anti-Spam im Menü Sicherheit enthält Optionen, die Ihnen bei der Bekämpfung von Spam und unerwünschten Junk-Nachrichten helfen. Der Abschnitt enthält acht Anti-Spam-Funktionen; dazu gehören Funktionen zur Erkennung und Bekämpfung von Spam durch Heuristische Verfahren, die Bayes'sche Analyse, Schwarze Listen für DNS (DNSBL) und URI (URIBL), die Graue Liste und vieles mehr.

Anti-Virus 187
Der Abschnitt Anti-Virus im Menü Sicherheit enthält Optionen, die Ihnen die Erkennung durch Viren infizierter Nachrichten erleichtern und verhindern, dass diese Nachrichten Ihre Benutzer erreichen.

Anti-Spoofing 190
Der Abschnitt Anti-Spoofing enthält Werkzeuge, die Ihnen bei der Erkennung von Nachrichten helfen, die unter gefälschten ("gespooften") Absender-Adressen versandt werden. In diesem Abschnitt stehen sechs Anti-Spoofing-Methoden zur Verfügung, wie etwa die DKIM-Prüfung, Sender-ID, Prüfung durch Rückruf und viele mehr.

Anti-Abuse 222
Der Abschnitt Anti-Abuse enthält Werkzeuge, die Ihnen helfen, den Missbrauch Ihres E-Mail-Systems durch Dritte zu unterbinden. Zu diesem Missbrauch gehören die Durchleitung von Spam-Nachrichten im Relaisbetrieb, die übermäßige Inanspruchnahme von Übertragungs-Bandbreite, der übermäßig häufige Verbindungsaufbau mit dem Server und ähnliche Verhaltensweisen. Der Abschnitt Anti-Abuse enthält sechs Werkzeuge.

Filterung
Der Abschnitt Filterung enthält zwei Funktionsbereiche: Filterung der Inhalte der Nachrichten 252 und Filterung von Dateianlagen 263. Mithilfe der Filterung der Inhalte der Nachrichten können Filter-Regeln angelegt werden, die verschiedene Aktionen ausführen können. Nachrichten, die bestimmten Kriterien entsprechen, können abgewiesen, kopiert, an eine andere Adresse umgeleitet, in Quarantäne gegeben und auf vielfältige andere Weise behandelt werden. Mithilfe der Optionen zur Filterung von Dateianlagen können Dateitypen festgelegt werden, die zum Abweisen oder zur Quarantäne der Nachricht führen, in der sie gefunden werden. Sie können die Filterung systemweit und nach Domänen getrennt steuern.

Schwarze Listen 265
In den Schwarzen Listen können E-Mail-Adressen, Hosts und IP-Adressen erfasst werden, deren Nachrichten Sie abweisen lassen oder in Quarantäne geben wollen. Per Voreinstellung werden solche Nachrichten bereits während

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

der SMTP-Verbindung abgewiesen; Sie können die entsprechenden Einstellungen jedoch auf der Seite Aktion der Schwarzen Liste ändern und die Nachrichten stattdessen in Quarantäne geben lassen. Die gewünschte Vorgehensweise kann systemweit und nach Domänen getrennt vorgegeben werden, und auch die Schwarzen Listen selbst können systemweit und nach Domänen getrennt geführt werden.

Weiße Listen 275
In den Weißen Listen können E-Mail-Adressen, Hosts und IP-Adressen erfasst werden, deren Nachrichten von einigen Sicherheitsbeschränkungen ausgenommen sind. Die Funktionen Heuristik, Bayes, DNSBL, DKIM-Prüfung und auch fast alle anderen Sicherheitsfunktionen von SecurityGateway können so konfiguriert werden, dass Absender, Hosts und Nachrichten von der Bearbeitung durch diese Funktionen ausgenommen sind, falls sie einen Treffer auf einer Weißen Liste auslösen. Jede Weiße Liste kann systemweit und nach Domänen getrennt geführt werden.

Sieve-Skripte 284
SecurityGateway nutzt die zum Filtern von E-Mail entwickelte Filtersprache Sieve für viele seiner Funktionen, und die Übersicht über die Sieve-Skripte erlaubt einen Einblick in die Reihenfolge, in der die Funktionen ausgeführt werden. Es steht auch ein Editor für Sieve-Skripte zur Verfügung, mit dessen Hilfe Sie eigene benutzerdefinierte Skripte erstellen können.

4.1 Anti-Spam

Der Abschnitt Anti-Spam im Menü Sicherheit 154 enthält Optionen, die Ihnen bei der Abwehr von Spam, unverlangt zugesandten Nachrichten oder Junk-E-Mail helfen. In diesem Abschnitt sind acht Leistungsmerkmale zur Abwehr von Spam aufgeführt:

Outbreak Protection 157 - Die Outbreak Protection (OP), der Schutz gegen Ausbrüche und Massenangriffe, ist eine revolutionäre Technik zur Erkennung von Spam und Viren in Echtzeit, die Ihre E-Mail-Infrastruktur vorausschauend binnen Minuten nach einem Ausbruch von Spam oder Viren schützen kann. Da die Outbreak Protection besonders auf die Behandlung von Ausbrüchen und Massenangriffen ausgerichtet ist, ersetzt sie nicht andere, herkömmliche Schutzmechanismen gegen Viren und Spam, die SecurityGateway enthält. Sie ist vielmehr eine zusätzliche, besondere Schutzschicht.

Heuristik und Bayes 162 - SecurityGateway für E-Mail-Server nutzt eine angepasste Hochleistungsversion des beliebten quelloffenen Projekts SpamAssassin™ und stellt hierüber Heuristik-Regeln und Bayes'sche Bewertungsverfahren zur Verfügung. Nachrichten werden diesem Prozess übergeben und erhalten, in Abhängigkeit von ihrem Inhalt, eine Bewertung. SecurityGateway gestattet statt der Nutzung des internen Moduls auch wahlweise die Nutzung eines externen SpamAssassin™-Daemons.

Schwarze Listen für DNS (DNSBL) 169 - Schwarze Listen für DNS (nach der englischen Bezeichnung DNS Blacklists auch kurz als DNSBL bezeichnet) können helfen, zu verhindern, dass Spam-Nachrichten Ihre Benutzer erreichen. Für diese Sicherheitsfunktion können Sie mehrere Schwarze Listen für DNS konfigurieren; solche Dienste unterhalten Listen von Servern, von denen bekannt ist, dass sie

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Spam durchleiten. Die Listen werden immer abgefragt, wenn ein Dritter versucht, eine Nachricht an eine Ihrer Domänen zu senden. Ist die IP der Gegenstelle auf einer Schwarzen Liste erfasst, so wird die Nachricht abgewiesen, in Quarantäne gegeben oder gekennzeichnet.

Schwarze Liste für URI (URIBL) 172 - Schwarze Listen für URI (nach dem englischen Begriff URI Blacklists auch als "URIBL" abgekürzt) sind in Echtzeit arbeitende Schwarze Listen, mit deren Hilfe Nachrichten auf Grundlage der im Nachrichtentext enthaltenen Uniform Resource Identifier (üblicherweise Domänennamen oder Websites) abgewiesen oder gekennzeichnet werden können. Andere Begriffe für diese Dienste sind URI Blocklists und Spam URI Realtime Blocklists (SURBL).URIBL unterscheiden sich von Schwarzen Listen für DNS dadurch, dass sie Spam nicht anhand der Inhalte der Kopfzeilen oder IP-Adresse der Gegenstelle erkennen. URIBL blockieren Spam auf der Grundlage des Nachrichten-Inhalts selbst.

Graue Liste 176 - Die Graue Liste ist eine Abwehrmaßnahme gegen Spam, die den Mailserver des Absenders informiert, dass während der Zustellung ein vorübergehender Fehler aufgetreten ist, und dass die Zustellung etwas später erneut versucht werden soll. Bei dieser Maßnahme geht man davon aus, dass Spammer üblicherweise keinen erneuten Zustellversuch unternehmen, wenn eine Nachricht nicht zugestellt werden kann, legitime Absender aber durchaus weitere Zustellversuche unternehmen, sodass die Anzahl der Spam-Nachrichten verringert werden kann, die die Benutzer erhalten.

Zertifizierung von Nachrichten 179 - Die Zertifizierung von Nachrichten ist ein Vorgang, in dessen Rahmen eine vertrauenswürdige Quelle für das legitime Verhalten beim Versand von Nachrichten einsteht oder es "zertifiziert". Die Zertifizierung bezieht sich auf eine bestimmte Funktionseinheit, die mit der Nachricht verknüpft ist. Nachrichten aus einer Domäne, die durch eine solche vertrauenswürdige Quelle zertifiziert ist, können daher als weniger verdächtig angesehen werden. Sie können daher davon ausgehen, dass die zertifizierten Absenderdomänen vernünftige Verfahren einsetzen und keinen Spam oder problematische Nachrichten senden.

Schutz gegen Rückstreuung 182 - Als "Rückstreuung" (englisch "Backscatter") bezeichnet man Antwortnachrichten, die Ihre Benutzer empfangen, obwohl sie die Nachrichten, auf die geantwortet wird, gar nicht versandt haben. Diese Erscheinung tritt auf, wenn Spam-Nachrichten oder Nachrichten, die durch Viren versandt werden, als Antwortpfad eine gefälschte Adresse enthalten. Werden solche Nachrichten durch den Server des Empfängers abgewiesen, oder hat der Empfänger für sein Benutzerkonto einen Auto-Beantworter oder eine Abwesenheitsnachricht eingerichtet, so wird die Antwort an die gefälschte Adresse gerichtet. Um die Rückstreuung zu bekämpfen, kann SecurityGateway mithilfe einer Hash-Funktion und eines geheimen Schlüssels in Verbindung mit einem besonderen, zeitabhängigen Kode ein, der in die Antwortadresse, den "`Return-Path`", abgehender Nachrichten eingefügt wird. Tritt bei der Zustellung einer solchen Nachricht ein Fehler auf, und wird sie zurückgeleitet, oder geht eine automatisch erzeugte Antwort mit dem Antwortpfad "`mailer-daemon@...`" oder `NULL` ein, so erkennt SecurityGateway den besonderen Kode und bestätigt damit, dass die Nachricht eine echte automatisch erstellte Antwort auf eine Nachricht ist, die wirklich von einer Ihrer Domänen aus gesendet wurde. Enthält die Nachrichten den Kode nicht, oder ist seine Gültigkeit abgelaufen, so wird dies ebenfalls festgestellt und protokolliert, und die Nachricht kann abgewiesen werden.

Nachrichten-Bewertung 185 - SecurityGateway berechnet für jede Nachricht eine Nachrichten-Bewertung. Sie stützt sich auf mehrere Prüfungen, die während der Verarbeitung der Nachricht durchgeführt werden. Der Wert verkörpert die Berechnung der Wahrscheinlichkeit, dass die Nachricht eine Spam-Nachricht ist. Die Optionen auf der Seite Nachrichten-Bewertung bestimmen die Aktionen, die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

durchgeführt werden, falls die Bewertung einer Nachricht bestimmte Schwellwerte überschreite. Sie können Schwellwerte bestimmen, ab denen Nachrichten als Spam gekennzeichnet, in Quarantäne gegeben oder während der SMTP-Verbindung abgewiesen werden.

4.1.1 Outbreak Protection

Die Outbreak Protection (OP) ist eine revolutionäre Technik zur Erkennung von Spam und Viren in Echtzeit, die Ihre E-Mail-Infrastruktur vorausschauend binnen Minuten nach einem Ausbruch von Spam oder Viren schützen kann. Die OP arbeitet unabhängig vom Nachrichten-Inhalt im Einzelfall und analysiert auch den Nachrichten-Inhalt nicht nach lexikalischen Methoden. Sie benötigt daher weder heuristische Regeln, noch einen Inhaltsfilter oder Signaturen, die aktualisiert werden müssten. Sie kann auch nicht durch Hinzufügen von Seed-Texten, bewusst abgeänderte oder falsche Schreibweisen, Taktiken des Social Engineering, Sprachbarrieren oder Unterschiede in der Kodiertechnik umgangen oder außer Kraft gesetzt werden. Die OP stützt sich stattdessen auf eine mathematische Analyse der Nachrichtenstruktur und der Art und Weise, wie die Nachricht über SMTP übermittelt wurde, sowie etwaiger Eigenheiten, die dabei aufgetreten sind. Sie analysiert "Verhaltensmuster", die im Zusammenhang mit der Übermittlung der Nachricht auftreten, und vergleicht sie mit ähnlichen Mustern, die aufgrund der weltweiten Analyse von Millionen E-Mail-Nachrichten erfasst und in Echtzeit ausgewertet werden.

Da die Nachrichten weltweit und in Echtzeit ausgewertet werden, wird der Schutz binnen Minuten, oft sogar binnen Sekunden, nach Beginn eines neuen Ausbruchs oder Massenangriffs wirksam. Gerade bei Viren ist dieses Schutzniveau von entscheidender Bedeutung, da die Hersteller herkömmlicher Anti-Viren-Software eine Aktualisierung für die Signaturen ihrer Produkte oft erst Stunden nach Beginn eines Ausbruchs zur Verfügung stellen können, und da weitere Zeit vergeht, bis die Aktualisierungen flächendeckend eingesetzt werden. Während dieser Zeit sind Server ohne die Outbreak Protection für diesen bestimmten Ausbruch anfällig. Bei Spam-Nachrichten verhält es sich ähnlich, da es oft Zeit und Aufwand kostet, die Spam-Nachrichten zu analysieren und aus ihnen sichere Filterregeln abzuleiten, bevor die Nachrichten durch herkömmliche heuristische und inhaltsgestützte Systeme erkannt werden.

Es ist aber wichtig, sich zu vergegenwärtigen, dass die Leistungsmerkmale der Outbreak Protection die herkömmlichen Abwehrmaßnahmen gegen Viren und Spam nicht ersetzen sollen. Die OP stellt eine weitere, besondere Schutzschicht zur Verfügung, die bestehende Abwehrmaßnahmen auf Grundlage von Heuristik, Signaturen und Inhaltsauswertung in SecurityGateway ergänzt. Die OP ist besonders auf die Abwehr großflächiger Massenangriffe abgestimmt. Herkömmliche und auch einzeln abgestimmte oder individuell adressierte Nachrichten können mit den anderen Werkzeugen besser abgefangen werden.

Outbreak Protection stützt sich auf die Technologien Erkennung wiederkehrender Muster und Zero-Hour. Sie leitet aus Ihren eingehenden Nachrichten Muster ab und vergleicht sie mit Mustern, die aus Millionen anderer E-Mail-Nachrichten verschiedener Quellen weltweit täglich entnommen und analysiert werden. Der Inhalt einer Nachricht wird dabei unter keinen Umständen übermittelt, und die ausgewerteten Muster lassen keine Rückschlüsse auf den Inhalt einzelner Nachrichten zu.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Anti-Spam

Anti-Spam Outbreak Protection aktivieren
Die Spam-Abwehr durch die Outbreak Protection ist per Voreinstellung aktiv. Eingehende Nachrichten werden analysiert, um zu prüfen, ob sie Teil eines laufenden Ausbruchs oder Massenangriffs mit Spam sind. Die weiteren Optionen in diesem Abschnitt bestimmen, wie mit Nachrichten verfahren werden soll, die als Teil eines Ausbruchs erkannt werden. Sie bestimmen auch, welche Absender von der Verarbeitung durch die OP ausgenommen sind.

Falls Outbreak Protection feststellt, dass eine Nachricht Spam ist:
Die nachfolgend ausgewählte Option bestimmt, welche Aktion ausgeführt wird, falls OP eine Nachricht als Spam erkennt.

...Nachricht abweisen
Diese Option bewirkt, dass Nachrichten während der SMTP-Übermittlung abgewiesen werden, falls OP bestätigt, dass sie Teil eines Spam-Ausbruchs sind. Die Nachrichten werden nicht in Quarantäne gegeben und auch nicht als Spam gekennzeichnet und dann an die Empfänger zugestellt — sie werden bereits bei der Übermittlung durch den Server blockiert.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass die Outbreak Protection die als Spam erkannten Nachrichten in Quarantäne gibt.

...Nachricht annehmen
Per Voreinstellung nimmt die OP auch Nachrichten an, die als Spam erkannt wurden. Die Bewertung dieser Nachricht wird in Übereinstimmung mit der Option "*... [xx] Punkte zur Nachrichten-Bewertung hinzurechnen*" unten angepasst.

...Betreff kennzeichnen mit [*Text*]
Diese Option ist per Voreinstellung abgeschaltet. Falls Sie diese Option aktivieren, wird der Betreffzeile einer Nachricht eine Kennzeichnung vorangestellt, falls die Outbreak Protection festgestellt hat, dass es sich um eine Spam-Nachricht handelt. Die Voreinstellung für den Kennzeichnungstext lautet "*** SPAM ***"; Sie können den Text aber anpassen, falls Sie dies wünschen.

SecurityGateway kann auch im Rahmen anderer Verarbeitungsfunktionen wahlweise die Betreffzeile von Nachrichten kennzeichnen. Zwei weitere, nachfolgend beschriebene Funktionen der Outbreak Protection lassen sich beispielsweise entsprechend konfigurieren. Stimmen die Kennzeichnungstexte in diesen Funktionen überein, so wird die Kennzeichnung dem Betreff nur einmal hinzugefügt, auch wenn die Bedingungen mehrerer Funktionen für eine Kennzeichnung bei der Nachricht erfüllt sind. Werden jedoch unterschiedliche Kennzeichnungstexte konfiguriert, so werden diese Kennzeichnungen gesondert eingefügt. Geben Sie beispielsweise für alle Funktionen den Kennzeichnungstext "*SPAM*" an, so wird dieser Text nur insgesamt einmal in die Betreffzeile eingefügt, auch wenn die Nachrichten den Bedingungen mehrere Funktionen für

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

eine Kennzeichnung entspricht. Ändern Sie nun den Text für eine Funktion etwa in "*Junk*", und erfüllt die Nachricht die Bedingungen für eine Kennzeichnung nach beiden Funktionen, so werden ihrer Betreffzeile beide Kennzeichnungstexte vorangestellt.

...[xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Diese Option bewirkt, dass der Nachrichten-Bewertung der hier festgelegte Wert hinzugerechnet wird, falls die Outbreak Protection feststellt, dass es sich um eine Spam-Nachricht handelt. Diese Option ist per Voreinstellung aktiv und erhöht die Nachrichten-Bewertung um 5,5 Punkte.

Auch wenn SecurityGateway so konfiguriert ist, dass Nachrichten nicht abgewiesen oder in Quarantäne gegeben sondern zur Zustellung angenommen werden, kann die Nachricht später noch abgewiesen oder in Quarantäne gegeben werden, falls ihre Nachrichten-Bewertung entsprechend hoch ist. Die Höhe der Nachrichten-Bewertung hängt auch von der Konfiguration und den Ergebnissen der anderen Sicherheitsfunktionen 154 und den Optionen auf der Seite Nachrichten-Bewertung 185 ab.

Falls Outbreak Protection feststellt, dass eine Nachricht unter Spam-Verdacht steht:
Die Outbreak Protection kann manchmal nicht abschließend feststellen, ob es sich um eine Spam-Nachricht handelt. Solche zweifelhaften Nachrichten werden als "spamverdächtig" behandelt. Die folgenden Optionen bestimmen, wie die OP mit Nachrichten verfährt, die unter Spam-Verdacht stehen.

...Nachricht abweisen
Diese Option bewirkt, dass Nachrichten während der SMTP-Übermittlung abgewiesen werden, falls OP die Nachrichten als spamverdächtig einstuft. Da bei diesen Nachrichten lediglich ein Spam-*Verdacht* besteht, ist die Nutzung dieser Option nicht zu empfehlen, denn die Nachricht wird nicht in Quarantäne gegeben oder gekennzeichnet sondern abgewiesen.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass die Outbreak Protection die als spamverdächtig eingestuften Nachrichten in Quarantäne gibt.

...Nachricht annehmen
Per Voreinstellung nimmt die OP Nachrichten an, die als spamverdächtig eingestuft wurden. Die Bewertung dieser Nachricht kann, falls Sie dies wünschen, in Übereinstimmung mit der Option "*... [xx] Punkte zur Nachrichten-Bewertung hinzurechnen*" unten angepasst werden.

...Betreff kennzeichnen mit [*Text*]
Diese Option ist per Voreinstellung abgeschaltet. Falls Sie diese Option aktivieren, wird der Betreffzeile einer Nachricht eine Kennzeichnung vorangestellt, falls die Outbreak Protection die Nachricht als spamverdächtig eingestuft hat. Die Voreinstellung für den Kennzeichnungstext lautet "*** POTENTIAL SPAM ***"; Sie können den Text aber anpassen, falls Sie dies wünschen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

...[xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Diese Option bewirkt, dass der Nachrichten-Bewertung der hier festgelegte Wert hinzugerechnet wird, falls die Outbreak Protection eine Nachricht als spamverdächtig einstuft. Diese Option ist per Voreinstellung aktiv und erhöht die Nachrichten-Bewertung 185 um 2,0 Punkte.

Falls Outbreak Protection feststellt, dass es sich um eine Massennachricht handelt:
Die Outbreak Protection schlägt manchmal auch bei bestimmten Nachrichten an, wenn diese an sehr viele Empfänger gerichtet sind, aber nicht eindeutig als Spam erkannt werden können, etwa weil sie nicht durch einen bekannten Spammer oder ein Botnetz versandt wurden. Dies trifft manchmal auf legitime Massennachrichten und Newsletter zu. Die OP stuft solche Arten von Nachrichten als "Bulk", nicht aber als Spam ein. Die folgenden Optionen bestimmen, wie mit solchen Nachrichten verfahren wird.

...Nachricht abweisen
Diese Option bewirkt, dass Nachrichten während der SMTP-Übermittlung abgewiesen werden, falls OP die Nachrichten als "Bulk" einstuft. Die Nutzung dieser Option ist nicht zu empfehlen, da sie dazu führen kann, dass legitime Nachrichten mit großem Empfängerkreis abgewiesen werden.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass die Outbreak Protection die als "Bulk" eingestuften Nachrichten in Quarantäne gibt"

...Nachricht annehmen
Per Voreinstellung nimmt die OP Nachrichten an, die als "Bulk" eingestuft wurden, statt sie abzuweisen oder in Quarantäne zu geben. Solche Nachrichten können Teil sehr großer Mailinglisten oder Nachrichten mit großem Empfängerkreis sein.

...Betreff kennzeichnen mit [*Text*]
Diese Option ist per Voreinstellung abgeschaltet. Falls Sie diese Option aktivieren, wird der Betreffzeile einer Nachricht eine Kennzeichnung vorangestellt, falls die Outbreak Protection die Nachricht als "Bulk" eingestuft hat. Die Voreinstellung für den Kennzeichnungstext lautet "*** BULK ***"; Sie können den Text aber anpassen, falls Sie dies wünschen.

...[xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Diese Option bewirkt, dass der Nachrichten-Bewertung der hier festgelegte Wert hinzugerechnet wird, falls die Outbreak Protection eine Nachricht als "Bulk" einstuft. Diese Option ist per Voreinstellung aktiv und erhöht die Nachrichten-Bewertung um 3,0 Punkte.

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Per Voreinstellung sind Nachrichten von Absendern auf der Weißen Liste 275 von den Abwehrmaßnahmen der Outbreak Protection gegen Spam ausgenommen.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Diese Option ist per Voreinstellung aktiv. Sie nimmt Nachrichten von der Verarbeitung durch die Outbreak Protection aus, die über Verbindungen mit Echtheitsbestätigung übermittelt wurden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nachrichten von Mailservern der Domäne ausnehmen
Nachrichten, die über Ihre Mailserver der Domäne[79] übermittelt wurden, sind von der Verarbeitung durch die Outbreak Protection per Voreinstellung ausgenommen. Falls auch solche Nachrichten durch die Outbreak Protection verarbeitet werden sollen, deaktivieren Sie diese Option.

Anti-Virus

Anti-Virus Outbreak Protection aktivieren
Die Viren-Abwehr durch die Outbreak Protection ist per Voreinstellung aktiv. Eingehende Nachrichten werden analysiert, um zu prüfen, ob sie Teil eines laufenden Ausbruchs oder Massenangriffs mit Viren sind. Die weiteren Optionen in diesem Abschnitt bestimmen, wie mit Nachrichten verfahren werden soll, die als Teil eines Ausbruchs erkannt werden. Sie bestimmen auch, welche Absender von der Verarbeitung durch die OP ausgenommen sind.

Falls Outbreak Protection feststellt, dass eine Nachricht infiziert ist:
Die nachfolgend ausgewählte Option bestimmt, welche Aktion ausgeführt wird, falls OP eine Nachricht als infiziert erkennt.

...Nachricht abweisen
SecurityGateway weist per Voreinstellung solche Nachrichten während der SMTP-Übermittlung ab, von denen die Outbreak Protection festgestellt hat, dass sie Teil eines Viren-Ausbruchs sind.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass Nachrichten in Quarantäne gegeben werden, von denen die Outbreak Protection festgestellt hat, dass sie infiziert sind.

Nachrichten von IP-Adressen auf der Weißen Liste ausnehmen
Diese Option bewirkt, dass Nachrichten von den Abwehrmaßnahmen der Outbreak Protection gegen Viren ausgenommen sind, falls Sie von einer IP-Adresse auf der Weißen Liste[281] oder einem Host auf der Weißen Liste[278] gesendet wurden.

Nachrichten von Mailservern der Domäne ausnehmen
Diese Option bewirkt, dass Nachrichten, die über Ihre Mailserver der Domäne[79] übermittelt wurden, von den Abwehrmaßnahmen der Outbreak Protection gegen Viren ausgenommen sind.

Einstellungen für den Proxy

Die Outbreak Protection von SecurityGateway über HTTP mit dem Online-Dienst Outbreak Protection kommunizieren können. Falls die Outbreak Protection diese Verbindung über einen Proxy-Server herstellen muss, können Sie mithilfe der Optionen in diesem Abschnitt den HTTP-Proxy konfigurieren.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für die Outbreak Protection für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

4.1.2 Heuristik und Bayes

SecurityGateway für E-Mail-Server nutzt eine angepasste Hochleistungsversion des beliebten quelloffenen Projekts SpamAssassin™ und stellt hierüber Heuristik-Regeln und Bayes'sche Bewertungsverfahren zur Verfügung. Nachrichten werden diesem Prozess übergeben und erhalten, in Abhängigkeit von ihrem Inhalt, eine Bewertung. SecurityGateway gestattet statt der Nutzung des internen Moduls auch wahlweise die Nutzung eines externen SpamAssassin™-Daemons.

Konfiguration

Nachrichtenanalyse durch Heuristik-Regeln und Bayes'sche Bewertung
Per Voreinstellung ist diese Option aktiv. Nachrichten werden mithilfe der heuristischen Regeln und der Bayes'schen Bewertungsverfahren analysiert, und sie erhalten aufgrund des Ergebnisses dieser Analyse eine durch SpamAssassin erstellte Bewertung. Falls Sie diese Analyse nicht durchführen wollen, deaktivieren Sie diese Option. Die weiteren Optionen auf dieser Seite sind dann nicht mehr verfügbar.

Sie können die Aktualisierung der Heuristik-Regeln und verschiedene Optionen zur Bayes'schen Bewertung im Konfigurationsdialog für SGSpamD 164 konfigurieren. Sie erreichen diesen Dialog, indem Sie auf die Verknüpfung *Klicken Sie hier, um SGSpamD zu konfigurieren.* 164 unterhalb der Option "*Lokales integriertes SpamAssassin-Modul (SGSpamD) nutzen*" am Ende der Seite klicken.

Bewertung des SpamAssassins der Nachrichten-Bewertung hinzurechnen
Diese Option ist per Voreinstellung aktiv. Sie bewirkt, dass die Bewertung, die SpamAssassin errechnet hat, der Nachrichten-Bewertung hinzugerechnet wird. Indem Sie die durch SpamAssassin errechnete Bewertung der Nachrichten-Bewertung hinzurechnen, können Sie die Wahrscheinlichkeit erhöhen, dass Spam erkannt wird, obwohl weder die Bewertung des SpamAssassins noch die Ergebnisse aus anderen Prüfverfahren für sich allein genommen zu einem ausreichend hohen Wert führen könnten. Sie nutzen damit also eine zusätzliche Schutzschicht in der Spam-Abwehr.

Nachricht abweisen ab einer SpamAssassin-Bewertung von...
Diese Option legt einen Schwellwert für die Bewertung durch den SpamAssassin fest, ab dessen Erreichen eine Nachricht abgewiesen wird. Liegt die durch den SpamAssassin errechnete Bewertung mindestens bei dem hier angegebenen Wert, oder übersteigt sie ihn, so wird die Nachricht bereits während der SMTP-Verbindung abgewiesen, nicht aber in Quarantäne gegeben und nicht nach Durchlaufen der übrigen Prüfverfahren normal zugestellt. Falls Sie diese Option zusammen mit der folgenden Option "*Nachricht in Quarantäne geben ab einer SpamAssassin-Bewertung von...*" nutzen, soll der Wert, ab dem Nachrichten abgewiesen werden, immer über dem Wert liegen, ab dem Nachrichten in Quarantäne gegeben werden. Wären die beiden Schwellwerte vertauscht, so würde aufgrund der SpamAssassin-Bewertung keine Nachricht in Quarantäne gegeben werden, denn alle Nachrichten, die den Schwellwert für die Quarantäne erreichen, würden bereits abgewiesen sein. Die Voreinstellung für den Schwellwert zum Abweisen ist `12,0`.

Nachricht in Quarantäne geben ab einer SpamAssassin-Bewertung von...
Diese Option legt einen Schwellwert für die Bewertung durch den SpamAssassin fest, ab dessen erreichen eine Nachricht in Quarantäne gegeben wird. Liegt die durch den SpamAssassin errechnete Bewertung mindestens bei dem hier angegebenen Wert, oder übersteigt sie ihn, so wird die Nachricht in Quarantäne

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

gegeben. Nachrichten in Quarantäne können durch den Empfänger oder Administrator nach einer Anmeldung an SecurityGateway durchgesehen und verwaltet werden. Falls Sie diese Option zusammen mit der vorhergehenden Option "*Nachricht abweisen ab einer SpamAssassin-Bewertung von...*" nutzen, soll der Wert, ab dem Nachrichten in Quarantäne gegeben werden, niedriger angesetzt sein als der Wert, ab dem Nachrichten abgewiesen werden. Die Voreinstellung für diese Option beträgt `5,0`.

Sie sollten die Leistung der Heuristik und der Bayes-Verfahren überwachen und mit der Zeit die Schwellwerte zum Abweisen und für die Quarantäne an Ihre Bedürfnisse genau anpassen. Im allgemeinen sollten die voreingestellten Werte die meisten Spam-Nachrichten erfassen. Sie sollten nur vergleichsweise wenige falsche Negative (nicht erkannte Spam-Nachrichten) und nur selten falsche Positive (Nachrichten, die irrtümlich als Spam eingestuft werden) auslösen. Die Voreinstellung für den Schwellwert zum Abweisen von Nachrichten in Höhe von 12 ist ein guter Ausgangspunkt, da legitime Nachrichten in den meisten Fällen einen so hohen Wert nicht erreichen.

Ausschlüsse

Nachrichten ausnehmen, die größer sind als [xx] KB
Falls Sie Nachrichten über einer bestimmten Größe von der Verarbeitung durch Heuristik und Bayes ausnehmen wollen, geben Sie hier die Größe an, die die Nachrichten überschreiten müssen. Große Nachrichten werden selten als Spam-Nachrichten eingestuft. Indem sie aus dem Prüfvorgang ausgeschlossen werden, können unter Umständen die Systemressourcen deutlich entlastet werden.

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Per Voreinstellung nimmt SecurityGateway Nachrichten von der Verarbeitung durch Heuristik und Bayes aus, falls diese von einem Absender auf der Weißen Liste 275 stammen. Falls Sie diese Nachrichten nicht ausnehmen wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Diese Option bewirkt, dass Nachrichten von der Verarbeitung durch Heuristik und Bayes ausgenommen sind, falls sie über eine SMTP-Verbindung mit Echtheitsbestätigung übermittelt wurden. Diese Option ist per Voreinstellung aktiv.

Nachrichten von Mailservern der Domäne ausnehmen
Per Voreinstellung sind Nachrichten, die über Ihre Mailserver der Domäne 79 versandt werden, von der Verarbeitung durch Heuristik und Bayes ausgenommen. Falls Sie solche Nachrichten nicht ausnehmen wollen, deaktivieren Sie diese Option.

Standort (Alle Domänen)

Lokales integriertes SpamAssassin-Modul (SGSpamD) nutzen
Diese Option bewirkt, dass das in SecurityGateway integrierte SpamAssassin-Modul, das in einem eigenen Daemon implementiert ist, verwendet wird. Dieses Modul wird auch als SecurityGateway Spam Daemon (SGSpamD) bezeichnet. Um

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

SGSpamD zu konfigurieren, klicken Sie auf die Verknüpfung *Klicken Sie hier, um SGSpamD zu konfigurieren* 164. Falls Sie ein anderes SpamAssassin-Modul, das an einem externen Standort ausgeführt wird, nutzen möchten, wählen Sie stattdessen die folgende Option "*Externen SpamAssassin-Daemon...*".

Externen SpamAssassin-Daemon (SpamD) nutzen
Wählen Sie diese Option, um die Nachrichten durch einen SpamAssassin-Daemon an einem anderen Standort verarbeiten zu lassen und das integrierte Modul SGSpamD nicht zu nutzen.

Host-Adresse:
Geben Sie hier die IP-Adresse des externen SpamD ein.

Port:
Geben Sie hier den Port an, auf dem der externe SpamD ausgeführt wird.

Test
Um die Verbindung mit dem externen SpamD zu prüfen, klicken Sie auf dieses Steuerelement.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für Heuristik und Bayes für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.1.2.1 SGSpamD-Konfiguration

Das System der Heuristik-Regeln nutzt einen Prozess, in dem der Inhalt jeder Nachricht mit einem Satz feststehender Regeln verglichen wird, um festzustellen, wie wahrscheinlich ist ist, dass es sich um eine Spam-Nachricht handelt. Jeder Regel ist ein bestimmter Wert zugeordnet, sodass sich die Bewertung des SpamAssassins aus der Summe der Werte aller Regeln ergibt, deren Kriterien die Nachricht erfüllt. Die Regeln und ihre Werte werden regelmäßig angepasst und geändert, um mit aktuellen Trends in Spam- und Junk-Nachrichten schrittzuhalten. Der SGSpamD von SecurityGateway kann automatisch in bestimmten Intervallen nach Aktualisierungen für die Heuristik-Regeln suchen; alternativ können Sie auch von Hand nach solchen Aktualisierungen suchen.

Die Bayes'sche Bewertung ist ein statistisches Verfahren, das wahlweise benutzt werden kann, um Spam- und normale Nachrichten zu analysieren und die Genauigkeit der Spam-Erkennung mit der Zeit zu erhöhen. Sie können einen Ordner für Spam-Nachrichten und einen Ordner für normale Nachrichten bestimmen, die entweder manuell oder automatisch in bestimmten Intervallen ausgewertet werden. Alle Nachrichten, die sich zum Auswertungszeitpunkt in diesen Ordnern befinden, werden analysiert und indiziert; sie durchlaufen das "Bayes'sche Lernverfahren". Neue Nachrichten werden dann mit den Ergebnissen verglichen, die aus dem Lernverfahren gewonnen werden. Der durch Bayes'sche Bewertung ermittelte Wert für die Nachrichten kann die Bewertung des SpamAssassins erhöhen oder herabsetzen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Aktualisierungen für Heuristik-Regeln

Jeden Tag um Mitternacht nach Aktualisierungen für die Heuristik-Regeln suchen
Diese Option bewirkt, dass SecurityGateway jeden Tag um Mitternacht automatisch nach Aktualisierungen für die Heuristik-Regeln sucht.

Nach Aktualisierungen für Heuristik-Regeln in folgendem Intervall suchen [xx] Stunden
Wollen Sie nicht nur einmal pro Tag sondern in einem in Stunden festgelegten Intervall nach Aktualisierungen für die Heuristik-Regeln suchen, so aktivieren Sie diese Option und bestimmen Sie das Intervall in Stunden.

Nicht nach Aktualisierungen für die Heuristik-Regeln suchen
Diese Option bewirkt, dass SecurityGateway nicht automatisch nach Aktualisierungen für die Heuristik-Regeln sucht. Sie können dennoch von Hand nach den Aktualisierungen suchen, indem Sie die Verknüpfung "*Klicken Sie hier...*" weiter unten anklicken.

SA-Update als Teil der Aktualisierung ausführen
Falls Sie Aktualisierungen nicht nur von MDaemon Technologies, sondern auch von `updates.spamassassin.org` abrufen wollen, aktivieren Sie diese Option. Sie stellt sicher, dass die Regelsätze Ihres SpamAssassins immer auf dem aktuellen Stand gehalten werden. Die Option ist per Voreinstellung aktiv.

Klicken Sie hier, um jetzt nach Aktualisierungen für die Heuristik-Regeln zu suchen.
Um sofort nach Aktualisierungen für die Heuristik-Regeln zu suchen, klicken Sie auf diese Verknüpfung.

Bayes'sche Bewertung

Bayes'sche Bewertung aktivieren
Um das Bayes'sche Bewertungssystem des SGSpamD zu aktivieren, aktivieren Sie diese Option, Die SpamAssassin-Bewertung aller Nachrichten wird dann anhand der Ergebnisse der jeweils bekannten Bayes-Statistiken überprüft und, falls erforderlich, angepasst.

Die SpamAssassin-Bewertung kann erst dann anhand der Bayes'schen Bewertung angepasst werden, wenn genügend Proben von Spam- und von normalen Nachrichten vorliegen und analysiert wurden. Das Analyseverfahren bezeichnet man auch als "Bayes'sches Lernverfahren", und es ist erforderlich, damit ein ausreichender Vorrat an Statistikdaten für die Bayes'sche Bewertung zur Verfügung steht. Sobald Sie dem Bayes'schen Lernverfahren diese Nachrichten zur Analyse zur Verfügung gestellt haben, kann es die Ergebnisse dieser Auswertung verwenden, um die SpamAssassin-Bewertung der Nachrichten zu prüfen und anzupassen. Durch die laufende Analyse immer neuer Nachrichten wird die Bayes'sche Bewertung mit der Zeit immer genauer.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Normale Nachrichten, die erlernt werden müssen:
Dies ist die Mindestanzahl normaler Nachrichten, die analysiert werden müssen, bevor das Bayes'sche Bewertungssystem beginnen kann, selbst Nachrichten zu bewerten. Die Voreinstellung beträgt 200 Nachrichten.

Spam-Nachrichten, die erlernt werden müssen:
Dies ist die Mindestanzahl an Spam-Nachrichten, die analysiert werden müssen, bevor das Bayes'sche Bewertungssystem beginnen kann, selbst Nachrichten zu bewerten. Die Voreinstellung beträgt 200 Nachrichten.

Bayes'sches Lernverfahren

Bayes'sches Lernverfahren jeden Tag um Mitternacht ausführen
Diese Option bewirkt, dass das Bayes'sche Lernverfahren die Nachrichten in den Ordnern für Spam und normale Nachrichten einmal täglich automatisch auswertet. Die Auswertung beginnt jeweils um Mitternacht.

Bayes'sches Lernverfahren ausführen alle [xx] Stunden
Diese Option bewirkt, dass das Bayes'sche Lernverfahren die Nachrichten in den Ordnern für Spam und normale Nachrichten in dem hier angegebenen Intervall automatisch auswertet. Die Auswertung beginnt, sobald die hier in Stunden angegebene Zeit seit der letzten Auswertung vergangen ist.

Bayes'sches Lernverfahren nicht zeitgesteuert ausführen
Diese Option bewirkt, dass das Bayes'sche Lernverfahren nicht automatisch und zeitgesteuert ausgeführt wird. Sie können die Auswertung dennoch jederzeit von Hand auslösen, indem Sie auf die Verknüpfung "*Klicken Sie hier, um das Bayes'sche Lernverfahren jetzt auszuführen.*" weiter unten klicken.

Pfad zum Verzeichnis mit bekanntem Spam (falsche Negative):
Hier wird der Pfad für den Ordner angegeben, der die als Spam eingestuften Nachrichten enthält. Die Nachrichten können hier von Hand oder mithilfe der Optionen zum automatischen Bayes'schen Lernvorgang automatisch abgelegt werden.

Pfad zum Verzeichnis mit bekannten normalen Nachrichten (falsche Positive):
Hier wird der Pfad für den Ordner angegeben, der die als normal eingestuften Nachrichten enthält. Die Nachrichten können hier von Hand oder mithilfe der Optionen zum automatischen Bayes'schen Lernverfahren automatisch abgelegt werden.

Weiterleitungsadresse für Spam:
In diesem Eingabefeld können Sie die Adresse festlegen, an die Ihre Nutzer Spam-Nachrichten weiterleiten können. Diese weitergeleiteten Nachrichten kann das Bayes'sche Lernverfahren auswerten. Per Voreinstellung nutzt SecurityGateway eine Adresse nach dem Muster "`SpamLearn[@beliebigeSGDomäne.com]`"; Sie können diese Adresse aber frei anpassen. Nachrichten können nur über Verbindungen mit Echtheitsbestätigung durch SMTP-AUTH an diese Adresse gesendet werden. Die Nachrichten müssen als Dateianlagen des Typs "`message/rfc822`" weitergeleitet werden; Nachrichten eines anderen Typs werden nicht verarbeitet. Falls Sie in dieses Feld eine abweichende Adresse eintragen, dürfen Sie nur den Postfachnamen, nicht aber das Zeichen "@" und nicht die Domäne eintragen. Zulässige Einträge für dieses Feld sind beispielsweise "`Spam`", "`SpamLearn`", "`SpamMail`" und ähnliches. Nachrichten können an diese

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Adresse unter allen SecurityGateway-Domänen weitergeleitet werden (z.B. `SpamLearn@example.com`, `SpamLearn@company.mail` usw.).

Weiterleitungsadresse für normale Nachrichten:
In diesem Eingabefeld können Sie die Adresse festlegen, an die Ihre Nutzer normale Nachrichten weiterleiten können. Diese weitergeleiteten Nachrichten kann das Bayes'sche Lernverfahren auswerten. Per Voreinstellung nutzt SecurityGateway eine Adresse nach dem Muster "`NonSpamLearn[@beliebigeSGDomäne.com]`"; Sie können diese Adresse aber frei anpassen. Nachrichten können nur über Verbindungen mit Echtheitsbestätigung durch SMTP-AUTH an diese Adresse gesendet werden. Die Nachrichten müssen als Dateianlagen des Typs "`message/rfc822`" weitergeleitet werden; Nachrichten eines anderen Typs werden nicht verarbeitet. Falls Sie in dieses Feld eine abweichende Adresse eintragen, dürfen Sie nur den Postfachnamen, nicht aber das Zeichen "@" und nicht die Domäne eintragen. Zulässige Einträge für dieses Feld sind beispielsweise "`NonSpam`", "`NonSpamLearn`", "`NormaleMail`" und ähnliches. Nachrichten können an diese Adresse unter allen SecurityGateway-Domänen weitergeleitet werden (z.B. `NonSpamLearn@example.com`, `NonSpamLearn@company.mail` usw.).

Nachrichten vom Lernverfahren ausschließen bei einer Größe über [xx] Byte
Da größere Nachrichten üblicherweise keine Spam-Nachrichten sind, und da die Analyse solcher Nachrichten das System stark belasten kann, werden per Voreinstellung Nachrichten mit einer Größe über 50.000 Byte nicht analysiert. Sie können diesen Wert anpassen oder die Option auch deaktivieren, falls Sie die Nachrichten ohne Rücksicht auf ihre Größe analysieren wollen.

Klicken Sie hier, um das Bayes'schen Lernverfahren jetzt auszuführen.
Sie können durch einen Klick auf diese Verknüpfung jederzeit das Bayes'sche Lernverfahren auslösen. Falls das Lernverfahren auch zeitgesteuert durchgeführt wird, löst diese Verknüpfung eine zusätzliche Verarbeitung aus und beeinflusst den Zeitplan nicht.

Automatischer Bayes'scher Lernvorgang

Automatischen Bayes'schen Lernvorgang aktivieren
Sie können für den automatischen Bayes'schen Lernvorgang Schwellwerte für die Nachrichten-Bewertung von legitimen Nachrichten und Spam festlegen. Eine Nachricht, deren endgültige Nachrichten-Bewertung unterhalb der Schwelle für normale Nachrichten liegt, wird durch den automatischen Lernvorgang als normale Nachricht behandelt, und eine Nachricht, die über dem Schwellwert für Spam-Nachrichten liegt, wird als Spam behandelt. Der automatische Lernvorgang sollte zwar umsichtig eingesetzt werden, er kann aber sehr hilfreich sein, falls die Schwellwerte richtig gesetzt sind. Der Lernvorgang kann abgelaufene Token, die aus der Datenbank entfernt werden (vgl. Bayes'sche Datenbank weiter unten) automatisch ersetzen. Er kann dem Bayes'schen Lernverfahren auch laufend neue Nachrichten zur Auswertung liefern, ohne dass abgelaufene Token durch manuelles Training ersetzt werden müssten.

Nachrichten mit einer Bewertung unter [xx] als legitim behandeln
Nachrichten mit einer Nachrichten-Bewertung unter diesem Wert werden als legitime Nachrichten behandelt und entsprechend an das Bayes'sche Lernverfahren übergeben.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

...normale Nachrichten nur von Mailservern der Domäne und aus echtheitsbestätigten Verbindungen erlernen
Diese Option beschränkt den automatischen Bayes'schen Lernvorgang für legitime Nachrichten auf Nachrichten, die in echtheitsbestätigten Verbindungen oder durch einen Ihrer Mailserver der Domäne 79 übermittelt wurden. Bei Nutzung dieser Option werden eingehende Nachrichten von externen Quellen unabhängig von ihrer endgültigen Nachrichten-Bewertung nur dann für das Bayes'sche Lernverfahren herangezogen, wenn sie in einer echtheitsbestätigten Verbindung oder durch einen Mailserver der Domäne übermittelt wurden. Sie können dennoch von Hand die übrigen legitimen Nachrichten in den oben festgelegten Ordner für normale Nachrichten kopieren, sodass das System auch aus ihnen lernen kann.

Nachrichten mit einer Bewertung über [xx] als Spam behandeln
Nachrichten mit einer Nachrichten-Bewertung über diesem Wert werden als Spam-Nachrichten behandelt und entsprechend an das Bayes'sche Lernverfahren übergeben.

...Spam nur aus eingehenden Nachrichten erlernen
Diese Option beschränkt den automatischen Bayes'schen Lernvorgang für Spam-Nachrichten auf eingehende Nachrichten. Bei Nutzung dieser Option werden abgehende Nachrichten unabhängig von ihrer endgültigen Nachrichten-Bewertung nicht für das Bayes'sche Lernverfahren herangezogen. Sie können dennoch von Hand Nachrichten in den oben festgelegten Ordner für Spam kopieren.

Bayes'sche Datenbank

Automatisches Verfallen Bayes'scher Token aktivieren
Diese Option gestattet es dem Bayes'schen Bewertungssystem, abgelaufene Token automatisch aus der Datenbank zu entfernen, sobald die Zahl der Datenbank, die weiter unten als Höchstzahl angegeben ist, erreicht wurde. Die Begrenzung der Anzahl der Token kann verhindern, dass die Datenbank übermäßig groß wird und sich die Verarbeitung zu sehr verlangsamt.

Höchstzahl der Bayes'schen Token in der Datenbank:
Dies ist die Höchstzahl der Token, die gleichzeitig in der Datenbank abgelegt sein dürfen. Wird die Höchstzahl der Token erreicht, so löscht das Bayes'sche Bewertungssystem die ältesten Token, bis die Gesamtzahl der Token in der Datenbank auf 75 % der Höchstzahl, keinesfalls aber unter 100.000, gesunken ist. Unabhängig davon, wie viele Token verfallen sind, kann die Zahl der Token nicht unter den höheren der angegebenen Werte sinken. Beachte: 150.000 Token in der Datenbank belegen etwa 8 MB.

Erweitert

Höchstzahl der Threads zur Nachrichtenverarbeitung (1 - 6):
Diese Option bestimmt, wie viele Threads zur Nachrichtenverarbeitung SGSpamD gleichzeitig nutzen darf. Die zulässigen Werte gehen von 1 bis 6 Threads. Die Voreinstellung beträgt 4.

Höchstzahl der TCP-Verbindungen je Thread (10 - 200):
Diese Option bestimmt, wie viele TCP-Verbindungen SGSpamD je Verarbeitungsthread gleichzeitig aufbauen darf. Die zulässigen Werte gehen von 10 bis 200. Die Voreinstellung beträgt 200.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

4.1.3 Schwarze Listen für DNS (DNSBL)

Schwarze Listen für DNS (nach der englischen Bezeichnung DNS Blacklists auch kurz als DNSBL bezeichnet) können helfen, zu verhindern, dass Spam-Nachrichten Ihre Benutzer erreichen. Für diese Sicherheitsfunktion können Sie mehrere Schwarze Listen für DNS konfigurieren; solche Dienste unterhalten Listen von Servern, von denen bekannt ist, dass sie Spam durchleiten. Die Listen werden immer abgefragt, wenn ein Dritter versucht, eine Nachricht an eine Ihrer Domänen zu senden. Ist die IP der Gegenstelle auf einer Schwarzen Liste erfasst, so wird die Nachricht abgewiesen, in Quarantäne gegeben oder gekennzeichnet.

Diese Funktion kann in den meisten Fällen verhindern, dass Spam-Nachrichten Ihre Benutzer erreichen. Allerdings werden manche Server auch irrtümlich in eine Schwarze Liste eingetragen; diese Funktion kann daher zu Problemen führen, falls sie dazu verwendet wird, Nachrichten von IPs auf einer Schwarzen Liste unmittelbar abzuweisen. Sie ist dennoch nützlich, insbesondere zusammen mit den anderen Funktionen zur Spam-Abwehr, die SecurityGateway bietet, wie etwa den Schwarzen Listen für URI, der Nachrichten-Bewertung, und den Optionen Heuristik und Bayes.

Konfiguration

DNSBL-Abfragen aktivieren
Diese Option aktiviert die Abfrage der Schwarzen Listen für DNS bei eingehenden Nachrichten. SecurityGateway fragt die IP-Adresse des Absender-Hosts bei allen unten angegebenen DNSBL-Hosts ab. Ergibt die Abfrage einen Treffer, aus dem sich ergibt, dass die IP-Adresse in einer Schwarzen Liste erfasst ist, so wird die Nachricht abgewiesen, in Quarantäne gegeben oder angenommen und gekennzeichnet, je nach dem, welche Vorgehensweise Sie in den folgenden Optionen gewählt haben. Die Option ist per Voreinstellung aktiv.

Falls der Server des Absenders einer Nachricht erfasst ist:

...Nachricht abweisen
Diese Option bewirkt, dass eingehende Nachrichten, die durch IP-Adressen auf einer Schwarzen Liste übermittelt werden, während der SMTP-Verbindung abgewiesen werden. Falls es gewünscht ist, kann SecurityGateway beim Abweisen der Nachricht statt der sonst gesendeten Meldung "Benutzer unbekannt" auch eine benutzerdefinierte Meldung senden, die der Gegenstelle Auskunft darüber gibt, warum die Nachricht abgewiesen wurde. Mit jedem DNSBL-Host kann, wenn sein Eintrag erstellt wird, eine eigene Meldung verknüpft werden; hierzu dient das Eingabefeld *Meldung* weiter unten. Falls SecurityGateway statt der sonst gesendeten Meldung "Benutzer unbekannt" diese angepassten Meldungen senden soll, aktivieren Sie die Option *Beim Abweisen einer Nachricht "Meldung" statt "Benutzer unbekannt" senden* weiter unten.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass Nachrichten von IP-Adressen auf einer Schwarzen Liste in Quarantäne gegeben werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

...Nachricht annehmen
Per Voreinstellung werden Nachrichten von IP-Adressen auf einer Schwarzen Liste zur Zustellung angenommen. Sie können dann als Spam gekennzeichnet werde, ihrer Betreffzeile kann ein Kennzeichnungstext vorangestellt werden, und ihre Nachrichten-Bewertung kann angepasst werden. Diese Option gestattet es den Mailservern oder Benutzern, die diese Nachricht im weiteren Verlauf empfangen, die Nachricht auf Grundlage der DNSBL-Abfrageergebnisse von SecurityGateway selbst zu filtern.

...Betreff kennzeichnen mit [*Text*]
Diese Option bewirkt, dass der Betreffzeile einer Nachricht ein Kennzeichnungstext vorangestellt wird, falls die Nachricht von einer IP-Adresse auf einer Schwarzen Liste übermittelt wird. Wird diese Option aktiviert, so lautet die Voreinstellung für den Kennzeichnungstext "*** SPAM ***"; Sie können den Text aber anpassen, falls dies gewünscht ist.

SecurityGateway kann auch im Rahmen anderer Verarbeitungsfunktionen wahlweise die Betreffzeile von Nachrichten kennzeichnen. Die Funktionen Nachrichten-Bewertung 185 und Schwarze Listen für URI (URIBL) 172 lassen sich beispielsweise entsprechend konfigurieren. Stimmen die Kennzeichnungstexte in diesen Funktionen überein, so wird die Kennzeichnung dem Betreff nur einmal hinzugefügt, auch wenn die Bedingungen mehrerer Funktionen für eine Kennzeichnung bei der Nachricht erfüllt sind. Werden jedoch unterschiedliche Kennzeichnungstexte konfiguriert, so werden diese Kennzeichnungen gesondert eingefügt. Geben Sie beispielsweise für alle Funktionen den Kennzeichnungstext "*SPAM*" an, so wird dieser Text nur insgesamt einmal in die Betreffzeile eingefügt, auch wenn die Nachrichten den Bedingungen mehrere Funktionen für eine Kennzeichnung entspricht. Ändern Sie nun den Text für die Funktion DNSBL in "*DNS blacklisted*", und erfüllt die Nachricht die Bedingungen für eine Kennzeichnung nach beiden Funktionen, so werden ihrer Betreffzeile sowohl "*SPAM*" als auch "*DNS blacklisted*" vorangestellt.

... [XX] Punkte zur Nachrichten-Bewertung hinzurechnen
Diese Option bewirkt, dass der Nachrichten-Bewertung der hier festgelegte Wert hinzugerechnet wird, falls ein Treffer auf einer Schwarzen Liste gefunden wird. Diese Option ist per Voreinstellung aktiv und erhöht die Nachrichten-Bewertung um 5,0 Punkte.

Auch wenn SecurityGateway so konfiguriert ist, dass Nachrichten nicht abgewiesen oder in Quarantäne gegeben sondern zur Zustellung angenommen werden, kann die Nachricht später noch abgewiesen oder in Quarantäne gegeben werden, falls ihre Nachrichten-Bewertung entsprechend hoch ist. Die Höhe der Nachrichten-Bewertung hängt auch von der Konfiguration und den Ergebnissen der anderen Sicherheitsfunktionen 154 und den Optionen auf der Seite Nachrichten-Bewertung 185 ab.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausschlüsse

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Per Voreinstellung sind Nachrichten von Absendern auf der Weißen Liste[275] von den DNSBL-Abfragen ausgenommen. Falls Sie die DNSBL-Abfragen auch für Absender auf der Weißen Liste durchführen wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Diese Option ist per Voreinstellung aktiv. Sie nimmt Nachrichten von der DNSBL-Abfrage aus, die über Verbindungen mit Echtheitsbestätigung übermittelt wurden.

Nachrichten von Mailservern der Domäne sind immer ausgenommen.
Nachrichten, die durch einen Mailserver der Domäne[79] übermittelt werden, sind von den DNSBL-Abfragen immer ausgenommen.

DNSBL-Hosts (Alle Domänen)

Neuer Host:
Um der Liste der DNSBL-Hosts einen neuen Eintrag hinzuzufügen, tragen Sie in dieses Feld den Namen des Hosts ein, der abgefragt werden soll (zum Beispiel zen.spamhaus.org), tragen Sie in das nächste Feld die zugehörige *Meldung* ein, und klicken Sie dann auf *Hinzufügen*.

Meldung:
Dies ist die Meldung, die mit dem oben eingetragenen *Neuen Host* verknüpft wird. Die Meldung wird in das Protokoll eingetragen, wenn SecurityGateway eine IP-Adresse auf einer Schwarzen Liste findet. Sie wird auch der Gegenstelle während des SMTP-Protokolldialogs übermittelt, falls die Nachricht wegen des Treffers während der SMTP-Verbindung abgewiesen wird und die Option *Beim Abweisen einer Nachricht "Meldung" statt "Benutzer unbekannt" senden* weiter unten aktiv ist. Sie können in der Meldung das Makro IP verwenden; es wird durch die IP-Adresse ersetzt, die in einer Schwarzen Liste eingetragen ist.

Hinzufügen
Nachdem Sie den *Neuen Host* und die zugehörige *Meldung* eingetragen haben, klicken Sie auf dieses Steuerelement, um den neuen Eintrag der Liste der DNSBL-Hosts hinzuzufügen.

Entfernen
Falls Sie einen Eintrag aus der Liste der DNSBL-Hosts löschen wollen, wählen Sie den Eintrag aus, und klicken Sie auf dieses Steuerelement.

DNSBL-Abfragen beenden, sobald IP der Gegenstelle auf einem Host gefunden wird
Es kommt oft vor, dass die Kopfzeilen einer Nachricht mehrere IP-Adressen enthalten, und dass diese über mehrere DNSBL-Hosts abgefragt werden. Per Voreinstellung beendet SecurityGateway die Abfragen über die DNSBL-Hosts, sobald eine IP-Adresse auf einer Schwarzen Liste gefunden wurde. Falls Sie auch nach einem Treffer die Abfragen für alle anderen IP-Adressen über alle DNSBL-Hosts durchführen wolle, deaktivieren Sie diese Option.

Beim Abweisen einer Nachricht "Meldung" statt "Benutzer unbekannt" senden
Falls Sie die DNSBL-Optionen so konfiguriert haben, dass Nachrichten nach einem Treffer auf einer Schwarzen Liste abgewiesen werden, trägt SecurityGateway per Voreinstellung die *Meldung* in das Protokoll ein, die mit dem DNSBL-Host verknüpft ist, der den Treffer gemeldet hat. Diese Meldung wird während des SMTP-

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Protokolldialogs auch an den Server der Gegenstelle übermittelt. Falls Sie stattdessen an die Gegenstelle die Standard-Meldung "Benutzer unbekannt" senden wollen, deaktivieren Sie diese Option.

Erweitert (Alle Domänen)

Received-Kopfzeilen in abgerufenen Nachrichten prüfen
Per Voreinstellung fragt SecurityGateway nur die IP-Adresse der Gegenstelle, mit der gerade eine Verbindung besteht, über die DNSBL-Hosts ab. Falls Sie auch für die IP-Adressen, die in den Kopfzeilen `Received` der eingegangenen Nachrichten enthalten sind, die DNSBL-Abfragen durchführen wollen, aktivieren Sie diese Option.

Nur folgende Anzahl Received-Kopfzeilen prüfen (0 = alle)
Falls SecurityGateway auch die Kopfzeilen `Received` auf IP-Adressen untersucht, die auf einer Schwarzen Liste eingetragen sind, können Sie hier die Zahl der Kopfzeilen begrenzen, die geprüft werden sollen. Der Wert "0" bewirkt, dass alle vorhandenen Kopfzeilen `Received` geprüft werden.

Zahl der zu überspringenden neuesten Received-Kopfzeilen (0 = keine)
Falls SecurityGateway auch die Kopfzeilen `Received` auf IP-Adressen untersucht, die auf einer Schwarzen Liste eingetragen sind, können Sie hier festlegen, wie viele der neuesten Kopfzeilen SecurityGateway in der Prüfung überspringt. Je nach Konfiguration Ihres Mailsystems können die neuesten Kopfzeilen IP-Adressen vertrauter Gegenstellen oder anderer Hosts im lokalen Netz enthalten, für die eine DNSBL-Abfrage nicht erforderlich ist. Der Wert "0" bewirkt, dass keine der neuesten Kopfzeilen übersprungen werden.

Zahl der zu überspringenden ältesten Received-Kopfzeilen (0 = keine)
Falls SecurityGateway auch die Kopfzeilen `Received` auf IP-Adressen untersucht, die auf einer Schwarzen Liste eingetragen sind, können Sie hier festlegen, wie viele der ältesten Kopfzeilen SecurityGateway in der Prüfung überspringt. Die ältesten Kopfzeile enthalten häufig keine bedeutsamen Adressen, da sie beispielsweise durch den internen Mailserver des Absenders eingefügt wurden oder gefälscht sind, um legitim auszusehen. Der Wert "0" bewirkt, dass keine der ältesten Kopfzeilen übersprungen werden.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für die Schwarzen Listen für DNS für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.1.4 Schwarze Listen für URI (URIBL)

Schwarze Listen für URI (nach dem englischen Begriff URI Blacklists auch als "URIBL" abgekürzt) sind in Echtzeit arbeitende Schwarze Listen, mit deren Hilfe Nachrichten auf Grundlage der im Nachrichtentext enthaltenen Uniform Resource Identifier (üblicherweise Domänennamen oder Websites) abgewiesen oder gekennzeichnet werden können. Andere Begriffe für diese Dienste sind URI Blocklists und Spam URI Realtime Blocklists (SURBL).URIBL unterscheiden sich von Schwarzen Listen für DNS 169 dadurch, dass sie Spam nicht anhand der Inhalte der Kopfzeilen oder IP-Adresse der

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Gegenstelle erkennen. URIBL blockieren Spam auf der Grundlage des Nachrichten-Inhalts selbst. Umfassende Informationen über die Arbeitsweise der URIBL finden Sie unter www.surbl.org.

Konfiguration

URIBL-Abfragen aktivieren
Per Voreinstellung führt SecurityGateway URIBL-Abfragen für Nachrichten aus. Falls Sie diese Abfragen nicht ausführen wollen, deaktivieren Sie diese Option.

Falls eine Nachricht einen erfassten URI enthält:

...Nachricht abweisen
Diese Option bewirkt, dass eingehende Nachrichten während der SMTP-Verbindung abgewiesen werden, falls sie einen URI enthalten, der auf einer Schwarzen Liste erfasst ist. Für die meisten Anwendungsfälle ist diese Option nicht zu empfehlen, da die bloße Bezugnahme einer Nachricht auf einen URI, der auf einer Schwarzen Liste erfasst ist, nicht zugleich bedeuten muss, dass es sich um eine Spam-Nachricht handelt.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass eine Nachricht in Quarantäne gegeben wird, falls sie einen URI enthält, der auf einer Schwarzen Liste erfasst ist.

...Nachricht annehmen
Diese Option bewirkt, dass eine Nachricht zur Zustellung angenommen wird, auch wenn sie einen URI enthält, der auf einer Schwarzen Liste erfasst ist. Sie können solche Nachrichten als Spam kennzeichnen, der Betreffzeile einen Kennzeichnungstext voranstellen und die Nachrichten-Bewertung anpassen. Diese Option gestattet es den Mailservern oder Benutzern, die diese Nachricht im weiteren Verlauf empfangen, die Nachricht auf Grundlage der URIBL-Abfrageergebnisse von SecurityGateway selbst zu filtern.

...Betreff kennzeichnen mit [*Text*]
Diese Option bewirkt, dass der Betreffzeile einer Nachricht ein Kennzeichnungstext vorangestellt wird, falls die Nachricht einen URI enthält, der auf einer Schwarzen Liste erfasst ist. Wird diese Option aktiviert, so lautet die Voreinstellung für den Kennzeichnungstext "*** SPAM ***". Diese Option ist per Voreinstellung abgeschaltet.

SecurityGateway kann auch im Rahmen anderer Verarbeitungsfunktionen wahlweise die Betreffzeile von Nachrichten kennzeichnen. Die Funktionen Nachrichten-Bewertung 185 und Schwarze Listen für DNS (DNSBL) 169 lassen sich beispielsweise entsprechend konfigurieren. Stimmen die Kennzeichnungstexte in diesen Funktionen überein, so wird die Kennzeichnung dem Betreff nur einmal hinzugefügt, auch wenn die Bedingungen mehrerer Funktionen für eine Kennzeichnung bei der Nachricht erfüllt sind. Werden jedoch unterschiedliche Kennzeichnungstexte konfiguriert, so werden diese Kennzeichnungen gesondert eingefügt. Geben Sie beispielsweise für alle Funktionen den Kennzeichnungstext "*SPAM*" an, so wird dieser Text nur insgesamt einmal in die Betreffzeile eingefügt, auch wenn die Nachrichten den Bedingungen mehrere Funktionen für

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

eine Kennzeichnung entspricht. Ändern Sie nun den Text für die Funktion URIBL in "*URI blacklisted*", und erfüllt die Nachricht die Bedingungen für eine Kennzeichnung nach beiden Funktionen, so werden ihrer Betreffzeile sowohl "*SPAM*" als auch "*URI blacklisted*" vorangestellt.

...Bewertung des URIBL-Moduls der Nachrichten-Bewertung hinzurechnen
Ergibt eine URIBL-Abfragen einen Treffer für einen URI, der auf einer Schwarzen Liste erfasst ist, so wird per Voreinstellung die Bewertung, die der abgefragten Schwarzen Liste zugeordnet ist, der Nachrichten-Bewertung hinzugerechnet. Falls Sie die Nachrichten-Bewertung nicht anhand des Ergebnisses der URI-Abfragen anpassen wollen, deaktivieren Sie diese Option.

Auch wenn SecurityGateway so konfiguriert ist, dass Nachrichten nicht abgewiesen oder in Quarantäne gegeben sondern zur Zustellung angenommen werden, kann die Nachricht später noch abgewiesen oder in Quarantäne gegeben werden, falls ihre Nachrichten-Bewertung entsprechend hoch ist. Die Höhe der Nachrichten-Bewertung hängt auch von der Konfiguration und den Ergebnissen der anderen Sicherheitsfunktionen[154] und den Optionen auf der Seite Nachrichten-Bewertung[185] ab.

Ausschlüsse

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Per Voreinstellung sind Nachrichten von Absendern auf der Weißen Liste[275] von den URIBL-Abfragen ausgenommen. Falls Sie die URIBL-Abfragen auch für Absender auf der Weißen Liste durchführen wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Diese Option nimmt Nachrichten von der URIBL-Abfrage aus, die über Verbindungen mit Echtheitsbestätigung übermittelt wurden. Diese Option ist per Voreinstellung abgeschaltet.

Nachrichten von Mailservern der Domäne ausnehmen
Per Voreinstellungen werden die URIBL-Abfragen für eingehende Nachrichten und für Nachrichten, die durch einen Mailserver der Domäne[79] übermittelt wurden, durchgeführt. Falls Sie die URIBL-Abfragen für Nachrichten von Mailservern der Domäne nicht durchführen wollen, aktivieren Sie diese Option.

Schwarze Listen für URI (Alle Domänen)

In diesem Abschnitt sind alle URIBL-Hosts aufgeführt, die SecurityGateway abfragt.

Neu
Um eine neue Schwarze Liste für URI hinzuzufügen, klicken Sie auf das Steuerelement *Neu*. Hierdurch wird der Editor für Schwarze Listen für URI[175] aufgerufen (vgl. unten).

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Bearbeiten
Um eine Schwarze Liste für URI zu bearbeiten, wählen Sie den gewünschten Eintrag aus, und klicken Sie dann auf das Steuerelement*Bearbeiten*. Hierdurch wird der gewünschte Eintrag in den Editor für Schwarze Listen für URI 175 geladen.

Löschen
Um eine Schwarze Liste für URI zu löschen, wählen Sie den gewünschten Eintrag aus, und klicken Sie dann auf das Steuerelement *Löschen*.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für die Schwarzen Listen für URI für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

Editor für Schwarze Listen für URI

Der Editor für Schwarze Listen wird von der Übersicht über die Schwarzen Listen für URI aus durch Anklicken von *Neu* oder *Bearbeiten* aufgerufen. Mit seiner Hilfe können neue Schwarze Listen für URI hinzugefügt und bestehende Schwarze Listen bearbeitet werden.

Speichern und Beenden
Nachdem Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf dieses Steuerelement, um die Änderungen zu speichern und den Editor zu verlassen.

Schließen
Klicken Sie auf dieses Steuerelement, um etwaige Änderungen zu verwerfen und den Editor zu verlassen.

Schwarze Liste für URI

Abfrage dieser Schwarzen Liste für URI aktivieren
Mithilfe dieser Option können Sie eine Schwarze Liste für URI aktivieren und deaktivieren. Wenn Sie den Haken aus dem Kontrollkästchen eines Eintrags entfernen, wir dieser Eintrag zwar nicht aus der Liste gelöscht, aber SecurityGateway fragt die zugehörige Schwarze Liste für URI nicht mehr ab.

URIBL-Name:
Hier wird der Name der abzufragenden Schwarzen Liste für URI eingetragen.

Hostname oder IP:
Hier werden der Hostname oder die IP-Adresse eingetragen, die zu dem eben eingetragenen Namen der Schwarzen Liste gehören. Zur Abfrage der Schwarzen Liste stellt SecurityGateway eine Verbindung mit dieser Gegenstelle her.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Bewertung:
Die URIBL-Bewertung ist die Bewertung, die dieser Schwarzen Liste für URI zugeordnet ist. Wird ein URI aus einer geprüften Nachricht auf dieser Schwarzen Liste gefunden, so kann diese Bewertung der endgültigen Nachrichten-Bewertung[185] hinzugerechnet werden. Falls Sie die Option *...Bewertung des URIBL-Moduls der Nachrichten-Bewertung hinzurechnen* im Konfigurationsdialog für die Schwarze Liste für URI abgeschaltet haben, unterbleibt diese Hinzurechnung.

Bitmaske:
Die Bitmaske bezeichnet die abzufragende Liste oder Datenquelle und dient in den Fällen als Unterscheidungsmerkmal, in denen mehrere einzelne Listen zu einer einzigen, durch Bitmasken getrennten Liste zusammengefasst sind. Beispielsweise sind alle SURBL-Datenquellen unter *multi.surbl.org* in dieser Weise zusammengefasst. Nähere Informationen über diese Technik erhalten Sie unter www.surbl.org. Enthält die abgefragte Schwarze Liste für URI nur die Informationen einer einzigen Liste, so kann hier der Wert "0" eingetragen werden.

Vor Abfrage IP-Adresse des URIs auflösen
Diese Option bewirkt, dass die IP-Adressen aus den URIs, die die geprüften Nachrichten enthalten, vor der Abfrage dieser Schwarzen Liste für URI zunächst durch DNS-Abfrage aufgelöst werden. Ähnlich wie bei den Schwarzen Listen für DNS[169], enthalten auch einige Schwarze Listen für URI IP-Adressen, jedoch speichern sie nicht die IP-Adressen der Server, die die Nachrichten versenden, sondern die IP-Adressen der URIs, die in den Nachrichten enthalten sind.

4.1.5 Graue Liste

Die Graue Liste ist eine Abwehrmaßnahme gegen Spam, die den Mailserver des Absenders informiert, dass während der Zustellung ein vorübergehender Fehler aufgetreten ist, und dass die Zustellung etwas später erneut versucht werden soll. Bei dieser Maßnahme geht man davon aus, dass Spammer üblicherweise keinen erneuten Zustellversuch unternehmen, wenn eine Nachricht nicht zugestellt werden kann, legitime Absender aber durchaus weitere Zustellversuche unternehmen. Geht bei aktivierter Grauer Liste eine Nachricht ein, die nicht von einem Absender auf der Weißen Liste oder einem sonst bereits bekannten Absender stammt, so werden der Absender, der Empfänger und die IP-Adresse des Absenders protokolliert. Danach wird die Nachricht während der SMTP-Verbindung mit der Begründung abgewiesen, es liege ein vorübergehender Fehler vor. Während einer festgelegten Zeitspanne werden auch weitere Zustellversuche mit einem vorübergehenden Fehler abgewiesen. Da Spammer üblicherweise keine weiteren Zustellversuche unternehmen, nachdem eine Nachricht abgewiesen wurde, kann die Graue Liste die Zahl der Spam-Nachrichten verringern, die Ihren Benutzern zugehen. Selbst wenn aber ein Spammer später die Zustellung erneut versucht, ist der Spammer zu diesem Zeitpunkt möglicherweise bereits identifiziert, und wird durch andere Abwehrmaßnahmen gegen Spam (wie etwa die Schwarze Liste für DNS) erfolgreich blockiert.

Die Graue Liste kann zwar die Zahl der Spam-Nachrichten verringern, man muss sich dabei aber darüber im klaren sein, dass sie die Zustellung legitimer und sogar wichtiger Nachrichten verzögern kann. Legitime Nachrichten werden jedoch anzunehmenderweise später noch zugestellt, nachdem die Sperrdauer der Grauen

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Liste abgelaufen ist. Es treten für die einmal erfasste Kombination aus Server, Absender und Empfänger erst dann wieder Verzögerungen ein, wenn der Absender für einen in Tagen festgelegten Zeitraum keine weiteren Nachrichten an den Empfänger mehr gesendet hat. Es ist auch wichtig, zu beachten, dass sich nicht vorhersagen lässt, wie lange der Server eines Absenders wartet, bis er die Zustellung erneut versucht. Das Abweisen einer Nachricht mit einem vorübergehenden Fehler kann die Zustellung der Nachricht um wenige Minuten, aber auch um einen ganzen Tag verzögern. Wegen dieser und anderer möglicher Schwierigkeiten ist die Graue Liste in SecurityGateway per Voreinstellung abgeschaltet. Es stehen jedoch eine Reihe von Optionen zur Verfügung, die diese möglichen Schwierigkeiten begrenzen.

Zunächst nutzen einige Domänen einen Pool von Mailservern für den Versand abgehender Nachrichten. Da jeder Zustellversuch durch einen anderen Mailserver aus dem Pool durchgeführt werden kann, würde die Graue Liste jeden Zustellversuch wie einen neuen erstmaligen Zustellversuch einer neuen Nachricht, nicht aber wie einen erneuten Zustellversuch für dieselbe Nachricht behandeln. Hierdurch kann sich die Zeit, während der die Graue Liste die Zustellung einer Nachricht verhindert, vervielfachen. Die Prüfung des Absenders über das Sender Policy Framework (SPF) kann dieses Problem für Domänen lösen, deren SPF-Daten veröffentlicht sind. Außerdem steht eine Option zur Verfügung, die bewirkt, dass die IP-Adresse des übermittelnden Mailservers für die Graue Liste überhaupt außer Betracht bleibt. Diese Option verringert zwar den Wirkungsgrad der Grauen Liste, sie löst aber das Problem in Verbindung mit Server-Pools.

Weiter setzt eine Graue Liste üblicherweise eine große Datenbank voraus, da jede eingehende Verbindung nachverfolgt werden muss. SecurityGateway verringert die Notwendigkeit, diese Verbindungen nachzuverfolgen, indem die Verarbeitung durch die Graue Liste bereits während der SMTP-Verarbeitung stattfindet. Falls eine der zahlreichen anderen Sicherheitsmaßnahmen in SecurityGateway bereits vorher angeschlagen hat, kann die Nachricht schon abgewiesen sein, bevor sie überhaupt in die Phase eintritt, in der die Graue Liste sie üblicherweise verarbeiten würde. Aufgrund dieser Maßnahmen verringert sich die Datenbankgröße der Grauen Liste deutlich, und sie verringert die Systemleistung nur unmerklich.

Schließlich stehen noch mehrere Optionen zur Verfügung, die die Wirkungen der Grauen Liste auf legitime Nachrichten verringern; dazu gehören Optionen für den Ausschluss von Nachrichten, die von Absendern auf der Weißen Liste stammen oder über Verbindungen mit Echtheitsbestätigung übermittelt wurden. Nachrichten, die durch einen Ihrer Mailserver der Domäne übermittelt wurden, sind immer ausgenommen.

Nähere Informationen über die Graue Liste enthalten die folgenden Artikel:

http://de.wikipedia.org/wiki/Greylisting (Artikel in deutscher Sprache)

http://en.wikipedia.org/wiki/Greylisting (Artikel in englischer Sprache)

Konfiguration

Graue Liste aktivieren
Diese Option aktiviert die Graue Liste. Die Graue Liste ist per Voreinstellung abgeschaltet.

Ersten Zustellversuch mit Fehler 451 für diese Zeitdauer verzögern: [xx] Minuten
Mithilfe dieser Option legen Sie die Dauer in Minuten fest, für die jede Kombination aus Server, Absender und Empfänger (zusammenfassend auch als "Dreiergruppe"

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

bezeichnet) nach dem ersten Zustellversuch in der Grauen Liste verbleibt. Während dieser Zeit werden auch weitere Zustellversuche mit derselben Dreiergruppe mit einem vorübergehenden Fehlerkode abgewiesen. Nach Ablauf dieser Zeit werden für diese Dreiergruppe keine weiteren Verzögerungen in der Zustellung wirksam, solange der Eintrag der Dreiergruppe in der Datenbank der Grauen Liste nicht abläuft. Die Voreinstellung für diese Option beträgt 15 Minuten.

Zeitdauer, bis ungenutzte Einträge in der Grauen Liste verfallen: [xx] Tag(e/n)
Sobald die erste Verzögerungsdauer in der Grauen Liste für eine Dreiergruppe abgelaufen ist, werden für diese Dreiergruppe während der hier angegebenen Zeitdauer keine weiteren Verzögerungen in der Zustellung mehr wirksam. Ist hier beispielsweise ein Wert von 10 Tagen eingetragen, so werden für die Dreiergruppe keine Verzögerungen mehr wirksam, solange mindestens alle 10 Tage eine Nachricht eingeht, die zu dieser Dreiergruppe passt. Geht in diesem Zeitraum jedoch einmal keine Nachricht ein, so läuft der Eintrag ab und wird aus der Datenbank entfernt. Bei der nächsten Nachricht, die auf die Dreiergruppe passt, wird dann die Verzögerung für den ersten Zustellversuch wieder wirksam, und erst nach dieser Verzögerung treten, wiederum für den hier angegebenen Zeitraum, keine weiteren Verzögerungen mehr auf. Die Voreinstellung für diese Option beträgt 10 Tage.

IP-Adressen für die Graue Liste ignorieren (nur MAIL- und RCPT-Werte nutzen)
Diese Option bewirkt, dass die IP-Adresse des übermittelnden Servers nicht als eines der Daten in die Graue Liste aufgenommen wird. Hierdurch wird das mögliche Problem im Zusammenhang mit Server-Pools gelöst, es verringert sich aber auch der Wirkungsgrad der Grauen Liste. Diese Option ist per Voreinstellung abgeschaltet.

IP-Adressen aus Verbindungen ignorieren, die SPF-Prüfung bestehen
Diese Option bewirkt, dass nur der Absender und der Empfänger in die Graue Liste eingetragen werden und die IP-Adresse des übermittelnden Servers ignoriert wird, falls für den Server die Prüfung durch das SPF 194 erfolgreich verläuft. Diese Option ist per Voreinstellung aktiv.

Ausschlüsse

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Per Voreinstellung sind Nachrichten von Absendern auf der Weißen Liste 275 von der Grauen Liste ausgenommen, sodass die Zustellung ihrer Nachrichten nicht verzögert wird. Falls Sie die Graue Liste auch auf Absender auf der Weißen Liste anwenden wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Per Voreinstellung sind Nachrichten von der Grauen Liste ausgenommen, die über Verbindungen mit Echtheitsbestätigung übermittelt wurden. Falls Sie die Graue Liste auch auf solche Nachrichten anwenden wollen, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Nachrichten, die durch Ihre Mailserver der Domäne 79 übermittelt werden, sind von der Grauen Liste immer ausgenommen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für die Graue Liste für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.1.6 Zertifizierung von Nachrichten

Die Zertifizierung von Nachrichten ist ein Vorgang, in dessen Rahmen eine vertrauenswürdige Quelle für das legitime Verhalten beim Versand von Nachrichten einsteht oder es "zertifiziert". Die Zertifizierung bezieht sich auf eine bestimmte Funktionseinheit, die mit der Nachricht verknüpft ist. Nachrichten aus einer Domäne, die durch eine solche vertrauenswürdige Quelle zertifiziert ist, können daher als weniger verdächtig angesehen werden. Es ist auch angemessen sichergestellt, dass die Domäne des Absenders sich auf legitime Verhaltensweisen beim E-Mail-Versand beschränkt und weder Spam noch andere problematische Nachrichten versendet. Die Zertifizierung ist hilfreich, weil sie hilft, zu verhindern, dass Nachrichten irrtümlich oder unnötig einer Analyse zur Spam-Abwehr unterworfen werden. Sie kann auch den Ressourcenverbrauch für die Verarbeitung der Nachrichten verringern.

SecurityGateway implementiert die Zertifizierung von Nachrichten und unterstützt dazu ein neues Internet-E-Mail-Protokoll namens "Vouch-By-Reference" (kurz "VBR"). MDaemon Technologies wirkt im Domain Assurance Council (kurz "DAC") mit und fördert dadurch die Verbreitung dieser Technologie. VBR stellt den Mechanismus zur Verfügung, mit dessen Hilfe Zertifizierungsdienstleister (sie werden in den englischen Texten als Certification Service Provider, kurz "CSP" bezeichnet) oder "Zertifizierer" für die legitimen Verhaltensweisen bestimmter Domänen einstehen können.

Nachrichten, die angeblich durch einen CSP zertifiziert sind, müssen durch DKIM signiert 199 sein oder über einen Server versendet werden, der durch SPF 194 legitimiert ist. Dies ist erforderlich, damit sichergestellt werden kann, dass die Nachricht nicht gefälscht ist sondern wirklich aus der angeblichen Absender-Domäne stammt.

Zertifizierung eingehender Nachrichten

Haben Sie einen Certification Service Provider (CSP) bestimmt, behauptet ein Absender, durch diesen CSP zertifiziert zu sein, und wird diese Zertifizierung bestätigt, so können seine eingehenden Nachrichten von einigen Sicherheitsmaßnahmen gegen Spam ausgenommen werden, die SecurityGateway bereitstellt. Anstatt die Nachrichten von den Sicherheitsmaßnahmen völlig auszunehmen, können Sie auch einen bestimmten Wert von der Nachrichten-Bewertung dieser Nachrichten abziehen lassen. Bei erfolgreicher Zertifizierung ist die Wahrscheinlichkeit deutlich geringer, dass es sich um Spam handelt. Sie können den CSP ändern und weitere CSP hinzufügen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Zertifizierung abgehender Nachrichten

Bevor Sie SecurityGateway so konfigurieren können, dass die Zertifizierungsdaten in abgehende Nachrichten einer Domäne eingefügt werden, müssen Sie sicherstellen, dass diese Domäne durch einen oder mehrere CSP zertifiziert wird.

Nachdem Sie sich bei einem CSP registriert haben, konfigurieren Sie SecurityGateway anhand der folgenden Anleitung so, dass die Zertifizierungsdaten in die abgehenden Nachrichten einer Domäne eingefügt werden:

1. Stellen Sie sicher, dass die abgehenden Nachrichten der Domäne über DKIM 199 signiert werden, oder stellen Sie sicher, dass die DNS-Einträge der Domäne richtig konfiguriert werden und ausweisen, dass die Nachrichten über einen durch SPF 194 legitimierten Absender versandt werden. Dies ist erforderlich, damit sichergestellt ist, dass die Nachricht wirklich aus der fraglichen Domäne stammt. Nachrichten können nur zertifiziert werden, falls der Server des Empfängers feststellen kann, dass die Nachricht wirklich aus der angeblichen Absender-Domäne versandt wurde.
2. Klicken Sie im Navigationsbereich von SecurityGateway auf **Sicherheit»Zertifizierung von Nachrichten**, um die Seite Zertifizierung von Nachrichten aufzurufen.
3. Wählen Sie aus dem Auswahlmenü "*Für Domäne:*" am oberen rechten Rand der Seite die gewünschte Domäne aus.
4. Aktivieren Sie im Abschnitt Abgehende Nachrichten am Ende der Seite die Option *Zertifizierungsdaten in abgehende Nachrichten einfügen*.
5. Tragen Sie in das Eingabefeld der Option *Hostname(n) der Zertifizierungsdienstleister, die meine Nachrichten zertifizieren* die Hosts ein, die zu einem oder mehreren CSP gehören, die für die E-Mail-Nachrichten der Domäne einstehen. Trennen Sie mehrere Einträge durch Leerzeichen.
6. Klicken Sie auf **Speichern**.

VBR verlangt nicht, dass die zertifizierten Nachrichten durch Ihren CSP signiert oder an ihn gesendet werden. Der CSP signiert und validiert einzelne Nachrichten nicht — er steht für die legitimen Verhaltensweisen der Domäne beim E-Mail-Versand ein.

Eingehende Nachrichten

Systemweite Standard-Einstellungen für diese Domäne verwenden
Während Sie die besonderen Einstellungen einer Domäne für die Zertifizierung von Nachrichten bearbeiten, können Sie die systemweiten Standard-Einstellungen für die Behandlung eingehender Nachrichten auch für die gerade bearbeitete Domäne übernehmen. Klicken Sie hierzu auf diese Verknüpfung. Diese Option wird nur angezeigt, wenn Sie aus dem Auswahlmenü "*Für Domäne:*" am oberen Seitenrand eine Domäne ausgewählt haben.

Die unten angegebenen besonderen Einstellungen für diese Domäne verwenden
Während Sie die besonderen Einstellungen einer Domäne für die Zertifizierung von Nachrichten bearbeiten, können Sie mithilfe dieser Verknüpfung die Einstellungen für eingehende Nachrichten für die ausgewählte Domäne bearbeiten. Diese Option

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

wird nur angezeigt, wenn Sie aus dem Auswahlmenü "*Für Domäne:*" am oberen Seitenrand eine Domäne ausgewählt haben.

Eingehende Nachrichten zertifizieren
Per Voreinstellung versucht SecurityGateway, die Zertifizierung bei solchen Nachrichten zu bestätigen, deren Absender behauptet, sie seien durch einen der CSP zertifiziert, die Sie als vertrauenswürdig einstufen. Falls Sie bei eingehenden Nachrichten diese Prüfung nicht durchführen wollen, deaktivieren Sie diese Option.

Hostname(n) der vertrauenswürdigen Zertifizierungsdienstleister (mehrere Einträge durch Leerzeichen trennen):
Tragen Sie in dieses Eingabefeld die Hostnamen aller CSP ein, denen Sie vertrauen. Trennen Sie mehrere Einträge durch je ein Komma.

Falls der Absender zertifiziert ist:
Mithilfe der folgenden Optionen bestimmen Sie, wie SecurityGateway verfahren soll, wenn die Zertifizierung eines Absenders durch einen Ihrer vertrauenswürdigen CSP bestätigt wird.

...Nachricht nicht durch den Spam-Filter (Heuristik, Bayes und URIBL) bearbeiten
Diese Option bewirkt, dass Nachrichten von zertifizierten Absendern nicht durch einige der Sicherheitsfunktionen gegen Spam verarbeitet werden, die SecurityGateway zur Verfügung stellt. Diese Option ist per Voreinstellung aktiv.

... [xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Falls Sie zertifizierte Nachrichten nicht von den oben genannten Sicherheitsmaßnahmen ausnehmen wollen, wählen Sie diese Option, und bestimmen Sie den Wert, den Sie der Nachrichten-Bewertung 185 der fraglichen Nachrichten hinzurechnen wollen. Bei zertifizierten Nachrichten ist die Wahrscheinlichkeit geringer, dass es sich um Spam handelt. Dieser Wert sollte daher eine negative Zahl sein, sodass die Nachrichten-Bewertung herabgesetzt und damit positiv beeinflusst wird. Die Voreinstellung beträgt "`-3,0`".

Abgehende Nachrichten

Die Optionen in diesem Abschnitt stehen erst zur Verfügung, nachdem Sie aus dem Auswahlfeld "*Für Domäne:*" am oberen Seitenrand eine Domäne ausgewählt haben. Sie können für abgehende Nachrichten keine systemweiten Einstellungen für die Zertifizierung festlegen.

Zertifizierungsdaten in abgehende Nachrichten einfügen
Diese Option bewirkt, dass in alle abgehenden Nachrichten der ausgewählten Domäne Zertifizierungsdaten eingefügt werden, Diese Option ist per Voreinstellung abgeschaltet.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Hostname(n) der Zertifizierungsdienstleister, die meine Nachrichten zertifizieren (mehrere Einträge durch Leerzeichen trennen):
Tragen Sie in dieses Eingabefeld die Hostnamen des oder der CSP ein, die für die Nachrichten der ausgewählten Domäne einstehen. Trennen Sie mehrere Einträge durch Leerzeichen.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für die Zertifizierung von Nachrichten für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.1.7 Schutz gegen Rückstreuung

Rückstreuung

Als "Rückstreuung" (englisch "Backscatter") bezeichnet man Antwortnachrichten, die Ihre Benutzer empfangen, obwohl sie die Nachrichten, auf die geantwortet wird, gar nicht versandt haben. Diese Erscheinung tritt auf, wenn Spam-Nachrichten oder Nachrichten, die durch Viren versandt werden, als Antwortpfad eine gefälschte Adresse enthalten. Werden solche Nachrichten durch den Server des Empfängers abgewiesen, oder hat der Empfänger für sein Benutzerkonto einen Auto-Beantworter oder eine Abwesenheitsnachricht eingerichtet, so wird die Antwort an die gefälschte Adresse gerichtet. Dies kann dazu führen, dass sich in den Posteingängen Ihrer Benutzer zahlreiche falsche Nachrichten über Zustellfehler (sog. Delivery Status Notifications oder kurz "DSN") und Nachrichten von Auto-Beantwortern sammeln. Spammer und Urheber von Viren nützen diese Erscheinung bisweilen gezielt für Denial-of-Service-Angriffe (kurz "DoS") gegen E-Mail-Server, indem sie eine Flut ungültiger E-Mail-Nachrichten auslösen, die von den verschiedensten Servern weltweit ausgeht.

Schutz gegen Rückstreuung

Um die Rückstreuung zu bekämpfen, kann SecurityGateway mithilfe der Funktion zum Schutz gegen Rückstreuung helfen, sicherzustellen, dass nur legitime Nachrichten über Zustellfehler und Nachrichten von Auto-Beantwortern an Ihre Domänen zugestellt werden. SecurityGateway setzt dazu eine Hash-Funktion und einen geheimen Schlüssel in Verbindung mit einem besonderen, zeitabhängigen Kode ein, der in die Antwortadresse, den "`Return-Path`", abgehender Nachrichten eingefügt wird. Tritt bei der Zustellung einer solchen Nachricht ein Fehler auf, und wird sie zurückgeleitet, oder geht eine automatisch erzeugte Antwort mit dem Antwortpfad "`mailer-daemon@...`" oder `NULL` ein, so erkennt SecurityGateway den besonderen Kode und bestätigt damit, dass die Nachricht eine echte automatisch erstellte Antwort auf eine Nachricht ist, die wirklich von einer Ihrer Domänen aus gesendet wurde. Enthält die Nachrichten den Kode nicht, oder ist seine Gültigkeit abgelaufen, so wird dies ebenfalls festgestellt, und die Nachricht kann abgewiesen werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Konfiguration

Schutz gegen Rückstreuung aktivieren
Diese Option aktiviert den Schutz gegen Rückstreuung. Sobald die Option aktiv ist, beginnt SecurityGateway, den besonderen Kode zu erzeugen und in den Antwortpfad aller abgehenden Nachrichten einzufügen. SecurityGateway sucht auch in allein zurückgeleiteten Nachrichten nach diesem Kode. Der Schutz gegen Rückstreuung ist per Voreinstellung abgeschaltet.

Falls Sie diese Option abschalten, fügt SecurityGateway den besonderen Kode für den Schutz gegen Rückstreuung nicht mehr in abgehende Nachrichten ein. Eingehende Nachrichten über Zustellfehler und Nachrichten von Auto-Beantwortern werden aber weiterhin ausgewertet, damit sichergestellt ist, dass nicht etwa eine Nachricht mit einem gültigen Kode versehentlich abgewiesen wird.

Nachrichten abweisen, bei denen die Prüfung gegen Rückstreuung fehlschlägt
Diese Option bewirkt, dass Nachrichten über Zustellfehler und andere Nachrichten von Auto-Beantwortern automatisch abgewiesen werden, falls sie die Prüfung des Schutzes gegen Rückstreuung nicht bestehen. Nachrichten mit dem Antwortpfad "`mailer-daemon@...`" oder `NULL` bestehen diese Prüfung nicht, falls sie den besonderen Kode nicht enthalten oder die Gültigkeitsdauer des Kodes abgelaufen ist. Der Schutz gegen Rückstreuung arbeitet so zuverlässig, dass es keine falschen positiven Treffer oder "Unsicherheiten" in der Auswertung gibt. Eine Nachricht ist entweder gültig oder ungültig. Aus diesem Grund kann SecurityGateway ohne Bedenken so konfiguriert werden, dass ungültige Nachrichten abgewiesen werden; es muss dann nur sichergestellt sein, dass alle abgehenden Nachrichten den besonderen Kode des Schutzes gegen Rückstreuung enthalten. Die Ergebnisse der Prüfung durch den Schutz gegen Rückstreuung werden in jedem Fall protokolliert, und zwar auch dann, wenn das System Nachrichten nach fehlgeschlagener Prüfung nicht abweist.

Nachdem Sie den Schutz gegen Rückstreuung aktiviert haben, sollten Sie im Normalfall etwa eine Woche warten, bevor Sie SecurityGateway so konfigurieren, dass Nachrichten nach fehlgeschlagener Prüfung durch den Schutz gegen Rückstreuung abgewiesen werden. Während dieser Zeit könnten noch Nachrichten über Zustellfehler und Nachrichten von Auto-Beantwortern für solche Nachrichten eingehen, die versandt worden waren, bevor der Schutz gegen Rückstreuung aktiviert wurde. Würde der Schutz gegen Rückstreuung während dieser ersten Zeit bereits abweisen, so würden diese legitimen Antworten fälschlich abgewiesen werden. Nach etwa einer Woche wird es im Regelfall problemlos möglich sein, mit dem Abweisen von Nachrichten nach fehlgeschlagener Prüfung zu beginnen. Was vorstehend für den erstmaligen Einsatz des Schutzes gegen Rückstreuung gesagt wurde, gilt entsprechend, falls Sie einen neuen Schlüssel für den Schutz gegen Rückstreuung erstellen, die Option *Bisherigen Schlüssel danach noch aufbewahren für [xx] Tag(e)* aber nicht

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

einsetzen, um den bisherigen Schlüssel noch für eine Übergangszeit zu speichern.

Klicken Sie hier, um sofort einen neuen Schlüssel für den Schutz gegen Rückstreuung zu erzeugen.
Mithilfe dieser Verknüpfung können Sie sofort einen neuen Schlüssel für den Schutz gegen Rückstreuung erzeugen. Ist die Option *Bisherigen Schlüssel danach noch aufbewahren für [xx] Tag(e)* weiter unten aktiv, so können Nachrichten mit Kodes auf Basis des vorherigen Schlüssels noch für den dort angegebenen Zeitraum erfolgreich geprüft werden.

Ausschlüsse

IP-Adressen und Hosts auf der globalen Weißen Liste von Abwehrmaßnahmen ausnehmen
Per Voreinstellung sind Nachrichten von IP-Adressen auf der Weißen Liste 281 von den Beschränkungen des Schutzes gegen Rückstreuung ausgenommen. Falls Sie den Schutz gegen Rückstreuung auch auf IP-Adressen auf der Weißen Liste anwenden wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Per Voreinstellung sind eingehende Nachrichten von den Beschränkungen des Schutzes gegen Rückstreuung ausgenommen, falls sie über Verbindungen mit Echtheitsbestätigung übermittelt wurden. Falls Sie den Schutz gegen Rückstreuung auch auf solche Nachrichten anwenden wollen, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Nachrichten, die durch Ihre Mailserver der Domäne 79 übermittelt werden, sind per Voreinstellung von den Beschränkungen des Schutzes gegen Rückstreuung ausgenommen. Falls Sie den Schutz gegen Rückstreuung auch auf solche Nachrichten anwenden wollen, deaktivieren Sie diese Option.

Signatur für Antwortpfad der Nachrichten

Neuen Schlüssel für den Schutz gegen Rückstreuung erstellen alle [xx] Tag(e)
Per Voreinstellung wird alle 7 Tage ein neuer Schlüssel für den Schutz gegen Rückstreuung erzeugt. Der neue Schlüssel wird unmittelbar nach seiner Erstellung genutzt, um den Kode für den Schutz gegen Rückstreuung zu erzeugen und in abgehende Nachrichten einzufügen.

Bisherigen Schlüssel danach noch aufbewahren für [xx] Tag(e)
Per Voreinstellung speichert SecurityGateway den alten Schlüssel für den Schutz gegen Rückstreuung noch für 7 Tage ab dem Datum, an dem ein neuer Schlüssel erstellt wurde. Während dieser Zeit kann SecurityGateway zurücklaufende Nachrichten, die noch einen Kode auf Basis des alten Schlüssels enthalten, erfolgreich prüfen. Die Übergangszeit soll eingehalten werden, damit Nachrichten nicht versehentlich abgewiesen werden, nachdem ein neuer Schlüssel erstellt wurde. Es wird empfohlen, diese Option aktiviert zu lassen (siehe auch den Warnhinweis zur Option *Nachrichten abweisen, bei denen die Prüfung gegen Rückstreuung fehlschlägt* weiter oben).

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

4.1.8 Nachrichten-Bewertung

SecurityGateway berechnet für jede Nachricht eine Nachrichten-Bewertung. Sie stützt sich auf mehrere Prüfungen, die während der Verarbeitung der Nachricht durchgeführt werden. Der Wert verkörpert die Berechnung der Wahrscheinlichkeit, dass die Nachricht eine Spam-Nachricht ist. Die Funktionen Heuristik und Bayes 162, Schwarze Listen für DNS 169, DKIM-Prüfung 197 und viele andere Sicherheits-Funktionen 154 können wahlweise die Nachrichten-Bewertung anpassen. Die Optionen auf dieser Seite legen fest, welche Aktion ausgeführt werden soll, falls die Bewertung einer Nachricht bestimmte Schwellwerte überschreitet. Sie können Schwellwerte festlegen, ab deren Erreichen Nachrichten als Spam gekennzeichnet, in Quarantäne gegeben oder während der SMTP-Verbindung abgewiesen werden sollen. Sie können auch bestimmte Nachrichten von den Beschränkungen aufgrund der Nachrichten-Bewertung ausnehmen, etwa dann, wenn sie von Absendern auf der Weißen Liste stammen, in Verbindungen mit Echtheitsbestätigung übermittelt wurden oder abgehende Nachrichten sind. Die Optionen zur Nachrichten-Bewertung können systemweit und nach Domänen getrennt konfiguriert werden.

Konfiguration

Aktionen aufgrund der endgültigen Nachrichten-Bewertung aktivieren
SecurityGateway weist jeder Nachricht per Voreinstellung eine Nachrichten-Bewertung zu und führt dann, je nach Höhe der Bewertung, die unten beschriebenen Aktionen durch. Falls Sie den Nachrichten zwar eine Bewertung zuweisen, auf ihrer Grundlage aber keine Aktionen ausführen wollen, deaktivieren Sie diese Option.

Nachrichten abweisen ab einer Bewertung von [xx]
Per Voreinstellung werden Nachrichten während der SMTP-Übermittlung abgewiesen, falls ihre endgültige Bewertung der Wert 12,0 erreicht oder übersteigt. Falls Sie es wünschen, können Sie diesen Wert anpassen. Falls Sie nicht wünschen, dass Nachrichten aufgrund ihrer Bewertung abgewiesen werden, können Sie diese Option auch deaktivieren.

Nachrichten in Quarantäne geben ab einer Bewertung von [xx]
Per Voreinstellung werden Nachrichten in Quarantäne gegeben, falls ihre endgültige Bewertung den Wert 5,0 erreicht oder übersteigt. Falls Sie es wünschen, können Sie diesen Wert anpassen. Falls Sie nicht wünschen, dass Nachrichten aufgrund ihrer Bewertung in Quarantäne gegeben werden, können Sie diese Option auch deaktivieren. Falls Sie die Option "*Nachrichten abweisen ab einer Bewertung von [xx]*" weiter oben einsetzen, so werden Nachrichten in Quarantäne gegeben, falls ihre Bewertung den Wert der vorliegenden Option erreicht oder übersteigt, den Wert der Option zum Abweisen aber nicht erreicht. Nachrichten, deren Bewertung den Wert der Option zum Abweisen erreicht oder übersteigt, werden abgewiesen.

Betreffzeile der Nachrichten kennzeichnen ab einer Bewertung von [xx]
Diese Option bewirkt, dass die Betreffzeile der Nachrichten gekennzeichnet wird, deren endgültige Bewertung den hier angegebenen Wert erreicht oder übersteigt. Die Voreinstellung beträgt 5,0, jedoch ist die Option per Voreinstellung abgeschaltet.

Kennzeichnung für Betreff:
Ist die Option "*Betreffzeile der Nachrichten kennzeichnen...*" weiter oben aktiv, so wird die hier eingegeben Text der Betreffzeile der Nachrichten vorangestellt, deren Bewertung den hier angegeben Wert erreicht oder

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

übersteigt. Die Voreinstellung für diesen Kennzeichnungstext lautet "*** SPAM ***".

SecurityGateway kann auch im Rahmen anderer Verarbeitungsfunktionen wahlweise die Betreffzeile von Nachrichten kennzeichnen. Die Funktionen Schwarze Listen für DNS 169 und Schwarze Listen für URI (URIBL) 172 lassen sich beispielsweise entsprechend konfigurieren. Stimmen die Kennzeichnungstexte in diesen Funktionen überein, so wird die Kennzeichnung dem Betreff nur einmal hinzugefügt, auch wenn die Bedingungen mehrerer Funktionen für eine Kennzeichnung bei der Nachricht erfüllt sind. Werden jedoch unterschiedliche Kennzeichnungstexte konfiguriert, so werden diese Kennzeichnungen gesondert eingefügt. Geben Sie beispielsweise für alle Funktionen den Kennzeichnungstext "*SPAM*" an, so wird dieser Text nur insgesamt einmal in die Betreffzeile eingefügt, auch wenn die Nachrichten den Bedingungen mehrere Funktionen für eine Kennzeichnung entspricht. Ändern Sie nun den Text für die Funktion URIBL in "*URI blacklisted*", und erfüllt die Nachricht die Bedingungen für eine Kennzeichnung nach beiden Funktionen, so werden ihrer Betreffzeile sowohl "*SPAM*" als auch "*URI blacklisted*" vorangestellt.

Ausschlüsse

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Per Voreinstellung sind Nachrichten von Absendern auf der Weißen Liste 275 von den Beschränkungen der Nachrichten-Bewertung ausgenommen. Falls Sie diese Optionen zur Nachrichten-Bewertung auch auf Absender auf der Weißen Liste anwenden wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Per Voreinstellung sind alle Nachrichten von den Beschränkungen der Nachrichten-Bewertung ausgenommen, falls sie über Verbindungen mit Echtheitsbestätigung übermittelt wurden. Falls Sie diese Optionen zur Nachrichten-Bewertung auch auf solche Nachrichten anwenden wollen, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Diese Option bewirkt, dass Nachrichten, die durch Ihre Mailserver der Domäne 79 übermittelt werden, von den Beschränkungen der Nachrichten-Bewertung ausgenommen sind. Diese Option ist per Voreinstellung abgeschaltet.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für die Nachrichten-Bewertung für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

4.2 Anti-Virus

Der Abschnitt Anti-Virus im Menü Sicherheit 154 enthält Optionen, mit deren Hilfe Sie vireninfizierte Nachrichten identifizieren und verhindern können, dass diese an Ihre Benutzer zugestellt werden. Der Abschnitt Anti-Virus enthält zwei Elemente:

Virenprüfung 187 - SecurityGateway bietet umfassenden Schutz gegen Viren und unterstützt daher zwei Anti-Virus-Module: Clam AntiVirus (ClamAV™) und IKARUS Anti-Virus. ClamAV ist ein quelloffenes, unter der GPL lizensiertes, Anti-Virus-Toolkit, das besonders für E-Mail-Gateways entwickelt wurde. IKARUS Anti-Virus bietet verlässlichen Schutz gegen Schadsoftware. Es kombiniert herkömmliche Techniken zur Virenabwehr mit den neuesten vorausschauend arbeitenden Techniken. SecurityGateway enthält auch die Outbreak Protection 157, den Schutz gegen Ausbrüche und Massenangriffe, der eine weitere Schutzebene gegen die Verbreitung von Viren bietet.

Aktualisierung konfigurieren 189 - Da Bedrohungen durch Viren unvermittelt entstehen und sich schnell ausweiten können, muss die Datenbank der Viren-Signaturen regelmäßig aktualisiert und stets aktuell gehalten werden; es könnten sonst Viren nicht erkannt werden. Die Optionen auf der Seite Aktualisierung konfigurieren veranlassen SecurityGateway, automatisch nach aktualisierten Viren-Signaturen zu suchen. Von dieser Seite aus kann auch eine sofortige Aktualisierung außerhalb des Zeitplans durchgeführt werden, und die Protokolle über die Aktualisierungen können angezeigt werden.

4.2.1 Virenprüfung

SecurityGateway bietet umfassenden Schutz gegen Viren und unterstützt daher zwei Anti-Virus-Module: Clam AntiVirus (ClamAV™) und IKARUS Anti-Virus. ClamAV ist ein quelloffenes, unter der GPL lizensiertes, Anti-Virus-Toolkit, das besonders für E-Mail-Gateways entwickelt wurde. IKARUS Anti-Virus bietet verlässlichen Schutz gegen Schadsoftware. Es kombiniert herkömmliche Techniken zur Virenabwehr mit den neuesten vorausschauend arbeitenden Techniken. SecurityGateway enthält auch die Outbreak Protection 157, den Schutz gegen Ausbrüche und Massenangriffe, der eine weitere Schutzebene gegen die Verbreitung von Viren bietet.

Konfiguration

Virenprüfung aktivieren
Die Virenprüfung durch SecurityGateway ist per Voreinstellung aktiv. Falls Sie nicht wünschen, dass die Nachrichten auf Viren geprüft werden, deaktivieren Sie dieses Kontrollkästchen.

Falls das Anti-Virus-Modul feststellt, dass eine Nachricht infiziert ist:
Mithilfe dieser Option legen Sie fest, welche Aktion ausgeführt werden soll, falls in einer Nachricht ein Virus festgestellt wird.

Falls Sie die Option "*Versuchen, infizierte Nachrichten zu desinfizieren*" weiter unten aktiviert haben, versucht SecurityGateway zunächst, eine infizierte Nachricht zu desinfizieren, also den Virus aus ihr zu entfernen. Die Nachricht wird nicht sofort abgewiesen oder in Quarantäne

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

gegeben. Wird die Nachricht erfolgreich desinfiziert, so wird sie angenommen und zugestellt; kann die Nachricht nicht desinfiziert werden, so wird sie abgewiesen oder in Quarantäne gegeben.

...Nachricht abweisen
Diese Option bewirkt, dass Nachrichten während der SMTP-Verbindung abgewiesen werden, falls in ihnen ein Virus festgestellt wird. Diese Option ist per Voreinstellung aktiv.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass infizierte Nachrichten nicht abgewiesen, sondern in die administrative Quarantäne 310 gegeben werden.

Nachrichten, die nicht geprüft werden können, in Quarantäne geben
Diese Option bewirkt dass Nachrichten in Quarantäne gegeben werden, falls sie - gleich, aus welchem Grund - durch das Anti-Virus-Modul nicht geprüft werden können. Ein Beispiel hierfür ist eine Nachricht, die als Dateianlage eine kennwortgeschütztes ZIP-Archiv enthält. Ist diese Option abgeschaltet, so werden Nachrichten normal zugestellt, auch wenn sie nicht geprüft werden können. Diese Option ist per Voreinstellung aktiv.

Nachricht weiterverarbeiten, wenn ein AntiVirus-Modul die Prüfung erfolgreich abgeschlossen hat
Diese Option bewirkt, dass Nachrichten weiterverarbeitet werden, falls sie wenigstens durch eines der Anti-Virus-Module erfolgreich geprüft werden konnten. Ist diese Option abgeschaltet, und können nicht beide Module die Nachricht erfolgreich prüfen, dann wird die Nachricht in Quarantäne gegeben.

Nachfolgend aufgeführte Dateien ausnehmen
Mithilfe dieser Option können Sie bestimmte Dateien oder Dateitypen bestimmen, die von der Option *Nachrichten, die nicht geprüft werden können, in Quarantäne geben* ausgenommen sind. Es sind Dateimasken und Jokerzeichen zulässig, wie etwa *.zip, secret?.zip, *.doc und weitere.

Versuchen, infizierte Nachrichten zu desinfizieren
Per Voreinstellung versucht SecurityGateway, einen erkannten Virus aus einer infizierten Nachricht zu entfernen (und die Nachricht damit zu "desinfizieren"), anstatt die Nachricht sofort abzuweisen oder in Quarantäne zu geben. Wird die Nachricht erfolgreich desinfiziert, so wird sie angenommen und zugestellt; kann die Nachricht nicht desinfiziert werden, so wird sie, in Abhängigkeit von der oben ausgewählten Option, abgewiesen oder in Quarantäne gegeben. Falls Sie nicht wünschen, dass infizierte Nachrichten desinfiziert werden, deaktivieren Sie dieses Kontrollkästchen. Infizierte Nachrichten werden dann sofort abgewiesen oder in Quarantäne gegeben.

Dateianlagen als Viren kennzeichnen, falls sie Makros enthalten
Diese Option bewirkt, dass Dokumente, die als Dateianlagen einer Nachricht beigefügt sind, und in denen Makros erkannt werden, als Viren gekennzeichnet werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausschlüsse

Nachrichten von IP-Adressen auf der Weißen Liste nicht durchsuchen
Um Nachrichten von der Virenprüfung auszunehmen, falls sie von einer IP-Adresse auf der Weißen Liste 281 stammen, aktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne nicht durchsuchen
Um Nachrichten von der Virenprüfung auszunehmen, falls sie von einem Mailserver der Domäne 79 stammen, aktivieren Sie diese Option.

Nachrichten, die von den unten aufgeführten E-Mail-Adressen aus gesendet wurden, nicht prüfen
Um Nachrichten von den hier aufgeführten Absendern von der Virenprüfung auszunehmen, aktivieren Sie diese Option.

Module für die Virenprüfung (Alle Domänen)

Nachrichten mithilfe des Moduls ClamAV prüfen
Das Modul ClamAV wird per Voreinstellung genutzt, um die Nachrichten auf Viren zu prüfen. Falls Sie das Modul ClamAV nicht zur Prüfung der Nachrichten nutzen möchten, deaktivieren Sie diese Option.

Nachrichten mithilfe des Moduls IKARUS Anti-Virus prüfen
Das Modul IKARUS Anti-Virus wird per Voreinstellung genutzt, um die Nachrichten auf Viren zu prüfen. Falls Sie das Modul IKARUS Anti-Virus nicht zur Prüfung der Nachrichten nutzen möchten, deaktivieren Sie diese Option.

Falls beide Optionen aktiv sind, prüft SecurityGateway jede Nachricht mit jedem Modul, also insgesamt zweimal. Das Schutzniveau wird dadurch erhöht, da es vorstellbar ist, dass ein Modul einen Virus erkennt, den das andere Modul nicht erkannt hat.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen zur Virenprüfung dieser Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.2.2 Aktualisierung konfigurieren

Da Bedrohungen durch Viren unvermittelt entstehen und sich schnell ausweiten können, muss die Datenbank der Viren-Signaturen regelmäßig aktualisiert und stets aktuell gehalten werden; es könnten sonst Viren nicht erkannt werden. Die Optionen auf der Seite Aktualisierung konfigurieren veranlassen SecurityGateway, automatisch nach aktualisierten Viren-Signaturen zu suchen. Von dieser Seite aus kann auch eine sofortige Aktualisierung außerhalb des Zeitplans durchgeführt werden, und die Protokolle über die Aktualisierungen können angezeigt werden.**Beachte: Diese Optionen beziehen sich nur auf das Modul ClamAV. Das Modul IKARUS Anti-Virus sucht alle 10 Minuten nach Aktualisierungen.**

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Viren-Aktualisierungen

Automatische Aktualisierungen für Viren-Signaturen aktivieren
Mithilfe dieser Option wird die regelmäßige Suche nach aktualisierten Viren-Signaturen für ClamAV durch SecurityGateway eingerichtet. Sie können wählen, ob einmal pro Stunde oder einmal pro Tag nach Aktualisierungen gesucht wird. Die automatische Aktualisierung ist per Voreinstellung aktiv.

Stündlich - Um [xx] Minuten nach der vollen Stunde
SecurityGateway sucht per Voreinstellung einmal pro Stunde zu der hier festgelegten Minute nach aktualisierten Viren-Signaturen für ClamAV. Tragen Sie hier beispielsweise "29" ein, so wird die Aktualisierung um 1.29 Uhr, 2.29 Uhr und jede Stunde zur selben Minute durchgeführt Um einen Wert zufällig zu erzeugen, klicken Sie auf die Verknüpfung *Zeitpunkt zufällig festlegen.* Die meist genutzten Zeitpunkte, zu denen besonders viele Systeme nach Aktualisierungen suchen, sind etwa die volle und die halbe Stunde (etwa 1.00 Uhr, 1.30 Uhr usw.). Da außerhalb dieser Zeiten die Auslastung der Quellen für die Aktualisierung geringer ist, kann die Aktualisierung beschleunigt werden, wenn sie zu einem anderen, zufällig gewählten Zeitpunkt durchgeführt wird.

Täglich - Um [xx:xx]
Falls Sie einmal täglich nach Aktualisierungen suchen möchten, wählen Sie diese Option, und legen Sie die Uhrzeit fest. Die Uhrzeit muss im 24-Stunden-Format eingegeben werden, und Stunden und Minuten müssen durch einen Doppelpunkt getrennt werden, etwa "13:05". Um einen Wert zufällig zu erzeugen, klicken Sie auf die Verknüpfung *Zeitpunkt zufällig festlegen*. Ein oft genutzter Zeitpunkt, zu dem besonders viele Systeme nach Aktualisierungen suchen, ist etwa Mitternacht (00:00 Uhr). Da außerhalb dieser Zeit die Auslastung der Quellen für die Aktualisierung geringer ist, kann die Aktualisierung beschleunigt werden, wenn sie zu einem anderen, zufällig gewählten Zeitpunkt durchgeführt wird.

Klicken Sie hier, um sofort nach aktualisierten Viren-Signaturen zu suchen.
Ein Klick auf diese Verknüpfung veranlasst SecurityGateway, sofort nach aktualisierten Viren-Signaturen zu suchen. Diese sofortige Suche wird zusätzlich zu der vorher bereits konfigurierten Suche nach Zeitplan durchgeführt.

Klicken Sie hier, um das Aktualisierungs-Protokoll für ClamAV einzusehen.
Um das Aktualisierungs-Protokoll für ClamAV einzusehen, klicken Sie hier.

Klicken Sie hier, um das Aktualisierungs-Protokoll für IKARUS Anti-Virus einzusehen.
Um das Aktualisierungs-Protokoll für IKARUS Anti-Virus einzusehen, klicken Sie hier.

4.3 Anti-Spoofing


Der Abschnitt Anti-Spoofing im Menü Sicherheit 154 enthält Werkzeuge, mit deren Hilfe Sie Nachrichten mit gefälschten ("gespooften") Absenderadressen identifizieren können. Der Abschnitt enthält die folgenden sechs Funktionen:

Rückwärtssuche 191 - Diese Abfragefunktionen prüfen, ob die Domäne eines Absenders wirklich besteht, und ob die IP-Adresse des sendenden Servers dieser Domäne zugeordnet oder mit ihr verknüpft ist.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Sender Policy Framework (SPF) 194 - SPF ist ein offener Standard für ein Prüfverfahren, das gefälschte Absenderadressen in E-Mail-Nachrichten erkennt. Es schützt besonders den Antwortpfad, die Domäne, die im SMTP-Protokolldialog als Teil der Absenderadresse übermittelt wird. Das Verfahren prüft, ob in den DNS-Einträgen der Domäne eine SPF-Regel hinterlegt ist, anhand derer dann genau festgestellt wird, welche Mailserver und Hosts für die Domäne E-Mail-Nachrichten versenden dürfen. Hat die Domäne eine SPF-Regelung veröffentlicht, und ist der übermittelnde Host in der Regelung nicht als berechtigt genannt, so können Sie davon ausgehen, dass die Absenderadresse gefälscht ist.

DKIM-Prüfung 197 - Diese Funktion prüft Signaturen nach den Standards DomainKeys Identified Mail (DKIM) in eingehenden Nachrichten. Ist eine eingehende Nachricht kryptografisch signiert, so ruft SecurityGateway den öffentlichen Schlüssel aus dem DNS-Eintrag der Domäne ab und prüft anhand dieses Schlüssels die DKIM-Signatur der Nachricht auf Gültigkeit. Die Domäne des Signaturerstellers ergibt sich dabei aus der Signatur selbst. Besteht die DKIM-Signatur die Prüfung, so wird die Nachricht in den nächsten Verarbeitungsschritt der Zustellung übergeben, und ihre Nachrichten-Bewertung 185 kann wahlweise angepasst werden. Die DKIM-Prüfung stellt sicher, dass eine Nachricht nicht nur tatsächlich von dem angegebenen Absender kommt, sondern dass sie auch zwischen dem Zeitpunkt der Signatur und der Zustellung nicht verändert wurde.

DKIM-Signatur 199 - Die Optionen zur Signaturerstellung bestimmen, ob die abgehenden Nachrichten aus Ihren Domänen kryptografisch signiert werden sollen. Zum Einsatz kommt dabei die Methode DomainKeys Identified Mail (DKIM). Sie können von hier aus auch die Selektoren und die Schlüssel erstellen, die für die Signatur abgehender Nachrichten nötig sind, und Sie bestimmen, welcher Selektor eingesetzt wird.

Prüfung durch Rückruf 217 - Dieses Anti-Spoofing-Verfahren prüft, ob die Adresse des angeblichen Absenders einer E-Mail-Nachricht gültig ist. SecurityGateway stellt dazu eine Verbindung mit dem Mail Exchanger der Domäne her, die während des SMTP-Protokolldialogs im Befehl "MAIL From" genannt wurde, und versucht dann, festzustellen, ob die Absenderadresse eine gültige Adresse in dieser Domäne ist. Ergibt diese Prüfung, dass die Adresse des Absenders nicht besteht, so kann SecurityGateway die Nachricht so behandeln, wie wenn sie von einer gefälschten Adresse aus gesendet worden wäre. Die Nachricht kann abgewiesen, in Quarantäne gegeben oder zur Zustellung angenommen werden. Weiter können ihre Nachrichten-Bewertung 185 angepasst und ihre Betreffzeile gekennzeichnet werden.

Auswertung der Absenderkopfzeile From 220 - Auf dieser Seite finden Sie Optionen, mit deren Hilfe Sie in betrügerischer Absicht gefälschte Absenderkopfzeilen ("From:") leichter entdecken können. Solche gefälschten Absenderkopfzeilen können durch Spam-Versender in die Nachrichten eingefügt werden, und sie können möglicherweise Benutzer zu der irrtümlichen Annahme verleiten, dass die Nachrichten von vertrauenswürdigen Absendern stammen.

4.3.1 Rückwärtssuche

PTR

Rückwärtssuche nach PTR-Eintrag bei eingehenden SMTP-Verbindungen durchführen
Per Voreinstellung fragt SecurityGateway bei allen eingehenden SMTP-Verbindungen die Pointer-Einträge ab. Falls dies nicht erwünscht ist, deaktivieren Sie diese Option.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

501 senden und Verbindung trennen, falls kein PTR-Eintrag existiert (Vorsicht)
Diese Option bewirkt, dass SecurityGateway einen Fehlerkode `501` sendet (Syntaxfehler in Parametern oder Argumenten) und die Verbindung trennt, falls für die Domäne kein PTR-Eintrag existiert. Diese Option ist per Voreinstellung abgeschaltet.

501 senden und Verbindung trennen, falls PTR-Eintrag nicht übereinstimmt
Diese Option bewirkt, dass SecurityGateway einen Fehlerkode `501` sendet (Syntaxfehler in Parametern oder Argumenten) und die Verbindung trennt, falls das Ergebnis der Abfrage des Pointer-Eintrags nicht mit der Gegenstelle übereinstimmt. Die Option ist per Voreinstellung abgeschaltet.

Echtheitsbestätigte Verbindungen von Abwehrmaßnahmen ausnehmen
Diese Option bewirkt, dass SecurityGateway die PTR-Abfrage bei eingehenden SMTP-Verbindungen aufschiebt, bis der SMTP-Befehl MAIL gegeben wurde. SecurityGateway kann dann feststellen, ob die Verbindung echtheitsbestätigt wird. Nach erfolgreicher Echtheitsbestätigung wird der Absender von Abwehrmaßnahmen ausgenommen. Diese Option ist per Voreinstellung abgeschaltet.

IP-Adressen auf der globalen Weißen Liste von Abwehrmaßnahmen ausnehmen
Diese Option bewirkt, dass IP-Adressen auf der globalen Weißen Liste 281 von den PTR-Abfragen ausgenommen sind. Diese Option ist per Voreinstellung abgeschaltet.

HELO/EHLO

Abfrage für HELO/EHLO-Domäne durchführen
Per Voreinstellung führt SecurityGateway für den Domänennamen, der in einer Verbindung mit dem Befehl `HELO/EHLO` übergeben wird, eine Abfrage durch. Der Client (die übermittelnde Gegenstelle) setzt den Befehl `HELO/EHLO` ein, um sich gegenüber dem Server zu identifizieren. Der Domänenname, der mit diesem Befehl übergeben wird, wird dann in den Abschnitt `from` der `Received`-Kopfzeilen eingetragen. Falls Sie diese Abfragen nicht durchführen wollen, deaktivieren Sie diese Option.

Bei gefälschter Identifikation Fehler 501 senden und Verbindung trennen (Vorsicht)
Diese Option bewirkt, dass ein Fehlerkode `501` gesendet und die Verbindung getrennt wird, falls das Ergebnis der Abfrage darauf hindeutet, dass die Identifikation der Gegenstelle gefälscht ist. Diese Option ist per Voreinstellung abgeschaltet.

Ergibt die Rückwärtssuche, dass der Server eine gefälschte Identifikation verwendet, so kann dieses Ergebnis in zahlreichen Fällen falsch sein. Mailserver identifizieren sich sehr häufig mit Daten, die nicht zu ihren IP-Adressen passen und nicht mit ihnen übereinstimmen. Die Gründe hierfür können in Beschränkungen durch den jeweiligen ISP liegen und sind sehr oft legitim. Sie sollten diese Option daher nur zurückhaltend nutzen; sie wird wahrscheinlich dazu führen, dass Ihr Server einige legitime Nachrichten abweist.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Post abweisen, falls die Domäne durch Rückwärtssuche nicht gefunden wurde
Ergibt die Abfrage eine Meldung "`Domäne nicht gefunden`", so bewirkt diese Option, dass die Nachricht mit einem Fehlerkode `451` (Angeforderte Aktion abgebrochen: lokaler Fehler bei der Verarbeitung) abgewiesen, die Verbindung danach aber bis zu ihrem Ende normal fortgesetzt wird. Diese Option ist per Voreinstellung abgeschaltet.

...Fehlerkode 501 senden (normalerweise wird Fehlerkode 451 gesendet)
Diese Option bewirkt, dass der Fehlerkode, der im Falle einer nicht gefundenen Domäne gesendet wird, nicht 451 sondern 501 (Syntaxfehler in Parametern oder Argumenten) lautet.

...und danach Verbindung trennen
Diese Option bewirkt, dass die Verbindung sofort getrennt wird, nachdem eine Rückwärtssuche ergeben hat, dass die Domäne nicht gefunden wurde.

Echtheitsbestätigte Verbindungen von Abwehrmaßnahmen ausnehmen
Diese Option bewirkt, dass SecurityGateway die Abfrage bei eingehenden SMTP-Verbindungen aufschiebt, bis der SMTP-Befehl MAIL gegeben wurde. SecurityGateway kann dann feststellen, ob die Verbindung echtheitsbestätigt wird. Nach erfolgreicher Echtheitsbestätigung wird der Absender von Abwehrmaßnahmen ausgenommen. Diese Option ist per Voreinstellung abgeschaltet.

IP-Adressen und Hosts auf der globalen Weißen Liste von Abwehrmaßnahmen ausnehmen
Diese Option bewirkt, dass IP-Adressen auf der globalen Weißen Liste 281 und Hosts auf der globalen Weißen Liste 278 von den Abfragen nach der HELO/EHLO-Domäne ausgenommen sind. Diese Option ist per Voreinstellung abgeschaltet.

Nachricht

Abfrage mit dem Inhalt des MAIL-Befehls durchführen
Per Voreinstellung führt SecurityGateway für den Domänennamen, der in einer Verbindung mit dem Befehl `MAIL` übergeben wird, eine Abfrage durch. Die Adresse, die mit dem Befehl `MAIL` übergeben wird, soll dem Antwortpfad der Nachricht entsprechen, und sie entspricht üblicherweise der E-Mail-Adresse oder dem Postfach, von dem die Nachricht ausgeht. Manchmal wird aber auch die Adresse übermittelt, an die Fehlermeldungen gerichtet werden sollen. Falls Sie diese Abfragen nicht durchführen wollen, deaktivieren Sie diese Option.

Bei gefälschter Identifikation Fehler 501 senden und Verbindung trennen (Vorsicht)
Diese Option bewirkt, dass ein Fehlerkode `501` gesendet und die Verbindung getrennt wird, falls das Ergebnis der Abfrage darauf hindeutet, dass die Identifikation der Gegenstelle gefälscht ist. Diese Option ist per Voreinstellung abgeschaltet.

Ergibt die Rückwärtssuche, dass der Server eine gefälschte Identifikation verwendet, so kann dieses Ergebnis in zahlreichen Fällen falsch sein. Mailserver identifizieren sich sehr häufig mit Daten, die nicht zu ihren IP-Adressen passen und nicht mit ihnen übereinstimmen. Die Gründe

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

hierfür können in Beschränkungen durch den jeweiligen ISP liegen und sind sehr oft legitim. Sie sollten diese Option daher nur zurückhaltend nutzen; sie wird wahrscheinlich dazu führen, dass Ihr Server einige legitime Nachrichten abweist.

Post abweisen, falls die Domäne durch Rückwärtssuche nicht gefunden wurde
Ergibt die Abfrage für den Domänennamen, der mit dem Befehl `MAIL` übermittelt wurde, eine Meldung "`Domäne nicht gefunden`", so bewirkt diese Option, dass die Nachricht mit einem Fehlerkode `451` (Angeforderte Aktion abgebrochen: lokaler Fehler bei der Verarbeitung) abgewiesen, die Verbindung danach aber bis zu ihrem Ende normal fortgesetzt wird. Diese Option ist per Voreinstellung abgeschaltet.

...Fehlerkode 501 senden (normalerweise wird Fehlerkode 451 gesendet)
Diese Option bewirkt, dass der Fehlerkode, der im Falle einer nicht gefundenen Domäne gesendet wird, nicht 451 sondern 501 (Syntaxfehler in Parametern oder Argumenten) lautet.

...und danach Verbindung trennen
Diese Option bewirkt, dass die Verbindung sofort getrennt wird, nachdem eine Rückwärtssuche ergeben hat, dass die Domäne nicht gefunden wurde.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Nachrichten aus Verbindungen mit Echtheitsbestätigung sind per Voreinstellungen von den Abfragen für den Befehl `MAIL` ausgenommen. Falls Sie diese Nachrichten ebenfalls in die Prüfung einbeziehen wollen, deaktivieren Sie diese Option.

Absender auf der globalen Weißen Liste ausnehmen
Nachrichten von Absendern, die auf der globalen Weißen Liste eingetragen sind, werden per Voreinstellung von den Abfragen ausgenommen. Falls Sie diese Absender ebenfalls in die Prüfung einbeziehen wollen, deaktivieren Sie diese Option.

Konfiguration

Warn-Kopfzeilen in verdächtige Nachrichten einfügen
Schlägt für eine Nachricht die Rückwärtssuche fehl, so fügt SecurityGateway per Voreinstellung eine Kopfzeile mit einer Warnmeldung in die Nachricht ein. Ein Mailserver oder Client, der die Nachricht empfängt, kann sie anhand dieser Kopfzeile filtern. Falls Sie die Kopfzeile in verdächtige Nachrichten nicht einfügen wollen, deaktivieren Sie diese Option.

4.3.2 SPF-Prüfung

Das Sender Policy Framework (SPF) ist ein offener Standard für ein Prüfverfahren, das gefälschte Absenderadressen in E-Mail-Nachrichten erkennt. Es schützt besonders den Antwortpfad, die Domäne, die im SMTP-Protokolldialog als Teil der Absenderadresse übermittelt wird. Das Verfahren prüft, ob in den DNS-Einträgen der Domäne eine SPF-Regel hinterlegt ist, anhand derer dann genau festgestellt wird, welche Mailserver und Hosts für die Domäne E-Mail-Nachrichten versenden dürfen. Hat die Domäne eine SPF-Regelung veröffentlicht, und ist der übermittelnde Host in

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

der Regelung nicht als berechtigt genannt, so können Sie davon ausgehen, dass die Absenderadresse gefälscht ist.

Weitere Informationen über das SPF erhalten Sie unter www.open-spf.org.

Konfiguration

Absender-Host über SPF prüfen
SecurityGateway prüft per Voreinstellung die DNS-Einträge der Domäne des Absenders, um festzustellen, ob der übermittelnde Host berechtigt ist, E-Mail für die Domäne zu versenden. Geprüft wird dabei die Domäne, die im Rahmen des SMTP-Protokolldialogs mit dem Befehl `MAIL` übergeben wird. Falls Sie keine Verarbeitung durch das SPF wünschen, deaktivieren Sie diese Option.

Führt Verarbeitung durch SPF zum Ergebnis HARD FAIL, dann:
Die folgenden Aktionen werden ausgeführt, falls die Verarbeitung einer Nachricht das Ergebnis HARD FAIL erbringt.

...Nachricht abweisen
Per Voreinstellung werden Nachrichten nach dem Ergebnis HARD FAIL während der SMTP-Übermittlung abgewiesen.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass Nachrichten nach dem Ergebnis HARD FAIL in Quarantäne gegeben werden.

...Nachricht annehmen
Diese Option bewirkt, dass Nachrichten auch nach dem Ergebnis HARD FAIL angenommen werden. Sie können die Betreffzeile solcher Nachrichten kennzeichnen lassen und ihre Nachrichten-Bewertung ändern.

...Betreff kennzeichnen mit [*Text*]
Falls Sie SecurityGateway so konfiguriert haben, dass eine Nachricht auch nach dem Ergebnis HARD FAIL noch angenommen wird, können Sie mithilfe dieser Option einen Kennzeichnungstext festlegen, der an den Anfang der Betreffzeile gesetzt wird. Per Voreinstellung wird, sobald diese Option aktiv ist, der Text "*** FRAUD ***" (Betrug) an den Anfang der Betreffzeile solcher Nachrichten gesetzt. Bei Nutzung dieser Option kann es dem Mailserver oder Client des Empfängers überlassen bleiben, ob er die Nachricht anhand der Kennzeichnung filtert. Die Option ist per Voreinstellung abgeschaltet.

SecurityGateway kann auch im Rahmen anderer Verarbeitungsfunktionen wahlweise die Betreffzeile von Nachrichten kennzeichnen. Die Funktionen DKIM-Prüfung 197 und Nachrichten-Bewertung 185 lassen sich beispielsweise entsprechend konfigurieren. Stimmen die Kennzeichnungstexte in diesen Funktionen überein, so wird die Kennzeichnung dem Betreff nur einmal hinzugefügt, auch wenn die Bedingungen mehrerer Funktionen für eine Kennzeichnung bei der Nachricht erfüllt sind. Werden jedoch unterschiedliche Kennzeichnungstexte konfiguriert, so werden diese Kennzeichnungen gesondert eingefügt. Die Voreinstellung für den Kennzeichnungstext in der vorliegenden Funktion lautet beispielsweise "*** FRAUD

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

> ***", für die Nachrichten-Bewertung hingegen lautet sie "*** SPAM ***". Da die beiden Texte nicht gleich sind, werden sie beide in die Betreffzeile einer Nachricht eingefügt, die die Kriterien für beide Optionen erfüllt. Gleichen Sie einen Text dem anderen an, so wird die Kennzeichnung nur noch einmal eingefügt.

... [xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Nimmt SecurityGateway eine Nachricht nach dem Ergebnis HARD FAIL zur Zustellung an, so rechnet SecurityGateway per Voreinstellung der Nachrichten-Bewertung dieser Nachricht den hier angegebene Wert hinzu. Ergibt sich schließlich eine ausreichend hohe Bewertung, so kann die Nachricht in Quarantäne gegeben oder abgewiesen werden, je nach den Einstellungen zur Nachrichten-Bewertung[185]. Die Voreinstellung für diese Option beträgt `5.0`.

Führt Verarbeitung durch SPF zum Ergebnis SOFT FAIL, dann:
Die folgenden Aktionen werden ausgeführt, falls die Verarbeitung einer Nachricht das Ergebnis SOFT FAIL erbringt.

...Nachricht abweisen
Diese Option bewirkt, dass Nachrichten nach dem Ergebnis SOFT FAIL während der SMTP-Übermittlung abgewiesen werden.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass Nachrichten nach dem Ergebnis SOFT FAIL in Quarantäne gegeben werden.

...Nachricht annehmen
Per Voreinstellung werden Nachrichten nach dem Ergebnis SOFT FAIL angenommen. Sie können die Betreffzeile solcher Nachrichten kennzeichnen lassen und ihre Nachrichten-Bewertung ändern.

...Betreff kennzeichnen mit [*Text*]
Falls Sie SecurityGateway so konfiguriert haben, dass eine Nachricht nach dem Ergebnis SOFT FAIL angenommen wird, können Sie mithilfe dieser Option einen Kennzeichnungstext festlegen, der an den Anfang der Betreffzeile gesetzt wird. Per Voreinstellung wird, sobald diese Option aktiv ist, der Text "*** FRAUD ***" (Betrug) an den Anfang der Betreffzeile solcher Nachrichten gesetzt. Bei Nutzung dieser Option kann es dem Mailserver oder Client des Empfängers überlassen bleiben, ob er die Nachricht anhand der Kennzeichnung filtert. Die Option ist per Voreinstellung abgeschaltet.

... [xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Nimmt SecurityGateway eine Nachricht nach dem Ergebnis SOFT FAIL zur Zustellung an, so rechnet SecurityGateway per Voreinstellung der Nachrichten-Bewertung dieser Nachricht den hier angegebene Wert hinzu. Ergibt sich schließlich eine ausreichend hohe Bewertung, so kann die Nachricht in Quarantäne gegeben oder abgewiesen werden, je nach den Einstellungen zur Nachrichten-Bewertung[185]. Die Voreinstellung für diese Option beträgt `2.0`.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Führt Verarbeitung durch SPF zum Ergebnis PASS, dann:

... [xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Mithilfe dieser Option können Sie die Nachrichten-Bewertung anpassen, wenn eine Nachricht in der SPF-Prüfung das Ergebnis PASS erbringt. Falls Sie die Bewertung anpassen wollen, sollten Sie hier einen negativen Wert eintragen, da dieser die Nachrichten-Bewertung herabsetzt und damit verbessert.

Ausschlüsse

Nachrichten von IP-Adressen auf der Weißen Liste ausnehmen
Diese Option bewirkt, dass Nachrichten, die von IP-Adressen auf der globalen Weißen Liste für IP-Adressen 281 aus gesendet werden, von der SPF-Prüfung ausgenommen sind. Diese Option ist per Voreinstellung abgeschaltet.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Nachrichten, die über echtheitsbestätigte Verbindungen gesendet werden, sind per Voreinstellung von der SPF-Prüfung ausgenommen. Falls Sie die SPF-Prüfung auch dann durchführen wollen, wenn die SMTP-Verbindung echtheitsbestätigt war, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Nachrichten, die über die Mailserver der Domäne 79 gesendet werden, sind per Voreinstellung von der SPF-Prüfung ausgenommen. Falls Sie die SPF-Prüfung auch dann durchführen wollen, wenn Nachrichten über diese Server übermittelt wurden, deaktivieren Sie diese Option.

Erweitert

Kopfzeile "Received-SPF" in Nachrichten einfügen
Per Voreinstellung in jede Nachricht eine Kopfzeile "`Received-SPF`" eingefügt. Sie enthält die Ergebnisse der SPF-Prüfung für die Nachricht. Falls Sie diese Kopfzeile nicht in die Nachrichten einfügen wollen, deaktivieren Sie diese Option.

...außer, wenn SFP-Verarbeitung das Ergebnis "none" meldet
Per Voreinstellung wird die Kopfzeile "`Received-SPF`" dann nicht in Nachrichten eingefügt, wenn das Ergebnis der SPF-Prüfung "none" lautet. Falls Sie die Kopfzeile auch dann in Nachrichten einfügen wollen, wenn für die Domäne des Absenders keine SPF-Daten gefunden wurden, deaktivieren Sie diese Option.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen zum SPF für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.3.3 DKIM-Prüfung

Auf dieser Seite können Sie konfigurieren, wie SecurityGateway Signaturen nach dem Standard DomainKeys Identified Mail (DKIM) in eingehenden Nachrichten prüft. Ist dieses Leistungsmerkmal aktiv, und ist eine eingehende Nachricht kryptografisch signiert 199, so ruft SecurityGateway den öffentlichen Schlüssel aus dem DNS-Eintrag der Domäne ab und prüft anhand dieses Schlüssels die DKIM-Signatur der Nachricht

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

auf Gültigkeit. Die Domäne des Signaturerstellers ergibt sich dabei aus der Signatur selbst. Besteht die DKIM-Signatur die Prüfung, so wird die Nachricht in den nächsten Verarbeitungsschritt der Zustellung übergeben, und ihre Nachrichten-Bewertung 185 kann wahlweise angepasst werden.

Weitere Informationen über DKIM erhalten Sie unter www.dkim.org.

Kryptografische Prüfung

Signaturen prüfen, die über DomainKeys-Identified-Mail (DKIM) erstellt wurden
Diese Option bewirkt, dass SecurityGateway eingehende Nachrichten, die durch DKIM signiert 199 wurden, prüft. Falls Sie die DKIM-Signaturen in Nachrichten nicht prüfen wollen, deaktivieren Sie diese Option.

Führt die Prüfung zum Ergebnis PASS, dann:

... [xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Mithilfe dieser Option können Sie die Nachrichten-Bewertung anpassen, wenn eine Nachricht in der DKIM-Prüfung das Ergebnis bestanden ("pass") erbringt. Per Voreinstellung beträgt der Wert für diese Option `0.0`, sodass die Bewertung nicht geändert wird. Falls Sie die Bewertung anpassen wollen, sollten Sie hier einen negativen Wert eintragen, da dieser die Nachrichten-Bewertung herabsetzt und damit verbessert. Der Wert `-0.5` in dieser Option verringert die Bewertung beispielsweise um 0,5 Punkte.

Ausschlüsse

Nachrichten von IP-Adressen auf der Weißen Liste ausnehmen
Nachrichten, die von IP-Adressen auf der Weißen Liste 281 aus gesendet werden, sind per Voreinstellung von der DKIM/DK-Prüfung ausgenommen. Falls Sie die DKIM-Signaturen auch dann prüfen wollen, wenn der Absender auf der Weißen Liste für IP-Adressen erfasst ist, aktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Nachrichten, die über echtheitsbestätigte Verbindungen gesendet werden, sind per Voreinstellung von der DKIM-Prüfung ausgenommen. Falls Sie die DKIM-Signaturen auch dann prüfen wollen, wenn die SMTP-Verbindung echtheitsbestätigt war, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Nachrichten, die über die Mailserver der Domäne 79 gesendet werden, sind per Voreinstellung von der DKIM-Prüfung ausgenommen. Falls Sie die DKIM-Signaturen auch dann prüfen wollen, wenn Nachrichten über diese Server übermittelt wurden, deaktivieren Sie diese Option.

Optionen zur DKIM-Prüfung (Alle Domänen)

Prüfer beachtet die Länge des Nachrichtentextes (Tag l=)
Ist diese Option aktiv, so beachtet SecurityGateway den Tag, der die Länge des Nachrichtentextes dokumentiert, sofern er in der DKIM-Signatur einer eingehenden Nachricht enthalten ist. Ist die tatsächliche Länge des Nachrichtentextes größer als der Wert in diesem Tag, so prüft SecurityGateway die Nachricht nur, bis die im Tag genannte Größe erreicht ist; im Übrigen wird die Nachricht nicht geprüft. Eine solche Abweichung ist ein Zeichen dafür, dass der Nachricht etwas hinzugefügt wurde; der ungeprüfte Teil der Nachricht kann daher als verdächtig gelten. Ist die tatsächliche Länge des Nachrichtentextes kleiner als

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

der Wert in diesem Tag, so besteht die Signatur die Prüfung nicht (die Prüfung führt zum Ergebnis "FAIL"). Eine solche Abweichung ist ein Zeichen dafür, dass ein Teil der Nachricht gelöscht wurde. Diese Option ist per Voreinstellung abgeschaltet.

Prüfer verlangt, dass Signaturen die Betreffzeile schützen
Diese Option veranlasst die Prüfroutine, zu verlangen, dass die DKIM-Signaturen eingehender Nachrichten auch die Betreffzeile schützen. Diese Option per Voreinstellung abgeschaltet.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen zur Prüfung signierter Nachrichten für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.3.4 DKIM-Signatur

Die Optionen zur Signaturerstellung bestimmen, ob die abgehenden Nachrichten aus Ihren Domänen kryptografisch signiert werden sollen. Die kryptografische Signatur wird nach der Methode DomainKeys Identified Mail (DKIM) erstellt. Sie können von hier aus auch die Selektoren und die Schlüssel erstellen, die für die Signatur abgehender Nachrichten nötig sind, und Sie bestimmen, welcher Selektor eingesetzt wird. Alle Schlüssel sind einmalig; unabhängig von dem angegebenen Selektor können die Schlüssel zweier Domänen nie übereinstimmen.

Weitere Informationen über DKIM erhalten Sie unter www.dkim.org.

Signatur über DKIM

Abgehende Nachrichten über DomainKeys Identified Mail (DKIM) signieren
Diese Option bewirkt, dass die abgehenden Nachrichten der Domäne über DomainKeys Identified Mail kryptografisch signiert werden. Eine Nachricht kann dabei nur signiert werden, falls Sie durch eine echtheitsbestätigte SMTP-Verbindung (SMTP AUTH) oder über einen Mailserver der Domäne 79 an SecurityGateway übermittelt wird. Hierdurch wird sichergestellt, dass nur echtheitsbestätigte Nachrichten signiert werden.

Nachrichten mithilfe dieses Selektors signieren:
Wählen Sie aus der Auswahlliste den Selektor aus, dessen zugehöriges Schlüsselpaar aus öffentlichen und geheimen Schlüsseln Sie für die Signatur der Nachrichten der Domäne nutzen wollen. Um einen neuen Selektor zu erstellen, klicken Sie auf *Neu*, tragen Sie dann den *Namen des Selektors* in das Eingabefeld ein, und klicken Sie schließlich auf *Speichern und Beenden*.

Neu
Klicken Sie auf dieses Steuerelement, um einen neuen Selektor zu erstellen, mit dessen Hilfe Sie die Nachrichten der Domäne signieren können. Tragen Sie den Namen des Selektors in das Eingabefeld ein, und klicken Sie schließlich auf *Speichern und Beenden*.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Löschen
Um einen Selektor zu löschen, wählen Sie ihn aus der Auswahlliste, und klicken Sie dann auf *Löschen*.

Hinweise zur DNS-Konfiguration (öffentlicher Schlüssel) für diesen Selektor anzeigen
Um die DNS-Konfiguration für einen Selektor einzusehen, wählen Sie den Selektor aus dem Auswahlmenü oben aus, und klicken Sie dann auf diese Verknüpfung. SecurityGateway zeigt Ihnen die DKIM-Informationen an, die den DNS-Einträgen der Domäne hinzugefügt werden müssen. Dritte können die Signaturen in Ihren Nachrichten erst dann prüfen, wenn diese Informationen im DNS veröffentlicht sind. Die Hinweise für die DNS-Konfiguration enthalten folgende Daten:

DNS-Eintrag für den DKIM-Selektor
Andere Server benötigen diese Informationen, um die über DKIM signierten Nachrichten der Domäne zu prüfen. Die Informationen enthalten den Selektor, die Domäne, den öffentlichen Schlüssel und weitere erforderliche Daten.

Falls Sie die abgehenden Nachrichten aus einer Domäne signieren wollen, müssen Sie die vorstehenden Informationen den DNS-Einträgen der Domäne hinzufügen. Ohne diese im DNS veröffentlichten Informationen können Mailserver, die Ihre Nachrichten empfangen, die Signaturen nicht prüfen. Nähere Informationen, auch zu weiteren Parametern, die Sie in den DNS-Einträgen veröffentlichen können, erhalten Sie unter www.dkim.org und auf der Seite DomainKeys Distribution Options (Optionen zur Veröffentlichung von DomainKeys) unter domainkeys.sourceforge.net.

Optionen zur DKIM-Signatur (Alle Domänen)

Signaturen verfallen nach [xx] Tagen (Tag x=, Voreinstellung 7 Tage)
Diese Option begrenzt die Gültigkeitsdauer der DKIM-Signaturen. Nachrichten mit abgelaufenen Signaturen bestehen die Prüfung nicht mehr. Diese Option entspricht dem Tag "x=" der Signaturen. Diese Option ist per Voreinstellung aktiv, und die voreingestellte Gültigkeitsdauer beträgt 7 Tage.

Signaturen enthalten die Abfragemethode(n) (Tag q=)
Diese Option bindet den Tag für die Abfragemethode (z.B. q=dns) in die DKIM-Signatur ein. Diese Option ist per Voreinstellung aktiv.

Signaturen enthalten die Länge des Nachrichtentextes (Tag l=)
Diese Option bestimmt, ob die Länge des Nachrichtentextes (Tag "l=") in die DKIM-Signaturen eingebunden werden soll. Diese Option ist per Voreinstellung aktiv.

Signaturen enthalten den Inhalt der Ursprungs-Kopfzeile (Tag z=)
Diese Option bindet den Tag "z=" in die DKIM-Signatur ein. Der Tag enthält eine Kopie der ursprünglichen Kopfzeilen der Nachricht; er kann die Größe der Signaturen daher erheblich erhöhen. Diese Option ist per Voreinstellung abgeschaltet.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kanonisierung

Der Begriff "Kanonisierung" bezeichnet einen Vorgang, in dessen Verlauf die Kopfzeilen und der Nachrichtentext einer Nachricht in einen kanonischen Standard umgesetzt werden, bevor die DKIM-Signatur erstellt wird. Der Vorgang wird bisweilen auch als Normalisierung bezeichnet. Er ist erforderlich, da manche E-Mail-Server und Relaissysteme verschiedene an sich unbedeutende Änderungen an der Nachricht vornehmen, während sie sie verarbeiten. Ohne die Kanonisierung vor der Signaturerstellung könnten auch solche unbedeutenden Änderungen die Signatur ungültig machen. Die Signatur und die Prüfung der Signatur nach dem DKIM-Standard unterstützen derzeit zwei Methoden der Kanonisierung: einfach und tolerant. Die einfache Methode ist strikter, und sie erlaubt nahezu keine Änderungen an der Nachricht. Die tolerante Methode ist hingegen weniger strikt und lässt unbedeutende Änderungen an der Nachricht zu.

Kopfzeilen kanonisieren nach Methode: Einfach, Tolerant
Diese Methode wird bei Erstellung der Signatur auf die Kopfzeilen der Nachricht angewendet. Die einfache Methode lässt keinerlei Änderungen an den Kopfzeilen zu. Die tolerante Methode lasst die Änderung von Namen der Kopfzeile in Kleinschreibung, die Zusammenfassung mehrerer aufeinander folgender Leerzeichen zu einem einzigen Leerzeichen und weitere unbedeutende Änderungen zu. Sie lässt jedoch keine Änderung an den Inhalten der Kopfzeilen zu. Die Voreinstellung ist "Einfach".

Nachrichtentext kanonisieren nach Methode: Einfach, Tolerant
Diese Methode wird bei der Erstellung der Signatur auf den Inhalt der Nachricht angewendet. Die einfache Methode ignoriert Leerzeilen am Ende des Nachrichtentextes — sonstige Änderungen am Nachrichtentext sind nicht zulässig. Die tolerante Methode ignoriert Leerzeilen am Ende der Nachricht und Leerzeichen am Zeilenende, sie führt mehrere aufeinander folgende Leerzeichen in allen Zeilen zu je einem Leerzeichen zusammen, und sie lässt weitere unbedeutende Änderungen zu. Die Voreinstellung ist "Einfach".

4.3.5 DMARC

"DMARC" steht für Domain-based Message Authentication, Reporting, and Conformance (domänengestützte Echtheitsbestätigung, Berichte und Übereinstimmung). Die Spezifikation für DMARC beschreibt ein anpassungsfähiges Verfahren, mit dessen Hilfe der Missbrauch von Nachrichten, beispielsweise durch eingehenden Spam und Phishing-Nachrichten, deren Absenderkopfzeile `From:` gefälschte Inhalte enthält, verringert werden kann. DMARC ermöglicht es den Domäneninhabern, das Domain Name System (DNS) zu nutzen, um Servern, die Nachrichten empfangen, die eigenen DMARC-Richtlinien bekannt zu machen. Diese Richtlinien geben empfangenden Servern Auskunft darüber, wie sie Nachrichten behandeln sollen, die angeblich von der Domäne stammen, für die die Richtlinien veröffentlicht sind, bei denen aber nicht festgestellt werden kann, dass sie tatsächlich von dieser Domäne stammen. Die empfangenden Server fragen die Richtlinien über eine DNS-Abfrage ab, während sie die eingehenden Nachrichten verarbeiten. Die Richtlinien können bestimmen, dass die Server Nachrichten in Quarantäne geben oder abweisen, falls sie nicht den Richtlinien entsprechen. Sie können aber auch bestimmen, dass keine besonderen Maßnahmen getroffen werden und die Nachrichten normal verarbeitet werden. Neben diesen Regelungen über die Behandlung von Nachrichten können die DNS-Einträge für DMARC auch Anforderungen enthalten, dass der empfangende Server an bestimmte Empfänger DMARC-Berichte senden soll. Diese Berichte enthalten Informationen über die Anzahl eingehender Nachrichten, die angeblich von der Domäne stammen, sowie

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Informationen über erfolgreiche und fehlgeschlagene Bestätigung der Echtheit der Nachrichten und Einzelheiten über Fehler in der Prüfung. Die Berichtsfunktionen von DMARC können hilfreich sein, um festzustellen, wie wirksam die eigenen Maßnahmen zur Sicherung der Echtheit von Nachrichten sind und wie oft der eigene Domänenname in gefälschten Nachrichten verwendet wird.

Der Konfigurationsdialog **Sicherheit » Anti-Spoofing** enthält drei Abschnitte, in denen die DMARC-Prüfung und die DMARC-Berichte für SecurityGateway konfiguriert werden können: DMARC-Prüfung, DMARC-Berichte und DMARC-Einstellungen.

DMARC-Prüfung 208

Während der DMARC-Prüfung fragt SecurityGateway die DMARC-Richtlinien durch eine DNS-Abfrage ab; diese Abfrage bezieht sich auf die Domäne in der Absenderkopfzeile `From:` (Von:) jeder eingehenden Nachricht. Die Abfrage prüft zunächst, ob die Domäne DMARC nutzt und ruft bejahendenfalls den DMS-Eintrag für DMARC 203 ab. Diese DNS-Eintrag enthält die DMARC-Richtlinie und verwandte Informationen. DMARC nutzt außerdem das SPF 194 und DKIM 197, um jede eingehende Nachricht zu prüfen, und die Prüfung durch SPF 194 oder DKIM 197 muss erfolgreich verlaufen, damit auch die DMARC-Prüfung erfolgreich sein kann. Besteht eine Nachricht diese Prüfungen, so wird sie durch den üblichen Filter- und Zustellvorgang in SecurityGateway normal weiterbearbeitet. Besteht eine Nachricht die Prüfung nicht, dann richtet sich ihre weitere Behandlung nach den DMARC-Richtlinien der angeblichen Absenderdomäne und danach, wie SecurityGateway für die Behandlung solcher Nachrichten konfiguriert ist.

Besteht eine Nachricht die DMARC-Prüfung nicht, und ist für die angebliche Absenderdomäne die DMARC-Richtlinie "`p=none`" veröffentlicht, so ergreift SecurityGateway keine Abwehrmaßnahmen, und die Nachricht wird normal weiterverarbeitet. Ist für die angebliche Absenderdomäne jedoch eine restriktive DMARC-Richtlinie veröffentlicht, also "`p=quarantine`" oder "`p=reject`", dann kann SecurityGateway die Nachricht automatisch in den Quarantäne-Ordner 308 des Empfängers leiten, die `Betreffzeile` kennzeichnen oder die Nachrichten-Bewertung 185 anpassen. In Nachrichten, für deren angebliche Absenderdomänen restriktive Richtlinien veröffentlicht sind, fügt SecurityGateway je nach veröffentlichter Richtlinie die Kopfzeilen "`X-SGDMARC-Fail-policy: quarantine`" oder "`X-SGDMARC-Fail-policy: reject`" ein. Hiermit können Sie durch ein Sieve-Skript 284 oder durch den Inhaltsfilter weitere Maßnahmen auslösen, die diese Kopfzeilen auswerten und Nachrichten beispielsweise in einen besonderen Ordner zur genaueren Untersuchung leiten.

Die DMARC-Prüfung ist per Voreinstellung aktiv und wird für die meisten Einsatzgebiete von SecurityGateway empfohlen.

DMARC-Berichte 212

Die DMARC-Einträge, die SecurityGateway aus dem DNS abfragt, können Tags enthalten, durch die der Domäneninhaber anzeigt, dass er bestimmte zusammengefasste Statistik- und Fehlerberichte über die DMARC-gestützte Behandlung solcher Nachrichten erhalten will, die angeblich aus seiner Domäne stammen. Die Optionen im Konfigurationsdialog DMARC-Berichte bestimmen, ob Ihr System die angeforderten Arten von Berichten versenden soll, und welche Metadaten die Berichte enthalten sollen. Zusammengefasste Berichte werden jeden Tag um Mitternacht (UTC-Zeit) gesendet. Fehlerberichte werden für jede Nachricht dann gesendet, wenn eine fehlgeschlagene Prüfung den Fehlerbericht auslöst. Alle Berichte werden als XML-Dateien in ZIP-Archiven versandt, die als Dateianlage an die Berichtsnachrichten angehängt werden. Es stehen verschiedene

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Auswertungsprogramme zur Verfügung, mit deren Hilfe die Empfänger die Berichte einsehen und auswerten können. Per Voreinstellung versendet SecurityGateway nur zusammengefasste Berichte.

DMARC-Einstellungen 216

Der Konfigurationsdialog DMARC-Einstellungen enthält Optionen zur Aufnahme bestimmter Daten in DMARC-Berichte, zur Protokollierung von DNS-Einträgen für DMARC und zur Aktualisierung der Liste öffentlicher Domänenendungen, die SecurityGateway für DMARC nutzt.

Wechselwirkung zwischen DMARC-Prüfung und Mailinglisten

DMARC soll sicherstellen, dass die Domäne in der Absenderkopfzeile `From:` eingehender Nachrichten nicht gefälscht ist sondern dem wirklichen Absender entspricht. DMARC muss daher überprüfen, ob der Server, der die Nachricht übermittelt, zum Versand von Nachrichten für die Absenderdomäne auch wirklich berechtigt ist. Bei Mailinglisten kann dies zu einem besonderen Problem führen. Es ist nämlich bei Mailinglisten üblich, dass diese die Listennachrichten für alle, auch fremde, Listenmitglieder versenden, dass dabei die Absenderkopfzeile `From:` unverändert bleibt und noch die ursprüngliche Domäne des Absenders enthält. Empfängt ein Server eine solche Listennachricht, und führt er eine DMARC-Prüfung für die Nachricht aus, dann stellt er hierbei fest, dass ein Server die Nachricht versandt hat, der eigentlich gar nicht berechtigt ist, für die Domäne in der Absenderkopfzeile `From:` Nachrichten zu versenden. Ist für die Domäne in der Absenderkopfzeile `From:` eine restriktive DMARC-Richtlinie veröffentlicht, so kann dies dazu führen, dass der Server des Empfängers die Listennachricht in Quarantäne gibt oder sogar abweist. Außerdem kann in bestimmten Fällen der Empfänger der Listennachricht automatisch aus der Mailingliste entfernt werden. Um dieses Problem zu umgehen, ersetzt SecurityGateway den Inhalt der Absenderkopfzeile `From:` in Listennachrichten dann durch die E-Mail-Adresse der Mailingliste, wenn für die Domäne des Absenders eine restriktive DMARC-Richtlinie veröffentlicht ist. Sie können SecurityGateway aber auch so konfigurieren, dass Listennachrichten aus Domänen mit restriktiven DMARC-Richtlinien abgewiesen werden. Falls Sie MDaemon ab Version 14.5 als E-Mail-Server verwenden, werden per Voreinstellung die Absenderkopfzeilen `From:` durch die Adresse der Mailingliste ersetzt, falls für die Domäne des Absenders eine restriktive DMARC-Richtlinie veröffentlicht ist.

Die Nutzung von DMARC für Ihre Domänen

Die Nutzung von DMARC für eigene Domänen, die die Server der Nachrichtenempfänger in die Lage versetzt, DMARC zur Prüfung solcher Nachrichten einzusetzen, die angeblich aus den eigenen Domänen stammen, hängt von mehreren Voraussetzungen ab. Sie müssen zunächst sicherstellen, dass Sie für die betroffenen Domänen gültige DNS-Einträge für SPF 194 und DKIM 199 erstellt haben. SPF oder DKIM oder beide Verfahren zugleich müssen funktionsfähig eingerichtet sein, damit DMARC nutzbar ist. Falls Sie DKIM nutzen, müssen Sie auch die Signatur von Nachrichten über DKIM 199 konfigurieren, damit SecurityGateway die Nachrichten der betroffenen Domänen signiert. Sie müssen außerdem für die betroffenen Domänen DNS-Einträge für DMARC anlegen. Diese Einträge sind `TXT`-Einträge in einem bestimmten, vorgegebenen Format, die die Server der Nachrichtenempfänger abfragen, um Informationen über die DMARC-Richtlinie und verschiedene weitere Parameter zu erhalten. Solche weiteren Parameter sind insbesondere die Art der Echtheitsbestätigung, die Sie nutzen, die Festlegung, ob Sie zusammengefasste

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Berichte erhalten wollen, und die E-Mail-Adresse, an die die Berichte gesendet werden sollen. Ist DMARC richtig eingerichtet, und erhalten Sie XML-Berichte für DMARC, so stehen Ihnen eine Reihe von Online-Werkzeugen zur Verfügung, mit deren Hilfe Sie die Berichte auswerten und mögliche Probleme erkennen können.

Erstellen eines DMARC-Ressourceneintrags vom Typ TXT

Nachfolgend finden Sie einen Überblick über grundlegende und häufig genutzte Bestandteile eines DMARC-Eintrags. Nähere Informationen und Hinweise zu fortgeschrittenen Konfigurationsmöglichkeiten erhalten Sie auf der Website www.dmarc.org.

Feld "Owner" (Inhaber)

Das Feld "Owner" (es wird auch als "Name" oder "left-hand" bezeichnet) im DMARC-Ressourceneintrag muss immer den Inhalt **_dmarc**haben. Falls Sie die Domäne oder Subdomäne angeben wollen, auf die sich der Eintrag bezieht, so können Sie das Format **_dmarc.domänen.name** hierfür nutzen.

Ein Beispiel hierzu:

Ein DMARC-Eintrag für die Domäne **example.com**

```
_dmarc IN TXT "v=DMARC1;p=none"
```

Dieser Eintrag wirkt für E-Mail-Nachrichten von benutzer@example.com und allen Subdomänen von example.com, also beispielsweise benutzer@support.example.com.

```
_dmarc.support.example.com IN TXT "v=DMARC1;p=none"
```

Dieser Eintrag wirkt nur für E-Mail-Nachrichten von benutzer@support.example.com, nicht jedoch beispielsweise für benutzer@example.com.

```
_dmarc.support IN TXT "v=DMARC1;p=none"
```

Dieser Eintrag wirkt für E-Mail-Nachrichten von benutzer@support.example.com, benutzer@a.support.example.com, benutzer@a.b.support.example.com und so weiter.

Tags und Parameter für die DMARC-Einträge

Zwingend erforderliche Tags

Tag	Parameter	Erläuterung
v=	**DMARC1**	Dieser Tag bestimmt die Version. Er muss der erste Tag in dem Textfeld des Ressourceneintrags sein. DMARC-Tags sind üblicherweise unabhängig von Groß- und Kleinschreibung; dies gilt aber nicht für diesen Tag. Er muss immer in Großbuchstaben gesetzt sein: **DMARC1**. Ein Beispiel hierzu: `_dmarc IN TXT "v=DMARC1;p=none"`

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

p=	**none** **quarantine** **reject**	Dieser Tag bestimmt die Richtlinie (p steht für policy). Er muss der zweite Tag in dem Textfeld des Ressourceneintrags sein und auf den Tag **v=** folgen. **p=none** (keine) bedeutet, dass der Server des Nachrichtenempfängers auf Grundlage der DMARC-Prüfung keine Aktion vornehmen soll. Nachrichten, die die DMARC-Prüfung nicht bestehen, sollen aufgrund der nicht bestandenen DMARC-Prüfung nicht in Quarantäne gegeben oder abgewiesen werden. Sie können aber aus anderen Gründen in Quarantäne gegeben oder abgewiesen werden, etwa wegen einer Spam-Bewertung oder aufgrund anderer Sicherheitsprüfungen als DMARC. Die Nutzung der Richtlinie **p=none** wird bisweilen als Überwachungs- oder Beobachtungsmodus bezeichnet, da die Richtlinie mit dem Tag **rua=** gemeinsam verwendet werden kann, um zusammengefasste Berichte über die Nachrichten zu erhalten, gleichzeitig aber Abwehrmaßnahmen nach dem Fehlschlagen von DMARC-Prüfungen zu verhindern. Solange Sie Ihre DMARC-Implementation noch nicht ausführlich und gründlich getestet haben und sicher sind, dass Sie Abwehrmaßnahmen verlangen sollen (wie etwa durch Nutzung der restriktiveren Richtlinie **p=quarantine**), sollten Sie diese Richtlinie nutzen. **p=quarantine** (Quarantäne) bedeutet, dass der Server des Nachrichtenempfängers Nachrichten als verdächtig behandeln soll, falls diese laut Absenderkopfzeile **From:** aus Ihrer Domäne stammen, aber die DMARC-Prüfung nicht bestehen. Je nach der Konfiguration des Servers des Nachrichtenempfängers können solche Nachrichten zusätzlichen Prüfmaßnahmen unterworfen werden, auch können Sie in die Spam-Ordner der Empfänger einsortiert, an einen anderen Server geleitet oder weiteren Maßnahmen unterworfen werden. **p=reject** (abweisen) bedeutet, dass der Server des Nachrichtenempfängers alle Nachrichten abweisen soll, die die DMARC-Prüfung nicht bestehen. Manche Server sind unter Umständen so konfiguriert, dass sie solche Nachrichten entgegen der Richtlinie annehmen, sie dann aber in Quarantäne geben oder zusätzlichen Prüfmaßnahmen unterwerfen. Diese Richtlinie ist die restriktivste Richtlinie; Sie sollten sie nur dann einsetzen, wenn sie endgültig sicher sind, dass Ihre E-Mail-Richtlinien und ihre Infrastruktur sowie die E-Mail-Dienste, die Sie nutzen wollen, und die Benutzerkonten richtig eingerichtet sind und funktionieren. Wollen Sie Ihren Benutzern beispielsweise gestatten, Mitglieder in Mailinglisten von Drittanbietern zu werden, Weiterleitungsdienste zu nutzen, Funktionen zum "Teilen" oder Weiterleiten von Website-Inhalten oder vergleichbare Leistungsmerkmale zu nutzen, dann führt die Nutzung der Richtlinie **p=reject** mit hoher Wahrscheinlichkeit dazu, dass auch legitime

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

		Nachrichten abgewiesen werden. Es kann auch dazu führen, dass Benutzer automatisch aus Mailinglisten entfernt oder gar nicht erst in sie aufgenommen werden. Ein Beispiel hierzu: `_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:dmarc-berichte@example.net"`

Optionale Tags

Die nachfolgend aufgeführten Tags sind wahlfrei. Enthält ein Ressourceneintrag diese Tags nicht, dann werden die jeweiligen Vorgaben angenommen und verwendet

Tag	Parameter	Erläuterung
sp=	**none** **quarantine** **reject** — **Vorgabe:** Falls **sp=** nicht verwendet wird, wirkt der Tag **p=** auf die Domäne und die Subdomänen.	Dieser Tag bestimmt die Richtlinien, die für Subdomänen der Domäne wirken sollen, auf die sich der DMARC-Ressourceneintrag bezieht. Wird dieser Tag beispielsweise in einem Eintrag verwendet, der sich auf example.com bezieht, dann wirkt die Richtlinie aus dem Tag **p=** auf E-Mail-Nachrichten aus der Domäne example.com, und die Richtlinie aus dem Tag **sp=** wirkt auf E-Mail-Nachrichten aus Subdomänen von example.com, etwa mail.example.com. Wird dieser Tag nicht verwendet, so wirkt der Tag **p=** auf die Domäne und alle ihre Subdomänen. Ein Beispiel hierzu: `_dmarc IN TXT "v=DMARC1;p=quarantine;sp=reject"`

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

rua=	Kommagetrennte Liste der E-Mail-Adressen, an die zusammengefasste DMARC-Berichte gesendet werden sollen. Die Adressen müssen als URIs im Format **mailto:benutzer@example.com** angegeben werden.
	—
	Vorgabe: keine
	Falls dieser Tag nicht verwendet wird, werden keine zusammengefassten Berichte gesendet.
		Dieser Tag zeigt an, dass Sie zusammengefasste DMARC-Berichte von den Servern der Nachrichtenempfänger erhalten wollen, bei denen Nachrichten mit Adressen aus Ihrer Domäne in der Absenderkopfzeile **From:** eingehen. Geben Sie mindestens eine E-Mail-Adresse als URI im Format **mailto:benutzer@example.com** an, und trennen Sie mehrere URIs durch Kommata.
		Ein Beispiel hierzu:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:benutzer01@example.com,mailto:benutzer02@example.com"`
		Die E-Mail-Adressen gehören üblicherweise zu der Domäne, auf die sich der DMARC-Ressourceneintrag bezieht. Falls Sie die Berichte an eine E-Mail-Adresse in einer anderen Domäne senden wollen, dann muss die DNS-Zonendatei dieser anderen Domäne einen besonderen DMARC-Eintrag enthalten, der anzeigt, dass die Domäne die fremden DMARC-Berichte akzeptiert.
		Ein Beispielseintrag für die Domäne example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;rua=mailto:nicht-lokaler-benutzer@example.net"`
		Hierzu der erforderliche Eintrag für die Domäne example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

ruf=	Kommagetrennte Liste der E-Mail-Adressen, an die DMARC-Fehlerberichte gesendet werden sollen. Die Adressen müssen als URIs im Format **mailto:benutzer@example.com** angegeben werden.
	—
	Vorgabe: keine
	Falls dieser Tag nicht verwendet wird, werden keine DMARC-Fehlerberichte gesendet.
		Dieser Tag zeigt an, dass Sie DMARC-Fehlerberichte von den Servern der Nachrichtenempfänger erhalten wollen, bei denen Nachrichten mit Adressen aus Ihrer Domäne in der Absenderkopfzeile **From:** eingehen. Damit die Fehlerberichte versandt werden, müssen die Bedingungen aus dem Tag **fo=** erfüllt sein. Wird der Tag **fo=** nicht verwendet, so werden per Voreinstellung die DMARC-Fehlerberichte dann versendet, wenn bei einer Nachricht alle DMARC-Prüfungen (also SPF und DKIM) fehlschlagen. Geben Sie mindestens eine E-Mail-Adresse als URI im Format **mailto:benutzer@example.com** an, und trennen Sie mehrere URIs durch Kommata.
		Ein Beispiel hierzu:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:dmarc-failures@example.com"`
		Die E-Mail-Adressen gehören üblicherweise zu der Domäne, auf die sich der DMARC-Ressourceneintrag bezieht. Falls Sie die Berichte an eine E-Mail-Adresse in einer anderen Domäne senden wollen, dann muss die DNS-Zonendatei dieser anderen Domäne einen besonderen DMARC-Eintrag enthalten, der anzeigt, dass die Domäne die fremden DMARC-Berichte akzeptiert.
		Ein Beispielseintrag für die Domäne example.com:
		`_dmarc IN TXT "v=DMARC1;p=quarantine;ruf=mailto:non-local-user@example.net"`
		Hierzu der erforderliche Eintrag für die Domäne example.net:
		`example.com._report._dmarc TXT "v=DMARC1"`

Ausführliche Informationen über die Spezifikation für DMARC erhalten Sie auf der Website www.dmarc.org.

4.3.5.1 DMARC-Prüfung

Während der DMARC-Prüfung fragt SecurityGateway die DMARC-Richtlinien durch eine DNS-Abfrage ab; diese Abfrage bezieht sich auf die Domäne in der Absenderkopfzeile `From:` (Von:) jeder eingehenden Nachricht. Die Abfrage prüft zunächst, ob die Domäne DMARC nutzt und ruft bejahendenfalls den DMS-Eintrag für DMARC[203] ab. Diese DNS-Eintrag enthält die DMARC-Richtlinie und verwandte Informationen. DMARC nutzt außerdem das SPF[194] und DKIM[197], um jede eingehende Nachricht zu prüfen, und die Prüfung durch SPF[194] oder DKIM[197] muss erfolgreich verlaufen, damit auch die DMARC-Prüfung erfolgreich sein kann. Besteht eine Nachricht diese Prüfungen, so wird sie durch den üblichen Filter- und Zustellvorgang in SecurityGateway normal weiterbearbeitet. Besteht eine Nachricht die Prüfung nicht, dann richtet sich ihre weitere Behandlung nach den DMARC-Richtlinien der angeblichen Absenderdomäne und danach, wie SecurityGateway für die Behandlung solcher Nachrichten konfiguriert ist.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Besteht eine Nachricht die DMARC-Prüfung nicht, und ist für die angebliche Absenderdomäne die DMARC-Richtlinie "p=none" veröffentlicht, so ergreift SecurityGateway keine Abwehrmaßnahmen, und die Nachricht wird normal weiterverarbeitet. Ist für die angebliche Absenderdomäne jedoch eine restriktive DMARC-Richtlinie veröffentlicht, also "p=quarantine" oder "p=reject", dann kann SecurityGateway die Nachricht automatisch in den Quarantäne-Ordner 308 des Empfängers leiten, die Betreffzeile kennzeichnen oder die Nachrichten-Bewertung 185 anpassen. In Nachrichten, für deren angebliche Absenderdomänen restriktive Richtlinien veröffentlicht sind, fügt SecurityGateway je nach veröffentlichter Richtlinie die Kopfzeilen "X-SGDMARC-Fail-policy: quarantine" oder "X-SGDMARC-Fail-policy: reject" ein. Hiermit können Sie durch ein Sieve-Skript 284 oder durch den Inhaltsfilter weitere Maßnahmen auslösen, die diese Kopfzeilen auswerten und Nachrichten beispielsweise in einen besonderen Ordner zur genaueren Untersuchung leiten.

DMARC-Prüfung

DMARC-Prüfung und -Berichterstellung aktivieren
Ist diese Option aktiv, so fragt SecurityGateway die DMARC-Einträge aus dem DNS für die Domänen ab, die in den Absenderkopfzeilen From: der eingehenden Nachrichten als Absender genannt sind. Falls Sie die entsprechenden Optionen im Konfigurationsdialog DMARC-Berichte 212 aktivieren, sendet SecurityGateway auch zusammengefasste Berichte und Fehlerberichte. DMARC nutzt SPF 194 und DKIM 197 zur Echtheitsbestätigung von Nachrichten. Es muss daher mindestens eines dieser beiden Leistungsmerkmale aktiv sein, bevor DMARC genutzt werden kann. Die DMARC-Prüfung und die DMARC-Berichte sind per Voreinstellung aktiv. Ihre Nutzung empfiehlt sich in den meisten Einsatzbedingungen.

Falls Sie DMARC deaktivieren, kann dies Ihre Benutzer einem erhöhten Aufkommen an Spam, Phishing-Nachrichten und überhaupt Nachrichten mit gefälschten Absenderinformationen aussetzen. Es kann auch dazu führen, dass manche Listennachrichten Ihres Systems durch andere Server abgewiesen werden, und dass Benutzer aus Ihren Listen automatisch entfernt werden. Sie sollten DMARC daher nur dann deaktivieren, wenn Sie sich ganz sicher sind, dass Sie dieses Leistungsmerkmal nicht benötigen.

Falls die Prüfung das Ergebnis REJECT meldet:
Mit dieser Option bestimmen Sie, welche Aktion ausgeführt werden soll, falls eine eingehende Nachricht die DMARC-Prüfung nicht besteht und die DMARC-Richtlinie im DNS-Eintrag der angeblichen Absenderdomäne auf p=reject gesetzt ist.

...Nachricht abweisen
Diese Option bewirkt, dass die Nachricht während der SMTP-Übermittlung abgewiesen wird, falls die DMARC-Prüfung das Ergebnis REJECT meldet. Diese Option ist per Voreinstellung aktiv.

Auch wenn Sie die Nachrichten nicht aufgrund des Ergebnisses REJECT abweisen lassen, ist zu beachten, dass die Nachrichten hiervon unabhängig aus anderen Gründen abgewiesen werden können, etwa wegen der SPF- und

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

DKIM-Einstellungen oder weil die Nachrichten-Bewertung den entsprechenden Schwellwert überschreitet.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass die Nachrichten nicht abgewiesen sondern in Quarantäne[308] gegeben werden, falls die DMARC-Prüfung das Ergebnis REJECT meldet. In Verbindung mit dieser Option können Sie auch die Optionen *...Betreffzeile kennzeichnen mit [Text]* und *...[xx] Punkte der Nachrichten-Bewertung hinzurechnen* weiter unten nutzen.

...Nachricht annehmen
Diese Option bewirkt, dass SecurityGateway Nachrichten auch dann annimmt, wenn die DMARC-Prüfung das Ergebnis REJECT meldet. Sie können auch für solche Nachrichten die Betreffzeile kennzeichnen und die Nachrichten-Bewertung[185] anpassen lassen.

...Betreffzeile kennzeichnen mit [*Text*]
Ist SecurityGateway so konfiguriert, dass Nachrichten, deren DMARC-Prüfung das Ergebnis REJECT meldet, zur Zustellung angenommen oder in Quarantäne gegeben werden, so können Sie mithilfe dieser Option die Betreffzeile dieser Nachrichten kennzeichnen lassen. Der hier angegebene Text wird am Beginn der Betreffzeile eingefügt. Per Voreinstellung wird hierfür der Text "*** FRAUD ***" ("Betrug") genutzt. Die Nutzung dieser Option überlässt dem Mailserver des Empfängers oder dem Mailclient die Entscheidung, ob und wie die Nachricht aufgrund der Kennzeichnung behandelt werden soll. Diese Option ist per Voreinstellung abgeschaltet.

SecurityGateway bietet auch in anderen Leistungsmerkmalen die Möglichkeit, die Betreffzeilen verarbeiteter Nachrichten zu kennzeichnen. So verfügen auch die Konfigurationsdialoge für SPF[194] und Nachrichten-Bewertung[185] über diese Option. Sind für diese Optionen gleichlautende Texte konfiguriert, so wird die Kennzeichnung nur einmal angebracht, und zwar auch dann, wenn die Nachricht die Voraussetzungen für die Kennzeichnung durch mehrere Optionen erfüllt. Sind jedoch unterschiedliche Texte konfiguriert, so werden alle Kennzeichnungen angebracht, bei denen die Voraussetzungen erfüllt sind. Ein Beispiel hierzu: Der voreingestellte Text für diese Option lautet "*** FRAUD ***", der voreingestellte Text für die Nachrichten-Bewertung hingegen "*** SPAM ***". Da sich beide Texte unterscheiden, werden bei Nachrichten beide Kennzeichnungen angebracht, wenn sie die Voraussetzungen für beide Kennzeichnungen erfüllen. Wird aber einer der genannten Texte dem anderen angeglichen, so wird die Kennzeichnung im Beispiel nur einmal angebracht.

...[xx] Punkte der Nachrichten-Bewertung hinzurechnen
Ist SecurityGateway so konfiguriert, dass Nachrichten, deren DMARC-Prüfung das Ergebnis REJECT meldet, zur Zustellung angenommen oder in

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Quarantäne gegeben werden, so rechnet diese Option per Voreinstellung den hier angegebenen Wert der Nachrichten-Bewertung[185] hinzu. Überschreitet die Nachrichten-Bewertung dann die entsprechenden Schwellwerte, so kann die Nachricht deswegen in Quarantäne gegeben oder abgewiesen werden, auch wenn sie allein wegen der fehlgeschlagenen DMARC-Prüfung nicht in Quarantäne gegeben oder abgewiesen werden würde. Per Voreinstellung wird der Wert 5.0 der Nachrichten-Bewertung hinzugerechnet.

Falls die Prüfung das Ergebnis QUARANTINE meldet:
Mit dieser Option bestimmen Sie, welche Aktion ausgeführt werden soll, falls eine eingehende Nachricht die DMARC-Prüfung nicht besteht und die DMARC-Richtlinie im DNS-Eintrag der angeblichen Absenderdomäne auf p=quarantine gesetzt ist.

...Nachricht abweisen
Diese Option bewirkt, dass die Nachricht während der SMTP-Übermittlung abgewiesen wird, falls die DMARC-Prüfung das Ergebnis QUARANTINE meldet.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass die Nachrichten nicht abgewiesen sondern in Quarantäne[308] gegeben werden, falls die DMARC-Prüfung das Ergebnis QUARANTINE meldet. In Verbindung mit dieser Option können Sie auch die Optionen *...Betreffzeile kennzeichnen mit [Text]* und *...[xx] Punkte der Nachrichten-Bewertung hinzurechnen* weiter unten nutzen.

...Nachricht annehmen
Diese Option bewirkt, dass SecurityGateway Nachrichten auch dann annimmt, wenn die DMARC-Prüfung das Ergebnis QUARANTINE meldet. Sie können auch für solche Nachrichten die Betreffzeile kennzeichnen und die Nachrichten-Bewertung[185] anpassen lassen.

...Betreffzeile kennzeichnen mit [*Text*]
Ist SecurityGateway so konfiguriert, dass Nachrichten, deren DMARC-Prüfung das Ergebnis QUARANTINE meldet, zur Zustellung angenommen oder in Quarantäne gegeben werden, so können Sie mithilfe dieser Option die Betreffzeile dieser Nachrichten kennzeichnen lassen. Der hier angegebene Text wird am Beginn der Betreffzeile eingefügt. Per Voreinstellung wird hierfür der Text "*** FRAUD ***" ("Betrug") genutzt. Die Nutzung dieser Option überlässt dem Mailserver des Empfängers oder dem Mailclient die Entscheidung, ob und wie die Nachricht aufgrund der Kennzeichnung behandelt werden soll. Diese Option ist per Voreinstellung abgeschaltet.

SecurityGateway bietet auch in anderen Leistungsmerkmalen die Möglichkeit, die Betreffzeilen verarbeiteter Nachrichten zu kennzeichnen. So verfügen auch die Konfigurationsdialoge für SPF[194] und Nachrichten-Bewertung[185] über diese Option. Sind für diese Optionen gleichlautende Texte konfiguriert, so wird die Kennzeichnung nur einmal angebracht, und zwar auch dann, wenn die Nachricht die Voraussetzungen für die Kennzeichnung durch mehrere Optionen erfüllt. Sind jedoch unterschiedliche Texte konfiguriert, so werden alle Kennzeichnungen

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

angebracht, bei denen die Voraussetzungen erfüllt sind. Ein Beispiel hierzu: Der voreingestellte Text für diese Option lautet "*** FRAUD ***", der voreingestellte Text für die Nachrichten-Bewertung hingegen "*** SPAM ***". Da sich beide Texte unterscheiden, werden bei Nachrichten beide Kennzeichnungen angebracht, wenn sie die Voraussetzungen für beide Kennzeichnungen erfüllen. Wird aber einer der genannten Texte dem anderen angeglichen, so wird die Kennzeichnung im Beispiel nur einmal angebracht.

...[xx] Punkte der Nachrichten-Bewertung hinzurechnen
Ist SecurityGateway so konfiguriert, dass Nachrichten, deren DMARC-Prüfung das Ergebnis QUARANTINE meldet, zur Zustellung angenommen oder in Quarantäne gegeben werden, so rechnet diese Option per Voreinstellung den hier angegebenen Wert der Nachrichten-Bewertung 185 hinzu. Überschreitet die Nachrichten-Bewertung dann die entsprechenden Schwellwerte, so kann die Nachricht deswegen in Quarantäne gegeben oder abgewiesen werden, auch wenn sie allein wegen der fehlgeschlagenen DMARC-Prüfung nicht in Quarantäne gegeben oder abgewiesen werden würde. Per Voreinstellung wird der Wert 2.0 der Nachrichten-Bewertung hinzugerechnet.

Ausschlüsse

Nachrichten von IP-Adressen auf der Weißen Liste ausnehmen
Diese Option bewirkt, dass Nachrichten, die von IP-Adressen auf der Weißen Liste für IP-Adressen 281 aus gesendet werden, von der DMARC-Prüfung ausgenommen sind. Diese Option ist per Voreinstellung aktiv. Falls Sie die DMARC-Prüfung auch für IP-Adressen auf der Weißen Liste durchführen wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Nachrichten, die über echtheitsbestätigte Verbindungen gesendet werden, sind per Voreinstellung von der DMARC-Prüfung ausgenommen. Falls Sie die DMARC-Prüfung auch dann durchführen wollen, wenn die SMTP-Verbindung echtheitsbestätigt war, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Nachrichten, die über die Mailserver der Domäne 79 gesendet werden, sind per Voreinstellung von der DMARC-Prüfung ausgenommen. Falls Sie die DMARC-Prüfung auch dann durchführen wollen, wenn Nachrichten über diese Server übermittelt wurden, deaktivieren Sie diese Option.

4.3.5.2 DMARC-Berichte

Die DMARC-Einträge, die SecurityGateway aus dem DNS abfragt, können Tags enthalten, durch die der Domäneninhaber anzeigt, dass er bestimmte zusammengefasste Statistik- und Fehlerberichte über die DMARC-gestützte Behandlung solcher Nachrichten erhalten will, die angeblich aus seiner Domäne stammen. Die Optionen im Konfigurationsdialog DMARC-Berichte bestimmen, ob Ihr System die angeforderten Arten von Berichten versenden soll, und welche Metadaten die Berichte enthalten sollen. Zusammengefasste Berichte werden jeden Tag um Mitternacht (UTC-Zeit) gesendet. Fehlerberichte werden für jede Nachricht

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

dann gesendet, wenn eine fehlgeschlagene Prüfung den Fehlerbericht auslöst. Alle Berichte werden als XML-Dateien in ZIP-Archiven versandt, die als Dateianlage an die Berichtsnachrichten angehängt werden. Es stehen verschiedene Auswertungsprogramme zur Verfügung, mit deren Hilfe die Empfänger die Berichte einsehen und auswerten können. Per Voreinstellung versendet SecurityGateway nur zusammengefasste Berichte.

Die Optionen in diesem Konfigurationsdialog sind nur verfügbar, wenn die Option *DMARC-Prüfung und -Berichterstellung aktivieren* im Konfigurationsdialog DMARC-Prüfung 208 aktiv ist. Die DMARC-Spezifikation verlangt außerdem die Nutzung von STARTTLS 126 immer dann, wenn der Empfänger der Berichte dieses Leistungsmerkmal unterstützt. Sie sollten daher, soweit möglich, STARTTLS aktivieren.

DMARC-Berichte

Zusammengefasste DMARC-Berichte senden
Diese Option bewirkt, dass SecurityGateway zusammengefasste DMARC-Berichte an die Domänen sendet, die sie anfordern. Ergibt eine DNS-Abfrage nach den DMARC-Ressourceneinträgen der Domäne in der Absenderkopfzeile `From:` einer eingehenden Nachricht, dass der DMARC-Eintrag der Domäne den Tag "`rua=`" enthält (z.B. `rua=mailto:dmarc-berichte@example.com`), so zeigt dies an, dass der Inhaber der Domäne zusammengefasste DMARC-Berichte erhalten will. SecurityGateway speichert dann die DMARC-Daten für die Domäne und die eingehenden Nachrichten, die einen Absender der Domäne ausweisen. SecurityGateway speichert außerdem die E-Mail-Adressen, an die die Berichte gesandt werden sollen, das auf die Nachrichten angewendete Prüfverfahren (SPF, DKIM oder beide), das Prüfergebnis (bestanden oder nicht bestanden), den übermittelnden Server mit IP-Adresse, die angewendete DMARC-Richtlinie und weitere relevante Daten. Jeden Tag um Mitternacht (UTC-Zeit) nutzt SecurityGateway die gespeicherten Daten, um für die erfassten Domänen Berichte zu erstellen und sie an die angegebenen E-Mail-Adressen zu senden. Nach dem Versand löscht SecurityGateway die DMARC-Daten und beginnt die Speicherung erneut.

SecurityGateway unterstützt nicht den DMARC-Tag "`ri=`", der das Intervall für den Versand der zusammengefassten Berichte festlegt. SecurityGateway sendet die zusammengefassten Berichte stets um Mitternacht (UTC-Zeit) an alle Domänen, für die DMARC-Daten seit dem letzten Versand neu gespeichert wurden.

Um aus den gespeicherten DMARC-Daten die Berichte automatisch zu erstellen und zu versenden und die Daten danach zu löschen, muss SecurityGateway um Mitternacht (UTC-Zeit) ausgeführt werden. Läuft SecurityGateway zu diesem Zeitpunkt nicht, so werden keine Berichte erstellt und die DMARC-Daten nicht gelöscht; dies wird auch nicht nachgeholt, wenn SecurityGateway wieder gestartet wird. Die Speicherung der DMARC-Daten wird fortgesetzt, sobald SecurityGateway wieder läuft, die Berichte werden aber erst wieder um Mitternacht (UTC-Zeit) oder beim nächsten

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

> Anklicken des Steuerelements "*Zusammengefasste Berichte jetzt senden*" erstellt und versandt.

DMARC-Fehlerberichte senden (Berichte werden jeweils nach Auftreten von Fehlern gesendet)
Diese Option bewirkt, dass SecurityGateway DMARC-Fehlerberichte an die Domänen sendet, die sie anfordern. Ergibt eine DNS-Abfrage nach den DMARC-Ressourceneinträgen der Domäne in der Absenderkopfzeile `From:` einer eingehenden Nachricht, dass der DMARC-Eintrag der Domäne den Tag "`ruf=`" enthält (z.B. `ruf=mailto:dmarc-fehler@example.com`), so zeigt dies an, dass der Inhaber der Domäne DMARC-Fehlerberichte erhalten will. Anders als die zusammengefassten Berichte werden die Fehlerberichte in Echtzeit unmittelbar nach dem Auftreten der sie auslösenden Fehler erstellt, und sie enthalten ausführliche Einzelheiten über den Vorgang und die Fehler, die zum Fehlschlagen der Prüfung geführt haben. Die Administratoren der betroffenen Domänen können diese Berichte verwenden, um die Fehler zu analysieren, Probleme in ihren E-Mail-Systemen und deren Konfiguration zu beseitigen und andere Probleme festzustellen, etwa auf laufende Phishing-Angriffe aufmerksam zu werden.

Der Tag "`fo=`" im DMARC-Eintrag einer Domäne bestimmt, auf welche Arten von Fehlern hin ein Fehlerbericht erstellt wird. Per Voreinstellung wird ein Fehlerbericht nur erstellt, wenn sowohl die SPF- wie auch die DKIM-Prüfung fehlschlagen. Domänen können aber verschiedene Parameter im Tag "`fo=`" angeben und damit bestimmen, dass sie Berichte nur erhalten wollen, falls SPF fehlschlägt, falls DKIM fehlschlägt, oder falls eine Kombination der Prüfverfahren fehlschlägt. Aus diesem Grund können nach dem Fehlschlagen der DMARC-Prüfung für eine Nachricht auch mehrere Fehlerberichte erstellt werden. Ihre Zahl hängt von der Anzahl der Empfänger im Tag "`ruf=`", den Parameter im Tag "`fo=`" sowie der Anzahl fehlgeschlagener Versuche zur Echtheitsbestätigung ab, die während der Prüfung der Nachricht aufgetreten sind. Falls Sie die Anzahl der Empfänger begrenzen wollen, an die SecurityGateway die Berichte sendet, können Sie dazu die Option "*Höchstzahl zu berücksichtigender DMARC-Empfänger 'rua' und 'ruf'*" weiter unten nutzen.

Zur Festlegung des Formats der Fehlerberichte beachtet SecurityGateway nur den Tag `rf=afrf` (Berichte über Fehler in der Echtheitsbestätigung mithilfe des Formats für Berichte über missbräuchliche Nutzung ARF); dies entspricht auch der Vorgabe bei DMARC. Alle Berichte werden in diesem Format gesendet, und zwar auch dann, wenn der DMARC-Eintrag der betreffenden Domäne den Tag `rf=iodef` enthält.

Für die DMARC-Fehlerberichte unterstützt SecurityGateway folgende Standards vollständig: RFC 5965: Ein erweiterbares Format für E-Mail-Feedback-Berichte, RFC 6591: Berichte über Fehler in der Echtheitsbestätigung mithilfe des Formats für Berichte über missbräuchliche Nutzung ARF, RFC 6652: Berichte über Fehler bei der SPF-Verarbeitung mithilfe des Formats für Berichte über missbräuchliche Nutzung ARF, RFC 6651: Erweiterungen für Fehlerberichte bei DomainKeys Identified Mail (DKIM) und RFC 6692: Ursprungsports im Format für Berichte über missbräuchliche Nutzung ARF.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

> Verlangt der DMARC-Tag "fo=" auch Berichte über Fehler bei der SPF-Prüfung, so sendet SecurityGateway SPF-Fehlerberichte nach RFC 6522. Aus diesem Grund müssen die Erweiterungen für diese Spezifikation im SPF-Eintrag der Domäne enthalten sein. SPF-Fehlerberichte werden nicht unabhängig von der DMARC-Verarbeitung gesendet; sie werden ferner nicht gesendet, falls die Erweiterungen nach RFC 6522 fehlen.
>
> Verlangt der DMARC-Tag "fo=" auch Berichte über Fehler bei der DKIM-Prüfung, so sendet SecurityGateway DKIM-Fehlerberichte nach RFC 6651. Aus diesem Grund müssen die Erweiterungen für diese Spezifikation in der Kopfzeile für die DKIM-Signatur enthalten sein, und für die Domäne muss ein gültiger TXT-Eintrag zu den DKIM-Berichten im DNS veröffentlicht sein. Die DKIM-Fehlerberichte werden nicht unabhängig von der DMARC-Verarbeitung gesendet; sie werden ferner nicht gesendet, falls die Erweiterungen nach RFC 6651 fehlen.

Höchstzahl zu berücksichtigender DMARC-Empfänger "rua" und "ruf" (0 = keine Begrenzung)
Falls Sie die Anzahl der Empfänger begrenzen wollen, an die SecurityGateway zusammengefasste DMARC-Berichte und DMARC-Fehlerberichte sendet, geben Sie hier die zulässige Höchstzahl der Empfänger ein. Enthalten die Tags "rua=" oder "ruf=" im DMARC-Eintrag einer Domäne mehr Empfänger, als hier zugelassen sind, dann sendet SecurityGateway die Berichte an die angegebenen Empfänger in der Reihenfolge, in der sie in den Tags erscheinen, bis die Höchstzahl erreicht ist. Per Voreinstellung ist die Zahl der Empfänger nicht begrenzt.

Kopien aller Berichte per E-Mail senden an:
Falls Sie Kopien aller zusammengefassten DMARC-Berichte und DMARC-Fehlerberichte (nur bei Nutzung der Tags fo=0 und fo=1) per E-Mail an bestimmte Empfänger senden lassen wollen, tragen Sie die E-Mail-Adressen der Empfänger hier ein. Trennen Sie mehrere Adressen durch Kommata.

Metadaten für DMARC-Berichte

Die folgenden Optionen dienen dazu, Informationen und Angaben zu Ihrer Organisation, sog. Metadaten, zu erfassen, die in die DMARC-Berichte aufgenommen werden.

Standard-Domäne
Dies ist die SecurityGateway-Domäne, die für die Erstellung der DMARC-Berichte verantwortlich ist. Sie können die Domäne aus dem Rollmenü auswählen.

Kontakt-E-Mail-Adresse
Hier können Sie eine lokale E-Mail-Adresse angeben, mit der sich die Empfänger der Berichte bei Fragen zum Bericht in Verbindung setzen können. Trennen Sie mehrere Adressen durch Kommata.

Kontaktdaten
Hier können Sie zusätzliche Kontaktdaten für die Empfänger der Berichte angeben, etwa eine Website oder Rufnummer.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Antwortpfad für Berichte
Hier können Sie den SMTP-Antwortpfad (die Bounce-Adresse) für die Nachrichten angeben, mit denen SecurityGateway die DMARC-Berichte versendet. Dieser Antwortpfad ist für Zustellfehler relevant; um solche Fehler zu ignorieren, geben Sie hier`noreply@<meinedomäne.com>` an.

4.3.5.3 DMARC-Einstellungen

Der Konfigurationsdialog DMARC-Einstellungen enthält Optionen zur Aufnahme bestimmter Daten in DMARC-Berichte, zur Protokollierung von DNS-Einträgen für DMARC und zur Aktualisierung der Liste öffentlicher Domänenendungen, die SecurityGateway für DMARC nutzt.

DMARC-Einstellungen

Durch DKIM vereinheitlichte Kopfzeilen in DMARC-Fehlerberichten aufführen
Diese Option bewirkt, dass die durch DKIM vereinheitlichten Kopfzeilen 199 in die DMARC-Fehlerberichte 212 aufgenommen werden. Diese Option ist per Voreinstellung abgeschaltet.

Durch DKIM vereinheitlichten Nachrichtentext in DMARC-Fehlerberichten aufführen
Diese Option bewirkt, dass die durch DKIM vereinheitlichten Nachrichtentexte 199 in die DMARC-Fehlerberichte 212 aufgenommen werden. Diese Option ist per Voreinstellung abgeschaltet.

Die beiden vorgenannten Optionen sind für die Fehlersuche hilfreich. Die Daten, die sie in die Fehlerberichte aufnehmen, legen aber den Inhalt der E-Mail-Nachrichten offen.

Reservierte IPs in DMARC-Berichten durch "X.X.X.X" ersetzen
Per Voreinstellung ersetzt SecurityGateway ihre reservierten IP-Adressen in DMARC-Berichten durch "`X.X.X.X`". Um Ihre reservierten IP-Adressen in den DMARC-Berichten sichtbar zu machen, deaktivieren Sie diese Option. Diese Option wirkt nicht auf durch DKIM vereinheitlichte Daten.

Vollständige DMARC-Einträge im Protokoll vermerken
Per Voreinstellung protokolliert SecurityGateway die vollständigen DMARC-Ressourceneinträge, die als Antwort auf die DNS-Abfrage während der DMARC-Prüfung übermittelt wurden. Um die vollständigen Ressourceneinträge nicht zu protokollieren,

Kopfzeile "Precedence: bulk" in E-Mail-Nachrichten mit DMARC-Berichten einfügen
Per Voreinstellung fügt SecurityGateway in die E-Mail-Nachrichten mit DMARC-Berichten eine Kopfzeile ein, die diese Nachrichten als Massennachrichten kennzeichnet. Falls Sie diese Kopfzeile nicht in die Nachrichten einfügen lassen wollen, deaktivieren Sie diese Option.

Vollständige DMARC-Einträge im Protokoll vermerken
Per Voreinstellung protokolliert SecurityGateway die vollständigen DMARC-Ressourceneinträge, die als Antwort auf die DNS-Abfrage während der DMARC-Prüfung übermittelt wurden. Um die vollständigen Ressourceneinträge nicht zu protokollieren, deaktivieren Sie diese Option.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nachrichten abweisen, deren Kopfzeile "From" nicht mit DMARC kompatibel ist
Diese Option bewirkt, dass Nachrichten abgewiesen werden, falls sie die DMARC-Anforderungen an die Zusammensetzung der Absenderkopfzeile "From" nicht erfüllen. Hierbei handelt es sich um Nachrichten mit mehreren Absenderkopfzeilen "From" oder mit mehreren E-Mail-Adressen innerhalb einer Absenderkopfzeile "From". Solche Nachrichten sind derzeit von der DMARC-Verarbeitung ausgenommen. Diese Option ist per Voreinstellung abgeschaltet, da das Vorhandensein mehrerer Adressen innerhalb derselben Absenderkopfzeile "From" nicht gegen die Protokollspezifikation verstößt. Wenn Sie diese Option aktivieren, steigert dies den Schutz durch DMARC. Diese Option wird nur wirksam, wenn die DMARC-Prüfung 208 aktiv ist.

Höchstalter in Tagen für Liste öffentlicher Domänenendungen bis zur Aktualisierung
DMARC benötigt eine Liste öffentlicher Domänenendungen, um verlässlich die richtigen Domänen festzustellen, für die DNS-Abfragen nach DMARC-Ressourceneinträgen durchzuführen sind. Per Voreinstellung aktualisiert SecurityGateway die durch SecurityGateway gespeicherte Liste öffentlicher Domänenendungen, sobald sie ein Alter von 15 Tagen überschreitet. Durch Bearbeiten dieses Werts erreichen Sie, dass die Liste öffentlicher Domänenendungen häufiger oder seltener aktualisiert wird. Falls Sie diese Option deaktivieren, wird die Liste nicht mehr automatisch aktualisiert.

URL für Liste öffentlicher Domänenendungen
Hier wird der URL zu der Liste öffentlicher Domänenendungen festgelegt, die SecurityGateway zum Abruf der Liste nutzt. Per Voreinstellung nutzt SecurityGateway die unter http://publicsuffix.org/list/effective_tld_names.dat erreichbare Datei.

Liste öffentlicher Domänenendungen jetzt aktualisieren
Um die Liste öffentlicher Domänenendungen sofort manuell zu aktualisieren, klicken Sie auf dieses Steuerelement. Auch für diese Aktualisierung wird der *URL für Liste öffentlicher Domänenendungen* verwendet.

4.3.6 Prüfung durch Rückruf

Das Anti-Spoofing-Verfahren der Prüfung durch Rückruf prüft, ob die Adresse des angeblichen Absenders einer E-Mail-Nachricht gültig ist. SecurityGateway stellt dazu eine Verbindung mit dem Mail Exchanger der Domäne her, die während des SMTP-Protokolldialogs im Befehl "MAIL From" genannt wurde, und versucht dann, festzustellen, ob die Absenderadresse eine gültige Adresse in dieser Domäne ist. Ergibt diese Prüfung, dass die Adresse des Absenders nicht besteht, so kann SecurityGateway die Nachricht so behandeln, wie wenn sie von einer gefälschten Adresse aus gesendet worden wäre. Die Nachricht kann abgewiesen, in Quarantäne gegeben oder zur Zustellung angenommen werden. Weiter können ihre Nachrichten-Bewertung 185 angepasst und ihre Betreffzeile gekennzeichnet werden. Mit der Prüfung durch Rückruf sind ganz allgemein gewisse mögliche Schwierigkeiten und Nachteile verbunden; diese Funktion ist daher per Voreinstellung abgeschaltet.

Sie erhalten allgemeine Informationen über die Prüfung durch Rückruf in dem englischsprachigen Artikel "Callback verification" auf Wikipedia.org.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Konfiguration

Absender durch Rückruf prüfen
Diese Option bewirkt, dass die Gültigkeit von Absenderadressen durch die Rückruf-Prüfung bestätigt wird. SecurityGateway nutzt dazu die Adresse, die der übermittelnde Server mit dem SMTP-Befehl "`MAIL From`" übermittelt hat. SecurityGateway stellt zur Domäne des angeblichen Absenders eine Verbindung her und prüft, ob die Adresse dort existiert. Die Prüfung durch Rückruf ist per Voreinstellung abgeschaltet.

Zuerst Befehl VRFY versuchen (falls durch Mailserver des Absenders unterstützt)
Per Voreinstellung versucht SecurityGateway zuerst, die Absenderadresse über den SMTP-Befehl "`VRFY`" zu prüfen, falls der Server der Gegenstelle mitteilt, dass dieser Befehl unterstützt wird. Server teilen mit, dass sie VRFY unterstützen, indem Sie zu Beginn des SMTP-Protokolldialogs die Meldung "`250-VRFY`" an SecurityGateway senden. Falls Sie diese Option deaktivieren, oder falls die Gegenstelle VRFY nicht unterstützt, nutzt SecurityGateway stattdessen die Befehle "`MAIL From`" und "`RCPT To`". Um die Absenderadresse auf Gültigkeit zu prüfen, sendet SecurityGateway diese Befehle so, als leiteten sie den Versand einer Nachricht an die fragliche Adresse ein. Tatsächlich wird allerdings keine Nachricht gesendet.

Nachricht von dieser Adresse aus senden:
Hier wird die Absenderadresse angegeben, die SecurityGateway für den SMTP-Befehl "`MAIL From`" nutzt, falls eine Absenderadresse NULL durch die Gegenstelle nicht zugelassen wird, oder falls die Option "*Zuerst NULL als Absenderadresse versuchen*" unten abgeschaltet ist. Die Voreinstellung für diese Option lautet "`postmaster`". Die Domäne, die hieran angefügt wird, ist die Domäne des Empfängers (z.B. `postmaster@RecipientsDomain.com`). Falls Sie hier eine vollständige E-Mail-Adresse angeben, wird stattdessen nur diese E-Mail-Adresse genutzt. Der Eintrag "xyz@example.com" in in dieser Option führt beispielsweise dazu, dass die Domäne des Empfängers nicht verwendet wird.

An den E-Mail-Server des Absenders wird tatsächlich keine Nachricht gesendet. SecurityGateway stellt eine Verbindung mit dem Server her und sendet dann die Befehle `MAIL From` und `RCPT To` so, als leiteten sie den Versand einer Nachricht ein. Danach trennt SecurityGateway jedoch die Verbindung, ohne eine Nachricht zu senden. SecurityGateway kann dadurch feststellen, ob die Gegenstelle eine Nachricht für die fragliche Absenderadresse zur Zustellung annehmen würde und ob die Gegenstelle folglich die Adresse als gültig betrachtet.

Zuerst NULL als Absenderadresse versuchen
Bei Nutzung der Befehle "`MAIL From`" und "`RCPT To`" zur Prüfung einer Absenderadresse versucht SecurityGateway zuerst, eine leere Absenderadresse (also "`MAIL From <>`") zu senden. Ist diese Option abgeschaltet, oder lässt der Server der Gegenstelle leere Absenderadressen nicht zu, so nutzt SecurityGateway den Eintrag aus der Option "*Nachricht von dieser Adresse aus senden:*" weiter oben.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Falls die Rückruf-Prüfung für einen Absender fehlschlägt, dann:
Falls die Prüfung durch Rückruf ergibt, dass die Adresse des Absenders ungültig ist, kann die Nachricht abgewiesen, in Quarantäne gegeben oder angenommen werden. Im letzten Fall kann sie gekennzeichnet, und ihre Nachrichten-Bewertung[185] kann angepasst werden. Im folgenden können Sie die Option wählen, die Sie für Nachrichten einsetzen wollen, bei denen die Prüfung durch Rückruf fehlgeschlagen ist.

...Nachricht abweisen
Diese Option bewirkt, dass Nachrichten, bei denen die Prüfung durch Rückruf fehlschlägt, während der SMTP-Übermittlung abgewiesen werden.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass Nachrichten, bei denen die Prüfung durch Rückruf fehlschlägt, in Quarantäne gegeben werden. Diese Option ist per Voreinstellung aktiv.

...Nachricht annehmen
Diese Option bewirkt, dass Nachrichten, bei denen die Prüfung durch Rückruf fehlgeschlagen ist, trotzdem angenommen werden. Sie können die Betreffzeile solcher Nachrichten kennzeichnen lassen und ihre Nachrichten-Bewertung ändern.

...Betreff kennzeichnen mit [*Text*]
Falls Sie SecurityGateway so konfiguriert haben, dass eine Nachricht auch nach einer fehlgeschlagenen Prüfung durch Rückruf angenommen wird, können Sie mithilfe dieser Option einen Kennzeichnungstext festlegen, der an den Anfang der Betreffzeile gesetzt wird. Per Voreinstellung wird, sobald diese Option aktiv ist, der Text "*** CBV ***" an den Anfang der Betreffzeile solcher Nachrichten gesetzt; Sie können den Text aber ändern. Bei Nutzung dieser Option kann es dem Mailserver oder Client des Empfängers überlassen bleiben, ob er die Nachricht anhand der Kennzeichnung filtert. Die Option ist per Voreinstellung abgeschaltet.

SecurityGateway kann auch im Rahmen anderer Verarbeitungsfunktionen wahlweise die Betreffzeile von Nachrichten kennzeichnen. Die Funktionen Nachrichten-Bewertung[185] und Schwarze Listen für URI (URIBL)[172] lassen sich beispielsweise entsprechend konfigurieren. Stimmen die Kennzeichnungstexte in diesen Funktionen überein, so wird die Kennzeichnung dem Betreff nur einmal hinzugefügt, auch wenn die Bedingungen mehrerer Funktionen für eine Kennzeichnung bei der Nachricht erfüllt sind. Werden jedoch unterschiedliche Kennzeichnungstexte konfiguriert, so werden diese Kennzeichnungen gesondert eingefügt. Geben Sie beispielsweise für alle Funktionen den Kennzeichnungstext "*SPAM*" an, so wird dieser Text nur insgesamt einmal in die Betreffzeile eingefügt, auch wenn die Nachrichten den Bedingungen mehrere Funktionen für eine Kennzeichnung entspricht. Ändern Sie nun den Text für die Funktion URIBL in "*URI blacklisted*", und erfüllt die Nachricht die Bedingungen für eine Kennzeichnung nach beiden Funktionen, so werden ihrer Betreffzeile sowohl "*SPAM*" als auch "*URI blacklisted*" vorangestellt.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

... [xx] Punkte zur Nachrichten-Bewertung hinzurechnen
Nimmt SecurityGateway eine Nachricht nach fehlgeschlagener Prüfung durch Rückruf zur Zustellung an, so rechnet SecurityGateway per Voreinstellung der Nachrichten-Bewertung dieser Nachricht den hier angegebene Wert hinzu. Die Voreinstellung für diese Option beträgt `1.0`. Sie können diesen Wert ändern, und Sie können die Option abschalten, falls sich eine fehlgeschlagene Prüfung durch Rückruf nicht auf die Bewertung auswirken soll.

Auch wenn SecurityGateway so konfiguriert ist, dass Nachrichten nicht abgewiesen oder in Quarantäne gegeben sondern zur Zustellung angenommen werden, kann die Nachricht später noch abgewiesen oder in Quarantäne gegeben werden, falls ihre Nachrichten-Bewertung entsprechend hoch ist. Die Höhe der Nachrichten-Bewertung hängt auch von der Konfiguration und den Ergebnissen der anderen Sicherheitsfunktionen[154] und den Optionen auf der Seite Nachrichten-Bewertung[185] ab.

Ausschlüsse

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Diese Option bewirkt, dass Nachrichten von Absendern auf der Weißen Liste[275] von der Prüfung durch Rückruf ausgenommen sind. Diese Option ist per Voreinstellung aktiv. Falls Sie die Prüfung durch Rückruf auch auf Absender auf der Weißen Liste anwenden wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Nachrichten, die über echtheitsbestätigte Verbindungen gesendet werden, sind per Voreinstellung von der Prüfung durch Rückruf ausgenommen. Falls Sie die Prüfung Rückruf auch dann durchführen wollen, wenn die SMTP-Verbindung echtheitsbestätigt war, deaktivieren Sie diese Option.

Nachrichten von lokalen Absendern sind immer ausgenommen.
Nachrichten, die durch einen lokalen Absender übermittelt werden, sind von der Prüfung durch Rückruf immer ausgenommen

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen für die Prüfung durch Rückruf für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.3.7 Auswertung der Absenderkopfzeile From

Dieses Leistungsmerkmal ändert die Absenderkopfzeile "From:" eingehender Nachrichten aus Sicherheitsgründen so, dass im Namensfeld der Absenderkopfzeile, das üblicherweise nur den Namen enthält, sowohl der Name als auch die E-Mail-Adresse erscheinen. Das Leistungsmerkmal will verhindern, dass Benutzer über die Absender eingehender Nachrichten getäuscht werden und meinen, dass eine Nachricht von einer bestimmten Person stammt, wohingegen sie tatsächlich

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

beispielsweise von einem Angreifer gesandt wurde. Eine solche Täuschung wird durch den Umstand begünstigt, dass viele E-Mail-Clients nur den Namen des Absenders und nicht auch seine E-Mail-Adresse anzeigen. Der Empfänger sieht die eigentliche E-Mail-Adresse üblicherweise erst, wenn er die Nachricht geöffnet oder einen sonstigen Vorgang durchgeführt hat, etwa, das Kontextmenü zu öffnen, oder den Mauszeiger auf dem Eintrag stehen zu lassen. Aus diesem Grund erstellen Angreifer E-Mail-Nachrichten oft so, dass in dem sichtbaren Feld der Absenderkopfzeile "From:" ein legitim erscheinender Name einer Person oder eines Unternehmens erscheint, wohingegen die E-Mail-Adresse, die Hinweise auf eine missbräuchliche Verwendung gibt, nicht angezeigt wird. So kann beispielsweise die Absenderkopfzeile "From:" einer Nachricht "Ehrenwerte Bank und Treuhand" <langfinger.klepto@example.com> lauten, woraufhin der E-Mail-Client nur den Teil "Ehrenwerte Bank und Treuhand" als Absender anzeigt. Dieses Leistungsmerkmal ändert daher den sichtbaren Teil der Absenderkopfzeile, um eine solche Täuschung offenzulegen und beide Datenelemente anzuzeigen. In dem genannten Beispiel erscheint dann der Absender beim Empfänger als ""Ehrenwerte Bank und Treuhand (langfinger.klepto@example.com)" <langfinger.klepto@example.com> und zeigt damit dem Empfänger an, dass die Nachricht missbräuchlich versandt wurde.

Auswertung der Absenderkopfzeile From

E-Mail-Adresse dem Anzeigenamen hinzufügen
Diese Option bewirkt, dass der Teil der Absenderkopfzeile "From:", der dem Empfänger angezeigt wird, in eingehenden Nachrichten geändert wird. Er enthält nach der Änderung sowohl den Namen wie auch die E-Mail-Adresse des Absenders. Durch diesen Vorgang ändert sich der Inhalt der Kopfzeile nach folgendem Schema: "Name des Absenders" <postfach@example.com> wird zu "Name des Absenders (postfach@example.com)" <postfach@example.com>. Diese Änderung wird nur in Nachrichten an lokale Benutzer durchgeführt, und sie ist per Voreinstellung abgeschaltet. Diese Option sollte umsichtig genutzt werden, da manche Benutzer eine solche Änderung des Absenders unter Umständen ablehnen, auch wenn sie ihnen bei der Erkennung missbräuchlicher Nachrichten helfen kann.

E-Mail-Adresse dem Namen voranstellen
Ist die Option *E-Mail-Adresse dem Anzeigenamen hinzufügen* weiter oben aktiv, so können Sie mithilfe dieser Option die Reihenfolge von Namen und E-Mail-Adressen in den geänderten Absenderkopfzeilen vertauschen. Die E-Mail-Adresse erscheint dann an erster Stelle. In dem oben angeführten Beispiel "Name des Absenders" <postfach@example.com> ergibt sich dann "postfach@example.com (Name des Absenders)" <postfach@example.com>.

In Anzeigenamen enthaltene falsche E-Mail-Adressen durch tatsächliche E-Mail-Adressen ersetzen
Eine weitere Taktik beim Spam-Versand ist es, in den Anzeigenamen (dies ist ein Teil der Absenderkopfzeile "From:") legitim erscheinende Namen und E-Mail-Adressen einzusetzen, obwohl die E-Mail-Adresse des tatsächlichen Absenders anders lautet. Mithilfe dieser Option können Sie in solchen E-Mail-Nachrichten die im Anzeigenamen sichtbare E-Mail-Adresse durch die tatsächliche E-Mail-Adresse des Absenders ersetzen lassen. Ein Beispiel hierzu: "Franks Firma (frank@company.test)" <spoof@example.com> würde geändert werden in "Franks Firma (spoof@example.com)" <spoof@example.com>.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausschlüsse

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Per Voreinstellung sind Nachrichten, die über echtheitsbestätigte Verbindungen übermittelt werden, von den Leistungsmerkmalen zur Auswertung der Absenderkopfzeile From ausgenommen. Falls Sie diese Leistungsmerkmale auch auf Nachrichten aus echtheitsbestätigten Verbindungen anwenden wollen, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Per Voreinstellung sind Nachrichten, die durch einen Mailserver der Domäne 79 übermittelt werden, von den Leistungsmerkmalen zur Auswertung der Absenderkopfzeile From ausgenommen. Falls Sie diese Leistungsmerkmale auch auf Nachrichten anwenden wollen, die durch Mailserver der Domäne übermittelt werden, deaktivieren Sie diese Option.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Optionen dieser Domäne für die Auswertung der Absenderkopfzeile From anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.4 Anti-Abuse

Der Abschnitt Anti-Abuse im Menü Sicherheit 154 enthält Werkzeuge, die Ihnen dabei helfen, den Missbrauch Ihres E-Mail-Systems durch Dritte zu unterbinden, insbesondere durch Relaisversand von Spam-Nachrichten, die In-Anspruch-Nahme erheblicher Anteile der Bandbreite, das Herstellen zu vieler Verbindungen mit dem Server und weiteres. Der Abschnitt Anti-Abuse ist in acht Unterabschnitte untergliedert:

Relaiskontrolle 224 - Geht eine Nachricht ein, die weder von einer lokalen Domäne stammt noch an eine lokale Domäne gerichtet ist, so müsste SecurityGateway die Nachricht für einen Dritten zustellen. Man spricht dabei von Relaisbetrieb des Servers. Diese Einstellungen bestimmen insbesondere, welche Gegenstellen diesen Relaisbetrieb nutzen dürfen. Hier wird auch festgelegt, ob die Adresse, die mit den SMTP-Befehlen `MAIL` und `RCPT` übergeben wird, bestehen muss, falls sie eine lokale Domäne enthält.

SMTP-Echtheitsbestätigung 225 - Diese Seite kontrolliert die Optionen für SMTP-AUTH, die SMTP-Echtheitsbestätigung, die den SMTP-Verbindungsaufbau um einen Schritt zur Echtheitsbestätigung erweitern. Benutzer können sich hierdurch am Server anmelden, bevor sie Nachrichten versenden; so wird sichergestellt, dass die Identität der Benutzer bekannt und gültig ist. Eine erfolgreiche SMTP-Echtheitsbestätigung kann wahlweise dazu benutzt werden, zahlreiche andere Prüfschritte zu überspringen, mit deren Hilfe sonst Spam-Versender und unberechtigte Nutzer entdeckt werden, die unter falscher Identität Nachrichten im Relaisbetrieb durch Ihren Server leiten wollen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

IP-Abschirmung[227] - Die IP-Abschirmung besteht aus einer Liste von Domänennamen und zugehörigen IP-Adressen, die während der Auswertung des SMTP-Befehls `MAIL FROM` geprüft werden. Eine SMTP-Verbindung, die von einer der hier erfassten Domänen stammen soll, wird nur zugelassen, falls sie IP-Adresse des übermittelnden Servers mit einer zugelassenen IP-Adresse übereinstimmt, die für diese Domäne erfasst ist.

Dynamischer Filter[229] - Mithilfe dieser Funktion kann SecurityGateway das Verhalten von übermittelnden Servern verfolgen und auswerten und so verdächtige Aktivität erkennen und entsprechend reagieren. Der Dynamische Filter kann beispielsweise eine IP-Adresse für zukünftige Verbindungen mit Ihrem Server sperren, sobald eine bestimmte Anzahl von Fehlern "Empfänger unbekannt" während einer Nachrichten-Verbindung mit dieser IP-Adresse aufgetreten ist. Sie können Absender sperren, die innerhalb einer in Minuten vorgegebenen Zeitspanne mehr als eine eine bestimmte Anzahl von Verbindungen zum Server aufbauen, und Sie können Absender sperren, bei denen die Echtheitsbestätigung öfter als zulässig fehlgeschlagen ist. Eine Sperre durch den Dynamischen Filter ist aber nicht endgültig. Die IP-Adresse gilt nur für einen Zeitraum, den Sie festlegen, und es werden alle gesperrten IP-Adressen und die Zeit, während der sie bereits gesperrt sind, aufgeführt.

Länder-Filter[230] - Der Länder-Filter ist ein auf geographische Daten gestütztes Filtersystem. Mit seiner Hilfe können Sie Verbindungsversuche abweisen, falls diese Verbindungsversuche von bestimmten geographischen Regionen ausgehen, die Sie als nicht zugelassen definiert haben. SecurityGateway stellt fest, mit welchem Land die IP-Adressen in Verbindung stehen, von denen eingehende Verbindungen ausgehen. Verbindungen, die von gesperrten Regionen ausgehen, werden abgewiesen. Per Voreinstellung weist der Länder-Filter nur solche Verbindungen ab, in denen eine Echtheitsbestätigung über AUTH versucht wird. Diese Vorgehensweise ist beispielsweise dann sinnvoll, wenn Sie in einem bestimmten Land keine Benutzer haben, gleichwohl aber von dort aus Nachrichten empfangen wollen. Es werden dann nur Verbindungen abgewiesen, in denen eine Anmeldung an einem Benutzerkonto Ihres Servers versucht wird.

Teergrube[231] - Mithilfe der Teergrube können Sie eine Verbindung gezielt verzögern, sobald der Absender einer Nachricht eine bestimmte Anzahl von RCPT-Befehlen übermittelt hat. Auf diese Weise sollen Spammer davon abgehalten werden, unerwünschte Massennachrichten ("Spam") an Ihre Domänen zu senden. Sie können die Anzahl der RCPT-Befehle vorgeben, die zulässig sind, bevor eine Verbindung in die Teergrube gezogen wird, und sie können weiter die Verzögerung in Sekunden angeben, die nach dem Empfang jedes weiteren RCPT-Befehls in derselben Verbindung eintreten soll. Hinter dieser Technik steht der Gedanke, dass Spammer das Interesse verlieren, in Zukunft weitere Spam-Nachrichten an Ihren Server zu übermitteln, falls sie für den Versand jeder einzelnen Nachricht unverhältnismäßig lange brauchen.

Bandbreitenbegrenzung[233] - Mithilfe der Bandbreitenbegrenzung können Sie die Bandbreite begrenzen, die SecurityGateway in Anspruch nehmen darf. Sie können dabei grenzen für das gesamte System und für einzelne Domänen gesondert festlegen. Die Bandbreitenbegrenzung wirkt sich auf alle eingehenden und abgehenden SMTP-Verbindungen aus. Sie können Absender auf der Weißen Liste, Verbindungen mit Echtheitsbestätigung und die Mailserver der Domäne von den Beschränkungen ausnehmen.

Erkennung des Hijackings von Benutzerkonten[234] -

Die Optionen in diesem Abschnitt dienen dazu, zu erkennen, ob ein Benutzerkonto auf Ihrem Server möglicherweise gehijackt oder sonst kompromittiert wurde, und

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

sodann den weiteren Versand von Nachrichten von diesem Benutzerkonto aus über Ihren Server automatisch zu unterbinden. Ein Beispiel für ein solches Hijacking ist, dass ein Spam-Versender sich die E-Mail-Adresse und das Kennwort eines Benutzerkontos verschafft; die Leistungsmerkmale zum Erkennen dieses Hijackings können dann den Spam-Versender daran hindern, von dem "gekaperten" Benutzerkonto aus massenhaft Spam- und Junk-Nachrichten über Ihren Server zu versenden. Sie können bestimmen, wie viele Nachrichten ein Benutzerkonto während einer in Minuten festgelegten Zeitspanne versenden darf, und Sie können wahlweise das Benutzerkonto sperren lassen, sobald diese Grenze erreicht wurde.

4.4.1 Relaiskontrolle

Geht eine Nachricht ein, die weder von einer lokalen Domäne stammt noch an eine lokale Domäne gerichtet ist, so müsste SecurityGateway die Nachricht für einen Dritten zustellen. Man spricht dabei von Relaisbetrieb des Servers. SecurityGateway lässt den Relaisbetrieb nicht per Voreinstellung allgemein zu; Sie können aber auf dieser Seite beispielsweise festlegen, ob der Relaisbetrieb für Mailserver der Domäne[79] zugelassen ist. Die Einstellungen bestimmen auch, welche Gegenstellen diesen Relaisbetrieb nutzen dürfen. Hier wird auch festgelegt, ob die Adresse, die mit den SMTP-Befehlen `MAIL` und `RCPT` übergeben wird, bestehen muss, falls sie eine lokale Domäne enthält.

Relaisbetrieb

Relaisbetrieb ist auf diesem Server gesperrt...
SecurityGateway leitet Nachrichten nur durch, wenn sie entweder von einer durch SecurityGateway verwalteten Domäne stammen oder an eine solche gerichtet sind. Spammer nutzen Server, die offenen und unkontrollierten Relaisbetrieb bieten, um ihre Spuren zu verwischen, und ein offener Relaisbetrieb kann daher dazu führen, dass Ihre Domäne durch einen oder mehrere DNSBL-Dienste[169] als Spam-Quelle erfasst wird.

...außer für Nachrichten von einem Mailserver der Domäne
Diese Option bewirkt, dass Nachrichten im Relaisbetrieb durchgeleitet werden, wenn sie von einem Mailserver der Domäne[79] versandt werden. Bei solchen Nachrichten ist es nicht erforderlich, dass sie aus einer lokalen Domäne stammen oder an eine solche gerichtet sind. Die Option ist per Voreinstellung abgeschaltet.

Nur Mailserver der Domäne dürfen lokale Nachrichten senden
Per Voreinstellung nimmt SecurityGateway Nachrichten mit Absendern aus lokalen Domänen nur entgegen, wenn der übermittelnde Server ein Mailserver der Domäne[79] ist und dieser Domäne zugeordnet wurde. Falls Sie den Versand lokaler Nachrichten nicht auf die Mailserver der Domäne beschränken wollen, deaktivieren Sie diese Option.

...außer die Nachricht ist AN ein lokales Benutzerkonto gerichtet
Diese Option bewirkt, dass lokale Nachrichten, die nicht von einem Ihrer Mailserver der Domäne[79] versandt werden, dann angenommen werden, wenn sie an ein lokales Benutzerkonto gerichtet sind. Diese Option ist per Voreinstellung aktiv.

...außer die Nachricht stammt aus echtheitsbestätigter SMTP-Verbindung
Diese Option bewirkt, dass SecurityGateway Nachrichten mit Absendern aus lokalen Domänen auch dann zur Zustellung annimmt, wenn sie zwar nicht über

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

einen Mailserver der Domäne, aber über eine SMTP-Verbindung mit Echtheitsbestätigung versandt werden. Ein Beispiel für einen entsprechenden Anwendungsfall ist es, wenn ein Benutzer seine abgehenden Nachrichten nicht über den Mailserver seiner Domäne sondern direkt über SecurityGateway sendet. Diese Option ist per Voreinstellung aktiv.

...außer die Nachricht stammt von IP-Adresse oder Host auf der Weißen Liste
Diese Option bewirkt, dass lokale Nachrichten auch durch IP-Adressen und Hosts auf einer Weißen Liste 275 versandt werden dürfen, selbst wenn sie nicht zu einem Ihrer Mailserver der Domäne 79 gehören. Diese Option ist per Voreinstellung abgeschaltet.

Prüfung der Benutzerkonten

SMTP-MAIL-Adresse muss existieren, falls sie eine lokale Domäne enthält
Per Voreinstellung prüft SecurityGateway bei Nachrichten, die angeblich aus einer lokalen Domäne stammen, ob der Parameter für den Befehl MAIL (also die Absenderadresse), der während des SMTP-Protokolldialogs übermittelt wird, zu einem gültigen Benutzerkonto gehört. Gehört die Adresse nicht zu einem gültigen Benutzerkonto, so wird die Nachricht abgewiesen.

...außer die Nachricht wurde über einen Mailserver der Domäne versandt
Diese Option bewirkt, dass Nachrichten von dem Erfordernis "*SMTP-MAIL-Adresse muss existieren...*" ausgenommen sind, falls sie durch einen Mailserver der Domäne 79 versandt werden. Diese Option ist per Voreinstellung aktiv.

...außer die Nachricht stammt aus echtheitsbestätigter SMTP-Verbindung
Diese Option bewirkt, dass Nachrichten von dem Erfordernis "*SMTP-MAIL-Adresse muss existieren...*" ausgenommen sind, falls sie über eine Verbindung mit Echtheitsbestätigung versandt werden. Diese Option ist per Voreinstellung aktiv.

...außer die Nachricht stammt von IP-Adresse oder Host auf der Weißen Liste
Diese Option bewirkt, dass Nachrichten von dem Erfordernis "*SMTP-MAIL-Adresse muss existieren...*" ausgenommen sind, falls sie durch eine IP-Adresse oder einen Host auf der Weißen Liste 275 versandt werden. Diese Option ist per Voreinstellung abgeschaltet.

SMTP-RCPT-Adresse muss existieren, falls sie eine lokale Domäne enthält
SecurityGateway prüft bei Nachrichten, die an eine lokale Domäne gerichtet sind, ob der Parameter für den Befehl RCPT (also die Empfängeradresse), der während des SMTP-Protokolldialogs übermittelt wird, zu einem gültigen Benutzerkonto gehört. Gehört die Adresse nicht zu einem gültigen Benutzerkonto, so wird die Nachricht abgewiesen.

4.4.2 SMTP-Echtheitsbestätigung

Diese Seite kontrolliert die Optionen für SMTP-AUTH, die SMTP-Echtheitsbestätigung, die den SMTP-Verbindungsaufbau um einen Schritt zur Echtheitsbestätigung erweitern. Benutzer können sich hierdurch am Server anmelden, bevor sie Nachrichten versenden; so wird sichergestellt, dass die Identität der Benutzer bekannt und gültig ist. Eine erfolgreiche SMTP-Echtheitsbestätigung kann wahlweise dazu benutzt werden, zahlreiche andere Prüfschritte zu überspringen, mit deren Hilfe sonst Spam-Versender und

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

unberechtigte Nutzer entdeckt werden, die unter falscher Identität Nachrichten im Relaisbetrieb durch Ihren Server leiten wollen.

SMTP-Echtheitsbestätigung

Echtheitsbestätigung ist immer erforderlich, wenn Nachrichten von lokalen Benutzerkonten stammen
Diese Option bewirkt, dass Nachrichten, die angeblich von einem lokalen Benutzerkonto aus versendet werden, nur über Verbindungen mit Echtheitsbestätigung zugelassen sind. Wird eine solche Nachricht in einer Verbindung ohne vorherige Echtheitsbestätigung übermittelt, so wird die Nachricht abgewiesen. Diese Option ist per Voreinstellung abgeschaltet.

...außer die Nachricht ist an ein lokales Benutzerkonto gerichtet
Falls Sie die Option *Echtheitsbestätigung ist immer erforderlich, wenn Nachrichten von lokalen Benutzerkonten stammen* weiter oben aktivieren, können Sie mithilfe dieser Option Nachrichten an lokale Empfänger von diesem Erfordernis ausnehmen. Wird dann eine Nachricht von einem lokalen Benutzerkonto aus an ein anderes lokales Benutzerkonto übermittelt, so ist hierfür keine Echtheitsbestätigung erforderlich. Diese Option ist per Voreinstellung abgeschaltet.

...außer die Nachricht stammt von einem Mailserver der Domäne
Diese Option bewirkt, dass Nachrichten von dem Erfordernis *Echtheitsbestätigung ist immer erforderlich, wenn Nachrichten von lokalen Benutzerkonten stammen* oben ausgenommen sind, falls sie durch einen Mailserver der Domäne 79 versandt werden.

... außer die Nachricht stammt von IP-Adresse oder Host auf der Weißen Liste
Diese Option bewirkt, dass das Benutzerkonto nicht der SMTP-Echtheitsbestätigung unterworfen ist, falls die Nachricht von einer IP-Adresse 281 oder einem Host 278 auf der Weißen Liste stammt.

Anmeldedaten müssen mit denen des E-Mail-Absenders übereinstimmen
Diese Option bewirkt, dass Absender immer ihre eigenen, zur Absenderadresse passenden Anmeldedaten für die Echtheitsbestätigung verwenden müssen. Ein Absender, der beispielsweise die Adresse *frank@example.com* verwendet, muss sich dann mithilfe der Anmeldedaten für das Benutzerkonto *frank@example.com* anmelden, um unter dieser Adresse Nachrichten zu versenden. Wollte er sich etwa mit den Anmeldedaten für das Benutzerkonto *frank02@example.com* anmelden, dann dürfte er keine Nachrichten mit dem Absender *frank@example.com* versenden, selbst wenn die Anmeldedaten für *frank02@example.com* gültig wären. Diese Option ist per Voreinstellung abgeschaltet.

Post von "Postmaster", "Abuse", "Webmaster" nur über Verbindung mit Echtheitsbestätigung
Trägt eine E-Mail-Nachricht die Absenderadresse *postmaster*, *abuse* oder *webmaster* einer lokalen Domäne, so ist die Echtheitsbestätigung per Voreinstellung erforderlich. Diese Sicherheitsvorkehrung ist erforderlich, da viele Spammer und unberechtigte Benutzer wissen, dass solche Benutzerkonten oder Aliasnamen auf vielen Servern bestehen, und versuchen, mithilfe dieser Konten Nachrichten durch den Server zu leiten oder sich als offizielle Benutzer auszugeben.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen zur SMTP-Echtheitsbestätigung für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.4.3 IP-Abschirmung

Die IP-Abschirmung besteht aus einer Liste von Domänennamen und zugehörigen IP-Adressen, die während der Auswertung des SMTP-Befehls `MAIL FROM` geprüft werden. Eine SMTP-Verbindung, die von einer der hier erfassten Domänen stammen soll, wird nur zugelassen, falls sie IP-Adresse des übermittelnden Servers mit einer zugelassenen IP-Adresse übereinstimmt, die für diese Domäne erfasst ist.

Konfiguration

IP-Abschirmung aktivieren
Mithilfe dieser Option können Sie die IP-Abschirmung aktivieren.

... Kopfzeile FROM durch die Datenbank der IP-Abschirmung prüfen lassen
Diese Option bewirkt, dass die IP-Abschirmung neben der Adresse aus dem SMTP-Befehl MAIL auch die Adresse aus der Absenderkopfzeile FROM der Nachrichten auswertet. Diese Option ist per Voreinstellung abgeschaltet.

Die Nutzung dieser Option kann bei bestimmten Arten zu Schwierigkeiten führen. Betroffen sein können beispielsweise Nachrichten aus bestimmten Mailinglisten. Sie sollten diese Option daher nur dann aktivieren, wenn Sie sich sicher sind, dass Sie die Option benötigen.

Derzeit definierte Domänen/IP-Paare

Hier erscheint die Liste der Domänen und der ihnen zugeordneten IP-Adressen. Die Zuordnung wird für alle Nachrichten geprüft, die angeblich aus einer dieser Domänen stammen. Die IP-Adresse des Servers, der die Nachricht übermittelt, muss für die zugehörige Domäne erfasst sein.

Nachrichten an gültige lokale Benutzer ausnehmen
Per Voreinstellung wird die Prüfung über die IP-Abschirmung für Nachrichten übersprungen, die an gültige lokale Benutzer gerichtet sind. Falls Sie solche Nachrichten nicht von der Prüfung über die IP-Abschirmung ausnehmen wollen, deaktivieren Sie dieses Kontrollkästchen.

Neu
Um der Liste einen neuen Eintrag aus Domäne und IP-Adresse hinzuzufügen, klicken Sie auf *Neu*. Es öffnet sich der Dialog Eintrag in IP-Abschirmung.

Bearbeiten
Um einen bestehenden Eintrag zu bearbeiten, klicken Sie doppelt auf den Eintrag, oder klicken Sie den Eintrag in der Liste einfach an, und klicken Sie dann auf

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Bearbeiten. In beiden Fällen öffnet sich der Dialog Eintrag in IP-Abschirmung für den gewünschten Eintrag.

Löschen
Um einen Eintrag aus der Liste zu löschen, wählen Sie den Eintrag aus, und klicken Sie dann auf *Löschen*.

Eintrag in IP-Abschirmung

Information zu Domäne und IP

Dieser Dialog wird aufgerufen, wenn ein neuer Eintrag in die IP-Abschirmung eingefügt oder ein bestehender Eintrag bearbeitet werden soll.

Speichern und Beenden
Nachdem Sie die Domäne, die IP-Adresse und etwaige Kommentare für den Eintrag eingegeben oder bearbeitet haben, klicken Sie auf *Speichern und Beenden*, um den Eintrag zu speichern und zur Übersicht über die IP-Abschirmung zurückzukehren.

Schließen
Um zur Übersicht über die IP-Abschirmung zurückzukehren, ohne die neu eingegebenen oder geänderten Daten zu speichern, klicken Sie auf *Schließen*.

Domäne
Geben Sie hier den Domänennamen ein, den Sie der IP-Abschirmung hinzufügen wollen.

IP Adresse
Geben Sie hier die Adresse ein, die mit der oben angegebenen Domäne verknüpft werden soll. Bei Nachrichten, die angeblich aus dieser Domäne stammen, muss die IP-Adresse des übermittelnden Servers mit der hier eingegebenen IP-Adresse übereinstimmen.

Kommentar
In dieses Textfeld können Sie Kommentare für den Eintrag eingeben.

Ausschlüsse

Nachrichten an gültige lokale Benutzer ausnehmen
Diese Option bewirkt, dass Nachrichten von der Verarbeitung durch die IP-Abschirmung ausgenommen sind, falls sie an gültige lokale Benutzer gerichtet sind.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Diese Option bewirkt, dass eingehende Nachrichten von der Verarbeitung durch die IP-Abschirmung ausgenommen sind, falls sie über eine echtheitsbestätigte Verbindung an den Server übermittelt werden.

Nachrichten von Mailservern der Domäne ausnehmen
Diese Option bewirkt, dass eingehende Nachrichten von der Verarbeitung durch die IP-Abschirmung ausgenommen sind, falls sie von einem Mailserver der Domäne 79 übermittelt werden. Diese Option ist per Voreinstellung aktiv. Falls Sie auch Nachrichten, die durch Mailserver der Domäne übermittelt wurden, durch die IP-Abschirmung verarbeiten lassen wollen, deaktivieren Sie diese Option.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

4.4.4 Dynamischer Filter

Mithilfe dieser Funktion kann SecurityGateway das Verhalten von übermittelnden Servern verfolgen und auswerten und so verdächtige Aktivität erkennen und entsprechend reagieren. Der Dynamische Filter kann beispielsweise eine IP-Adresse für zukünftige Verbindungen mit Ihrem Server sperren, sobald eine bestimmte Anzahl von Fehlern "Empfänger unbekannt" während einer Nachrichten-Verbindung mit dieser IP-Adresse aufgetreten ist. Sie können Absender sperren, die innerhalb einer in Minuten vorgegebenen Zeitspanne mehr als eine eine bestimmte Anzahl von Verbindungen zum Server aufbauen, und Sie können Absender sperren, bei denen die Echtheitsbestätigung öfter als zulässig fehlgeschlagen ist. Eine Sperre durch den Dynamischen Filter ist aber nicht endgültig. Die IP-Adresse gilt nur für einen Zeitraum, den Sie festlegen, und es werden alle gesperrten IP-Adressen und die Zeit, während der sie bereits gesperrt sind, aufgeführt.

Automatischer IP-Filter

Dynamischen Filter aktivieren
Mithilfe dieser Option wird der Dynamische Filter aktiviert. Per Voreinstellung sind die Funktionen des Dynamischen Filters abgeschaltet.

Absender nach dieser Anzahl fehlgeschlagener RCPT-Befehle sperren:
Ist der Dynamische Filter aktiv, so wird eine IP-Adresse vorübergehend gesperrt, sobald während einer SMTP-Verbindung die hier festgelegte Zahl an RCPT-Befehlen fehlgeschlagen ist. Diese Funktion wirkt der bei Spammern beliebten Taktik entgegen, zahlreiche RCPT-Befehle zu senden und so E-Mail-Adressen durchzuprobieren, da in solchen Versuchen üblicherweise viele ungültige Adressen enthalten sind und die hier festgelegte Grenze schnell erreicht wird. Die Voreinstellung für diesen Wert beträgt 10.

Absender sperren nach mehr als [xx] Verbindungsversuchen innerhalb von [xx] Minuten
Diese Option bestimmt, wie oft eine Gegenstelle innerhalb eines in Minuten festgelegten Zeitraums eine Verbindung mit SecurityGateway herstellen darf. Wird die Zahl der zugelassenen Verbindungen in diesem Zeitraum überschritten, so wird die Gegenstelle vorübergehend gesperrt. Diese Option ist per Voreinstellung abgeschaltet.

Absender nach dieser Anzahl fehlgeschlagener Echtheitsbestätigungen sperren:
Hier wird die Anzahl der Fehlversuche festgelegt, die ein Absender bei der Echtheitsbestätigung zur Verfügung hat. Die Verwendung eines falschen Kennworts durch einen Absender führt beispielsweise zu einem Fehlversuch. Per Voreinstellung wird die IP-Adresse eines Absenders vorübergehend gesperrt, sobald er dreimal erfolglos versucht hat, die Echtheitsbestätigung durchzuführen. Falls Sie nicht wünschen, dass solche Absender gesperrt werden, deaktivieren Sie diese Option. Die Absender können dann die Echtheitsbestätigung unbegrenzt oft versuchen.

Sperrdauer für Absender in Minuten:
Hier wird die Dauer in Minuten festgelegt, für die eine IP-Adresse gesperrt bleibt, nachdem sie gegen eine der oben konfigurierten Beschränkungen verstoßen hat. Die Voreinstellung für die Sperrdauer beträgt 10 Minuten.

SMTP-Verbindung trennen, nachdem Absender gesperrt wurde
Per Voreinstellung wird eine SMTP-Verbindung sofort getrennt, nachdem eine IP-Adresse gesperrt wurde. Dabei wird der Protokolldialog unabhängig davon

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

abgebrochen, an welcher Stelle er sich gerade befindet. Falls Sie die SMTP-Verbindung nach Sperren einer IP-Adresse nicht sofort trennen wollen, deaktivieren Sie diese Option.

Ausschlüsse

Nachrichten von IP-Adressen und Hosts auf der Weißen Liste ausnehmen
Per Voreinstellung sind alle IP-Adressen und Hosts, die in einer Weißen Liste[275] eingetragen sind, von den Beschränkungen des Dynamischen Filters ausgenommen. Falls Sie diese Beschränkungen auch auf Hosts und IP-Adressen aus den Weißen Listen anwenden wollen, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Falls eine eingehende Nachricht über eine Verbindung mit Echtheitsbestätigung übermittelt wurde, ist sie per Voreinstellung von den Beschränkungen des Dynamischen Filters ausgenommen. Falls Sie diese Beschränkungen auch auf Verbindungen mit Echtheitsbestätigung anwenden wollen, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Nachrichten, die durch einen Mailserver der Domäne[79] übermittelt werden, sind per Voreinstellung von den Beschränkungen des Dynamischen Filters ausgenommen, Falls Sie diese Beschränkungen auch auf Mailserver der Domäne anwenden wollen, deaktivieren Sie diese Option.

Liste gesperrter IP-Adressen

In diesem Abschnitt sind alle derzeit gesperrten IP-Adressen und die Zeit aufgeführt, die seit Wirksamwerden der Sperre für jede IP-Adresse verstrichen ist. Sie können einen Eintrag aus der Liste entfernen, indem Sie ihn auswählen und dann in der Symbolleiste über der Liste auf *Löschen* klicken.

4.4.5 Länder-Filter

Länder-Filter

Der Länder-Filter ist ein auf geographische Daten gestütztes Filtersystem. Mit seiner Hilfe können Sie Verbindungsversuche abweisen, falls diese Verbindungsversuche von bestimmten geographischen Regionen ausgehen, die Sie als nicht zugelassen definiert haben. SecurityGateway stellt fest, mit welchem Land die IP-Adressen in Verbindung stehen, von denen eingehende Verbindungen ausgehen. Verbindungen, die von gesperrten Regionen ausgehen, werden abgewiesen. Per Voreinstellung weist der Länder-Filter nur solche Verbindungen ab, in denen eine Echtheitsbestätigung über AUTH versucht wird. Diese Vorgehensweise ist beispielsweise dann sinnvoll, wenn Sie in einem bestimmten Land keine Benutzer haben, gleichwohl aber von dort aus Nachrichten empfangen wollen. Es werden dann nur Verbindungen abgewiesen, in denen eine Anmeldung an einem Benutzerkonto Ihres Servers versucht wird.

Länder-Filter aktivieren
Um den Länder-Filter zu nutzen, aktivieren Sie diese Option, und aktivieren Sie danach die Kontrollkästchen für alle Regionen und Länder, die Sie sperren möchten. Klicken Sie zum Abschluss auf **Speichern**.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

... nur Versuche zur Echtheitsbestätigung unterbinden (Nachrichten, die keine Echtheitsbestätigung benötigen, sind weiterhin zugelassen)
Per Voreinstellung weist der Länder-Filter eingehende Verbindungen nur dann ab, wenn in ihnen eine Echtheitsbestätigung versucht wird. Nachrichten, für deren Übermittlung keine Echtheitsbestätigung erforderlich ist, sind dann weiterhin zugelassen. Um alle Verbindungsversuche abzuweisen, die von den festgelegten Ländern ausgehen, deaktivieren Sie diese Option.

Kopfzeile "X-SGOrigin-Country" in Nachrichten einfügen
Per Voreinstellung fügt SecurityGateway den Nachrichten die Kopfzeile "X-SGOrigin-Country" hinzu. Diese Kopfzeile kann für den Inhaltsfilter und für andere Zwecke verwendet werden. Die Kopfzeile enthält keine vollständigen Namen für Länder und Kontinente sondern das aus zwei Buchstaben bestehende Länderkürzel nach ISO 3166 sowie die Kurzbezeichnung des Kontinents. Falls Sie diese Kopfzeile nicht in die Nachrichten einfügen lassen wollen, deaktivieren Sie diese Option.

Alles auswählen/abwählen
Mithilfe dieser Schaltflächen können Sie alle Länder und Regionen in der Liste auswählen und abwählen.

Ausschlüsse

Verbindungen von IP-Adressen auf der Weißen Liste ausnehmen
Per Voreinstellung sind alle IP-Adressen auf der Weißen Liste[281] von den Beschränkungen durch den Länder-Filter ausgenommen. Um die Beschränkungen durch den Länder-Filter auch auf IP-Adressen auf der Weißen Liste anzuwenden, deaktivieren Sie diese Option.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen zum SPF für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.4.6 Teergrube

Mithilfe der Teergrube können Sie eine Verbindung gezielt verzögern, sobald der Absender einer Nachricht eine bestimmte Anzahl von RCPT-Befehlen übermittelt hat. Auf diese Weise sollen Spammer davon abgehalten werden, unerwünschte Massennachrichten ("Spam") an Ihre Domänen zu senden. Sie können die Anzahl der RCPT-Befehle vorgeben, die zulässig sind, bevor eine Verbindung in die Teergrube gezogen wird, und sie können weiter die Verzögerung in Sekunden angeben, die nach dem Empfang jedes weiteren RCPT-Befehls in derselben Verbindung eintreten soll. Hinter dieser Technik steht der Gedanke, dass Spammer das Interesse verlieren, in Zukunft weitere Spam-Nachrichten an Ihren Server zu übermitteln, falls sie für den Versand jeder einzelnen Nachricht unverhältnismäßig lange brauchen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Einstellungen zur Teergrube

Teergrube aktivieren
Um die Teergrube zu aktivieren, aktivieren Sie dieses Kontrollkästchen. Die Teergrube ist per Voreinstellung abgeschaltet.

Verzögerung für EHLO/HELO bei SMTP (in Sekunden):
Mithilfe dieser Option können Sie die Antwort von SecurityGateway auf die SMTP-Befehle `EHLO/HELO` SMTP gezielt verzögern. Bereits eine geringfügige Verzögerung von zehn Sekunden kann die Zahl der empfangenen Spam-Nachrichten und damit die Nachverarbeitungszeit erheblich verringern. Spammer sind meist auf die möglichst schnelle Zustellung ihrer Nachrichten angewiesen und warten daher nicht sehr lange auf eine Antwort auf die Befehle `EHLO/HELO`. Schon eine kurze Verzögerung bewirkt manchmal dass die Programme zum Spamversand nicht mehr auf eine Antwort warten sondern aufgeben und mit dem nächsten Empfänger fortfahren. Verbindungen mit dem MSA-Port (dieser wird auf der Seite E-Mail-Protokoll 92 festgelegt) sind von dieser Verzögerung immer ausgenommen. Die Voreinstellung für diese Option beträgt "0", sodass die Antwort auf die Befehle `EHLO/HELO` nicht verzögert wird.

Für echtheitsbestätigte IPs tritt nur eine HELO/EHLO-Verzögerung pro Tag ein
Verzögern Sie die Antworten auf die Befehle EHLO/HELO, so tritt für eine IP-Adresse, die eine Verbindung mit Echtheitsbestätigung herstellt, pro Tag nur einmal eine Verzögerung ein. Diese Verzögerung tritt unmittelbar, bevor die Verbindung zum ersten Mal echtheitsbestätigt wird, ein. Diese Option ist per Voreinstellung abgeschaltet.

SMTP-RCPT-Schwellwert für Teergrube:
Mithilfe dieser Option legen Sie fest, wie viele SMTP-Befehle RCPT eine Gegenstelle während einer Verbindung zur Übermittlung von Nachrichten senden darf, bevor SecurityGateway die Verbindung in die Teergrube zieht und gezielt verzögert. Wird hier beispielsweise der Wert 10 eingetragen, und versucht die Gegenstelle, eine Nachricht an 20 Empfänger zu senden (sie übermittelt dazu 20 RCPT-Befehle), so lässt SecurityGateway die ersten 10 Empfänger normal zu und verzögert jeden nachfolgenden RCPT-Befehl um die unter *SMTP-RCPT-Verzögerung für Teergrube* festgelegte Zeitdauer. Die Voreinstellung für diesen Wert beträgt 5.

SMTP-RCPT-Verzögerung für Teergrube (in Sekunden):
Sobald eine Gegenstelle den *SMTP-RCPT-Schwellwert für Teergrube* erreicht hat, verursacht SecurityGateway nach jedem weiteren RCPT-Befehl, der in der selben Verbindung durch die Gegenstelle gesendet wird, die hier in Sekunden festgelegte Verzögerung. Per Voreinstellung wird jeder nachfolgende RCPT-Befehl um 10 Sekunden verzögert.

Anpassungsfaktor:
Dieser Wert ist der Muliplikator, um den die Verzögerung mit der Zeit immer weiter erhöht wird. Ist der Schwellwert erreicht, und wird die Verbindung um die oben angegebene Verzögerungsdauer gezielt verlangsamt, so wird jede Verzögerungsdauer mit diesem Faktor multipliziert; hieraus ergibt sich dann die Dauer der folgenden Verzögerung. Ist die Verzögerungsdauer beispielsweise auf 10 eingestellt, und beträgt der Anpassungsfaktor 1,5, so dauert die erste Verzögerung 10 Sekunden, die zweite 15 Sekunden, die dritte 22,5 Sekunden, dann 33,75 Sekunden, und so weiter (im Beispiel 10 x 1,5 = 15, 15 x 1,5 =

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

22,5 usw.). Die Voreinstellung für den Anpassungsfaktor beträgt 1, sodass die Verzögerung nicht verlängert wird.

Ausschlüsse

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Per Voreinstellung sind alle Nachrichten von Absendern, die in einer Weißen Liste 275 erfasst sind, von den Beschränkungen der Teergrube ausgenommen. Um die Beschränkungen der Teergrube auch auf Absender anzuwenden, die in einer Weißen Liste erfasst sind, deaktivieren Sie diese Option.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Per Voreinstellung sind alle Nachrichten aus Verbindungen mit Echtheitsbestätigung von den Beschränkungen der Teergrube ausgenommen. Um die Beschränkungen der Teergrube auch auf solche Nachrichten anzuwenden, deaktivieren Sie diese Option.

Nachrichten von Mailservern der Domäne ausnehmen
Per Voreinstellung sind alle Nachrichten, die über einen Mailserver der Domäne 79 gesendet werden, von den Beschränkungen der Teergrube ausgenommen. Um die Beschränkungen der Teergrube auch auf Mailserver der Domäne anzuwenden, deaktivieren Sie diese Option.

4.4.7 Bandbreitenbegrenzung

Mithilfe der Bandbreitenbegrenzung können Sie die Bandbreite begrenzen, die SecurityGateway in Anspruch nehmen darf. Sie können dabei grenzen für das gesamte System und für einzelne Domänen gesondert festlegen. Die Bandbreitenbegrenzung wirkt sich auf alle eingehenden und abgehenden SMTP-Verbindungen aus. Sie können Absender auf der Weißen Liste, Verbindungen mit Echtheitsbestätigung und die Mailserver der Domäne von den Beschränkungen ausnehmen. Die Bandbreitenbegrenzung rechnet in Kilobyte (KB) pro Sekunde, wobei die Voreinstellung für eingehende und abgehende SMTP-Verbindungen 10 beträgt und beide Optionen per Voreinstellung abgeschaltet sind.

Bevor die Bandbreitenbegrenzung wirksam wird, können bis zu 8 KB Daten gesendet und empfangen werden. Dieses Volumen kann bereits die Begrenzungen überschreiten, die Sie für diese Funktion festlegen.

Bandbreitenbegrenzung

Eingehende SMTP-Verbindungen begrenzen auf: [xx] KB pro Sekunde
Diese Option bewirkt, dass die Bandbreite für eingehende SMTP-Verbindungen begrenzt wird. Die Voreinstellung beträgt 10 KB pro Sekunde, jedoch ist diese Option per Voreinstellung abgeschaltet.

Abgehende SMTP-Verbindungen begrenzen auf: [xx] KB pro Sekunde
Diese Option bewirkt, dass die Bandbreite für abgehende SMTP-Verbindungen begrenzt wird. Die Voreinstellung beträgt 10 KB pro Sekunde, jedoch ist diese Option per Voreinstellung abgeschaltet.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausschlüsse

Nachrichten von Absendern auf der Weißen Liste ausnehmen
Diese Option bewirkt, dass alle Absender, die in einer Weißen Liste[275] erfasst sind, von den Beschränkungen der Bandbreitenbegrenzung ausgenommen sind. Diese Option ist per Voreinstellung abgeschaltet.

Nachrichten aus echtheitsbestätigten Verbindungen ausnehmen
Diese Option bewirkt, dass Verbindungen mit Echtheitsbestätigung von den Beschränkungen der Bandbreitenbegrenzung ausgenommen sind. Diese Option ist per Voreinstellung abgeschaltet.

Nachrichten von Mailservern der Domäne ausnehmen
Diese Option bewirkt, dass Verbindungen mit den Mailservern der Domäne[79] von den Beschränkungen der Bandbreitenbegrenzung ausgenommen sind. Diese Option ist per Voreinstellung abgeschaltet.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen zur Bandbreitenbegrenzung für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.4.8 Erkennung des Hijackings von Benutzerkonten

Erkennung des Hijackings von Benutzerkonten

Die Optionen in diesem Abschnitt dienen dazu, zu erkennen, ob ein Benutzerkonto auf Ihrem Server möglicherweise gehijackt oder sonst kompromittiert wurde, und sodann den weiteren Versand von Nachrichten von diesem Benutzerkonto aus über Ihren Server automatisch zu unterbinden. Ein Beispiel für ein solches Hijacking ist, dass ein Spam-Versender sich die E-Mail-Adresse und das Kennwort eines Benutzerkontos verschafft; die Leistungsmerkmale zum Erkennen dieses Hijackings können dann den Spam-Versender daran hindern, von dem "gekaperten" Benutzerkonto aus massenhaft Spam- und Junk-Nachrichten über Ihren Server zu versenden. Sie können bestimmen, wie viele Nachrichten ein Benutzerkonto während einer in Minuten festgelegten Zeitspanne versenden darf, und Sie können wahlweise das Benutzerkonto sperren lassen, sobald diese Grenze erreicht wurde. Sie können bestimmte Benutzerkonten von der Hijacking-Erkennung ausnehmen, indem Sie die Option *Benutzerkonto von der "Erkennung für Hijacking" ausnehmen* in den Benutzerkonten-Einstellungen[34] für das betroffene Benutzerkonto aktivieren. Sie können die Voreinstellung für diese benutzerspezifische Option auf der Seite Benutzer-Optionen[73] konfigurieren.

Die Erkennung des Hijackings von Benutzerkonten wirkt nur auf lokale Benutzerkonten und nur, soweit diese echtheitsbestätigte Verbindungen nutzen. Das Benutzerkonto des Postmasters ist von diesem Leistungsmerkmal automatisch ausgenommen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Benutzerkonten dürfen höchstens [xx] Nachrichten in [xx] Minuten senden
Diese Option begrenzt die Zahl der Nachrichten, die lokale Benutzerkonten innerhalb des hier in Minuten angegebenen Zeitraums senden dürfen, auf die hier angegebene Zahl. Falls ein Benutzerkonto versucht, mehr als die hier angegebene Zahl von Nachrichten zu versenden, weist SecurityGateway die Verbindung zwar nicht ab, aber die überzähligen Nachrichten werden so lange mit einem Fehler 452 abgewiesen, bis die Zeitbegrenzung abgelaufen ist. Danach werden Nachrichten des Benutzerkontos wieder zur Zustellung angenommen.

Benutzerkonten sperren, sobald sie diese Begrenzung überschreiten
Diese Option bewirkt, dass Benutzerkonten gesperrt werden, sobald sie versuchen, mehr als die zugelassene Anzahl von Nachrichten zu senden. Bei einer solche Sperre sendet der Server den Fehler 552 und trennt die Verbindung. Das Benutzerkonto wird anschließend sofort gesperrt. Das gesperrte Benutzerkonto kann keine Nachrichten mehr versenden und abrufen. SecurityGateway nimmt eingehende Nachrichten für das Benutzerkonto aber weiterhin entgegen. Der Postmaster wird von einer solche Sperrung per E-Mail benachrichtigt. Er kann die Sperrung des Benutzerkonto aufheben, indem er auf die Benachrichtigung antwortet.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen zur Bandbreitenbegrenzung für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.5 RMail™

RMail™ ist ein Dienst von RPost®. Die Nutzung von RMail™ ist selbsterklärend. Die Empfänger benötigen hierfür keine besondere Software. RMail™ verbessert die Nutzung von E-Mail-Diensten für Verbraucher und Unternehmen aller Größenordnungen, in allen Sektoren und Bereichen.

Der RMail™-Dienst wird durch das Leistungsmerkmal Registered Email™ von RPost umgesetzt - den weltweiten Standard für Zustellnachweise bei E-Mail-Nachrichten. Der RMail™-Dienst erweitert Ihrer E-Mail-Plattform und bietet folgende Leistungsmerkmale:

- Sendungsverfolgung für wichtige Nachrichten - Sie können Sendung und Zustellung verfolgen und wissen so genau, wann die Nachrichten zugestellt und geöffnet werden.
- Nachweis von Zustellung, Uhrzeit und genauem Inhalt.
- Einfache Verschlüsselung von E-Mail-Nachrichten und Dateianlagen mit vertraulichen Inhalten aus Sicherheitsgründen oder, um rechtliche Anforderungen zu erfüllen.
- RMail™ ermöglicht es allen Beteiligten, Vorgänge und Vereinbarungen einfach mithilfe von E-Signaturen abzuschließen.

Bei Nutzung eines Test-Benutzerkontos für RPost ist jeder Benutzer auf Versand und Empfang von insgesamt 5 verschlüsselten Nachrichten pro Monat beschränkt. Weitere Nachrichten können über RPost erworben werden. Informationen über

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Bezugsmodelle und Preise für höhere Nachrichtenzahlen erhalten Sie auf der Website RPost.com.

Sie können den RMail™-Dienst auf der Seite Sicherheit » RMail[235] aktivieren und konfigurieren. Sie können seine Nutzung auch mithilfe von Aktionen in Regeln des Inhaltsfilters[258] steuern.

Verschlüsselung

RMail-Dienst Verschlüsselung aktivieren
Diese Option bewirkt, dass der RMail-Dienst Verschlüsselung für Nachrichten genutzt werden kann. Sie können SecurityGateway so konfigurieren, dass die RMail-Verschlüsselung für alle Nachrichten oder nur für solche Nachrichten verwendet wird, deren Betreffzeilen mit bestimmten Schlüsselwörtern beginnen.

Kalendereinladungen ausnehmen
Diese Option bewirkt, dass Kalendereinladungen, wie etwa Besprechungsanfragen, von der Verarbeitung durch RMail ausgenommen werden.

Alle Nachrichten verschlüsseln
Diese Option bewirkt, dass alle Nachrichten mithilfe des RMail-Dienstes Verschlüsselung verschlüsselt werden.

Nur folgende Nachrichten verschlüsseln...
Diese Option bewirkt, dass nur solche Nachrichten mithilfe des RMail-Dienstes Verschlüsselung verschlüsselt werden, deren Betreffzeilen mit einem der nachfolgend angegebenen Schlüsselwörter beginnen.

Nachrichten verschlüsseln, falls ihre Betreffzeile mit folgendem Text beginnt...
Ist die Option *Nur folgende Nachrichten verschlüsseln...* weiter oben aktiv, so wird der RMail-Dienst Verschlüsselung nur für solche Nachrichten verwendet, deren Betreffzeilen mit einem der hier angegebenen Schlüsselwörter beginnen. Sie können die Liste der Schlüsselwörter mithilfe der Schaltflächen Hinzufügen und Entfernen verwalten.

Steuertext aus Betreffzeile entfernen
Diese Option bewirkt, dass der Text aus der Betreffzeile entfernt wird, der die Verarbeitung durch RMail ausgelöst hat.

Nachrichten verschlüsseln, falls sie an folgende Empfänger gerichtet sind...
Diese Option bewirkt, dass Nachrichten dann verschlüsselt werden, wenn sie an bestimmte Empfänger gerichtet sind.

Sendungs- und Zustellungsverfolgung (Track & Prove)

RMail-Dienst Sendungs- und Zustellungsverfolgung (Track & Prove) aktivieren
Diese Option bewirkt, dass der RMail-Dienst Sendungs- und Zustellungsverfolgung (Track & Prove) für Nachrichten genutzt werden kann. Sie können SecurityGateway so konfigurieren, dass die RMail-Sendungs- und Zustellungsverfolgung für alle Nachrichten oder nur für solche Nachrichten verwendet wird, die bestimmte Schlüsselwörter enthalten. Mithilfe dieses Leistungsmerkmals können die Benutzer ihre Nachrichten nachverfolgen und Berichte mit Zeitstempeln erhalten, in denen vermerkt ist, wann Nachrichten zugestellt und geöffnet wurden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kalendereinladungen ausnehmen
Diese Option bewirkt, dass Kalendereinladungen, wie etwa Besprechungsanfragen, von der Verarbeitung durch RMail Track & Prove ausgenommen werden.

Alle Nachrichten verfolgen
Diese Option bewirkt, dass alle Nachrichten mithilfe des RMail-Dienstes Sendungs- und Zustellungsverfolgung nachverfolgt werden.

Nur folgende Nachrichten verfolgen...
Diese Option bewirkt, dass nur solche Nachrichten mithilfe des RMail-Dienstes Sendungs- und Zustellungsverfolgung nachverfolgt werden, die eines der nachfolgend angegebenen Schlüsselwörter enthalten. Die Schlüsselwörter können in der Betreffzeile oder im Nachrichtentext enthalten sein.

Nachrichten verfolgen, falls ihre Betreffzeile oder ihr Nachrichtentext folgenden Text enthält...
Ist die Option *Nur folgende Nachrichten verfolgen...* weiter oben aktiv, so wird der RMail-Dienst Sendungs- und Zustellungsverfolgung nur für solche Nachrichten verwendet, die eines der hier angegebenen Schlüsselwörter enthalten. Die Schlüsselwörter können in der Betreffzeile oder im Nachrichtentext enthalten sein. Sie können die Liste der Schlüsselwörter mithilfe der Schaltflächen Hinzufügen und Entfernen verwalten.

Steuertext aus Betreffzeile entfernen
Diese Option bewirkt, dass der Text aus der Betreffzeile entfernt wird, der die Verarbeitung durch RMail Track & Prove ausgelöst hat.

E-Signatur

RMail-Dienst E-Signatur (E-Sign) aktivieren
Diese Option bewirkt, dass der RMail-Dienst E-Signatur (E-Sign) für Nachrichten zur elektronischen Signatur von Dokumenten genutzt werden kann. Sie können SecurityGateway so konfigurieren, dass die RMail-E-Signatur für alle Nachrichten oder nur für solche Nachrichten verwendet wird, die bestimmte Schlüsselwörter enthalten.

Kalendereinladungen ausnehmen
Diese Option bewirkt, dass Kalendereinladungen, wie etwa Besprechungsanfragen, von der Verarbeitung durch RMail E-Sign ausgenommen werden.

Alle Nachrichten signieren
Diese Option bewirkt, dass alle Nachrichten mithilfe des RMail-Dienstes E-Signatur elektronisch signiert werden.

Nur folgende Nachrichten signieren...
Diese Option bewirkt, dass nur solche Nachrichten mithilfe des RMail-Dienstes E-Signatur elektronisch signiert werden, die eines der nachfolgend angegebenen Schlüsselwörter enthalten. Die Schlüsselwörter können in der Betreffzeile oder im Nachrichtentext enthalten sein.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nachrichten signieren, falls ihre Betreffzeile oder ihr Nachrichtentext folgenden Text enthält...
Ist die Option *Nur folgende Nachrichten signieren...* weiter oben aktiv, so wird der RMail-Dienst E-Signatur nur für solche Nachrichten verwendet, die eines der hier angegebenen Schlüsselwörter enthalten. Die Schlüsselwörter können in der Betreffzeile oder im Nachrichtentext enthalten sein. Sie können die Liste der Schlüsselwörter mithilfe der Schaltflächen Hinzufügen und Entfernen verwalten.

Steuertext aus Betreffzeile entfernen
Diese Option bewirkt, dass der Text aus der Betreffzeile entfernt wird, der die Verarbeitung durch RMail Sign ausgelöst hat.

4.6 Data Leak Prevention (Verhinderung von Datendiebstahl)

Die Verhinderung von Datendiebstahl (englisch auch "Data Leak Prevention") ist ein Leistungsmerkmal, das auf dem Inhaltsfilter für Nachrichten 252 aufgebaut ist. Mit seiner Hilfe können Sie Filterregeln erstellen, die in Nachrichten nach bestimmten Arten besonders schutzwürdiger Informationen suchen, und die verhindern, dass solche Nachrichten zugestellt werden. Es sind bereits zahlreiche vordefinierte Regeln enthalten. Diese Regeln suchen nach Daten wie Kreditkarten-Nummern, Daten für Bankkonten, Passnummern und vergleichbaren Daten. Diese Regeln werden per Voreinstellung nur auf abgehende Nachrichten angewendet. Nachrichten, die zu Treffern für diese Regeln führen, werden in die Administrative Quarantäne 310 verschoben. Sie können die voreingestellten Regeln wie alle anderen Regeln verwalten und bearbeiten.

Mithilfe dieser Seite können Sie die Regeln für die Verhinderung von Datendiebstahl verwalten. Sie können von hier aus die Regeln erstellen, bearbeiten und löschen, und Sie können bestehende Regeln mithilfe eines Kontrollkästchens schnell aktivieren und deaktivieren. Die Regeln für die Verhinderung von Datendiebstahl legen, wie auch die sonstigen Regeln für den Inhaltsfilter, die Kriterien fest, anhand derer SecurityGateway jede Nachricht prüft, die verarbeitet wird. Stimmt eine Nachricht mit einer Regel überein, so können eine Reihe von Aktionen durchgeführt werden. Sie können Regeln erstellen, die nach bestimmten Kopfzeilen, Absendern und Empfängern, sowie bestimmtem Text in einer Kopfzeile oder dem Nachrichtentext suchen oder prüfen, wie groß eine Nachricht ist. Daneben stehen zahlreiche weitere Kriterien zur Verfügung. Stimmt eine Nachricht mit den Kriterien einer Regel überein, so kann die Regel unter anderem bewirken, dass die Nachricht abgewiesen, gelöscht, in Quarantäne gegeben, kopiert oder an eine andere Adresse umgeleitet wird.

Die Liste der Regeln für die Verhinderung von Datendiebstahl enthält drei Spalten: Aktiviert, Beschreibung und Vorschau. Die Spalte Aktiviert enthält für jeden Eintrag ein eigenes Kontrollkästchen, mit dessen Hilfe Sie die Regel schnell aktivieren und deaktivieren können. In der Spalte Beschreibung erscheint der *Name der Regel*, den Sie während der Erstellung der Regel festgelegt haben. Die Spalte Vorschau enthält für jede Regel ein Symbol, mit dessen Hilfe Sie sich einen Tooltipp zu der zugehörigen Regel anzeigen lassen können. Lassen Sie dazu die Maus über dem Symbol stehen. Der Tooltipp zeigt das Sieve-Skript 284, das nach der Erstellung der Regel über den Editor für Regeln zur Verhinderung von Datendiebstahl 239 zur Umsetzung der Regel angelegt wurde.

Die Symbolleiste am oberen Seitenrand enthält die folgenden vier Optionen:

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Neu
Um eine neue Regel zu erstellen, klicken Sie auf *Neu.* Es öffnet sich der Editor für Regeln zur Verhinderung von Datendiebstahl 239, in dem Sie die Regel erstellen können.

Bearbeiten
Um eine Regel zu bearbeiten, wählen Sie die Regel in der Liste aus, und klicken Sie in der Symbolleiste auf *Bearbeiten.* Es öffnet sich der Editor für Regeln zur Verhinderung von Datendiebstahl 239, und die Regel wird zur Bearbeitung geladen. Sie können eine Regel stattdessen auch durch Doppelklick zur Bearbeitung öffnen.

Löschen
Um eine Regel oder mehrere Regeln zu löschen, wählen Sie die gewünschten Einträge in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Einträge wirklich löschen wollen. Sie können mithilfe der Strg-Taste und der Hochschalttaste mehrere Einträge auswählen.

Für Domäne:
Mithilfe des Auswahlmenüs *Für Domäne:* bestimmen Sie, welche Regeln in der Liste angezeigt werden. Sie können sich Globale Regeln anzeigen lassen, die auf alle Domänen wirken, oder nur die Regeln einer bestimmten Domäne.

Editor für Regeln zur Verhinderung von Datendiebstahl

Mithilfe des Editors für Regeln zur Verhinderung von Datendiebstahl können Sie neue Regeln erstellen oder bestehende Regeln bearbeiten. Um eine neue Regel zu erstellen, klicken Sie in der Symbolleiste für die Regeln des Inhaltsfilters auf *Neu*. Gehen Sie dann die Optionen, die der Editor bietet, der Reihe nach durch. Sobald Sie alle Daten eingetragen haben, klicken Sie auf *Speichern und Beenden*, um die neue Regel anzulegen.

Diese Regel ist aktiv
Zur Erstellung einer neuen Regel muss dieses Kontrollkästchen aktiv sein. Sie können bestehende Regeln deaktivieren, indem Sie den Haken aus dem zugehörigen Kontrollkästchen entfernen. SecurityGateway lässt deaktivierte Regeln bei der Prüfung von Nachrichten außer Betracht. Die Option entspricht der Spalte *Aktiviert* in der Übersicht über die Regeln des Inhaltsfilters.

Für Domäne:
In dieser Option legen Sie fest, auf welche Domänen die Regel angewendet wird. Wird hier "--Global--" ausgewählt, so wirkt die Regel auf Nachrichten an alle und von allen SecurityGateway-Domänen. Wird hier eine bestimmte Domäne ausgewählt, so wirkt die Regel nur auf Nachrichten an alle und von allen Nachrichten dieser Domäne.

Name der Regel:
Tragen Sie in dieses Feld einen Titel oder einen kurzen Beschreibungstext für Ihre Regel ein. Diese Option entspricht der Spalte *Beschreibung* in der Übersicht über die Regeln des Inhaltsfilters.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Regel anwenden, falls:

alle Bedingungen erfüllt sind (AND)
Wählen Sie diese Option aus, falls eine Nachricht nur dann einen Treffer in dieser Regel auslösen soll, falls sie ALLE Bedingungen erfüllt, die weiter unten angegeben werden. Die Option bewirkt, dass die Bedingungen logisch mit "UND" verknüpft werden, etwa nach dem Muster "falls Bedingung A erfüllt ist UND Bedingung B erfüllt ist, dann die angegebene Aktion ausführen".

eine beliebige Bedingung erfüllt ist (OR)
Wählen Sie diese Option aus, falls eine Nachricht dann einen Treffer in dieser Regel auslösen soll, falls sie EINE BELIEBIGE der Bedingungen erfüllt, die weiter unten angegeben werden. Die Option bewirkt, dass die Bedingungen logisch mit "ODER" verknüpft werden, etwa nach dem Muster "falls Bedingung A erfüllt ist ODER Bedingung B erfüllt ist, dann die angegebene Aktion ausführen".

Bedingungen:
In diesem Abschnitt erscheinen alle Bedingungen, die Sie für diese Regel festgelegt haben, verbunden mit den Aktionen, die durchgeführt werden soll, falls eine Nachricht mit den Bedingungen der Regel übereinstimmt. Sie können eine Bedingung durch Anklicken in diesem Bereich bearbeiten. Sie können eine Bedingung durch Anklicken der Verknüpfung "(Entfernen)" neben der Bedingung löschen. Um der Regel eine neue Bedingung hinzuzufügen, klicken Sie unterhalb dieses Bereichs auf die Verknüpfung "*Klicken Sie hier, um eine Bedingung für diese Regel hinzuzufügen.*".

Klicken Sie hier, um eine Bedingung für diese Regel hinzuzufügen
Klicken Sie unterhalb des Abschnitts Bedingungen auf die Verknüpfung "*Klicken Sie hier, um eine Bedingung für diese Regel hinzuzufügen.*", um der Regel eine Bedingung hinzuzufügen. Nachdem Sie die Bedingung hinzugefügt haben, können Sie weitere Bedingungen hinzufügen, indem Sie erneut auf die Verknüpfung klicken. Die einzelnen Arten von Bedingungen sind im Abschnitt Bedingungen für die Regeln 254 weiter unten näher beschrieben.

Aktion:
Aus diesem Auswahlmenü wählen Sie die Aktion, die durchgeführt werden soll, falls eine Nachricht mit den Bedingungen der Regel übereinstimmt. Falls für eine Aktion weitere Angaben erforderlich sind, erscheint unterhalb dieses Auswahlmenüs ein entsprechendes Eingabefeld, in dem Sie die nötigen Angaben machen können. Die einzelnen Arten von Aktionen sind im Abschnitt Aktionen 258 weiter unten näher beschrieben. Nachdem Sie alle Bedingungen für die Regel festgelegt und eine Aktion ausgewählt haben, klicken Sie auf *Speichern und Beenden*, um den Editor zu verlassen und die neue Regel in die Liste der Regel einzutragen.

Bedingungen für die Regeln

Um einer Regel eine Bedingung hinzuzufügen, klicken Sie auf die Verknüpfung "*Klicken Sie hier, um eine Bedingung für diese Regel hinzuzufügen.*". Es öffnet sich der Dialog *Bedingungen für die Regel*. Um eine solche Bedingung zu erstellen, müssen Sie zunächst das Nachrichten-Attribut oder Element bestimmen, anhand dessen Sie die Prüfung in der Bedingung durchführen wollen. Dann müssen Sie festlegen, wie ein Vergleich mit diesem Element oder eine Prüfung des Elements durchgeführt werden soll: Es kann geprüft werden, ob das Element einen Text enthält oder einem Text

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

genau entspricht, ob eine Kopfzeile besteht, und vieles mehr. Zur Verfügung stehen mehrere Elemente, die geprüft werden können, und verschiedene Vergleichsmethoden. Nachdem Sie das Element ausgewählt, die Vergleichsmethode festgelegt und etwa nötige Informationen eingegeben haben, klicken Sie auf *Speichern und Beenden*, um die Bedingung Ihrer Regel hinzuzufügen.

Zu vergleichendes Element:
Diese Liste enthält folgende Elemente, die Sie in einer Nachricht vergleichen und prüfen können:

- **MAIL (Von)**—Diese Prüfung betrifft den Inhalt des SMTP-Befehls "`MAIL From`". Er bezeichnet den Absender der Nachricht; der Inhalt des Befehls muss aber nicht zwangsläufig mit dem Inhalt der Absender-Kopfzeile `From` in der Nachricht selbst übereinstimmen. Manchmal enthält die Kopfzeile `From` zusätzliche oder abweichende Informationen. Zusätzlich zu den neun üblichen Vergleichsmethoden (siehe unten) stehen noch die Prüfungen "`ist ein lokaler Benutzer`" und "`ist kein lokaler Benutzer`" zur Verfügung.
- **RCPT (An)**—Diese Prüfung betrifft den Inhalt des SMTP-Befehls "`RCPT To`". Er bezeichnet den Empfänger der Nachricht; der Inhalt des Befehls muss aber nicht zwangsläufig mit dem Inhalt der Adressaten-Kopfzeile `To` in der Nachricht selbst übereinstimmen. Manchmal enthält die Kopfzeile `To` zusätzliche oder abweichende Informationen. Zusätzlich zu den neun üblichen Vergleichsmethoden (siehe unten) stehen noch die Prüfungen "`ist ein lokaler Benutzer`" und "`ist kein lokaler Benutzer`" zur Verfügung.
- **MAIL (Von) und RCPT (An)**—Dieses Element prüft die Parameter der SMTP-Befehle "`MAIL From`" und "`RCPT To`", um zu bestimmen, ob es sich bei der ausgewerteten Nachricht um eine eingehende, abgehende oder interne Nachricht handelt (siehe "*Weitere Vergleichs-Methoden*" weiter unten).
- **IP**—Wählen Sie dieses Element, um einen Vergleich anhand der IP-Adresse des übermittelnden Servers oder Clients durchzuführen.
- **Kopfzeile**—Wählen Sie dieses Element, falls Sie eine Kopfzeile angeben möchten, anhand derer Sie einen Vergleich vornehmen wollen. Nachdem Sie dieses Element gewählt haben, erscheint das Eingabefeld *Name der Kopfzeile*. In dieses Feld müssen Sie die Kopfzeile eintragen, anhand derer Sie den Vergleich vornehmen wollen. Zusätzlich zu den neun üblichen Vergleichsmethoden kann dieses Element auch noch anhand der Vergleichs-Methoden "`Kopfzeile existiert`" und "`Kopfzeile existiert nicht`" verglichen werden. **Beachte:** Im Feld *Name der Kopfzeile* dürfen Sie den Namen der Kopfzeile nicht mit einem Doppelpunkt abschließen. Sie müssen beispielsweise für einen Vergleich mit der Absender-Kopfzeile From als *Name der Kopfzeile* "`From`" eintragen, nicht aber "`From:`".
- **Betreff**—Dieses Element ist die Kopfzeile `Subject` (Betreff) der Nachrichten. Mithilfe dieses Elements können Sie Vergleiche mit dem Betreff der Nachrichten durchführen.
- **Nachrichtentext**—Wählen Sie dieses Element, um einen Vergleich mit dem Inhalt des Nachrichtentextes durchzuführen.
- **Nachrichtentext oder Betreff**—Mithilfe dieses Elements können Sie eine Regel erstellen, die dann zu einem Treffer führt, wenn entweder der *Nachrichtentext* oder der *Betreff* der Nachricht den Kriterien der Regel entspricht. Dieses Element soll die Erstellung der Regeln vereinfachen, weil es im Ergebnis dieselbe Wirkung hat wie eine Regel, in der zwei getrennte

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Elemente mit "ODER" verknüpft sind, von denen eine den *Nachrichtentext* und das andere die *Betreffzeile* der Nachricht nach demselben Text durchsucht.

Vergleichs-Methode:
Die folgende Liste enthält die Methoden, mit deren Hilfe Sie Vergleiche und Prüfungen für das Element durchführen können, das Sie in der Option *Zu vergleichendes Element* weiter oben ausgewählt haben. Für alle Elemente stehen verschiedene Vergleichsmethoden zur Verfügung, die sich nur in Bezug auf ein Element unterscheiden. Für das Elemente `Mail (Von) und RCPT (An)` bestehen besondere Vergleichsmethoden, und für `Mail (Von)`, `RCPT (An)` und `Kopfzeile` stehen jeweils weitere Vergleichsmethoden zur Verfügung.

Übliche Vergleichs-Methoden:
Jede der folgenden Vergleichsmethoden oder Operatoren vergleicht das oben in der Option *Zu vergleichendes Element* angegebene Element mit dem *Suchausdruck,* den Sie in das Eingabefeld unterhalb des Feldes *Vergleichs-Methode* eintragen müssen. Alle nachfolgend aufgeführten Vergleichs-Methoden stehen für alle zu vergleichenden Elemente, jedoch nicht für `Mail (Von) und RCPT (An)` zur Verfügung. Für `Mail (Von) und RCPT (An)` bestehen besondere Vergleichsmethoden-

- **enthält**—Diese Methode ergibt einen Treffer (Ergebnis "wahr"), falls der *Suchausdruck* ein Teil des *zu vergleichenden Elements* ist, das oben ausgewählt wurde. Wählen Sie beispielsweise `MAIL (Von)` als zu vergleichendes Element, und wählen Sie dann `enthält` als Vergleichs-Methode und "example.com" als *Suchausdruck*, so erfüllt jede Nachricht von einer Adresse, die "example.com" enthält, die Bedingung.
- **enthält nicht**—Diese Methode ergibt einen Treffer (Ergebnis "wahr"), falls der *Suchausdruck* kein Teil des *zu vergleichenden Elements* ist, das oben ausgewählt wurde. Wählen Sie beispielsweise `MAIL (Von)` als zu vergleichendes Element, und wählen Sie dann `enthält nicht` als Vergleichs-Methode und "example.com" als *Suchausdruck*, so erfüllt jede Nachricht die Bedingung, außer Nachrichten von Adressen, die "example.com" enthalten.
- **enthält Wort/Wörter**—Diese Methode arbeitet ähnlich wie "enthält". Sie führt aber nur dann zu einem Treffer, wenn die zu suchende Zeichenkette zwischen zwei Wortbegrenzungsankern eingeschlossen ist. Hierdurch wird vermieden, dass manuell ein Regulärer Ausdruck nach dem Muster `\b(Wort1|Wort2|Wort3)\b` erstellt werden muss. Ein Beispiel hierzu: Eine Regel, die nach Nachrichtentexten sucht, die das *Wort* "Katze" *enthalten*, führt nur für solche Nachrichten zu einem Treffer, die das eigenständige Wort "Katze" enthalten. Sie führt dann nicht zu einem Treffer, wenn der Nachrichtentext Wörter wie *Katzenwels* oder *Schleichkatze* enthält.
- **enthält nicht Wort**—Diese Methode arbeitet ähnlich wie "enthält nicht". Sie führt aber nur dann zu einem Treffer, wenn die auszuschließende Zeichenkette zwischen zwei Wortbegrenzungsankern eingeschlossen ist. Ein Beispiel hierzu: Eine Regel, die nach Nachrichtentexten sucht, die das *Wort* "Katze" *nicht enthalten*, führt nur für solche Nachrichten zu einem Treffer, die das eigenständige Wort "Katze" nicht enthalten. Sie führt dann nicht zu einem Treffer, wenn der Nachrichtentext Wörter wie *Katzenwels* oder *Schleichkatze* enthält.
- **entspricht**—Diese Methode arbeitet ähnlich wie *enthält* weiter oben, der

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Suchausdruck muss aber mit dem Inhalt des *zu vergleichenden Elements* genau übereinstimmen; eine teilweise Übereinstimmung reicht nicht aus. Wählen Sie beispielsweise `IP` als zu vergleichendes Element, und wählen Sie dann `entspricht` als Vergleichs-Methode und "192.168.0.1" als *Suchausdruck*, so erfüllen nur Nachrichten die Bedingung, die von genau der angegebenen IP-Adresse stammen.

- **entspricht nicht**—Diese Methode arbeitet spiegelverkehrt zur vorherigen Methode. Entspricht der Inhalt des *zu vergleichenden Elements* nicht genau dem *Suchausdruck*, so ist die Bedingung erfüllt. Wählen Sie beispielsweise `IP` als zu vergleichendes Element, und wählen Sie dann `entspricht nicht` als Vergleichs-Methode und "192.168.0.1" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, außer den Nachrichten, die von genau der angegebenen IP-Adresse stammen.
- **beginnt mit**—Diese Methode ergibt einen Treffer, falls der Inhalt des *zu vergleichenden Elements* mit dem *Suchausdruck* beginnt. Wählen Sie beispielsweise `Betreff` als zu vergleichendes Element, und wählen Sie , und wählen Sie dann `beginnt mit` als Vergleichs-Methode und "[AlleMitarbeiter]" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, deren Betreffzeile mit dem Text "[AlleMitarbeiter]" beginnt.
- **beginnt nicht mit**—Diese Methode arbeitet spiegelverkehrt zur vorherigen Methode. Beginnt der Inhalt des *zu vergleichenden Elements* nicht mit dem *Suchausdruck*, so ist die Bedingung erfüllt. Wählen Sie beispielsweise `Betreff` als zu vergleichendes Element, und wählen Sie dann `beginnt nicht mit` als Vergleichs-Methode und "[AlleMitarbeiter]" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, außer denen, deren Betreffzeile mit dem Text "[AlleMitarbeiter]" beginnt.
- **endet auf**—Diese Methode ergibt einen Treffer, falls der Inhalt des *zu vergleichenden Elements* mit dem *Suchausdruck* endet. Wählen Sie beispielsweise `RCPT (An)` als zu vergleichendes Element, und wählen Sie dann `endet auf` als Vergleichs-Methode und ".cn" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, die an einen Empfänger gerichtet sind, dessen Adresse auf ".cn" endet.
- **endet nicht auf**—Diese Methode ergibt einen Treffer, falls der Inhalt des *zu vergleichenden Elements* nicht mit dem *Suchausdruck* endet. Wählen Sie beispielsweise `RCPT (An)` als zu vergleichendes Element, und wählen Sie dann `endet nicht auf` als Vergleichs-Methode und ".cn" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, außer denen, die an einen Empfänger gerichtet sind, dessen Adresse auf ".cn" endet.
- **stimmt mit Regulärem Ausdruck überein**—Wählen Sie diese Option, um für den Vergleich und die Prüfung des *zu vergleichenden Elements* einen **Regulären Ausdruck** zu nutzen.

Weitere Vergleichs-Methoden:

- **ist ein lokaler Benutzer**—Diese Vergleichs-Methode steht nur für die Optionen `MAIL (Von)` und `RCPT (An)` oben zur Verfügung. Bei ihrer Nutzung ist die Bedingung erfüllt, falls die Adresse zu einem lokalen SecurityGateway-Benutzer gehört. Wählen Sie beispielsweise `MAIL (Von)` als das *zu vergleichende Element*, so ist die Bedingung nur bei Nachrichten von lokalen Benutzern erfüllt.
- **ist kein lokaler Benutzer**—Diese Vergleichs-Methode steht nur für die Optionen `MAIL (Von)` und `RCPT (An)` oben zur Verfügung. Bei ihrer

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nutzung ist die Bedingung erfüllt, falls die Adresse nicht zu einem lokalen SecurityGateway-Benutzer gehört. Wählen Sie beispielsweise `MAIL (Von)` als das *zu vergleichende Element*, so ist die Bedingung nur bei Nachrichten von externen Benutzern erfüllt, nicht jedoch bei Nachrichten von lokalen Benutzern.

- **Kopfzeile existiert**—Diese Vergleichs-Methode steht nur zur Verfügung, falls Sie oben als *zu vergleichendes Element* die `Kopfzeile` ausgewählt haben. Wählen Sie diese Option, und geben Sie dann den *Namen der Kopfzeile* in das entsprechende Feld ein, so ist die Bedingung nur erfüllt, falls die angegebene Kopfzeile in der Nachricht enthalten ist. Geben Sie beispielsweise "X-Meine-benutzerdefinierte-Kopfzeile" als *Namen der Kopfzeile* ein*,* so erfüllen alle Nachrichten die Bedingung, die diese Kopfzeile enthalten. Nachrichten ohne die Kopfzeile erfüllen die Bedingung nicht.
- **Kopfzeile existiert nicht**—Diese Vergleichs-Methode steht nur zur Verfügung, falls Sie oben als *zu vergleichendes Element* die `Kopfzeile` ausgewählt haben. Wählen Sie diese Option, und geben Sie dann den *Namen der Kopfzeile* in das entsprechende Feld ein, so ist die Bedingung nur erfüllt, falls die angegebene Kopfzeile in der Nachricht nicht enthalten ist. Geben Sie beispielsweise "X-Meine-benutzerdefinierte-Kopfzeile" als *Namen der Kopfzeile* ein*,* so erfüllen alle Nachrichten die Bedingung, die diese Kopfzeile nicht enthalten. Nachrichten mit dieser Kopfzeile erfüllen die Bedingung nicht.
- **Nachricht ist/ist nicht [eingehend|abgehend|intern]**—Diese Vergleichs-Methoden sind nur für das Element `MAIL (Von) und RCPT (An)` verfügbar. Es werden die Parameter der SMTP-Befehle "MAIL From" und "RCPT To" dazu verwendet, um zu prüfen, ob eine Nachricht eingehend, abgehend oder intern ist, oder ob eine Nachricht nicht eingehend, nicht abgehend oder nicht intern ist.

  Eingehend—Dies sind Nachrichten, die an lokale Benutzer gerichtet sind und nicht von lokalen Benutzern derselben Domäne stammen.

  Outbound—Dies sind Nachrichten, die von lokalen Benutzern stammen und nicht an lokale Benutzer derselben Domäne gerichtet sind.

  Internal—Dies sind Nachrichten, die von lokalen Benutzern stammen und an lokale Benutzer derselben Domäne gerichtet sind.

Aktionen

Nachdem Sie die Bedingungen für Ihre Regel festgelegt haben, müssen Sie im Editor für die Regeln noch mithilfe des entsprechenden Feldes die *Aktion* festlegen, die der Inhaltsfilter ausführen soll, falls eine Nachricht die Bedingungen der Regel erfüllt. Es stehen sieben Aktionen zur Verfügung:

- **Abweisen**—Diese Aktion bewirkt, dass eine Nachricht abgewiesen wird, falls sie die Bedingungen der Regel erfüllt. Nach Auswahl dieser Option erscheint weiter unten das Eingabefeld *SMTP-Meldung.* In dieses Eingabefeld können Sie einen Text eintragen, der beim Abweisen der Nachricht im SMTP-Protokolldialog übermittelt wird. Tragen Sie beispielsweise "Wir wollen Ihren Spam nicht haben!" in das Feld *SMTP-Meldung* ein, so übermittelt SecurityGateway für Nachrichten, die die Bedingungen der Regel erfüllen, im SMTP-Protokolldialog "`550 Wir wollen Ihren Spam nicht haben!`" und

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

weist die Nachricht ab. Bitte bedenken Sie beim Abfassen dieser Meldung, dass sie allenfalls auch für ausländische Serverbetreiber verständlich sein sollte; es ist daher sinnvoll, immer auch einen englischen Textteil vorzusehen.

- **Verwerfen**—Diese Aktion bewirkt, dass eine Nachricht verworfen wird, falls sie die Bedingungen der Regel erfüllt. Anders als bei der Aktion `Abweisen` wird bei dieser Aktion keine SMTP-Meldung übermittelt, und es wird auch keine Nachricht über einen Zustellfehler versandt. Die Nachricht wird ohne weiteres gelöscht.
- **Quarantäne**—Diese Aktion bewirkt, dass eine Nachricht, die die Bedingungen der Regel erfüllt, in den Quarantäne-Ordner 308 des Benutzers verschoben wird, falls der Empfänger ein lokaler Benutzer ist. Ist der Empfänger ein externer Benutzer, so wird die Nachricht stattdessen in die Administrative Quarantäne 310 verschoben.
- **Administrative Quarantäne**—Diese Aktion bewirkt, dass eine Nachricht in die Administrative Quarantäne 310 gegeben wird, falls sie die Bedingungen der Regel erfüllt.
- **Umleiten**—Diese Aktion bewirkt, dass eine Nachricht an eine andere Adresse umgeleitet wird, falls sie die Bedingungen der Regel erfüllt. Nach Auswahl dieser Aktion erscheint ein Eingabefeld *An,* in das Sie die Zieladresse für die Umleitung eingeben können. Umgeleitete Nachrichten werden dem ursprünglichen Empfänger nicht zugestellt; sie werden ohne weiteres an die angegebene Adresse versandt.
- **Kopie**—Diese Aktion bewirkt, dass eine Kopie der Nachricht an eine zusätzliche E-Mail-Adresse versandt wird. Nach Auswahl dieser Aktion erscheint ein Eingabefeld *An,* in das Sie die Zieladresse des zusätzlichen Empfängers eingeben können. Die Aktion ähnelt der Aktion `Umleiten`, jedoch erhalten sowohl der ursprüngliche Empfänger als auch die für die Aktion festgelegte Adresse je eine Kopie der Nachricht. Um Kopien einer Nachricht an mehrere zusätzliche Empfänger zu senden, müssen Sie für jede Adresse eine gesonderte Aktion anlegen.
- **Hinweis senden (Warnung)**—Diese Aktion bewirkt, dass ein Hinweis oder eine Warnung per E-Mail an einen bestimmten Empfänger versandt wird, sobald eine Nachricht die Bedingungen der Regel erfüllt. Nach Auswahl dieser Aktion erscheinen weitere Eingabefelder, in denen Sie *Empfänger (An), Absender (Von), Betreff* und *Nachrichtentext* (den Inhalt der Nachricht) festlegen können. Sie können mithilfe mehrere Makros verschiedene Daten dynamisch und automatisch in die Nachricht einfügen. Findet SecurityGateway ein Makro im Nachrichtentext, so wird das Makro durch den entsprechenden Inhalt ersetzt. Folgende Makros stehen Ihnen zur Verfügung:

  $SENDER$—Dieses Makro wird durch die Adresse aus dem SMTP-Befehl `MAIL From` ersetzt; diese Adresse wird der Nachricht entnommen, die die Bedingungen der Regel erfüllt hat. Ein Beispiel hierzu: "sender@example.net".

  $SENDERMAILBOX$—Dieses Makro wird nur durch den Postfachnamen aus der E-Mail-Adresse ersetzt, die im SMTP-Befehl `MAIL From` übergeben wurde. Bei der Adresse "absender@example.net" ist dies "absender".

  $SENDERDOMAIN$—Dieses Makro wird nur durch den Domänennamen aus der E-Mail-Adresse ersetzt, die im SMTP-Befehl `MAIL From`

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

übergeben wurde. Bei der Adresse "absender@example.net" ist dies "example.net".

$RECIPIENT$—Dieses Makro wird ersetzt durch die Adresse aus dem SMTP-Befehl `RCPT To` ersetzt, der für die Nachricht übermittelt wurde, die die Bedingungen der Regel erfüllt. Ein Beispiel hierzu: "empfaenger@example.com".

$RECIPIENTMAILBOX$—Dieses Makro wird nur durch den Postfachnamen aus der E-Mail-Adresse ersetzt, die im SMTP-Befehl `RCPT To` übermittelt wurde. Bei der Adresse "empfaenger@example.com" ist dies "empfaenger".

$RECIPIENTDOMAIN$—Dieses Makro wird nur durch den Domänennamen aus der E-Mail-Adresse ersetzt, die im SMTP-Befehl `RCPT To` übermittelt wurde. Bei der Adresse "empfaenger@example.com" ist dies "example.com"

$SUBJECT$—Dieses Makro wird ersetzt durch den Inhalt der Betreffzeile der Nachricht, die die Bedingungen der Regel erfüllt hat.

$MESSAGEID$—Dieses Makro wird ersetzt durch den Inhalt der Kopfzeile `Message-ID` (Nachrichten-ID) der Nachricht.

$DATESTAMP$—Dieses Makro wird ersetzt durch das `Datum` der Nachricht.

$CURRENTTIME$—Dieses Makro wird ersetzt durch die Zeit, zu der SecurityGateway die Hinweisnachricht erstellt.

$HELONAME$—Dieses Makro wird durch den Domänennamen ersetzt, der im Befehl HELO während des SMTP-Protokolldialogs für die Nachricht übermittelt wurde, die die Bedingungen der Regel erfüllt.

- **Punkte der Nachrichtenbewertung hinzurechnen**—Diese Aktion bewirkt, dass eine bestimmte Punktzahl der Nachrichtenbewertung hinzugerechnet wird, falls eine Nachricht die Bedingungen dieser Regel erfüllt.

- **Senden als registrierte E-Mail-Nachricht (RMail)**—Diese Aktion bewirkt, dass für Nachrichten, die die Bedingungen der Regel erfüllen, die Leistungsmerkmale für registrierte E-Mail-Nachrichten (RMail) genutzt werden.

  Verschlüsseln—Diese Option bewirkt, dass die Nachricht verschlüsselt wird.

  Sendungs- und Zustellungsverfolgung (Track & Prove)—Diese Option bewirkt, dass das Leistungsmerkmal Sendungs- und Zustellungsverfolgung ("Track & Prove") von RMail genutzt wird.

  E-Signatur—Diese Option bewirkt, dass das Leistungsmerkmale E-Signatur von RMail zur elektronischen Signatur von Dokumenten genutzt wird.

- **Nachricht für REQUIRETLS kennzeichnen**—Diese Aktion bewirkt, dass RequireTLS 126 für die Nachricht anwendbar ist.

- **Als sichere Web-Nachricht senden**—Diese Aktion bewirkt, dass die Nachricht nicht über den normalen Zustellweg für E-Mail-Nachrichten sondern über das Webportal für Sichere Nachrichten 112 versandt wird.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Reguläre Ausdrücke

Die Bedingungen für die Regeln[254] zur Verhinderung von Datendiebstahl unterstützen auch die Vergleichs-Methode "`stimmt mit Regulärem Ausdruck überein`". Reguläre Ausdrücke (nach der englischen Bezeichnung *Regular Expressions* auch kurz als "regexp" bezeichnet) sind ein vielseitiges System, mit dessen Hilfe Sie nicht nur nach bestimmten Texten, Zeichenketten und Strings, sondern auch nach Textmustern suchen können. Ein Textmuster mit Regulären Ausdrücken besteht aus einer Folge bestimmter besonderer Zeichen, die *Metazeichen* genannt werden, und alphanumerischer Textzeichen, die auch "*terminale Zeichen* oder *gewöhnliche Zeichen*" genannt werden (etwa abc, 123 usw.). Mithilfe des Textmusters wird dann nach Übereinstimmungen in Texten gesucht — und das Ergebnis der Suche kann positiv oder negativ sein.

Die Implementation der Regulären Ausdrücke in SecurityGateway nutzt die Bibliothek PERL Compatible Regular Expression (PCRE). Sie erhalten nähere Informationen über diese Implementation der Regulären Ausdrücke unter http://www.pcre.org/ und http://perldoc.perl.org/perlre.html.

Eine umfassende Darstellung der Regulären Ausdrücke bietet *Reguläre Ausdrücke (3. Auflage 2007)*, erschienen bei O'Reilly Media, Inc. Die englische Originalfassung *Mastering Regular Expressions, Third Edition*, ist ebenfalls bei O'Reilly Media, Inc. erschienen.

Metazeichen

Metazeichen sind besondere Zeichen, die innerhalb Regulärer Ausdrücke bestimmte Funktionen erfüllen. Das System der Regulären Ausdrücke, das in SecurityGateway implementiert ist, gestattet die Verwendung folgender Metazeichen:

```
\ | () [] ^ $ * + ? .
```

Metazeichen	Beschreibung
\	Wird der *Backslash* ("\" oder "umgekehrter Schrägstrich") vor ein Metazeichen gesetzt, so wird das folgende Metazeichen maskiert, also als gewöhnliches Zeichen behandelt. Dies ist nötig, wenn der Reguläre Ausdruck nach einem der besonderen Zeichen suchen soll, die sonst als Metazeichen verwendet werden. Beispielsweise muss ein Ausdruck, der nach dem Pluszeichen ("+") suchen soll, dafür die Zeichenkette "\+" enthalten.
|	Das *Alternativzeichen* (auch "Oder-Zeichen" oder "senkrechter Strich" genannt) wird verwendet, wenn entweder die Zeichenkette vor oder nach dem Oder-Zeichen mit dem zu durchsuchenden

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

	Text übereinstimmen soll. Der Reguläre Ausdruck "abc|xyz" sucht beispielsweise nach dem Vorkommen der Zeichenketten "abc" oder "xyz" in einem Text.
[...]	Eine von eckigen Klammern ("[" und "]") umschlossene Zeichenkette bedeutet, dass jedes beliebige Zeichen in der Kette mit dem zu durchsuchenden Text übereinstimmen soll. Ein Bindestrich ("-") zwischen den Zeichen in Klammern definiert eine Zeichenreihe. Wird beispielsweise die Zeichenkette "abc" mit dem Regulären Ausdruck "[a-z]" durchsucht, dann ergeben sich drei Treffer: "*a*", "*b*" und "*c*". Lautet statt dessen der Suchausdruck "[az]", so ergibt sich nur ein Treffer: "*a*".
^	Das sog. "Caret" bezeichnet einen Zeilenanfang. In der Zeichenkette "abc ab a" ergibt der Suchausdruck "^a" einen Treffer, und zwar das erste Zeichen der durchsuchten Zeichenkette. Der Ausdruck "^ab" ergibt ebenfalls einen Treffer, und zwar die *ersten beiden* Zeichen in der durchsuchten Zeichenkette.
[^...]	Folgt das Caret ("^") direkt auf eine öffnende eckige Klammer ("["), so erfüllt es einen anderen Zweck. Es legt fest, dass die in der Klammer folgenden Zeichen keinen Treffer in der zu durchsuchenden Zeichenkette ergeben dürfen. Der Ausdruck "[^0-9]" bedeutet beispielsweise, dass das zu suchende Zeichen keine Ziffer sein darf.
(...)	Die runden Klammern beeinflussen die Reihenfolge, in der die Muster ausgewertet werden, und dient außerdem als *getaggtes* Suchmuster, das in Ausdrücken zum Suchen und Ersetzen verwendet werden kann. Die Ergebnisse einer Suche durch einen Regulären Ausdruck werden zwischengespeichert und können in der Anweisung zum *Ersetzen* verwendet werden, um einen neuen Ausdruck zu bilden. In der Anweisung zum *Ersetzen* können die Zeichen "&" oder "\0" enthalten sein; diese werden durch die Zeichenketten ersetzt, die während der Suche durch den Regulären Ausdruck gefunden wurden. Findet der Suchausdruck "a(bcd)e" beispielsweise eine Zeichenkette, so ersetzen die Ausdrücke "123-&-123" oder "123-\0-123" den gefundenen Text durch "123-abcde-123". In ähnlicher Weise können die besonderen Zeichen

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

	"\1", "\2", "\3" u.s.w. in dem Ausdruck verwendet werden, der Zeichenketten *ersetzen* soll. Diese Zeichen werden nur durch die unmittelbaren Ergebnisse des Suchmusters, nicht aber durch die vollständige gefundene Zeichenkette ersetzt. Die Zahl nach dem Backslash legt bei Regulären Ausdrücken mit mehr als einem Suchmuster fest, auf welches Suchmuster verwiesen werden soll. Lautet der Suchausdruck beispielsweise "(123)(456)", und lautet der Ausdruck zum Ersetzen "a-\2-b-\1", so wird eine gefundene Zeichenkette durch "a-456-b-123" ersetzt, wohingegen ein Ausdruck zum Ersetzen "a-\0-b" durch "a-123456-b" ersetzt wird.
$	Das Dollarzeichen ("$") bezeichnet ein Zeilenende. In der Zeichenkette "13 321 123" ergibt der Ausdruck "3$" einen Treffer, und zwar das letzte Zeichen der Kette. Der Ausdruck "123$" ergibt ebenfalls einen Treffer, und zwar die *letzten drei* Zeichen in der Zeichenkette.
*	Das Zeichen Stern ("*") bestimmt, dass das ihm vorausgehende Zeichen mehrmals hintereinander vorkommen darf, aber nicht vorkommen muss. Daher ergibt "1*abc" für die Zeichenketten "111abc" und "abc" jeweils einen Treffer.
+	Etwas anders als der Stern, bestimmt das Pluszeichen "+", dass das ihm vorausgehende Zeichen mindestens einmal in der Zeichenkette vorkommen muss, aber auch mehrfach vorkommen darf. Daher ergibt "1+abc" einen Treffer bei der Zeichenkette "111abc", nicht aber bei "abc".
?	Das Fragezeichen ("?") bestimmt, dass das ihm vorausgehende Zeichen mehrmals vorkommen darf, aber nicht vorkommen muss. Daher ergibt "1*abc" einen Treffer für den Text "abc" sowie einen Treffer für die Zeichenkette "1abc" aus dem Text "111abc".
.	Das Metazeichen Punkt (".") ergibt einen Treffer für jedes beliebige andere Zeichen. Daher ergibt ". +abc" einen Treffer für "123456abc", "a.c" ergibt einen Treffer für "aac", "abc", "acc" usw.

4.6.1 Medizinische Begriffe

Sie können mithilfe der hier beschriebenen Optionen zur Verhinderung von Datendiebstahl[238] Nachrichten nach medizinischen Begriffen durchsuchen und in Abhängigkeit von bestimmten Bewertungskriterien Aktionen für diese Nachrichten ausführen. Es steht Ihnen eine Liste von annähernd 2000

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

medizinischen Begriffen zur Verfügung, die bereits erfasst sind. Sie können dieser Liste nach Bedarf benutzerdefinierte Begriffe hinzufügen und solche auch aus ihr entfernen. Jedem Begriff ist ein Punktwert als Bewertung zugewiesen. Die Nachrichten werden nach diesen Begriffen durchsucht, und die Bewertungen aller jeweils gefundenen Begriffe werden zusammengezählt. Ergibt sich für eine Nachricht eine Bewertung über den angegebenen Schwellwerten, so werden die den Schwellwerten zugeordneten Aktionen ausgeführt. Sie können Nachrichten wahlweise in Quarantäne geben oder sie mithilfe des Verschlüsselungsdienstes RMail 235 verarbeiten lassen. Sie können bestimmen, ob eingehende und lokale Nachrichten von der Suche nach medizinischen Begriffen ausgenommen werden.

Konfiguration

Nachrichten beim Versand nach medizinischen Begriffen durchsuchen
Um Nachrichten nach medizinischen Begriffen zu durchsuchen, aktivieren Sie diese Option. Jedem Begriff ist ein Punktwert zur Bewertung zugeordnet. Die Summe der Punktwerte aller Begriffe, die in einer Nachricht gefunden werden, bestimmt, ob eine Aktion für die Nachricht ausgeführt wird und welche Aktion dies ist.

Nachrichten in Administrative Quarantäne geben ab einer Bewertung von [xx]
Ist diese Option aktiv, und erreicht die Summe der Punktwerte aller medizinischen Begriffe in einer Nachricht mindestens diesen Wert, dann wird die Nachricht in die administrative Quarantäne 310 verschoben.

Verschlüsselung über RMail nutzen für Nachrichten ab einer Bewertung von [xx]
Ist diese Option aktiv, und erreicht die Summe der Punktwerte aller medizinischen Begriffe in einer Nachricht mindestens diesen Wert, dann werden die Optionen für den Verschlüsselungsdienstes RMail 235 auf die Nachricht angewandt.

Eingehende Nachrichten nicht durchsuchen (Empfänger ist lokaler Benutzer, und Absender ist kein lokaler Benutzer derselben Domäne)
Diese Option schließt eingehende Nachrichten von der Suche nach medizinischen Begriffen aus, falls der Empfänger ein lokaler Benutzer und der Absender kein lokaler Benutzer derselben Domäne sind.

Interne Nachrichten nicht durchsuchen (Absender und Empfänger sind lokale Benutzer derselben Domäne)
Diese Option schließt eingehende Nachrichten von der Suche nach medizinischen Begriffen aus, falls der Absender und Empfänger lokale Benutzer derselben Domäne sind.

Derzeit definierte Begriffe

In dieser Liste sind alle als medizinische Begriffe definierten Begriffe und die zugehörigen Punktwerte zur Bewertung erfasst. Bei der Prüfung einer Nachricht auf medizinische Begriffe werden die Punktwerte aller hier erfassten und in der Nachricht gefundenen Begriffe zusammengezählt. Hieraus ergibt sich die Gesamtbewertung. Falls diese Bewertung einen der oben konfigurierten Schwellwerte erreicht oder übersteigt, werden die zugehörigen Aktionen ausgeführt.

Hinzufügen und Bearbeiten von Begriffen
Um einen neuen Begriff in die Liste aufzunehmen, klicken Sie auf **Neu**. Um einen bestehenden Begriff zu bearbeiten, klicken Sie auf **Bearbeiten**, und nehmen Sie dann die gewünschten Änderungen an dem Begriff oder seiner Bewertung vor.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Nachdem Sie die Änderungen vorgenommen haben, klicken Sie auf **Speichern und Beenden**.

Löschen von Begriffen
Um einen Begriff oder mehrere Begriffe aus der Liste zu löschen, wählen Sie die gewünschten Begriffe aus, und klicken Sie dann auf **Löschen**. Es erscheint eine Sicherheitsabfrage, die Sie mit **Ja** beantworten müssen, um die Löschung durchzuführen.

Import einer Liste von medizinischen Begriffen
Um eine Liste medizinischer Begriffe zu importieren, gehen Sie folgendermaßen vor:

1. Erstellen Sie eine Datei im Format "Nur Text". Setzen Sie folgendes auf die erste Zeile: `"Term","Score" ("Begriff","Bewertung")`
2. Setzen Sie danach auf jede Zeile in demselben Format je einen Begriff und den zugehörigen Punktwert. Ein Beispiel hierzu: `"Abacavir","10"`
3. Wenn Sie die Datei fertiggestellt haben, speichern Sie sie mit der Dateiendung ".csv". Ein Beispiel hierzu: `"Medizinische_Begriffe.csv"`
4. Klicken Sie auf der Seite Medizinische Begriffe auf **Import**.
5. Klicken Sie auf **Datei auswählen**, suchen Sie die soeben erstellte Datei auf, und klicken Sie auf **Öffnen**.
6. Falls Sie die derzeit bestehende Liste medizinischer Begriffe ersetzen wollen, aktivieren Sie das Kontrollkästchen der Option **Bestehende Begriffe löschen**. **Achtung: Hierdurch wird die gesamte bestehende Liste der medizinischen Begriffe gelöscht und durch die importierte Liste ersetzt.** Falls Sie die aus der Datei importierten Begriffe der bestehenden Liste medizinischer Begriffe hinzufügen wollen, lassen Sie diese Option deaktiviert.
7. Klicken Sie auf **Begriffe importieren**.
8. Klicken Sie auf **Schließen**.

Export der Liste von medizinischen Begriffen
Um die derzeit bestehende Liste von medizinischen Begriffen zu exportieren, klicken Sie auf **Export**, wählen Sie einen Speicherort aus, und klicken Sie dann auf **Speichern**.

To export the list of currently defined terms, click **Export**, choose a location, and click **Save**.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Optionen dieser Domäne für die medizinischen Begriffe anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

4.7 Filter

4.7.1 Inhalte der Nachrichten

Mithilfe dieser Seite können Sie die Regeln für die Filterung von Nachrichten-Inhalten verwalten. Sie können von hier aus die Regeln erstellen, bearbeiten und löschen, und Sie können bestehende Regeln mithilfe eines Kontrollkästchens schnell aktivieren und deaktivieren. Die Filterregeln legen die Kriterien fest, anhand derer SecurityGateway jede Nachricht prüft, die verarbeitet wird. Stimmt eine Nachricht mit einer Regel überein, so können eine Reihe von Aktionen durchgeführt werden. Sie können Regeln erstellen, die nach bestimmten Kopfzeilen, Absendern und Empfängern, sowie bestimmtem Text in einer Kopfzeile oder dem Nachrichtentext suchen oder prüfen, wie groß eine Nachricht ist. Daneben stehen zahlreiche weitere Kriterien zur Verfügung. Stimmt eine Nachricht mit den Kriterien einer Regel überein, so kann die Regel unter anderem bewirken, dass die Nachricht abgewiesen, gelöscht, in Quarantäne gegeben, kopiert oder an eine andere Adresse umgeleitet wird.

Die Liste der Regeln des Inhaltsfilters enthält drei Spalten: Aktiviert, Beschreibung und Vorschau. Die Spalte Aktiviert enthält für jeden Eintrag ein eigenes Kontrollkästchen, mit dessen Hilfe Sie die Regel schnell aktivieren und deaktivieren können. In der Spalte Beschreibung erscheint der *Name der Regel*, den Sie während der Erstellung der Regel festgelegt haben. Die Spalte Vorschau enthält für jede Regel ein Symbol, mit dessen Hilfe Sie sich einen Tooltipp zu der zugehörigen Regel anzeigen lassen können. Lassen Sie dazu die Maus über dem Symbol stehen. Der Tooltipp zeigt das Sieve-Skript 284, das nach der Erstellung der Regel über den Editor für Regeln des Inhaltsfilters 252 zur Umsetzung der Regel angelegt wurde.

Die Symbolleiste am oberen Seitenrand enthält die folgenden vier Optionen:

Neu
Um eine neue Regel zu erstellen, klicken Sie auf *Neu.* Es öffnet sich der Editor für Regeln des Inhaltsfilters 252, in dem Sie die Regel erstellen können.

Bearbeiten
Um eine Regel zu bearbeiten, wählen Sie die Regel in der Liste aus, und klicken Sie in der Symbolleiste auf *Bearbeiten.* Es öffnet sich der Editor für Regeln des Inhaltsfilters 252, und die Regel wird zur Bearbeitung geladen. Sie können eine Regel stattdessen auch durch Doppelklick zur Bearbeitung öffnen.

Löschen
Um eine Regel oder mehrere Regeln zu löschen, wählen Sie die gewünschten Einträge in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie die Einträge wirklich löschen wollen. Sie können mithilfe der Strg-Taste und der Hochschalttaste mehrere Einträge auswählen.

Für Domäne:
Mithilfe des Auswahlmenüs *Für Domäne:* bestimmen Sie, welche Regeln in der Liste angezeigt werden. Sie können sich Globale Regeln anzeigen lassen, die auf alle Domänen wirken, oder nur die Regeln einer bestimmten Domäne.

Editor für Regeln des Inhaltsfilters

Mithilfe des Editors für Regeln des Inhaltsfilters können Sie neue Regeln erstellen oder bestehende Regeln bearbeiten. Um eine neue Regel zu erstellen, klicken Sie in

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

der Symbolleiste für die Regeln des Inhaltsfilters auf *Neu*. Gehen Sie dann die Optionen, die der Editor bietet, der Reihe nach durch. Sobald Sie alle Daten eingetragen haben, klicken Sie auf *Speichern und Beenden*, um die neue Regel anzulegen.

Diese Regel ist aktiv
Zur Erstellung einer neuen Regel muss dieses Kontrollkästchen aktiv sein. Sie können bestehende Regeln deaktivieren, indem Sie den Haken aus dem zugehörigen Kontrollkästchen entfernen. SecurityGateway lässt deaktivierte Regeln bei der Prüfung von Nachrichten außer Betracht. Die Option entspricht der Spalte *Aktiviert* in der Übersicht über die Regeln des Inhaltsfilters.

Für Domäne:
In dieser Option legen Sie fest, auf welche Domänen die Regel angewendet wird. Wird hier "--Global--" ausgewählt, so wirkt die Regel auf Nachrichten an alle und von allen SecurityGateway-Domänen. Wird hier eine bestimmte Domäne ausgewählt, so wirkt die Regel nur auf Nachrichten an alle und von allen Nachrichten dieser Domäne.

Name der Regel:
Tragen Sie in dieses Feld einen Titel oder einen kurzen Beschreibungstext für Ihre Regel ein. Diese Option entspricht der Spalte *Beschreibung* in der Übersicht über die Regeln des Inhaltsfilters.

Regel anwenden, falls:

alle Bedingungen erfüllt sind (AND)
Wählen Sie diese Option aus, falls eine Nachricht nur dann einen Treffer in dieser Regel auslösen soll, falls sie ALLE Bedingungen erfüllt, die weiter unten angegeben werden. Die Option bewirkt, dass die Bedingungen logisch mit "UND" verknüpft werden, etwa nach dem Muster "falls Bedingung A erfüllt ist UND Bedingung B erfüllt ist, dann die angegebene Aktion ausführen".

eine beliebige Bedingung erfüllt ist (OR)
Wählen Sie diese Option aus, falls eine Nachricht dann einen Treffer in dieser Regel auslösen soll, falls sie EINE BELIEBIGE der Bedingungen erfüllt, die weiter unten angegeben werden. Die Option bewirkt, dass die Bedingungen logisch mit "ODER" verknüpft werden, etwa nach dem Muster "falls Bedingung A erfüllt ist ODER Bedingung B erfüllt ist, dann die angegebene Aktion ausführen".

Bedingungen:
In diesem Abschnitt erscheinen alle Bedingungen, die Sie für diese Regel festgelegt haben, verbunden mit den Aktionen, die durchgeführt werden soll, falls eine Nachricht mit den Bedingungen der Regel übereinstimmt. Sie können eine Bedingung durch Anklicken in diesem Bereich bearbeiten. Sie können eine Bedingung durch Anklicken der Verknüpfung "(Entfernen)" neben der Bedingung löschen. Um der Regel eine neue Bedingung hinzuzufügen, klicken Sie unterhalb dieses Bereichs auf die Verknüpfung "*Klicken Sie hier, um eine Bedingung für diese Regel hinzuzufügen.*".

Klicken Sie hier, um eine Bedingung für diese Regel hinzuzufügen
Klicken Sie unterhalb des Abschnitts Bedingungen auf die Verknüpfung "*Klicken Sie hier, um eine Bedingung für diese Regel hinzuzufügen.*", um der Regel eine Bedingung hinzuzufügen. Nachdem Sie die Bedingung hinzugefügt haben, können Sie weitere Bedingungen hinzufügen, indem Sie erneut auf die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Verknüpfung klicken. Die einzelnen Arten von Bedingungen sind im Abschnitt Bedingungen für die Regeln 254 weiter unten näher beschrieben.

Aktion:
Aus diesem Auswahlmenü wählen Sie die Aktion, die durchgeführt werden soll, falls eine Nachricht mit den Bedingungen der Regel übereinstimmt. Falls für eine Aktion weitere Angaben erforderlich sind, erscheint unterhalb dieses Auswahlmenüs ein entsprechendes Eingabefeld, in dem Sie die nötigen Angaben machen können. Die einzelnen Arten von Aktionen sind im Abschnitt Aktionen 258 weiter unten näher beschrieben. Nachdem Sie alle Bedingungen für die Regel festgelegt und eine Aktion ausgewählt haben, klicken Sie auf *Speichern und Beenden*, um den Editor zu verlassen und die neue Regel in die Liste der Regel einzutragen.

Bedingungen für die Regeln

Um einer Regel eine Bedingung hinzuzufügen, klicken Sie auf die Verknüpfung "*Klicken Sie hier, um eine Bedingung für diese Regel hinzuzufügen.*". Es öffnet sich der Dialog *Bedingungen für die Regel*. Um eine solche Bedingung zu erstellen, müssen Sie zunächst das Nachrichten-Attribut oder Element bestimmen, anhand dessen Sie die Prüfung in der Bedingung durchführen wollen. Dann müssen Sie festlegen, wie ein Vergleich mit diesem Element oder eine Prüfung des Elements durchgeführt werden soll: Es kann geprüft werden, ob das Element einen Text enthält oder einem Text genau entspricht, ob eine Kopfzeile besteht, und vieles mehr. Zur Verfügung stehen mehrere Elemente, die geprüft werden können, und verschiedene Vergleichsmethoden. Nachdem Sie das Element ausgewählt, die Vergleichsmethode festgelegt und etwa nötige Informationen eingegeben haben, klicken Sie auf *Speichern und Beenden*, um die Bedingung Ihrer Regel hinzuzufügen.

Zu vergleichendes Element:
Diese Liste enthält folgende Elemente, die Sie in einer Nachricht vergleichen und prüfen können:

- **MAIL (Von)**—Diese Prüfung betrifft den Inhalt des SMTP-Befehls "`MAIL From`". Er bezeichnet den Absender der Nachricht; der Inhalt des Befehls muss aber nicht zwangsläufig mit dem Inhalt der Absender-Kopfzeile `From` in der Nachricht selbst übereinstimmen. Manchmal enthält die Kopfzeile `From` zusätzliche oder abweichende Informationen. Zusätzlich zu den neun üblichen Vergleichsmethoden (siehe unten) stehen noch die Prüfungen "`ist ein lokaler Benutzer`" und "`ist kein lokaler Benutzer`" zur Verfügung.
- **RCPT (An)**—Diese Prüfung betrifft den Inhalt des SMTP-Befehls "`RCPT To`". Er bezeichnet den Empfänger der Nachricht; der Inhalt des Befehls muss aber nicht zwangsläufig mit dem Inhalt der Adressaten-Kopfzeile `To` in der Nachricht selbst übereinstimmen. Manchmal enthält die Kopfzeile `To` zusätzliche oder abweichende Informationen. Zusätzlich zu den neun üblichen Vergleichsmethoden (siehe unten) stehen noch die Prüfungen "`ist ein lokaler Benutzer`" und "`ist kein lokaler Benutzer`" zur Verfügung.
- **MAIL (Von) und RCPT (An)**—Dieses Element prüft die Parameter der SMTP-Befehle "`MAIL From`" und "`RCPT To`", um zu bestimmen, ob es sich bei der ausgewerteten Nachricht um eine eingehende, abgehende oder interne Nachricht handelt (siehe "*Weitere Vergleichs-Methoden*" weiter unten).
- **IP**—Wählen Sie dieses Element, um einen Vergleich anhand der IP-Adresse

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

des übermittelnden Servers oder Clients durchzuführen.

- **Kopfzeile**—Wählen Sie dieses Element, falls Sie eine Kopfzeile angeben möchten, anhand derer Sie einen Vergleich vornehmen wollen. Nachdem Sie dieses Element gewählt haben, erscheint das Eingabefeld *Name der Kopfzeile*. In dieses Feld müssen Sie die Kopfzeile eintragen, anhand derer Sie den Vergleich vornehmen wollen. Zusätzlich zu den neun üblichen Vergleichsmethoden kann dieses Element auch noch anhand der Vergleichs-Methoden "`Kopfzeile existiert`" und "`Kopfzeile existiert nicht`" verglichen werden. **Beachte:** Im Feld *Name der Kopfzeile* dürfen Sie den Namen der Kopfzeile nicht mit einem Doppelpunkt abschließen. Sie müssen beispielsweise für einen Vergleich mit der Absender-Kopfzeile From als *Name der Kopfzeile* "`From`" eintragen, nicht aber "`From:`".
- **Betreff**—Dieses Element ist die Kopfzeile `Subject` (Betreff) der Nachrichten. Mithilfe dieses Elements können Sie Vergleiche mit dem Betreff der Nachrichten durchführen.
- **Nachrichtentext**—Wählen Sie dieses Element, um einen Vergleich mit dem Inhalt des Nachrichtentextes durchzuführen.
- **Nachrichtentext oder Betreff**—Mithilfe dieses Elements können Sie eine Regel erstellen, die dann zu einem Treffer führt, wenn entweder der *Nachrichtentext* oder der *Betreff* der Nachricht den Kriterien der Regel entspricht. Dieses Element soll die Erstellung der Regeln vereinfachen, weil es im Ergebnis dieselbe Wirkung hat wie eine Regel, in der zwei getrennte Elemente mit "ODER" verknüpft sind, von denen eine den *Nachrichtentext* und das andere die *Betreffzeile* der Nachricht nach demselben Text durchsucht.

Vergleichs-Methode:
Die folgende Liste enthält die Methoden, mit deren Hilfe Sie Vergleiche und Prüfungen für das Element durchführen können, das Sie in der Option *Zu vergleichendes Element* weiter oben ausgewählt haben. Für alle Elemente stehen verschiedene Vergleichsmethoden zur Verfügung, die sich nur in Bezug auf ein Element unterscheiden. Für das Elemente `Mail (Von) und RCPT (An)` bestehen besondere Vergleichsmethoden, und für `Mail (Von)`, `RCPT (An)` und `Kopfzeile` stehen jeweils weitere Vergleichsmethoden zur Verfügung.

Übliche Vergleichs-Methoden:
Jede der folgenden Vergleichsmethoden oder Operatoren vergleicht das oben in der Option *Zu vergleichendes Element* angegebene Element mit dem *Suchausdruck,* den Sie in das Eingabefeld unterhalb des Feldes *Vergleichs-Methode* eintragen müssen. Alle nachfolgend aufgeführten Vergleichs-Methoden stehen für alle zu vergleichenden Elemente, jedoch nicht für `Mail (Von) und RCPT (An)` zur Verfügung. Für `Mail (Von) und RCPT (An)` bestehen besondere Vergleichsmethoden-

- **enthält**—Diese Methode ergibt einen Treffer (Ergebnis "wahr"), falls der *Suchausdruck* ein Teil des *zu vergleichenden Elements* ist, das oben ausgewählt wurde. Wählen Sie beispielsweise `MAIL (Von)` als zu vergleichendes Element, und wählen Sie dann `enthält` als Vergleichs-Methode und "example.com" als *Suchausdruck*, so erfüllt jede Nachricht von einer Adresse, die "example.com" enthält, die Bedingung.
- **enthält nicht**—Diese Methode ergibt einen Treffer (Ergebnis "wahr"), falls der *Suchausdruck* kein Teil des *zu vergleichenden Elements* ist, das oben ausgewählt wurde. Wählen Sie beispielsweise `MAIL (Von)` als zu

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

vergleichendes Element, und wählen Sie dann `enthält nicht` als Vergleichs-Methode und "example.com" als *Suchausdruck*, so erfüllt jede Nachricht die Bedingung, außer Nachrichten von Adressen, die "example.com" enthalten.

- **enthält Wort/Wörter**—Diese Methode arbeitet ähnlich wie "enthält". Sie führt aber nur dann zu einem Treffer, wenn die zu suchende Zeichenkette zwischen zwei Wortbegrenzungsankern eingeschlossen ist. Hierdurch wird vermieden, dass manuell ein Regulärer Ausdruck nach dem Muster `\b(Wort1|Wort2|Wort3)\b` erstellt werden muss. Ein Beispiel hierzu: Eine Regel, die nach Nachrichtentexten sucht, die das *Wort* "Katze" *enthalten*, führt nur für solche Nachrichten zu einem Treffer, die das eigenständige Wort "Katze" enthalten. Sie führt dann nicht zu einem Treffer, wenn der Nachrichtentext Wörter wie *Katzenwels* oder *Schleichkatze* enthält.
- **enthält nicht Wort**—Diese Methode arbeitet ähnlich wie "enthält nicht". Sie führt aber nur dann zu einem Treffer, wenn die auszuschließende Zeichenkette zwischen zwei Wortbegrenzungsankern eingeschlossen ist. Ein Beispiel hierzu: Eine Regel, die nach Nachrichtentexten sucht, die das *Wort* "Katze" *nicht enthalten*, führt nur für solche Nachrichten zu einem Treffer, die das eigenständige Wort "Katze" nicht enthalten. Sie führt dann nicht zu einem Treffer, wenn der Nachrichtentext Wörter wie *Katzenwels* oder *Schleichkatze* enthält.
- **entspricht**—Diese Methode arbeitet ähnlich wie *enthält* weiter oben, der *Suchausdruck* muss aber mit dem Inhalt des *zu vergleichenden Elements* genau übereinstimmen; eine teilweise Übereinstimmung reicht nicht aus. Wählen Sie beispielsweise `IP` als zu vergleichendes Element, und wählen Sie dann `entspricht` als Vergleichs-Methode und "192.168.0.1" als *Suchausdruck*, so erfüllen nur Nachrichten die Bedingung, die von genau der angegebenen IP-Adresse stammen.
- **entspricht nicht**—Diese Methode arbeitet spiegelverkehrt zur vorherigen Methode. Entspricht der Inhalt des *zu vergleichenden Elements* nicht genau dem *Suchausdruck*, so ist die Bedingung erfüllt. Wählen Sie beispielsweise `IP` als zu vergleichendes Element, und wählen Sie dann `entspricht nicht` als Vergleichs-Methode und "192.168.0.1" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, außer den Nachrichten, die von genau der angegebenen IP-Adresse stammen.
- **beginnt mit**—Diese Methode ergibt einen Treffer, falls der Inhalt des *zu vergleichenden Elements* mit dem *Suchausdruck* beginnt. Wählen Sie beispielsweise `Betreff` als zu vergleichendes Element, und wählen Sie , und wählen Sie dann `beginnt mit` als Vergleichs-Methode und "[AlleMitarbeiter]" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, deren Betreffzeile mit dem Text "[AlleMitarbeiter]" beginnt.
- **beginnt nicht mit**—Diese Methode arbeitet spiegelverkehrt zur vorherigen Methode. Beginnt der Inhalt des *zu vergleichenden Elements* nicht mit dem *Suchausdruck*, so ist die Bedingung erfüllt. Wählen Sie beispielsweise `Betreff` als zu vergleichendes Element, und wählen Sie dann `beginnt nicht mit` als Vergleichs-Methode und "[AlleMitarbeiter]" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, außer denen, deren Betreffzeile mit dem Text "[AlleMitarbeiter]" beginnt.
- **endet auf**—Diese Methode ergibt einen Treffer, falls der Inhalt des *zu vergleichenden Elements* mit dem *Suchausdruck* endet. Wählen Sie beispielsweise `RCPT (An)` als zu vergleichendes Element, und wählen Sie

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

dann `endet auf` als Vergleichs-Methode und ".cn" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, die an einen Empfänger gerichtet sind, dessen Adresse auf ".cn" endet.

- **endet nicht auf**—Diese Methode ergibt einen Treffer, falls der Inhalt des *zu vergleichenden Elements* nicht mit dem *Suchausdruck* endet. Wählen Sie beispielsweise `RCPT (An)` als zu vergleichendes Element, und wählen Sie dann `endet nicht auf` als Vergleichs-Methode und ".cn" als *Suchausdruck*, so erfüllen alle Nachrichten die Bedingung, außer denen, die an einen Empfänger gerichtet sind, dessen Adresse auf ".cn" endet.
- **stimmt mit Regulärem Ausdruck überein**—Wählen Sie diese Option, um für den Vergleich und die Prüfung des *zu vergleichenden Elements* einen **Regulären Ausdruck** zu nutzen.

Weitere Vergleichs-Methoden:

- **ist ein lokaler Benutzer**—Diese Vergleichs-Methode steht nur für die Optionen `MAIL (Von)` und `RCPT (An)` oben zur Verfügung. Bei ihrer Nutzung ist die Bedingung erfüllt, falls die Adresse zu einem lokalen SecurityGateway-Benutzer gehört. Wählen Sie beispielsweise `MAIL (Von)` als das *zu vergleichende Element*, so ist die Bedingung nur bei Nachrichten von lokalen Benutzern erfüllt.
- **ist kein lokaler Benutzer**—Diese Vergleichs-Methode steht nur für die Optionen `MAIL (Von)` und `RCPT (An)` oben zur Verfügung. Bei ihrer Nutzung ist die Bedingung erfüllt, falls die Adresse nicht zu einem lokalen SecurityGateway-Benutzer gehört. Wählen Sie beispielsweise `MAIL (Von)` als das *zu vergleichende Element*, so ist die Bedingung nur bei Nachrichten von externen Benutzern erfüllt, nicht jedoch bei Nachrichten von lokalen Benutzern.
- **Kopfzeile existiert**—Diese Vergleichs-Methode steht nur zur Verfügung, falls Sie oben als *zu vergleichendes Element* die `Kopfzeile` ausgewählt haben. Wählen Sie diese Option, und geben Sie dann den *Namen der Kopfzeile* in das entsprechende Feld ein, so ist die Bedingung nur erfüllt, falls die angegebene Kopfzeile in der Nachricht enthalten ist. Geben Sie beispielsweise "X-Meine-benutzerdefinierte-Kopfzeile" als *Namen der Kopfzeile* ein, so erfüllen alle Nachrichten die Bedingung, die diese Kopfzeile enthalten. Nachrichten ohne die Kopfzeile erfüllen die Bedingung nicht.
- **Kopfzeile existiert nicht**—Diese Vergleichs-Methode steht nur zur Verfügung, falls Sie oben als *zu vergleichendes Element* die `Kopfzeile` ausgewählt haben. Wählen Sie diese Option, und geben Sie dann den *Namen der Kopfzeile* in das entsprechende Feld ein, so ist die Bedingung nur erfüllt, falls die angegebene Kopfzeile in der Nachricht nicht enthalten ist. Geben Sie beispielsweise "X-Meine-benutzerdefinierte-Kopfzeile" als *Namen der Kopfzeile* ein, so erfüllen alle Nachrichten die Bedingung, die diese Kopfzeile nicht enthalten. Nachrichten mit dieser Kopfzeile erfüllen die Bedingung nicht.
- **Nachricht ist/ist nicht [eingehend|abgehend|intern]**—Diese Vergleichs-Methoden sind nur für das Element `MAIL (Von) und RCPT (An)` verfügbar. Es werden die Parameter der SMTP-Befehle "MAIL From" und "RCPT To" dazu verwendet, um zu prüfen, ob eine Nachricht eingehend, abgehend oder intern ist, oder ob eine Nachricht nicht eingehend, nicht abgehend oder nicht intern ist.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Eingehend—Dies sind Nachrichten, die an lokale Benutzer gerichtet sind und nicht von lokalen Benutzern derselben Domäne stammen.

Outbound—Dies sind Nachrichten, die von lokalen Benutzern stammen und nicht an lokale Benutzer derselben Domäne gerichtet sind.

Internal—Dies sind Nachrichten, die von lokalen Benutzern stammen und an lokale Benutzer derselben Domäne gerichtet sind.

Aktionen

Nachdem Sie die Bedingungen für Ihre Regel festgelegt haben, müssen Sie im Editor für die Regeln noch mithilfe des entsprechenden Feldes die *Aktion* festlegen, die der Inhaltsfilter ausführen soll, falls eine Nachricht die Bedingungen der Regel erfüllt. Es stehen sieben Aktionen zur Verfügung:

- **Abweisen**—Diese Aktion bewirkt, dass eine Nachricht abgewiesen wird, falls sie die Bedingungen der Regel erfüllt. Nach Auswahl dieser Option erscheint weiter unten das Eingabefeld *SMTP-Meldung.* In dieses Eingabefeld können Sie einen Text eintragen, der beim Abweisen der Nachricht im SMTP-Protokolldialog übermittelt wird. Tragen Sie beispielsweise "Wir wollen Ihren Spam nicht haben!" in das Feld *SMTP-Meldung* ein, so übermittelt SecurityGateway für Nachrichten, die die Bedingungen der Regel erfüllen, im SMTP-Protokolldialog "`550 Wir wollen Ihren Spam nicht haben!`" und weist die Nachricht ab. Bitte bedenken Sie beim Abfassen dieser Meldung, dass sie allenfalls auch für ausländische Serverbetreiber verständlich sein sollte; es ist daher sinnvoll, immer auch einen englischen Textteil vorzusehen.
- **Verwerfen**—Diese Aktion bewirkt, dass eine Nachricht verworfen wird, falls sie die Bedingungen der Regel erfüllt. Anders als bei der Aktion `Abweisen` wird bei dieser Aktion keine SMTP-Meldung übermittelt, und es wird auch keine Nachricht über einen Zustellfehler versandt. Die Nachricht wird ohne weiteres gelöscht.
- **Quarantäne**—Diese Aktion bewirkt, dass eine Nachricht, die die Bedingungen der Regel erfüllt, in den Quarantäne-Ordner 308 des Benutzers verschoben wird, falls der Empfänger ein lokaler Benutzer ist. Ist der Empfänger ein externer Benutzer, so wird die Nachricht stattdessen in die Administrative Quarantäne 310 verschoben.
- **Administrative Quarantäne**—Diese Aktion bewirkt, dass eine Nachricht in die Administrative Quarantäne 310 gegeben wird, falls sie die Bedingungen der Regel erfüllt.
- **Umleiten**—Diese Aktion bewirkt, dass eine Nachricht an eine andere Adresse umgeleitet wird, falls sie die Bedingungen der Regel erfüllt. Nach Auswahl dieser Aktion erscheint ein Eingabefeld *An,* in das Sie die Zieladresse für die Umleitung eingeben können. Umgeleitete Nachrichten werden dem ursprünglichen Empfänger nicht zugestellt; sie werden ohne weiteres an die angegebene Adresse versandt.
- **Kopie**—Diese Aktion bewirkt, dass eine Kopie der Nachricht an eine zusätzliche E-Mail-Adresse versandt wird. Nach Auswahl dieser Aktion erscheint ein Eingabefeld *An,* in das Sie die Zieladresse des zusätzlichen Empfängers eingeben können. Die Aktion ähnelt der Aktion `Umleiten`, jedoch erhalten sowohl der ursprüngliche Empfänger als auch die für die Aktion festgelegte Adresse je eine Kopie der Nachricht. Um Kopien einer Nachricht

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

an mehrere zusätzliche Empfänger zu senden, müssen Sie für jede Adresse eine gesonderte Aktion anlegen.

- **Hinweis senden (Warnung)**—Diese Aktion bewirkt, dass ein Hinweis oder eine Warnung per E-Mail an einen bestimmten Empfänger versandt wird, sobald eine Nachricht die Bedingungen der Regel erfüllt. Nach Auswahl dieser Aktion erscheinen weitere Eingabefelder, in denen Sie *Empfänger (An), Absender (Von), Betreff* und *Nachrichtentext* (den Inhalt der Nachricht) festlegen können. Sie können mithilfe mehrere Makros verschiedene Daten dynamisch und automatisch in die Nachricht einfügen. Findet SecurityGateway ein Makro im Nachrichtentext, so wird das Makro durch den entsprechenden Inhalt ersetzt. Folgende Makros stehen Ihnen zur Verfügung:

  $SENDER$—Dieses Makro wird durch die Adresse aus dem SMTP-Befehl `MAIL From` ersetzt; diese Adresse wird der Nachricht entnommen, die die Bedingungen der Regel erfüllt hat. Ein Beispiel hierzu: "sender@example.net".

  $SENDERMAILBOX$—Dieses Makro wird nur durch den Postfachnamen aus der E-Mail-Adresse ersetzt, die im SMTP-Befehl `MAIL From` übergeben wurde. Bei der Adresse "absender@example.net" ist dies "absender".

  $SENDERDOMAIN$—Dieses Makro wird nur durch den Domänennamen aus der E-Mail-Adresse ersetzt, die im SMTP-Befehl `MAIL From` übergeben wurde. Bei der Adresse "absender@example.net" ist dies "example.net".

  $RECIPIENT$—Dieses Makro wird ersetzt durch die Adresse aus dem SMTP-Befehl `RCPT To` ersetzt, der für die Nachricht übermittelt wurde, die die Bedingungen der Regel erfüllt. Ein Beispiel hierzu: "empfaenger@example.com".

  $RECIPIENTMAILBOX$—Dieses Makro wird nur durch den Postfachnamen aus der E-Mail-Adresse ersetzt, die im SMTP-Befehl `RCPT To` übermittelt wurde. Bei der Adresse "empfaenger@example.com" ist dies "empfaenger".

  $RECIPIENTDOMAIN$—Dieses Makro wird nur durch den Domänennamen aus der E-Mail-Adresse ersetzt, die im SMTP-Befehl `RCPT To` übermittelt wurde. Bei der Adresse "empfaenger@example.com" ist dies "example.com"

  $SUBJECT$—Dieses Makro wird ersetzt durch den Inhalt der Betreffzeile der Nachricht, die die Bedingungen der Regel erfüllt hat.

  $MESSAGEID$—Dieses Makro wird ersetzt durch den Inhalt der Kopfzeile `Message-ID` (Nachrichten-ID) der Nachricht.

  $DATESTAMP$—Dieses Makro wird ersetzt durch das `Datum` der Nachricht.

  $CURRENTTIME$—Dieses Makro wird ersetzt durch die Zeit, zu der SecurityGateway die Hinweisnachricht erstellt.

  $HELONAME$—Dieses Makro wird durch den Domänennamen ersetzt, der im Befehl HELO während des SMTP-Protokolldialogs für die Nachricht übermittelt wurde, die die Bedingungen der Regel erfüllt.

- **Punkte der Nachrichtenbewertung hinzurechnen**—Diese Aktion bewirkt,

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

dass eine bestimmte Punktzahl der Nachrichtenbewertung hinzugerechnet wird, falls eine Nachricht die Bedingungen dieser Regel erfüllt.

- **Senden als registrierte E-Mail-Nachricht (RMail)**—Diese Aktion bewirkt, dass für Nachrichten, die die Bedingungen der Regel erfüllen, die Leistungsmerkmale für registrierte E-Mail-Nachrichten (RMail) genutzt werden.

  Verschlüsseln—Diese Option bewirkt, dass die Nachricht verschlüsselt wird.

  Sendungs- und Zustellungsverfolgung (Track & Prove)—Diese Option bewirkt, dass das Leistungsmerkmal Sendungs- und Zustellungsverfolgung ("Track & Prove") von RMail genutzt wird.

  E-Signatur—Diese Option bewirkt, dass das Leistungsmerkmale E-Signatur von RMail zur elektronischen Signatur von Dokumenten genutzt wird.

- **Nachricht für REQUIRETLS kennzeichnen**—Diese Aktion bewirkt, dass RequireTLS 126 für die Nachricht anwendbar ist.

- **Als sichere Web-Nachricht senden**—Diese Aktion bewirkt, dass die Nachricht nicht über den normalen Zustellweg für E-Mail-Nachrichten sondern über das Webportal für Sichere Nachrichten 112 versandt wird.

Reguläre Ausdrücke

Die Bedingungen für die Regeln 254 des Inhaltsfilters unterstützen auch die Vergleichs-Methode "`stimmt mit Regulärem Ausdruck überein`". Reguläre Ausdrücke (nach der englischen Bezeichnung *Regular Expressions* auch kurz als "regexp" bezeichnet) sind ein vielseitiges System, mit dessen Hilfe Sie nicht nur nach bestimmten Texten, Zeichenketten und Strings, sondern auch nach Textmustern suchen können. Ein Textmuster mit Regulären Ausdrücken besteht aus einer Folge bestimmter besonderer Zeichen, die *Metazeichen* genannt werden, und alphanumerischer Textzeichen, die auch "*terminale Zeichen* oder *gewöhnliche Zeichen*" genannt werden (etwa abc, 123 usw.). Mithilfe des Textmusters wird dann nach Übereinstimmungen in Texten gesucht — und das Ergebnis der Suche kann positiv oder negativ sein.

Die Implementation der Regulären Ausdrücke in SecurityGateway nutzt die Bibliothek PERL Compatible Regular Expression (PCRE). Sie erhalten nähere Informationen über diese Implementation der Regulären Ausdrücke unter http://www.pcre.org/ und http://perldoc.perl.org/perlre.html.

Eine umfassende Darstellung der Regulären Ausdrücke bietet *Reguläre Ausdrücke (3. Auflage 2007)*, erschienen bei O'Reilly Media, Inc. Die englische Originalfassung *Mastering Regular Expressions, Third Edition*, ist ebenfalls bei O'Reilly Media, Inc. erschienen.

Metazeichen

Metazeichen sind besondere Zeichen, die innerhalb Regulärer Ausdrücke bestimmte Funktionen erfüllen. Das System der Regulären Ausdrücke, das in SecurityGateway

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

implementiert ist, gestattet die Verwendung folgender Metazeichen:

```
\ | () [] ^ $ * + ? .
```

Metazeichen	Beschreibung
\	Wird der *Backslash* ("\" oder "umgekehrter Schrägstrich") vor ein Metazeichen gesetzt, so wird das folgende Metazeichen maskiert, also als gewöhnliches Zeichen behandelt. Dies ist nötig, wenn der Reguläre Ausdruck nach einem der besonderen Zeichen suchen soll, die sonst als Metazeichen verwendet werden. Beispielsweise muss ein Ausdruck, der nach dem Pluszeichen ("+") suchen soll, dafür die Zeichenkette "\+" enthalten.
|	Das *Alternativzeichen* (auch "Oder-Zeichen" oder "senkrechter Strich" genannt) wird verwendet, wenn entweder die Zeichenkette vor oder nach dem Oder-Zeichen mit dem zu durchsuchenden Text übereinstimmen soll. Der Reguläre Ausdruck "abc|xyz" sucht beispielsweise nach dem Vorkommen der Zeichenketten "abc" oder "xyz" in einem Text.
[...]	Eine von eckigen Klammern ("[" und "]") umschlossene Zeichenkette bedeutet, dass jedes beliebige Zeichen in der Kette mit dem zu durchsuchenden Text übereinstimmen soll. Ein Bindestrich ("-") zwischen den Zeichen in Klammern definiert eine Zeichenreihe. Wird beispielsweise die Zeichenkette "abc" mit dem Regulären Ausdruck "[a-z]" durchsucht, dann ergeben sich drei Treffer: "*a*", "*b*" und "*c*". Lautet statt dessen der Suchausdruck "[az]", so ergibt sich nur ein Treffer: "*a*".
^	Das sog. "Caret" bezeichnet einen Zeilenanfang. In der Zeichenkette "abc ab a" ergibt der Suchausdruck "^a" einen Treffer, und zwar das erste Zeichen der durchsuchten Zeichenkette. Der Ausdruck "^ab" ergibt ebenfalls einen Treffer, und zwar die *ersten beiden* Zeichen in der durchsuchten Zeichenkette.
[^...]	Folgt das Caret ("^") direkt auf eine öffnende eckige Klammer ("["), so erfüllt es einen anderen Zweck. Es legt fest, dass die in der Klammer folgenden Zeichen keinen Treffer in der zu durchsuchenden Zeichenkette ergeben dürfen. Der Ausdruck "[^0-9]" bedeutet beispielsweise, dass das zu suchende Zeichen keine Ziffer sein

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

	darf.
(...)	Die runden Klammern beeinflussen die Reihenfolge, in der die Muster ausgewertet werden, und dient außerdem als *getaggtes* Suchmuster, das in Ausdrücken zum Suchen und Ersetzen verwendet werden kann. Die Ergebnisse einer Suche durch einen Regulären Ausdruck werden zwischengespeichert und können in der Anweisung zum *Ersetzen* verwendet werden, um einen neuen Ausdruck zu bilden. In der Anweisung zum *Ersetzen* können die Zeichen "&" oder "\0" enthalten sein; diese werden durch die Zeichenketten ersetzt, die während der Suche durch den Regulären Ausdruck gefunden wurden. Findet der Suchausdruck "a(bcd)e" beispielsweise eine Zeichenkette, so ersetzen die Ausdrücke "123-&-123" oder "123-\0-123" den gefundenen Text durch "123-abcde-123". In ähnlicher Weise können die besonderen Zeichen "\1", "\2", "\3" u.s.w. in dem Ausdruck verwendet werden, der Zeichenketten *ersetzen* soll. Diese Zeichen werden nur durch die unmittelbaren Ergebnisse des Suchmusters, nicht aber durch die vollständige gefundene Zeichenkette ersetzt. Die Zahl nach dem Backslash legt bei Regulären Ausdrücken mit mehr als einem Suchmuster fest, auf welches Suchmuster verwiesen werden soll. Lautet der Suchausdruck beispielsweise "(123)(456)", und lautet der Ausdruck zum Ersetzen "a-\2-b-\1", so wird eine gefundene Zeichenkette durch "a-456-b-123" ersetzt, wohingegen ein Ausdruck zum Ersetzen "a-\0-b" durch "a-123456-b" ersetzt wird.
$	Das Dollarzeichen ("$") bezeichnet ein Zeilenende. In der Zeichenkette "13 321 123" ergibt der Ausdruck "3$" einen Treffer, und zwar das letzte Zeichen der Kette. Der Ausdruck "123$" ergibt ebenfalls einen Treffer, und zwar die *letzten drei* Zeichen in der Zeichenkette.
*	Das Zeichen Stern ("*") bestimmt, dass das ihm vorausgehende Zeichen mehrmals hintereinander vorkommen darf, aber nicht vorkommen muss. Daher ergibt "1*abc" für die Zeichenketten "111abc" und "abc" jeweils einen Treffer.
+	Etwas anders als der Stern, bestimmt das Pluszeichen "+", dass das ihm vorausgehende Zeichen mindestens einmal in der Zeichenkette vorkommen muss, aber auch mehrfach vorkommen

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

	darf. Daher ergibt "1+abc" einen Treffer bei der Zeichenkette "111abc", nicht aber bei "abc".
?	Das Fragezeichen ("?") bestimmt, dass das ihm vorausgehende Zeichen mehrmals vorkommen darf, aber nicht vorkommen muss. Daher ergibt "1*abc" einen Treffer für den Text "abc" sowie einen Treffer für die Zeichenkette "1abc" aus dem Text "111abc".
.	Das Metazeichen Punkt (".") ergibt einen Treffer für jedes beliebige andere Zeichen. Daher ergibt ". +abc" einen Treffer für "123456abc", "a.c" ergibt einen Treffer für "aac", "abc", "acc" usw.

4.7.2 Dateianlagen

Mithilfe der Optionen auf dieser Seite können Sie bestimmte Typen von Dateien festlegen; erscheinen diese Dateitypen als Dateianlagen in Nachrichten, so können die Nachrichten blockiert oder in Quarantäne gegeben werden. Sie können diese Einstellungen systemweit und für bestimmte Domänen gesondert treffen.

Dateianlagen, die blockiert werden sollen

In diesem Abschnitt geben Sie die Dateitypen an, die blockiert werden sollen. Enthält eine Nachricht Dateianlagen der hier aufgeführten Typen, so wird sie während der SMTP-Übermittlung abgewiesen.

Falls Sie für denselben Dateityp gleichzeitig festlegen, dass er gesperrt und in Quarantäne gegeben wird, so werden die Nachrichten mit Dateianlagen dieses Typs nicht in Quarantäne gegeben sondern **blockiert.**

Hinzufügen
Um einen neuen Dateityp in die Liste der zu blockierenden Dateitypen einzutragen, geben sie den Dateityp hier an, und klicken Sie auf *Hinzufügen*.

Entfernen
Um einen Dateityp aus der Liste der zu blockierenden Dateianlagen zu entfernen, wählen Sie den Dateityp aus der Liste aus, und klicken Sie auf *Entfernen*. Mithilfe der Strg-Taste können Sie auch mehrere Dateitypen auswählen.

Vorschläge
Mithilfe dieser Verknüpfungen können Sie einfach und schnell die am weitesten verbreiteten Gruppen von Dateitypen in die Liste der zu blockierenden Dateianlagen eintragen. Um eine Gruppe von Dateitypen der Liste hinzuzufügen, klicken Sie auf die entsprechende Verknüpfung.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ausführbare Dateien blockieren:
Diese Verknüpfung fügt die Dateitypen APP, CMD, COM, DMG, EXE, HTA, PIF, SCR und VBS der Liste der gesperrten Dateitypen hinzu.

Bilddateien blockieren:
Diese Verknüpfung fügt die Bild-Dateitypen BMP, GIF, JPG, PNG, TIF und TIFF der Liste der gesperrten Dateitypen hinzu.

Videodateien blockieren:
Diese Verknüpfung fügt die Video-Dateitypen 3GP, ASX, AVI, DIVX, M4U, MOV, MP4, MPEG, MPG, QT, RM, RTS, SWF, WM und WMV der Liste der gesperrten Dateitypen hinzu.

Audiodateien blockieren:
Diese Verknüpfung fügt die Audio-Dateitypen AAC, AIF, AIFF, AU, CDR, M3U, M4A, MID, MIDI, MOD, MP3, OGG, RA, WAV und WAVE der Liste der gesperrten Dateitypen hinzu.

Komprimierte Dateien blockieren:
Diese Verknüpfung fügt die komprimierten Dateien GZ, GZIP, RAR, TAR, TAR.GZ, TGZ und ZIP der Liste der gesperrten Dateitypen hinzu.

Nachrichten ausnehmen, wenn sie an die unten aufgeführten E-Mail-Adressen gerichtet sind
Sie können Nachrichten an bestimmte Empfängeradressen von der oben konfigurierten Blockierung von Dateianlagen ausnehmen. Aktivieren Sie hierzu diese Option, und fügen Sie die gewünschten Empfängeradressen hinzu. Jokerzeichen sind in den Adressen zulässig. Einige Beispiele hierzu:
`*@company.mail`, `user*@company.mail`, `admin@*.mail`

Dateianlagen, die in Quarantäne gegeben werden sollen

In diesem Abschnitt geben Sie die Dateitypen an, die in Quarantäne gegeben werden sollen. Enthält eine Nachricht Dateianlagen der hier aufgeführten Typen, so wird sie während der SMTP-Übermittlung angenommen, danach aber in Quarantäne gegeben.

Falls Sie für denselben Dateityp gleichzeitig festlegen, dass er gesperrt und in Quarantäne gegeben wird, so werden die Nachrichten mit Dateianlagen dieses Typs nicht in Quarantäne gegeben sondern **blockiert**.

Hinzufügen
Um einen neuen Dateityp in die Liste der in Quarantäne zu gebenden Dateitypen einzutragen, geben sie den Dateityp hier an, und klicken Sie auf *Hinzufügen*.

Entfernen
Um einen Dateityp aus der Liste der in Quarantäne zu gebenden Dateianlagen zu entfernen, wählen Sie den Dateityp aus der Liste aus, und klicken Sie auf *Entfernen*. Mithilfe der Strg-Taste können Sie auch mehrere Dateitypen auswählen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Vorschläge
Mithilfe dieser Verknüpfungen können Sie einfach und schnell die am weitesten verbreiteten Gruppen von Dateitypen in die Liste der in Quarantäne zu gebenden Dateianlagen eintragen. Um eine Gruppe von Dateitypen der Liste hinzuzufügen, klicken Sie auf die entsprechende Verknüpfung.

Ausführbare Dateien in Quarantäne geben:
Diese Verknüpfung fügt die Dateitypen APP, CMD, COM, DMG, EXE, HTA, PIF, SCR und VBS der Liste der in Quarantäne zu gebenden Dateitypen hinzu.

Bilddateien in Quarantäne geben:
Diese Verknüpfung fügt die Bild-Dateitypen BMP, GIF, JPG, PNG, TIF und TIFF der Liste der in Quarantäne zu gebenden Dateitypen hinzu.

Videodateien in Quarantäne geben:
Diese Verknüpfung fügt die Video-Dateitypen 3GP, ASX, AVI, DIVX, M4U, MOV, MP4, MPEG, MPG, QT, RM, RTS, SWF, WM und WMV der Liste der in Quarantäne zu gebenden Dateitypen hinzu.

Audiodateien in Quarantäne geben:
Diese Verknüpfung fügt die Audio-Dateitypen AAC, AIF, AIFF, AU, CDR, M3U, M4A, MID, MIDI, MOD, MP3, OGG, RA, WAV und WAVE der Liste der in Quarantäne zu gebenden Dateitypen hinzu.

Komprimierte Dateien in Quarantäne geben:
Diese Verknüpfung fügt die komprimierten Dateien GZ, GZIP, RAR, TAR, TAR.GZ, TGZ und ZIP der Liste der in Quarantäne zu gebenden Dateitypen hinzu.

Nachrichten ausnehmen, wenn sie an die unten aufgeführten E-Mail-Adressen gerichtet sind
Sie können Nachrichten an bestimmte Empfängeradressen von der oben konfigurierten Quarantäne für Dateianlagen ausnehmen. Aktivieren Sie hierzu diese Option, und fügen Sie die gewünschten Empfängeradressen hinzu. Jokerzeichen sind in den Adressen zulässig. Einige Beispiele hierzu: `*@company.mail`, `user*@company.mail`, `admin@*.mail`

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Einstellungen zum Filtern von Dateianlagen für diese Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen*.

4.8 Schwarze Listen

In den Schwarzen Listen können E-Mail-Adressen, Hosts und IP-Adressen erfasst werden, deren Nachrichten Sie abweisen lassen oder in Quarantäne geben

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

wollen. Per Voreinstellung werden solche Nachrichten bereits während der SMTP-Verbindung abgewiesen; Sie können die entsprechenden Einstellungen jedoch auf der Seite Aktion der Schwarzen Liste 274 ändern und die Nachrichten stattdessen in Quarantäne geben lassen. Die gewünschte Vorgehensweise kann systemweit und nach Domänen getrennt vorgegeben werden, und auch die Schwarzen Listen selbst können systemweit und nach Domänen getrennt geführt werden. Üblicherweise wird nur ein Eintrag zur gleichen Zeit einer Schwarzen Liste hinzugefügt; falls Sie jedoch in einem Durchgang mehrere Einträge hinzufügen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Einträge aus einer Textdatei lesen und der Schwarzen Liste hinzufügen. Die Schwarze Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt der Schwarzen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können. Es bestehen drei Arten von Schwarzen Listen, die alle systemweit und nach Domänen getrennt genutzt werden können:

Schwarze Liste für Adressen 266 - Mithilfe dieser Schwarze Liste können Sie Nachrichten abweisen oder in Quarantäne geben, die von bestimmten E-Mail-Adressen stammen.

Schwarze Liste für Hosts 269 - Mithilfe dieser Schwarzen Liste können Sie Nachrichten abweisen oder in Quarantäne geben, die durch bestimmte Hosts zugestellt werden (wie etwa mail.example.com, smtp.example.net usw.).

Schwarze Liste für IPs 271 - Mithilfe der Schwarzen Liste für IPs können Sie Nachrichten abweisen oder in Quarantäne geben, die von bestimmten IP-Adressen aus zugestellt werden.

4.8.1 Adressen

Mithilfe dieser Schwarze Liste können Sie Nachrichten abweisen oder in Quarantäne geben, die von bestimmten E-Mail-Adressen stammen. Per Voreinstellung werden solche Nachrichten bereits während der SMTP-Verbindung abgewiesen; Sie können die entsprechenden Einstellungen jedoch auf der Seite Aktion der Schwarzen Liste 274 ändern und die Nachrichten stattdessen in Quarantäne geben lassen. Die gewünschte Vorgehensweise kann systemweit und nach Domänen getrennt vorgegeben werden, und auch die Schwarzen Listen selbst können systemweit und nach Domänen getrennt geführt werden. Üblicherweise wird nur eine Adresse zur gleichen Zeit in die Schwarze Liste eingetragen; falls Sie jedoch in einem Durchgang mehrere Adressen eintragen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Adressen aus einer Textdatei lesen und in die Schwarze Liste eintragen. Die Schwarze Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt Ihrer Schwarzen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können.

Hinzufügen von Adressen zur Schwarzen Liste

Um eine Adresse in die Schwarze Liste einzutragen, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Neu.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Schwarzen Liste 268 aufgerufen (vgl. unten).

Bearbeiten einer Adresse in der Schwarzen Liste

Um eine bereits in der Schwarzen Liste erfasste Adresse zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie den gewünschten Eintrag aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Bearbeiten.* Hierdurch

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Schwarzen Liste 268 für den ausgewählten Eintrag aufgerufen.

Löschen von Adressen aus der Schwarzen Liste

Um eine Adresse oder mehrere Adressen aus der Schwarzen Liste zu löschen, wählen Sie die gewünschten Einträge aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Löschen*. Um mehr als einen Eintrag auszuwählen, halten Sie die Strg-Taste gedrückt, während Sie die gewünschten Einträge durch Anklicken auswählen. Nachdem Sie auf *Löschen* geklickt haben, erscheint ein Bestätigungsdialog mit der Abfrage, ob Sie die gewünschten Einträge wirklich löschen wollen.

Import von Adressen in die Schwarze Liste

Um eine Adressliste in die Schwarze Liste für Adressen zu importieren, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Listen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die Textdatei aus, deren Inhalt Sie in die Schwarze Liste importieren wollen. Klicken Sie auf *Listen importieren*, um mit dem Import zu beginnen.

Formate der CSV-Dateien

Sie können die CSV-Datei mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Jedes Datenelement muss in Anführungs- und Schlusszeichen gesetzt, und die Datenelemente in einer Zeile müssen durch ein Komma getrennt sein.

Import von Adressen in die Globale Schwarze Liste:
Die Spalte *Value* enthält die E-Mail-Adressen, die Sie in die Schwarze Liste eintragen wollen, die Spalte *Typ* muss jeweils den Eintrag `"BlackListAddressGlobal"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für den zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Value","Type","Comments"
"adresse01@example.net","BlackListAddressGlobal","Hier steht ein
Kommentar zu der Adresse."
"adresse01@example.org","BlackListAddressGlobal",""
"adresse02@example.net","BlackListAddressGlobal","Hier steht ein
weiterer Kommentar."
```

Import von Adressen in die besondere Schwarze Liste einer Domäne:
Die Spalte *Domain* enthält die Domäne, der diese Schwarze Liste zugeordnet ist. Wollen Sie beispielsweise Adressen in die Schwarze Liste der Domäne example.com eintragen, so muss `"example.com"` in der Spalte *Domain* erscheinen. Die Spalte *Value* enthält die E-Mail-Adressen, die Sie in die Schwarze Liste eintragen wollen, die Spalte *Typ* muss jeweils den Eintrag `"BlackListAddressDomain"` enthalten, und die Spalte *Comments* enthält den

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kommentar, der für den zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Domain","Value","Type","Comments"
"example.com","adresse01@example.net","BlackListAddressDomain","Hi
er steht ein Kommentar zu der Adresse."
"example.com","adresse01@example.org","BlackListAddressDomain",""
"example.com","adresse02@example.net","BlackListAddressDomain","Hi
er steht ein weiterer Kommentar."
```

Export von Adressen aus der Schwarzen Liste

Um den Inhalt einer Schwarzen Liste für Adressen zu exportieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Auswahlmenü Für Domäne: den Eintrag Global, oder wählen Sie eine Domäne aus.
2. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
3. Klicken Sie auf *Speichern*.
4. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
5. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

Eintrag in der Schwarzen Liste

Dieses Dialogfenster dient dem Hinzufügen neuer Adressen zur Schwarzen Liste und dem Bearbeiten bestehender Einträge. Es wird immer dann aufgerufen, wenn Sie in der Symbolleiste am oberen Seitenrand auf *Neu* oder *Bearbeiten* klicken.

Listeneintrag

Für Domäne:
Um eine Adresse in die besondere Schwarze Liste einer Domäne einzutragen, wählen Sie die Domäne aus diesem Auswahlmenü. Für einen Eintrag in die systemweite Schwarze Liste wählen Sie Global.

E-Mail-Adresse:
Tragen Sie in dieses Feld die E-Mail-Adresse ein, deren Nachrichten Sie abweisen oder in Quarantäne geben wollen. Sie bestimmen mithilfe der Einstellungen auf der Seite Aktion der Schwarzen Liste 274, ob die Nachrichten abgewiesen oder in Quarantäne gegeben werden. Um alle Adressen einer Domäne in die Schwarze Liste einzutragen, setzen Sie anstatt des Postfachnamens einen Stern. Ein Beispiel hierzu: "*@example.org" erfasst alle Absender, die unter der Domäne example.org Nachrichten versenden, in der Schwarzen Liste.

Kommentar:
In dieses Textfeld können Sie Kommentare oder Anmerkungen eintragen, die Sie zu diesem Eintrag erfassen wollen. Der Eintrag dient nur zu Ihrer Information.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Speichern und Beenden
Sobald Sie die Bearbeitung des Eintrags abgeschlossen haben, klicken Sie auf *Speichern und Beenden,* um den Eintrag in der Schwarzen Liste zu speichern.

Schließen
Um das Dialogfenster zu schließen, ohne den gerade bearbeiteten Eintrag zu speichern, klicken Sie auf dieses Steuerelement.

4.8.2 Hosts

Mithilfe dieser Schwarzen Liste können Sie Nachrichten abweisen oder in Quarantäne geben, die durch bestimmte Hosts zugestellt werden (wie etwa mail.example.com, smtp.example.net usw.). Per Voreinstellung werden solche Nachrichten bereits während der SMTP-Verbindung abgewiesen; Sie können die entsprechenden Einstellungen jedoch auf der Seite Aktion der Schwarzen Liste 274 ändern und die Nachrichten stattdessen in Quarantäne geben lassen. Die gewünschte Vorgehensweise kann systemweit und nach Domänen getrennt vorgegeben werden, und auch die Schwarzen Listen selbst können systemweit und nach Domänen getrennt geführt werden. Üblicherweise wird nur ein Host zur gleichen Zeit in die Schwarze Liste eingetragen; falls Sie jedoch in einem Durchgang mehrere Hosts eintragen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Hosts aus einer Textdatei lesen und in die Schwarze Liste eintragen. Die Schwarze Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt Ihrer Schwarzen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können.

Hinzufügen von Hosts zur Schwarzen Liste

Um einen Host in die Schwarze Liste für Hosts einzutragen, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Neu.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Schwarzen Liste 271 aufgerufen (vgl. unten).

Bearbeiten eines Hosts in der Schwarzen Liste

Um einen bereits in der Schwarzen Liste erfassten Host zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie den gewünschten Eintrag aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Bearbeiten.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Schwarzen Liste 271 für den ausgewählten Eintrag aufgerufen.

Löschen von Hosts aus der Schwarzen Liste

Um einen Host oder mehrere Hosts aus der Schwarzen Liste zu löschen, wählen Sie die gewünschten Einträge aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Löschen*. Um mehr als einen Eintrag auszuwählen, halten Sie die Strg-Taste gedrückt, während Sie die gewünschten Einträge durch Anklicken auswählen. Nachdem Sie auf *Löschen* geklickt haben, erscheint ein Bestätigungsdialog mit der Abfrage, ob Sie die gewünschten Einträge wirklich löschen wollen.

Import von Hosts in die Schwarze Liste

Um eine Liste von Hosts in die Schwarze Liste für Hosts zu importieren, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Listen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,*

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

und wählen Sie dann die Textdatei aus, deren Inhalt Sie in die Schwarze Liste importieren wollen. Klicken Sie auf *Listen importieren*, um mit dem Import zu beginnen.

Formate der CSV-Dateien

Sie können die CSV-Datei mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Jedes Datenelement muss in Anführungs- und Schlusszeichen gesetzt, und die Datenelemente in einer Zeile müssen durch ein Komma getrennt sein.

Import von Hosts in die Globale Schwarze Liste:

Die Spalte *Value* enthält den Host, den Sie in die Schwarze Liste eintragen wollen, die Spalte *Typ* muss jeweils den Eintrag `"BlackListHostGlobal"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für die zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Value","Type","Comments"
"example.net","BlackListHostGlobal","Hier steht ein Kommentar zu
dem Host."
"mail.domain.com","BlackListHostGlobal",""
"smtp.company.mail","BlackListHostGlobal","Hier steht ein weiterer
Kommentar."
```

Import von Hosts in die besondere Schwarze Liste einer Domäne:

Die Spalte *Domain* enthält die Domäne, der diese Schwarze Liste zugeordnet ist. Wollen Sie beispielsweise Hosts in die Schwarze Liste der Domäne example.com eintragen, so muss `"example.com"` in der Spalte *Domain* erscheinen. Die Spalte *Value* enthält den Host, den Sie in die Schwarze Liste eintragen wollen, die Spalte *Typ* muss jeweils den Eintrag `"BlackListHostDomain"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für den zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Domain","Value","Type","Comments"
"example.com","example.net","BlackListHostDomain","Hier steht ein
Kommentar zu dem Host."
"example.com","mail.domain.com","BlackListHostDomain",""
"example.com","smtp.company.mail","BlackListHostDomain","Hier
steht ein weiterer Kommentar."
```

Export von Hosts aus der Schwarzen Liste

Um den Inhalt einer Schwarzen Liste für Hosts zu exportieren, gehen Sie folgendermaßen vor:

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

1. Wählen Sie im Auswahlmenü Für Domäne: den Eintrag Global, oder wählen Sie eine Domäne aus.
2. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
3. Klicken Sie auf *Speichern*.
4. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
5. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

Eintrag in der Schwarzen Liste

Dieses Dialogfenster dient dem Hinzufügen neuer Hosts zur Schwarzen Liste und dem Bearbeiten bestehender Einträge. Es wird immer dann aufgerufen, wenn Sie in der Symbolleiste am oberen Seitenrand auf *Neu* oder *Bearbeiten* klicken.

Listeneintrag

Für Domäne:
Um einen Host in die besondere Schwarze Liste einer Domäne einzutragen, wählen Sie die Domäne aus diesem Auswahlmenü. Für einen Eintrag in die systemweite Schwarze Liste wählen Sie Global.

Host:
Tragen Sie in dieses Feld den Host ein, dessen Nachrichten Sie abweisen oder in Quarantäne geben wollen. Sie bestimmen mithilfe der Einstellungen auf der Seite Aktion der Schwarzen Liste 274, ob die Nachrichten abgewiesen oder in Quarantäne gegeben werden. Um alle Hosts einer Domäne in die Schwarze Liste einzutragen, setzen Sie in den Hostnamen einen Stern. Ein Beispiel hierzu: "`*.example.org`" erfasst alle Nachrichten aller Subdomänen von example.org, wie etwa `mail.example.org` und `smtp.example.org`, in der Schwarzen Liste.

Kommentar:
In dieses Textfeld können Sie Kommentare oder Anmerkungen eintragen, die Sie zu diesem Eintrag erfassen wollen. Der Eintrag dient nur zu Ihrer Information.

Speichern und Beenden
Sobald Sie die Bearbeitung des Eintrags abgeschlossen haben, klicken Sie auf *Speichern und Beenden,* um den Eintrag in der Schwarzen Liste zu speichern.

Schließen
Um das Dialogfenster zu schließen, ohne den gerade bearbeiteten Eintrag zu speichern, klicken Sie auf dieses Steuerelement.

4.8.3 IPs

Mithilfe der Schwarzen Liste für IPs können Sie Nachrichten abweisen oder in Quarantäne geben, die von bestimmten IP-Adressen aus zugestellt werden (wie etwa "`1.2.3.4`" und "`192.168.0.1`,"). Per Voreinstellung werden solche Nachrichten bereits während der SMTP-Verbindung abgewiesen; Sie können die entsprechenden Einstellungen jedoch auf der Seite Aktion der Schwarzen Liste 274 ändern und die Nachrichten stattdessen in Quarantäne geben lassen. Die gewünschte

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Vorgehensweise kann systemweit und nach Domänen getrennt vorgegeben werden, und auch die Schwarzen Listen selbst können systemweit und nach Domänen getrennt geführt werden. Üblicherweise wird nur ein Eintrag zur gleichen Zeit in die Schwarze Liste eingetragen; falls Sie jedoch in einem Durchgang mehrere Einträge hinzufügen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Einträge aus einer Textdatei lesen und in die Schwarze Liste eintragen. Die Schwarze Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt Ihrer Schwarzen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können.

Hinzufügen von IP-Adressen zur Schwarzen Liste

Um eine IP-Adresse in die Schwarze Liste für IPs einzutragen, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Neu.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Schwarzen Liste 273 aufgerufen (vgl. unten).

Bearbeiten einer IP-Adresse in der Schwarzen Liste

Um eine bereits in der Schwarzen Liste erfasste IP-Adresse zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie den gewünschten Eintrag aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Bearbeiten.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Schwarzen Liste 273 für den ausgewählten Eintrag aufgerufen.

Löschen von IP-Adressen aus der Schwarzen Liste

Um eine IP-Adresse oder mehrere IP-Adressen aus der Schwarzen Liste zu löschen, wählen Sie die gewünschten Einträge aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Löschen*. Um mehr als einen Eintrag auszuwählen, halten Sie die Strg-Taste gedrückt, während Sie die gewünschten Einträge durch Anklicken auswählen. Nachdem Sie auf *Löschen* geklickt haben, erscheint ein Bestätigungsdialog mit der Abfrage, ob Sie die gewünschten Einträge wirklich löschen wollen.

Import von IP-Adressen in die Schwarze Liste

Um eine Liste von IP-Adressen in die Schwarze Liste für IPs zu importieren, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Listen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die Textdatei aus, deren Inhalt Sie in die Schwarze Liste importieren wollen. Klicken Sie auf *Listen importieren*, um mit dem Import zu beginnen.

Formate der CSV-Dateien

Sie können die CSV-Datei mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Jedes Datenelement muss in Anführungs- und Schlusszeichen gesetzt, und die Datenelemente in einer Zeile müssen durch ein Komma getrennt sein.

Import von IP-Adressen in die Globale Schwarze Liste:
Die Spalte *Value* enthält die IP-Adresse, die Sie in die Schwarze Liste eintragen wollen (CIDR-Schreibweise und die Jokerzeichen *, ? und # sind zulässig), die Spalte *Typ* muss jeweils den Eintrag `"BlackListIPGlobal"` enthalten, und die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Spalte *Comments* enthält den Kommentar, der für die zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Value","Type","Comments"
"1.2.3.4","BlackListIPGlobal","Hier steht ein Kommentar zu der
Adresse."
"1.1.1.1","BlackListIPGlobal",""
"192.168.*.*","BlackListIPGlobal","Hier steht ein weiterer
Kommentar."
```

Import von IP-Adressen in die besondere Schwarze Liste einer Domäne:
Die Spalte *Domain* enthält die Domäne, der diese Schwarze Liste zugeordnet ist. Wollen Sie beispielsweise IP-Adressen in die Schwarze Liste der Domäne example.com eintragen, so muss `"example.com"` in der Spalte *Domain* erscheinen. Die Spalte *Value* enthält die IP-Adresse, die Sie in die Schwarze Liste eintragen wollen (CIDR-Schreibweise und die Jokerzeichen *, ? und # sind zulässig), die Spalte *Typ* muss jeweils den Eintrag `"BlackListIPDomain"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für den zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Domain","Value","Type","Comments"
"example.com","1.2.3.4","BlackListIPDomain","Hier steht ein
Kommentar zu der adresse."
"example.com","1.1.1.1","BlackListIPDomain",""
"example.com","192.168.*.*","BlackListIPDomain","Hier steht ein
weiterer Kommentar."
```

Export von IP-Adressen aus der Schwarzen Liste

Um den Inhalt einer Schwarzen Liste für IPs zu exportieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Auswahlmenü Für Domäne: den Eintrag Global, oder wählen Sie eine Domäne aus.
2. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
3. Klicken Sie auf *Speichern*.
4. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
5. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

Eintrag in der Schwarzen Liste

Dieses Dialogfenster dient dem Hinzufügen neuer IP-Adressen zur Schwarzen Liste und dem Bearbeiten bestehender Einträge. Es wird immer dann aufgerufen, wenn Sie in der Symbolleiste am oberen Seitenrand auf *Neu* oder *Bearbeiten* klicken.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Listeneintrag

Für Domäne:
Um eine IP-Adresse in die besondere Schwarze Liste einer Domäne einzutragen, wählen Sie die Domäne aus diesem Auswahlmenü. Für einen Eintrag in die systemweite Schwarze Liste wählen Sie Global.

IP-Adresse:
Tragen Sie in dieses Feld die IP-Adresse ein, deren Nachrichten Sie abweisen oder in Quarantäne geben wollen. Sie bestimmen mithilfe der Einstellungen auf der Seite Aktion der Schwarzen Liste 274, ob die Nachrichten abgewiesen oder in Quarantäne gegeben werden. Die CIDR-Schreibweise ist zulässig, und Sie können die Jokerzeichen *, ? und # verwenden, um Adressblöcke mit einem einzigen Eintrag zu erfassen.

Kommentar:
In dieses Textfeld können Sie Kommentare oder Anmerkungen eintragen, die Sie zu diesem Eintrag erfassen wollen. Der Eintrag dient nur zu Ihrer Information.

Speichern und Beenden
Sobald Sie die Bearbeitung des Eintrags abgeschlossen haben, klicken Sie auf *Speichern und Beenden,* um den Eintrag in der Schwarzen Liste zu speichern.

Schließen
Um das Dialogfenster zu schließen, ohne den gerade bearbeiteten Eintrag zu speichern, klicken Sie auf dieses Steuerelement.

4.8.4 Konfiguration

Löst eine Nachricht einen Treffer auf einer Schwarzen Liste 265 von SecurityGateway aus, weil sie mit einem Eintrag in der Schwarzen Liste übereinstimmt, so führt SecurityGateway die Aktionen durch, die auf dieser Seite festgelegt sind. Per Voreinstellung wird die entsprechende Nachricht während der SMTP-Verbindung abgewiesen; Sie können diese Einstellung aber ändern, sodass die Nachricht stattdessen in Quarantäne gegeben wird. Die gewünschte Vorgehensweise kann systemweit und nach Domänen getrennt vorgegeben werden. Um die Einstellungen für eine bestimmte Domäne zu konfigurieren, wählen Sie im Auswahlmenü am oberen Seitenrand *Für Domäne:* diese Domäne aus, treffen Sie die Einstellungen, und klicken Sie dann auf *Speichern*.

Konfiguration

Treffer auf der Weißen Liste haben Vorrang vor Treffern auf der Schwarzen Liste
Diese Option gibt Treffern auf der Weißen Liste 275 den Vorrang vor Treffern auf der Schwarzen Liste, falls Nachrichten zu Treffern sowohl auf einer Weißen als auch auf einer Schwarzen Liste führen. Per Voreinstellung ist diese Option abgeschaltet. Treffer auf der Schwarzen Liste erhalten dann Vorrang vor Treffern auf der Weißen Liste, falls eine Nachricht Treffer auf beiden Listen auslöst. Nachrichten können nach Treffern auch abgewiesen oder in Quarantäne gegeben werden; diese Behandlung richtet sich nach der Option *Falls eine Nachricht einen Treffer auf einer Schwarzen Liste auslöst* weiter unten.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Falls eine Nachricht einen Treffer auf einer Schwarzen Liste auslöst:
Hiermit wird die Aktion konfiguriert, die nach Empfang einer Nachricht durchgeführt wird, falls der Absender der Nachricht auf einer Schwarzen Liste erfasst ist.

...Nachricht abweisen
Diese Option bewirkt, dass die Nachricht des Absenders auf der Schwarzen Liste während der SMTP-Verbindung abgewiesen wird. Diese Option ist per Voreinstellung aktiv.

Verbindung mit dem sendenden Server trennen
Per Voreinstellung wird die SMTP-Verbindung auch dann normal fortgesetzt, wenn eine Nachricht abgewiesen wurde. Falls Sie stattdessen die Verbindung sofort beenden möchten, aktivieren Sie dieses Kontrollkästchen. SecurityGateway trennt dann die Verbindung mit dem sendenden Server unmittelbar, nachdem die Nachricht abgewiesen wurde.

...Nachricht in Quarantäne geben
Diese Option bewirkt, dass Nachrichten von Absendern auf der Schwarzen Liste nicht abgewiesen sondern in Quarantäne gegeben werden.

Ausnahmen - Domänen

Falls Sie in der Auswahlliste "*Für Domäne:*" am oberen Seitenrand eine Domäne auswählen, wenn Sie diese Einstellungen konfigurieren, so wird nach dem Speichern der Einstellungen diese Domäne im Feld angezeigt. Klicken Sie auf die Verknüpfung *Anzeigen/Bearbeiten* für die jeweilige Domäne, um die Aktion der Schwarzen Liste dieser Domäne anzuzeigen und zu bearbeiten. Um die Domäne auf die systemweiten Voreinstellungen zurückzusetzen, klicken Sie auf *Zurücksetzen.*

4.9 Weiße Listen

In den Weißen Listen können E-Mail-Adressen, Hosts und IP-Adressen erfasst werden, deren Nachrichten von einigen Sicherheitsbeschränkungen ausgenommen sind. Die Funktionen Heuristik und Bayes 162, DNSBL 169, DKIM-Prüfung 197 und auch fast alle anderen Sicherheitsfunktionen 154 von SecurityGateway können so konfiguriert werden, dass Absender, Hosts und Nachrichten von der Bearbeitung durch diese Funktionen ausgenommen sind, falls sie einen Treffer auf einer Weißen Liste auslösen. Jede Weiße Liste kann systemweit und nach Domänen getrennt geführt werden. Üblicherweise wird nur ein Eintrag zur gleichen Zeit einer Weißen Liste hinzugefügt; falls Sie jedoch in einem Durchgang mehrere Einträge hinzufügen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Einträge aus einer Textdatei lesen und der Weißen Liste hinzufügen. Die Weiße Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt der Weißen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können. Es bestehen drei Arten von Weißen Listen, die alle systemweit und nach Domänen getrennt genutzt werden können:

Weiße Liste für Adressen 276 - Mithilfe dieser Weißen Liste können Nachrichten ausgenommen werden, die von bestimmten E-Mail-Adressen stammen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Weiße Liste für Hosts 278 - Mithilfe dieser Weißen Liste können bestimmte Hosts von einzelnen Sicherheitsbeschränkungen ausgenommen werden, und Nachrichten, die von bestimmten Hosts (z.B. mail.example.com, smtp.example.net usw.) kommen, von Sicherheitsprüfungen ausgenommen werden.

Weiße Liste für IPs 281 - Mithilfe dieser Weißen Liste können bestimmte IP-Adressen von einzelnen Sicherheitsbeschränkungen ausgenommen werden, und Nachrichten, die von bestimmten Gegenstellen gesendet werden, können anhand der IP-Adresse der Gegenstelle von Sicherheitsprüfungen ausgenommen werden.

4.9.1 Adressen

Mithilfe dieser Weißen Liste können Nachrichten ausgenommen werden, die von bestimmten E-Mail-Adressen stammen. Die Funktionen Heuristik und Bayes 162, DNSBL 169, DKIM-Prüfung 197 und auch fast alle anderen Sicherheitsfunktionen 154 von SecurityGateway können so konfiguriert werden, dass Adressen und Nachrichten von diesen Adressen von der Bearbeitung durch diese Funktionen ausgenommen sind, falls sie einen Treffer auf einer Weißen Liste auslösen. Jede Weiße Liste kann systemweit und nach Domänen getrennt geführt werden. Üblicherweise wird nur ein Eintrag zur gleichen Zeit einer Weißen Liste hinzugefügt; falls Sie jedoch in einem Durchgang mehrere Einträge hinzufügen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Einträge aus einer Textdatei lesen und der Weißen Liste hinzufügen. Die Weiße Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt der Weißen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können.

Hinzufügen von Adressen zur Weißen Liste

Um eine Adresse in die Weiße Liste einzutragen, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Neu.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Weißen Liste 278 aufgerufen (vgl. unten).

Bearbeiten einer Adresse in der Weißen Liste

Um eine bereits in der Weißen Liste erfasste Adresse zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie den gewünschten Eintrag aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Bearbeiten.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Weißen Liste 278 für den ausgewählten Eintrag aufgerufen.

Löschen von Adressen aus der Weißen Liste

Um eine Adresse oder mehrere Adressen aus der Weißen Liste zu löschen, wählen Sie die gewünschten Einträge aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Löschen*. Um mehr als einen Eintrag auszuwählen, halten Sie die Strg-Taste gedrückt, während Sie die gewünschten Einträge durch Anklicken auswählen. Nachdem Sie auf *Löschen* geklickt haben, erscheint ein Bestätigungsdialog mit der Abfrage, ob Sie die gewünschten Einträge wirklich löschen wollen.

Import von Adressen in die Weiße Liste

Um eine Adressliste in die Weiße Liste für Adressen zu importieren, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Listen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die Textdatei aus, deren Inhalt Sie in die Weiße Liste

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

importieren wollen. Klicken Sie auf *Listen importieren*, um mit dem Import zu beginnen.

Formate der CSV-Dateien

Sie können die CSV-Datei mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Jedes Datenelement muss in Anführungs- und Schlusszeichen gesetzt, und die Datenelemente in einer Zeile müssen durch ein Komma getrennt sein.

Import von Adressen in die Globale Weiße Liste:

Die Spalte *Value* enthält die E-Mail-Adressen, die Sie in die Weiße Liste eintragen wollen, die Spalte *Typ* muss jeweils den Eintrag `"WhiteListAddressGlobal"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für den zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Value","Type","Comments"
"adresse01@example.net","WhiteListAddressGlobal","Hier steht ein
Kommentar zu der Adresse."
"adresse01@example.org","WhiteListAddressGlobal",""
"adresse02@example.net","WhiteListAddressGlobal","Hier steht ein
weiterer Kommentar."
```

Import von Adressen in die besondere Weiße Liste einer Domäne:

Die Spalte *Domain* enthält die Domäne, der diese Weiße Liste zugeordnet ist. Wollen Sie beispielsweise Adressen in die Weiße Liste der Domäne example.com eintragen, so muss `"example.com"` in der Spalte *Domain* erscheinen. Die Spalte *Value* enthält die E-Mail-Adressen, die Sie in die Weiße Liste eintragen wollen, die Spalte *Typ* muss jeweils den Eintrag `"WhiteListAddressDomain"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für den zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Domain","Value","Type","Comments"
"example.com","adresse01@example.net","WhiteListAddressDomain","Hi
er steht ein Kommentar zu der Adresse."
"example.com","adresse01@example.org","WhiteListAddressDomain",""
"example.com","adresse02@example.net","WhiteListAddressDomain","Hi
er steht ein weiterer Kommentar."
```

Export von Adressen aus der Weißen Liste

Um den Inhalt einer Weißen Liste für Adressen zu exportieren, gehen Sie folgendermaßen vor:

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

1. Wählen Sie im Auswahlmenü Für Domäne: den Eintrag Global, oder wählen Sie eine Domäne aus.
2. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
3. Klicken Sie auf *Speichern*.
4. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
5. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

Eintrag in der Weißen Liste

Dieses Dialogfenster dient dem Hinzufügen neuer Adressen zur Weißen Liste und dem Bearbeiten bestehender Einträge. Es wird immer dann aufgerufen, wenn Sie in der Symbolleiste am oberen Seitenrand auf *Neu* oder *Bearbeiten* klicken.

Listeneintrag

Für Domäne:
Um eine Adresse in die besondere Weiße Liste einer Domäne einzutragen, wählen Sie die Domäne aus diesem Auswahlmenü. Für einen Eintrag in die systemweite Weiße Liste wählen Sie Global.

E-Mail-Adresse:
Tragen Sie in dieses Feld die E-Mail-Adresse ein, deren Nachrichten Sie von allen Sicherheitsfunktionen ausnehmen wollen, die Sie so konfiguriert haben, dass Nachrichten von Absendern auf der Weißen Liste ausgenommen sind. Um alle Adressen einer Domäne in die Weiße Liste einzutragen, setzen Sie anstatt des Postfachnamens einen Stern. Ein Beispiel hierzu: "*@example.org" erfasst alle Absender, die unter der Domäne example.org Nachrichten versenden, in der Weißen Liste.

Kommentar:
In dieses Textfeld können Sie Kommentare oder Anmerkungen eintragen, die Sie zu diesem Eintrag erfassen wollen. Der Eintrag dient nur zu Ihrer Information.

Speichern und Beenden
Sobald Sie die Bearbeitung des Eintrags abgeschlossen haben, klicken Sie auf *Speichern und Beenden,* um den Eintrag in der Weißen Liste zu speichern.

Schließen
Um das Dialogfenster zu schließen, ohne den gerade bearbeiteten Eintrag zu speichern, klicken Sie auf dieses Steuerelement.

4.9.2 Hosts

Mithilfe dieser Weißen Liste können bestimmte Hosts von einzelnen Sicherheitsbeschränkungen ausgenommen werden, und Nachrichten, die von bestimmten Hosts (z.B. mail.example.com, smtp.example.net usw.) kommen, von Sicherheitsprüfungen ausgenommen werden. Die Funktionen Heuristik und Bayes 162, DNSBL 169, DKIM-Prüfung 197 und auch fast alle anderen Sicherheitsfunktionen 154 von SecurityGateway können so konfiguriert werden, dass Hosts und Nachrichten von

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

diesen Hosts von der Bearbeitung durch diese Funktionen ausgenommen sind, falls sie einen Treffer auf einer Weißen Liste auslösen. Jede Weiße Liste kann systemweit und nach Domänen getrennt geführt werden. Üblicherweise wird nur ein Eintrag zur gleichen Zeit einer Weißen Liste hinzugefügt; falls Sie jedoch in einem Durchgang mehrere Einträge hinzufügen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Einträge aus einer Textdatei lesen und der Weißen Liste hinzufügen. Die Weiße Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt der Weißen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können.

Hinzufügen von Hosts zur Weißen Liste

Um einen Host in die Weiße Liste für Hosts einzutragen, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Neu.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Weißen Liste 280 aufgerufen (vgl. unten).

Bearbeiten eines Hosts in der Weißen Liste

Um einen bereits in der Weißen Liste erfassten Host zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie den gewünschten Eintrag aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Bearbeiten.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Weißen Liste 280 für den ausgewählten Eintrag aufgerufen.

Löschen von Hosts aus der Weißen Liste

Um einen Host oder mehrere Hosts aus der Weißen Liste zu löschen, wählen Sie die gewünschten Einträge aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Löschen*. Um mehr als einen Eintrag auszuwählen, halten Sie die Strg-Taste gedrückt, während Sie die gewünschten Einträge durch Anklicken auswählen. Nachdem Sie auf *Löschen* geklickt haben, erscheint ein Bestätigungsdialog mit der Abfrage, ob Sie die gewünschten Einträge wirklich löschen wollen.

Import von Hosts in die Weiße Liste

Um eine Liste von Hosts in die Weiße Liste für Hosts zu importieren, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Listen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die Textdatei aus, deren Inhalt Sie in die Weiße Liste importieren wollen. Klicken Sie auf *Listen importieren*, um mit dem Import zu beginnen.

Formate der CSV-Dateien

Sie können die CSV-Datei mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Jedes Datenelement muss in Anführungs- und Schlusszeichen gesetzt, und die Datenelemente in einer Zeile müssen durch ein Komma getrennt sein.

Import von Hosts in die Globale Weiße Liste:

Die Spalte *Value* enthält den Host, den Sie in die Weiße Liste eintragen wollen, die Spalte *Typ* muss jeweils den Eintrag `"WhiteListHostGlobal"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für die zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Value","Type","Comments"
"example.net","WhiteListHostGlobal","Hier steht ein Kommentar zu
dem Host."
"mail.domain.com","WhiteListHostGlobal",""
"smtp.company.mail","WhiteListHostGlobal","Hier steht ein weiterer
Kommentar."
```

Import von Hosts in die besondere Weiße Liste einer Domäne:
Die Spalte *Domain* enthält die Domäne, der diese Weiße Liste zugeordnet ist. Wollen Sie beispielsweise Hosts in die Weiße Liste der Domäne example.com eintragen, so muss `"example.com"` in der Spalte *Domain* erscheinen. Die Spalte *Value* enthält den Host, den Sie in die Weiße Liste eintragen wollen, die Spalte *Typ* muss jeweils den Eintrag `"WhiteListHostDomain"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für den zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Domain","Value","Type","Comments"
"example.com","example.net","WhiteListHostDomain","Hier steht ein
Kommentar zu dem Host."
"example.com","mail.domain.com","WhiteListHostDomain",""
"example.com","smtp.company.mail","WhiteListHostDomain","Hier
steht ein weiterer Kommentar."
```

Export von Hosts aus der Weißen Liste

Um den Inhalt einer Weißen Liste für Hosts zu exportieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Auswahlmenü Für Domäne: den Eintrag Global, oder wählen Sie eine Domäne aus.
2. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
3. Klicken Sie auf *Speichern*.
4. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
5. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

Eintrag in der Weißen Liste

Dieses Dialogfenster dient dem Hinzufügen neuer Hosts zur Weißen Liste und dem Bearbeiten bestehender Einträge. Es wird immer dann aufgerufen, wenn Sie in der Symbolleiste am oberen Seitenrand auf *Neu* oder *Bearbeiten* klicken.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Listeneintrag

Für Domäne:
Um einen Host in die besondere Weißen Liste einer Domäne einzutragen, wählen Sie die Domäne aus diesem Auswahlmenü. Für einen Eintrag in die systemweite Weiße Liste wählen Sie Global.

Host:
Tragen Sie in dieses Feld den Host ein, dessen Nachrichten von allen Sicherheitsfunktionen ausgenommen werden sollen, für die Sie konfiguriert haben, dass Absender oder Hosts auf der Weißen Liste ausgenommen sind. Um alle Hosts einer Domäne in die Weiße Liste einzutragen, setzen Sie in den Hostnamen einen Stern. Ein Beispiel hierzu: "`*.example.org`" erfasst alle Nachrichten aller Subdomänen von example.org, wie etwa `mail.example.org` und `smtp.example.org`, in der Weißen Liste.

Kommentar:
In dieses Textfeld können Sie Kommentare oder Anmerkungen eintragen, die Sie zu diesem Eintrag erfassen wollen. Der Eintrag dient nur zu Ihrer Information.

Speichern und Beenden
Sobald Sie die Bearbeitung des Eintrags abgeschlossen haben, klicken Sie auf *Speichern und Beenden,* um den Eintrag in der Weißen Liste zu speichern.

Schließen
Um das Dialogfenster zu schließen, ohne den gerade bearbeiteten Eintrag zu speichern, klicken Sie auf dieses Steuerelement.

4.9.3 IPs

Mithilfe dieser Weißen Liste können bestimmte IP-Adressen von einzelnen Sicherheitsbeschränkungen ausgenommen werden, und Nachrichten, die von bestimmten Gegenstellen gesendet werden, können anhand der IP-Adresse der Gegenstelle von Sicherheitsprüfungen ausgenommen werden. Die Funktionen Heuristik und Bayes 162, DNSBL 169, DKIM-Prüfung 197 und auch fast alle anderen Sicherheitsfunktionen 154 von SecurityGateway können so konfiguriert werden, dass IPs und Nachrichten von diesen IPs von der Bearbeitung durch diese Funktionen ausgenommen sind, falls sie einen Treffer auf einer Weißen Liste auslösen. Jede Weiße Liste kann systemweit und nach Domänen getrennt geführt werden. Üblicherweise wird nur ein Eintrag zur gleichen Zeit einer Weißen Liste hinzugefügt; falls Sie jedoch in einem Durchgang mehrere Einträge hinzufügen wollen, steht Ihnen hierfür eine Importfunktion zur Verfügung. Sie kann mehrere Einträge aus einer Textdatei lesen und der Weißen Liste hinzufügen. Die Weiße Liste verfügt auch über eine Exportfunktion, mit deren Hilfe Sie den Inhalt der Weißen Liste in eine kommagetrennte Textdatei (Format CSV) speichern können.

Hinzufügen von IP-Adressen zur Weißen Liste

Um eine IP-Adresse in die Weiße Liste für IPs einzutragen, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Neu.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Weißen Liste 283 aufgerufen (vgl. unten).

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Bearbeiten einer IP-Adresse in der Weißen Liste

Um eine bereits in der Weißen Liste erfasste IP-Adresse zu bearbeiten, klicken Sie doppelt auf den zugehörigen Eintrag, oder wählen Sie den gewünschten Eintrag aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Bearbeiten.* Hierdurch wird das Dialogfenster zum Erstellen und Bearbeiten von Einträgen in der Weißen Liste 283 für den ausgewählten Eintrag aufgerufen.

Löschen von IP-Adressen aus der Weißen Liste

Um eine IP-Adresse oder mehrere IP-Adressen aus der Weißen Liste zu löschen, wählen Sie die gewünschten Einträge aus, und klicken Sie in der Symbolleiste am oberen Seitenrand auf *Löschen*. Um mehr als einen Eintrag auszuwählen, halten Sie die Strg-Taste gedrückt, während Sie die gewünschten Einträge durch Anklicken auswählen. Nachdem Sie auf *Löschen* geklickt haben, erscheint ein Bestätigungsdialog mit der Abfrage, ob Sie die gewünschten Einträge wirklich löschen wollen.

Import von IP-Adressen in die Weiße Liste

Um eine Liste von IP-Adressen in die Weiße Liste für IPs zu importieren, klicken Sie in der Symbolleiste am oberen Seitenrand auf *Import*. Es öffnet sich das Dialogfenster Listen importieren. Klicken Sie in diesem Dialogfenster zunächst auf *Durchsuchen,* und wählen Sie dann die Textdatei aus, deren Inhalt Sie in die Schwarze Liste importieren wollen. Klicken Sie auf *Listen importieren*, um mit dem Import zu beginnen.

Formate der CSV-Dateien

Sie können die CSV-Datei mithilfe eines beliebigen Texteditors (wie etwa Notepad) erstellen. Beachten Sie dabei das unten dokumentierte Format, und speichern Sie die Datei mit der Endung .csv. Die erste Zeile der CSV-Datei muss einen Feldraster enthalten, aus dem SecurityGateway entnehmen kann, in welcher Reihenfolge die Daten in den folgenden Zeilen erscheinen. Die Namen dieser Spalten müssen im Feldraster in englischer Sprache erscheinen. Jedes Datenelement muss in Anführungs- und Schlusszeichen gesetzt, und die Datenelemente in einer Zeile müssen durch ein Komma getrennt sein.

Import von IP-Adressen in die Globale Weiße Liste:

Die Spalte *Value* enthält die IP-Adresse, die Sie in die Weiße Liste eintragen wollen (CIDR-Schreibweise und die Jokerzeichen *, ? und # sind zulässig), die Spalte *Typ* muss jeweils den Eintrag `"WhiteListIPGlobal"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für die zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Value","Type","Comments"
"1.2.3.4","WhiteListIPGlobal","Hier steht ein Kommentar zu der
Adresse."
"1.1.1.1","WhiteListIPGlobal",""
"192.168.*.*","WhiteListIPGlobal","Hier steht ein weiterer
Kommentar."
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Import von IP-Adressen in die besondere Weiße Liste einer Domäne:
Die Spalte *Domain* enthält die Domäne, der diese Weiße Liste zugeordnet ist. Wollen Sie beispielsweise IP-Adressen in die Weiße Liste der Domäne example.com eintragen, so muss `"example.com"` in der Spalte *Domain* erscheinen. Die Spalte *Value* enthält die IP-Adresse, die Sie in die Schwarze Liste eintragen wollen (CIDR-Schreibweise und die Jokerzeichen *, ? und # sind zulässig), die Spalte *Typ* muss jeweils den Eintrag `"WhiteListIPDomain"` enthalten, und die Spalte *Comments* enthält den Kommentar, der für den zugehörigen Eintrag erfasst werden soll. Die Spalte *Comments* muss nicht zwingend verwendet werden. Wird sie aber verwendet, und soll für einen Eintrag kein Kommentar erfasst werden, so muss dies durch direkt aufeinander folgende Anführungs- und Schlusszeichen angezeigt werden.

Ein Beispiel für eine CSV-Datei:

```
"Domain","Value","Type","Comments"
"example.com","1.2.3.4","WhiteListIPDomain","Hier steht ein
Kommentar zu der Adresse."
"example.com","1.1.1.1","WhiteListIPDomain",""
"example.com","192.168.*.*","WhiteListIPDomain","Hier steht ein
weiterer Kommentar."
```

Export von IP-Adressen aus der Weißen Liste

Um den Inhalt einer Weißen Liste für IPs zu exportieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Auswahlmenü Für Domäne: den Eintrag Global, oder wählen Sie eine Domäne aus.
2. Klicken Sie in der Symbolleiste am oberen Seitenrand auf *Export.* Es erscheint ein Dialogfenster zum Herunterladen einer Datei.
3. Klicken Sie auf *Speichern*.
4. Wählen Sie einen Dateinamen und einen Speicherort für die Datei.
5. Klicken Sie auf *Speichern* und anschließend auf *Schließen*.

Eintrag in der Weißen Liste

Dieses Dialogfenster dient dem Hinzufügen neuer IP-Adressen zur Weißen Liste und dem Bearbeiten bestehender Einträge. Es wird immer dann aufgerufen, wenn Sie in der Symbolleiste am oberen Seitenrand auf *Neu* oder *Bearbeiten* klicken.

Listeneintrag

Für Domäne:
Um eine IP-Adresse in die besondere Weiße Liste einer Domäne einzutragen, wählen Sie die Domäne aus diesem Auswahlmenü. Für einen Eintrag in die systemweite Weiße Liste wählen Sie Global.

IP-Adresse:
Tragen Sie in dieses Feld die IP-Adresse ein, deren Nachrichten Sie von allen Sicherheitsfunktionen ausnehmen wollen, die Sie so konfiguriert haben, dass Nachrichten von Absendern oder IP-Adressen auf der Weißen Liste ausgenommen sind. Die CIDR-Schreibweise ist zulässig, und Sie können die Jokerzeichen *, ? und # verwenden, um Adressblöcke mit einem einzigen Eintrag zu erfassen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kommentar:
In dieses Textfeld können Sie Kommentare oder Anmerkungen eintragen, die Sie zu diesem Eintrag erfassen wollen. Der Eintrag dient nur zu Ihrer Information.

Speichern und Beenden
Sobald Sie die Bearbeitung des Eintrags abgeschlossen haben, klicken Sie auf *Speichern und Beenden,* um den Eintrag in der Schwarzen Liste zu speichern.

Schließen
Um das Dialogfenster zu schließen, ohne den gerade bearbeiteten Eintrag zu speichern, klicken Sie auf dieses Steuerelement.

4.10 Sieve-Skripte

Sieve ist eine als Standard empfohlene Filter-Sprache für die E-Mail-Filterung. Sie ist erweiterbar und extrem flexibel. SecurityGateway nutzt Sieve-Skripte als Teil der Kernfunktionen in weitem Umfang sowie als Grundlage für die Funktionen zum Filtern von Nachrichten-Inhalten 252. SecurityGateway unterstützt benutzerdefinierte Skripte, die für eine Vielzahl von Anwendungszwecken genutzt werden können. SecurityGateway unterscheidet nach zwei Kategorien von Skripten, die beide über die Seite Sieve-Skripte verwaltet werden:

Durch das System erzeugte Skripte—Durch diese Skripte sind die Kernfunktionen von SecurityGateway verwirklicht. Wird über die Administrator-Schnittstelle eine Änderung an der Konfiguration vorgenommen, so wird das Skript, auf das sich die Konfigurationsänderung auswirkt, und das auf der Seite Sieve-Skripte angezeigt wird, entsprechend angepasst. Durch das System erzeugte Skripte können nur auf diesem Weg bearbeitet werden. Sie sind gegen Schreibzugriffe geschützt und können daher über die Seite Sieve-Skripte nicht direkt bearbeitet werden. Obwohl also der Inhalt der durch das System erzeugten Skripte der direkten Bearbeitung entzogen ist, stehen Ihnen Steuerelemente zur Verfügung, mit denen Sie die Reihenfolge ändern können, in der die Skripte abgearbeitet werden.

Durch den Administrator erzeugte Skripte—Von der Seite Sieve-Skripte aus können Sie eigene benutzerdefinierte Skripte erstellen. Da Sieve eine äußerst flexible Filter-Methodik bereitstellt, können Sie eine beliebige Zahl dieser Skripte erstellen, um Ihre individuellen Anforderungen umzusetzen. Um diese Skripte zu erstellen, benötigen Sie allerdings ausreichende Kenntnisse über die Verfahren bei der SMTP-Übermittlung und über die Sieve-Filtersprache selbst. Die Sieve-Implementation für SecurityGateway enthält den Grundwortschatz, mehrere standardisierte Erweiterungen und eine erhebliche Zahl individueller Erweiterungen 296.

Diese Seite, sowie die Seiten Erstellen von Sieve-Skripten 287 und Sieve-Erweiterungen für SecurityGateway 296 enthalten zwar grundlegende Informationen über Sieve und über die Art der Nutzung in SecurityGateway, eine erschöpfende Darstellung der Sprache selbst würde aber den Rahmen dieses Handbuchs sprengen. Falls Sie an weiteren Informationen über Sieve interessiert sind, sollten Sie die, allerdings in englischer Sprache verfügbaren, offiziellen Dokumente auf der Website der IETF online einsehen: Sieve: An Email Filtering

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

> Language [Sieve: Eine-Filtersprache für E-Mail] (RFC-5228), Sieve's Copy Extension [Die Sieve-Erweiterung Kopieren] (RFC 3894), Sieve's Body Extension [Die Sieve-Erweiterung Nachrichtentext] (RFC-5173), Sieve's Reject Extension [Die Sieve-Erweiterung Abweisen] (RFC-5429), Sieve's Variables Extension [Die Sieve-Erweiterung Variablen] (RFC-5229) und Spamtest and VirusTest Extensions [Erweiterungen Spamtest und VirusTest] (RFC-3685).

Liste der Sieve-Skripte

Die Seite Sieve-Skripte enthält eine Übersicht aller durch das System und den Administrator definierten Skripte. Die Liste ist in sechs Abschnitte untergliedert: IP, HELO, AUTH, MAIL, RCPT und DATA. Diese Abschnitte entsprechen den einzelnen Nachrichten-Ereignisgruppen oder "Phasen" in der SMTP-Übermittlung, wobei jedes Skript in dem Abschnitt erscheint, zu dem es gehört. Die einzelnen Abschnitte werden nach einander abgearbeitet, wobei zuerst die globalen, dann die Domänen-spezifischen Skripte abgearbeitet werden. Die Skripte werden in der Reihenfolge abgearbeitet, in der sie in der Liste erscheinen. Mithilfe der Aufwärts- und Abwärts-Pfeile können Sie die Position eines Skripts und damit die Reihenfolge, in der die Skripte innerhalb eines Abschnitts abgearbeitet werden, beeinflussen.

Die Symbolleiste am oberen Seitenrand enthält die folgenden drei Optionen:

Neu
Um ein neues Skript zu erstellen, klicken Sie auf *Neu.* Es öffnet sich der Editor für Sieve-Skripte 286.

Bearbeiten
Um ein bestehendes Skript in den Editor für Sieve-Skripte 286 zu laden, wählen Sie das Skript aus, und klicken Sie dann in der Symbolleiste auf *Bearbeiten*. Sie können stattdessen auch auf das Skript doppelklicken. Durch das System erzeugte System erzeugte Skripte können nicht bearbeitet werden. Sie können trotzdem in den Editor für Sieve-Skripte geladen werden, sodass sie betrachtet werden können und ihr Inhalt in die Zwischenablage kopiert werden kann. Dieser Inhalt kann dann für ein neues, benutzerdefiniertes Skript verwendet werden.

Löschen
Um ein benutzerdefiniertes Skript zu löschen, wählen Sie das Skript in der Liste aus, und klicken Sie dann auf *Löschen*. Es erscheint eine Sicherheitsabfrage, auf die Sie bestätigen müssen, dass Sie das Skript wirklich löschen wollen. Durch das System erzeugte Skripte können nicht gelöscht werden.

Die Liste der Skripte ist in folgende fünf Spalten unterteilt:

Aktiviert
In dieser Spalte erscheint für jedes Skript ein Kontrollkästchen, mit dessen Hilfe Sie ein Skript schnell aktivieren und deaktivieren können. Um ein Skript zu aktivieren, setzen Sie einen Haken in das zugehörige Kontrollkästchen, um es zu deaktivieren, entfernen Sie den Haken. Nur benutzerdefinierte Skripte können mithilfe des Kontrollkästchens aktiviert und deaktiviert werden. Um ein durch das System erzeugtes Skript zu aktivieren oder zu deaktivieren, müssen Sie die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Konfigurationseinstellungen für die Funktion nutzen, die zu dem Skript gehört (z.B. Graue Liste, IP-Abschirmung, Bayes'sches automatisches Lernverfahren usw.).

Bereich
In dieser Spalte wird der Anwendungsbereich für das Skript angezeigt. Der Anwendungsbereich kann "global" oder Domänen-spezifisch sein. Globale Skripte werden für alle Nachrichten verarbeitet. Domänen-spezifische Skripte werden nur für die Nachrichten der zugehörigen Domäne verarbeitet.

Reihenfolge
Die Skripte werden in der Reihenfolge abgearbeitet, in der sie erscheinen. Sie können die Reihenfolge mithilfe der Aufwärts- und Abwärts-Pfeile in dieser Spalte verändern.

Name des Skripts
In dieser Spalte erscheint der Name oder die Bezeichnung, anhand derer das Skript identifiziert werden kann. Sie legen diesen Namen bei der Erstellung eines benutzerdefinierten Skripts fest.

Skript
Indem Sie die Maus über dem Symbol in dieser Spalte stehen lassen, können Sie einen Tooltipp aufrufen, der den Text des Skripts enthält. Um den Text eines Skripts eingehender zu untersuchen, klicken Sie auf das Skript doppelt, um es in den Editor für Sieve-Skripte 286 zu laden.

Editor für Sieve-Skripte

Der Editor für Sieve-Skripte wird immer dann aufgerufen, wenn Sie in der Symbolleiste der Übersicht über die Sieve-Skripte auf *Neu* oder *Bearbeiten* klicken. Er dient sowohl der Erstellung neuer als auch der Bearbeitung bestehender Sieve-Skripte. Nachdem Sie ein Skript im Editor erstellt oder bearbeitet haben, klicken Sie in der Symbolleiste des Editors auf *Speichern und Beenden*, um das Skript zu speichern und zur Liste der Sieve-Skripte zurückzukehren.

Eigenschaften des Skripts

Verarbeitung dieses Skripts aktivieren
Dieses Kontrollkästchen entspricht der Spalte *Aktiviert* in der Liste der Sieve-Skripte. Per Voreinstellung sind Skripte nach der Erstellung aktiv, sodass sie der Liste der Skripte hinzugefügt und während des weiter unten definierten *Nachrichten-Ereignisses* abgearbeitet werden. Um ein Skript zu deaktivieren, entfernen Sie den Haken aus dem Kontrollkästchen. Deaktivierte Skripte erscheinen zwar noch in der Liste, werden aber nicht mehr abgearbeitet. Durch das System erzeugte Skripte können mithilfe dieses Kontrollkästchens nicht aktiviert und deaktiviert werden. Sie müssen mithilfe der Konfigurationseinstellungen verwaltet werden, die zu den durch sie verwirklichten Funktionen gehören.

Name des Skripts:
Tragen Sie in dieses Feld einen Titel oder einen kurzen Beschreibungstext für Ihr Skript ein. Durch das System erzeugte Skripte können nicht umbenannt werden.

Nachrichten-Ereignis:
Beim Erstellen eines Skripts bestimmen Sie mithilfe dieses Auswahlmenüs, in welcher Phase der SMTP-Verbindung das Skript abgearbeitet werden soll.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Erstellen Sie beispielsweise ein Skript, das einen Vergleich mit dem Empfänger einer Nachricht durchführt, so wählen Sie hier zweckmäßigerweise RCPT oder DATA aus, da der Empfänger der Nachricht erst bekannt wird, wenn die SMTP-Verbindung die Phase erreicht hat, in der der Befehl RCPT gegeben wird. Die sechs Ereignisgruppen oder Phasen sind, in der Reihenfolge, in der sie eintreten: IP, HELO, AUTH, MAIL, RCPT und DATA.

Bereich:
Mithilfe dieser Option legen Sie den Anwendungsbereich des Skripts fest: Global oder *Domänen*-bezogen. Wählen Sie hier *Global* aus, so wird das Skript unabhängig von der Zieldomäne der Nachricht abgearbeitet. Wählen Sie hier *Domäne* aus, so wird das Skript nur für Nachrichten abgearbeitet, die für die angegebene Domäne eingehen. *Domäne* kann nur ausgewählt werden, falls als *Nachrichten-Ereignis* oben RCPT oder DATA ausgewählt wurde, da die Domäne des Empfängers erst bekannt ist, wenn eine dieser Phasen in der SMTP-Verbindung erreicht wurden.

Domäne:
Falls Sie im Feld *Bereich* den Eintrag *Domäne* auswählen, erscheint dieses zusätzliche Auswahlmenü. Mit seiner Hilfe können Sie die Domäne auswählen, mit der Sie dieses Skript verknüpfen wollen.

Text des Skripts:
In dieses Textfeld muss der eigentliche Text für das Skript in der Sieve-Filtersprache eingetragen werden. Einige Beispiel-Skripte und grundlegende Informationen über sie Sprache Sieve enthält der Abschnitt Erstellen von Sieve-Skripten 287.

4.10.1 Erstellen von Sieve-Skripten

Diese Seite bietet, neben den Seiten Sieve-Skripte 284 und Sieve-Erweiterungen für SecurityGateway 296, einen grundlegenden Überblick über die Sieve-Filtersprache für E-Mail und ihre Implementation in SecurityGateway. Der erste Abschnitt dieser Seite gibt einen Überblick über die grundlegenden Bestandteile eines Sieve-Skripts. Der nächste Abschnitt bietet einen Überblick über verschiedene Struktur-Elemente 289 der Sprache. Es folgen Übersichten über die Standard-Befehle für Steuerung 290, Test 291 und Aktionen 294, die unterstützt werden. Und schließlich finden sich am Ende der Seite mehrere Beispiel-Skripte 295, aus denen Sie Anregungen entnehmen können.

Falls Sie an weiteren Informationen über Sieve interessiert sind, sollten Sie die, allerdings in englischer Sprache verfügbaren, offiziellen Dokumente auf der Website der IETF online einsehen: Sieve: An Email Filtering Language (RFC-5228), Sieve's Copy Extension (RFC 3894), Sieve's Body Extension (RFC-5173), Sieve's Reject Extension (RFC-5429), Sieve's Variables Extension (RFC-5229) und Spamtest and VirusTest Extensions (RFC-3685).

Sie können auch unter www.mdaemon.com/Support/ die neuesten Optionen für technische Unterstützung und Hilfe zu SecurityGateway erhalten. Hierzu gehören die telefonische Unterstützung, Unterstützung per E-Mail, eine

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

> Wissensdatenbank, oft gestellte Fragen (FAQ), Foren und anderes mehr.

Bestandteile eines Sieve-Skripts

Ein Sieve-Skript besteht aus vier grundlegenden Bestandteilen:

1. **Anforderungen**—In diesem Teil werden die Sieve-Erweiterungen definiert, die für ein bestimmtes Skript erforderlich sind. Werden in einem Skript Befehle benutzt, die zu einer optionalen Erweiterung gehören, so müssen alle betroffenen optionalen Erweiterungen zwingend mithilfe des Befehls `require` am Beginn des Skripts bezeichnet und einbezogen werden. An das Ende der Parameter, die auf den Befehl `require` folgen, muss ein Strichpunkt gesetzt werden.

   Beispiele:

   ```
   require "securitygateway";
   ```

   -und-

   ```
   require ["securitygateway", "fileinto"];
   ```

2. **Bedingungen**—In diesem Teil des Skripts werden die Komponenten bezeichnet, nach denen Sie in einer Nachricht suchen wollen. Es werden auch die anzuwendenden Such- und Vergleichsverfahren bestimmt.

   Beispiele:

   ```
   if size :over 1M
   ```

   -und-

   ```
   if header :contains ["to", "cc"] "Frank Thomas"
   ```

3. **Aktionen**—Hier werden die Aktionen und Befehle festgelegt, die ausgeführt werden, falls die oben bestimmten Bedingungen das Ergebnis `True` erbringen. Jede Aktion muss durch einen Strichpunkt abgeschlossen sein, und jede Gruppe von Aktionen muss in geschweifte Klammern ("{" und "}") gesetzt sein.

   Beispiele:

   ```
   if size :over 1M { discard; }
   ```

   -und-

   ```
   if header :contains ["to", "cc"] "Frank Thomas" {
   bayes-learn "spam";
   fileinto "spam";
   }
   ```

4. **Kommentare**—Sie können zu Erläuterungszwecken Kommentare in Ihre Sieve-Skripte einfügen, etwa, als Gedächtnisstütze für den Zweck des Sieve-Skripts oder aus sonstigen Gründen. Es sind zwei Arten von Kommentaren zugelassen: einzeilige und mehrzeilige Kommentare. Einzeilige Kommentare beginnen mit "#"

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

und Enden am Zeilenende (also beim nächsten CRLF). Mehrzeilige Kommentare beginnen mit "/*", können sich über mehrere Zeilen erstrecken, und enden mit "*/".

Beispiele:

```
# Nachrichten über 1 MB werden verworfen
if size :over 1M { discard; }
```

-und-

```
if header :contains "from" "Frank Thomas" {
/* Frank Thomas sendet uns überwiegend Spam, deswegen
verschiebt
dieses Skript automatisch alle von ihm erhaltenen Nachrichten
in die Quarantäne der Benutzer. */
fileinto "spam";
}
```

Struktur-Elemente

Strings
Text-Strings oder Zeichenketten beginnen und enden mit je einem Anführungs- und Schlusszeichen. Ein Beispiel: `"Frank Thomas"`.

In Anführungs- und Schlusszeichen gesetzte Texte dürfen ihrerseits umgekehrte Schrägstriche (Backslashes) und Anführungs- und Schlusszeichen nur enthalten, wenn diesen Zeichen ein weiterer Backslash vorangestellt wird. Es werden daher in einem solchen String `\\` als `\` und `\"` als `"` behandelt. Anderen Zeichen soll in den Strings kein Escape-Zeichen vorangestellt werden.

Listen von Strings
Falls Sie in einem Skript eine Gruppe von Strings nutzen möchten, trennen Sie jeden in Anführungs- und Schlusszeichen gesetzten String durch ein Komma ab, und setzen sie die gesamte Gruppe in eckige Klammern.

Ein Beispiel:

```
if header :contains ["to", "cc"] ["me@xyz.com", "you@xyz.com",
"us@xyz.com"]
```

Der im Beispiel genannte Test zeigt das Ergebnis `True` , falls entweder die Kopfzeile To oder die Kopfzeile CC eine der drei aufgeführten Adressen enthält.

Kopfzeilen
Die Namen von Kopfzeilen dürfen keinen Doppelpunkt enthalten.

Ein Beispiel:

`if header :is "to:"` (unzulässig)

`if header :is "to"` (zulässig)

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Listen von Tests
Ähnlich wie Gruppen von Strings, können auch Gruppen von Tests in ein Skript eingefügt werden, indem die Gruppe in runde Klammern gesetzt wird. Diese Vorgehensweise ist bei Nutzung der Test-Befehle `allof` und `anyof` bisweilen nötig, da sie logischen "UND"- und "ODER"-Ausdrücken entsprechen.

Ein Beispiel:

```
if anyof (size :over 1M, header :contains "subject" ["big file",
"mega file"])
{
discard;
}
```

Parameter und Vergleichsoperatoren
Zu den meisten Befehlen gehört mindestens ein Parameter oder Argument, der festlegt, wie genau der Befehl verfahren soll. Es sind mehrere Arten von Parametern verfügbar, wie etwa Positions-Parameter, getaggte Parameter und optionale Parameter. Getaggte Parameter und Vergleichsoperatoren wird beispielsweise ein Doppelpunkt vorangestellt. `:contains`, `:is`, `:matches`, `:over` und `:under` sind Beispiele für getaggte Parameter. Einige getaggte Parameter sind auf bestimmte Befehle beschränkt. Weitere Informationen über die verschiedenen Typen von Parametern enthält RFC-5228.

Aktionen
Jede Aktion muss durch einen Strichpunkt abgeschlossen werden, und jede Gruppe von Aktionen muss in geschweifte Klammern gesetzt werden.

Ein Beispiel:

```
if header :contains ["to", "cc"] "Frank Thomas" {
bayes-learn "spam";
fileinto "spam";
}
```

Steuerbefehle

Die Sieve-Sprache kennt drei Steuerbefehle:

require
Dieser Steuerbefehl wird am Anfang eines Skripts eingesetzt und bestimmt, welche optionalen Erweiterungen in dem Skript verwendet werden.

Ein Beispiel:

```
require ["securitygateway", "fileinto"];
```

if / elsif / else
Der Befehl `if` ist der wichtigste Steuerbefehl. Obwohl es, technisch gesehen, drei in Wechselbeziehung stehende Befehle gibt, können `elsif` und `else` nicht unabhängig von `if` verwendet werden. Tritt `if` in einem Skript auf, so wird die zugehörige Bedingung darauf hin geprüft, ob sie wahr ist. Ist dies der Fall, so werden die hiermit verknüpften Aktionen ausgeführt.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Ergibt die Prüfung nach `if` das Ergebnis falsch, so wird als nächstes `elsif` geprüft. Ergibt `elsif` das Ergebnis wahr, so werden die hiermit verknüften Aktionen ausgeführt. Ergibt auch die Prüfung nach `elsif` das Ergebnis falsch, so wird der Vorgang mit dem jeweils nächsten Befehl `elsif` fortgesetzt, bis nach einer Prüfung das Ergebnis wahr eintritt.

Ergeben alle Prüfungen nach `if` und `elsif` das Ergebnis falsch, und folgt ein Befehl `else`, so werden die mit diesem Befehl verknüpften Aktionen ausgeführt.

stop
Der Befehl `stop` beendet die Verarbeitung des Skripts.

Test-Befehle

Nachfolgend sind die Standard-Test-Befehle beschrieben, die die Sieve-Implementation von SecurityGateway unterstützt. Die Befehle `body` und `envelope` sind jedoch Erweiterungen; falls Sie einen dieser Befehle in einem Skript verwenden wollen, müssen Sie sie mithilfe des Befehls `require` einbinden. Es stehen in der Erweiterung `securitygateway` noch zahlreiche weitere Test-Befehle zur Verfügung. Sie sind auf der Seite Sieve-Erweiterungen für SecurityGateway 296 beschrieben.

address
Durch diesen Befehl können Sie eine Kopfzeile auswerten, wobei die Auswertung auf eine in der Kopfzeile enthaltene E-Mail-Adresse beschränkt wird und sonstige Inhalte der Kopfzeile, wie etwa allgemeine Texte und Namen, außer Betracht bleiben. Enthält beispielsweise die Kopfzeile `"to"` den Text `"Frank Thomas" <frank@example.com>`, so würde die Prüfung `header :is "to" "frank@example.com"` ein negatives Ergebnis erbringen. Die Prüfung `address :is "to" "frank@example.com"` würde hingegen ein positives Ergebnis erbringen, weil hierbei nur die Adresse ausgewertet und berücksichtigt wird.

Für diesen Befehl stehen auch drei optionale getaggte Parameter zur Verfügung: `":localpart"`, `":domain"` und `":all"`. Der Parameter `:localpart` wertet nur den linken Teil der Adresse aus (im Beispiel oben "frank" aus "frank@example.com"), der Parameter `:domain` wertet nur die Domäne einer Adresse aus (im Beispiel "example.com"), und `:all` wertet die gesamte Adresse aus. Werden keine Parameter angegeben, so wird per Voreinstellung `:all` genutzt.

Ein Beispiel:

```
require "fileinto";
if address :domain :is "from" "spammer.com" {
fileinto "spam";
}
```

allof
Hierdurch wird eine logische UND-Verknüpfung hergestellt. Alle geprüften Bedingungen müssen wahr sein, damit die verknüpfte Aktion ausgeführt wird.

Ein Beispiel:

```
if allof (header :contains "from" "J.Lovell", header :contains
"to" "Bubba")
{
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

```
fileinto "spam";
}
```

anyof
Hierdurch wird eine logische ODER-Verknüpfung hergestellt. Es muss eine beliebige der geprüften Bedingungen wahr sein, damit die verknüpfte Aktion ausgeführt wird.

Ein Beispiel:

```
if anyof (size :over 1M, header :contains "subject" "große
Dateianlage")
{
reject "Ich möchte keine Nachrichten, die behaupten, große
Dateianlagen zu haben.";
}
```

body
Der Befehl `body` ist eine optionale Erweiterung. Um sie in einem Skript zu nutzen, müssen Sie daher den Befehl `require "body"` an den Beginn des Skripts setzen. Der Befehl wertet den Nachrichtentext einer Nachricht aus. Nähere Informationen hierzu erhalten Sie in dem Artikel Sieve's Body Extension (RFC-5173).

Ein Beispiel:

```
require ["body", "fileinto"];
if body :text :contains "Geheim-Formel" {
fileinto "admin";
}
```

envelope
Der Befehl `envelope` ist eine optionale Erweiterung. Um sie in einem Skript zu nutzen, müssen Sie daher den Befehl `require "envelope"` an dem Beginn des Skripts setzen. Der Befehl wertet die Inhalte des SMTP-Umschlags SMTP `MAIL From` und `RCPT To` aus; hierzu müssen als Parameter `"from"` und `"to"` eingesetzt werden.

Ein Beispiel:

```
require "envelope";
if envelope :is "from" "MrsFrank@company.com" {
redirect "frankshome@example.com";
}
```

exists
Diese Prüfung ergibt "wahr", falls die in den Parametern angegebenen Kopfzeilen in der Nachricht vorhanden sind. Es müssen jeweils alle angegebenen Kopfzeilen vorhanden sein.

Beispiele:

```
if exists "x-custom-header" {
redirect "admin@example.com";
}
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

-und-

```
if not exists ["from", "date"] {
discard;
}
```

false
Diese Prüfung ergibt immer das Ergebnis "falsch".

header
Diese Prüfung ergibt "wahr", falls der Inhalt der angegebenen Kopfzeile mit den angegebenen Bedingungen übereinstimmt. Wird kein Vergleichsoperator angegeben, so wird per Voreinstellung `:is` genutzt.

Ein Beispiel:

```
require "fileinto"
if header :is "x-custom-header" "01" {
fileinto "admin";
}
```

not
Die Verwendung dieses Befehls in Verbindung mit einer anderen Prüfung bedeutet, dass das Ergebnis der Prüfung umgekehrt sein muss, damit die mit der Prüfung verknüpfte Aktion ausgeführt wird. Beispielsweise bedeutet die Prüfung `if not exists ["from", "date"] { discard; }`, dass die Aktion `discard` ausgeführt wird, falls eine Nachricht die Kopfzeilen "from" und "date" nicht beide enthält. Würde in dem Beispiel der Befehl `not` weggelassen werden, so würde die Nachricht gelöscht werden, falls die Kopfzeilen beide existierten.

size
Zu dem Befehl `size` gehören die getaggten Parameter "`:over`" und "`:under`", nach denen jeweils ein numerischer Wert folgen muss. Diese Parameter bestimmen, ob die Größe einer Nachricht über oder unter dem angegebenen Wert liegen muss, damit die Prüfung das Ergebnis "wahr" erbringt. Um zu bestimmen, dass der Wert in Megabyte angegeben ist, können Sie dem Wert ein M anfügen, für Kilobyte ein K, und für Byte wird kein Buchstabe angefügt.

Ein Beispiel:

```
if size :over 500K {
discard;
}
```

true
Diese Prüfung ergibt immer das Ergebnis "wahr".

spamtest
Der Befehl `spamtest` ist eine optionale Sieve-Erweiterung, die in dem Dokument Spamtest and VirusTest Extensions (RFC-3685) auf der Website `ietf.org` näher beschrieben ist. Dieses Dokument enthält Einzelheiten zu dieser Erweiterung.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

virustest
Der Befehl `virustest` ist eine optionale Sieve-Erweiterung, die in dem Dokument Spamtest and VirusTest Extensions (RFC-3685) auf der Website `ietf.org` näher beschrieben ist. Dieses Dokument enthält Einzelheiten zu dieser Erweiterung.

Aktions-Befehle

Nachfolgend sind die Standard-Aktions-Befehle beschrieben, die von SecurityGateway unterstützt werden. Die Befehle `fileinto` und `reject` sind jedoch Erweiterungen; falls Sie einen dieser Befehle in einem Skript verwenden wollen, müssen Sie sie mithilfe des Befehls `require` einbinden. Es stehen in der Erweiterung `securitygateway` noch zahlreiche weitere Aktions-Befehle zur Verfügung. Sie sind auf der seite Sieve-Erweiterungen für SecurityGateway 296 beschrieben.

fileinto
Der Aktions-Befehl `fileinto` ist eine optionale Erweiterung. Um sie in einem Skript zu nutzen, müssen Sie daher den Befehl `require "fileinto"` an den Beginn des Skripts setzen. Zu diesem Befehl gehören zwei Parameter: `"spam"` und `"admin"`. `"spam"` verschiebt die Nachricht in die Quarantäne des Benutzers 308, und `"admin"` verschiebt sie in die Administrative Quarantäne 310.

Ein Beispiel:

```
require "fileinto";
if header :contains "from" "Frank Thomas" {
fileinto "spam";
}
```

discard
Durch diesen Befehl wird eine Nachricht ohne weiteres gelöscht. Es werden auch keine Statusnachrichten über den Löschvorgang versandt.

Ein Beispiel:

```
if size :over 2M { discard; }
```

keep
Diese Aktion bewirkt, dass die Nachricht an dem Standard-Speicherort gespeichert wird.

redirect
Dieser Befehl leitet die Nachricht an die in dem zugehörigen Parameter angegebene Adresse um, wobei der Nachrichtentext und die bestehenden Kopfzeilen nicht geändert werden. Dieser Befehl unterstützt auch die optionale Erweiterung `:copy`, die bewirkt, dass eine Kopie der Nachricht an die angegebene Adresse gesandt, die Nachricht selbst aber nicht umgeleitet wird. Es sind dann zusätzlich zum Versand der Kopie weitere Aktionen möglich.

Ein Beispiel:

```
require "copy";
if header :contains "subject" "Antwort auf XYZ" {
redirect :copy "offers@example.com";
bayes-learn "ham";
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

```
}
```

reject
Der Aktions-Befehl `reject` ist eine optionale Erweiterung. Um sie in einem Skript zu nutzen, müssen Sie daher den Befehl `require "reject"` an den Beginn des Skripts setzen. Dieser Befehl bewirkt, dass die Nachricht während der SMTP-Verbindung mit einem Antwortkode 5xx angewiesen wird; dabei kann eine kurze, im Parameter angegebene Meldung übermittelt werden.

Ein Beispiel:

```
require "reject";
if size :over 5M {
reject "Empfang nicht möglich! Diese Nachricht ist zu groß.";
}
```

vnd.mdaemon.securewebmsg
Dieser Aktions-Befehl bewirkt, dass eine Nachricht mithilfe des SecurityGateway-Portals für Sichere Nachrichten[112] versandt wird.

Ein Beispiel:

```
require
["securitygateway","reject","fileinto","envelope","body","regex"]
;
if allof(header :matches "subject" "[Sichere Nachricht]*")

{

vnd.mdaemon.securewebmsg;

}
```

Sieve-Beispielskripte

Alle Nachrichten abweisen, deren Betreffzeile "[SPAM]" enthält

```
require "reject";
if header :contains "subject" "[SPAM]"
{
reject "Ich will Ihren Spam nicht haben";
}
```

Alle Nachrichten an einen bestimmten Vor- und Nachnamen abweisen

```
require ["securitygateway","reject"];
if header :contains "to" "Vor- und Nachname"
{
bayes-learn "spam";
reject "Ich will Ihren Spam nicht haben";
}
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Benutzerdefiniertes Bayes'sches automatisches Lernverfahren

```
require ["securitygateway","comparator-i;ascii-numeric"];
if whitelisted
{
bayes-learn "ham";
}
elsif anyof(blacklisted,spamtotal :value "gt" :comparator
"i;ascii-numeric" "20.0")
{
bayes-learn "spam";
}
```

Treffer aus DNSBL in Graue Liste eintragen

```
require "securitygateway"];
if not lookup "rblip" "all" {greylist;}
```

Administrator benachrichtigen, wenn große Nachrichten eingehen

```
require ["securitygateway"];
if size :over 1M
{
alert text:
To: admin@company.mail
From: postmaster@$RECIPIENTDOMAIN$
Subject: Nachricht des Inhaltsfilters von SecurityGateway
X-Attach-Msg: No
$RECIPIENT$ hat eine Nachricht empfangen, die größer als 1MB ist.
.
;
}
```

Als sichere Nachricht senden, falls die Betreffzeile mit "[Sichere Nachricht]" beginnt

```
require
["securitygateway","reject","fileinto","envelope","body","regex"]
;
if allof(header :matches "subject" "[Sichere Nachricht]*")

{

vnd.mdaemon.securewebmsg;

}
```

4.10.2 Sieve-Erweiterungen

Um die in SecurityGateway enthaltenen Sieve-Erweiterungen in einem Skript zu nutzen, müssen Sie an den Beginn des Skripts den folgenden Befehl `require` stellen:

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

```
require "securitygateway";
```

Test-Befehle

ip

Die Prüfung `ip` kann zu einem beliebigen Zeitpunkt während des SMTP-Vorgangs durchgeführt werden (also während jeder Ereignisgruppe[286]).

- **cidr**—Der zweite Parameter ist die IP-Adresse oder das Muster, das mit der IP-Adresse des Clients verglichen wird. Es kann eine bestimmte IP-Adresse, ein Adressbereich in CIDR-Schreibweise (z.B. 10.0.0.0/24) oder ein Muster mit Jokerzeichen: ? (1 beliebiges Zeichen), * (kein Zeichen oder ein oder mehrere beliebige Zeichen), # (mindestens eine Ziffer) sein (z.B. 10.*.*.*).

  Beispiel-Kode: `if not ip :cidr "10.0.0.0/24" { greylist; }`

- **public**—Wahr, falls die IP-Adresse des Clients nicht zu einem privaten Subnetz nach RFC-1918 gehört, keine Loopback-Adresse und keine durch DHCP automatisch vergebene Adresse ist, ansonsten falsch (`127.0.0.0/8`, `192.168.0.0/16`, `10.0.0.0/8`, `172.16.0.0/12`, `169.254.0.0/16`).

  Beispiel-Kode: `if ip "public" { greylist; }`

- **private**—Logisches Gegenteil von public.
- **ssl**—Wahr, falls der Client erfolgreich eine verschlüsselte Verbindung (über SSL) aufgebaut hat.
- **des**—Wahr, falls der Client ein Mailserver der Domäne ist.

lookup

Es hängt vom ersten Parameter ab, wann die Prüfung `lookup` aufgerufen werden kann:

- **ptr**—Ist dies der erste Parameter, so kann die Prüfung `lookup` jederzeit durchgeführt werden. Der zweite Parameter kann ein normaler getaggter Parameter oder "resolves", "resolvestoclient" oder "error" sein.
  - **resolves**—Wahr, falls der PTR-Eintrag existiert.
  - **resolvestoclient**—Wahr, falls sich der PTR-Eintrag richtig auflösen lässt, also eine Abfrage des A-Eintrags für den PTR-Host die IP-Adresse des Clients ergibt.
  - **error**—Wahr, falls ein vorübergehender Fehler in der DNS-Abfrage aufgetreten ist.
- **helo**—Ist dies der erste Parameter, so kann die Prüfung `lookup` erst bei oder nach Gabe des Befehls HELO durchgeführt werden. Der zweite Parameter kann "resolves", "resolvestoclient" oder "error" sein.
  - **resolves**—Wahr, falls der HELO-Parameter eine gültige IP-Adresse oder ein gültiger Hostname ist.
  - **resolvestoclient**—Wahr, falls der HELO-Parameter richtig ist, also eine Abfrage des A-Eintrags für den Parameter die IP-Adresse des Clients ergibt.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **error**—Wahr, falls ein vorübergehender Fehler in der DNS-Abfrage aufgetreten ist.

- **mail**—Ist dies der erste Parameter, so kann die Prüfung `lookup` erst bei oder nach Gabe des Befehls MAIL durchgeführt werden. Der zweite Parameter kann "resolves", "resolvestoclient" oder "error" sein.
  - **resolves**—Wahr, falls die Domäne aus MAIL FROM eine gültige Domäne ist.
  - **resolvestoclient**—Wahr, falls die Domäne aus MAIL FROM richtig ist, also eine Abfrage des A-Eintrags der Domäne aus MAIL FROM die IP-Adresse des Clients ergibt.
  - **error**—Wahr, falls ein vorübergehender Fehler in der DNS-Abfrage aufgetreten ist.

- **spf**—Ist dies der erste Parameter, so kann die Prüfung `lookup` erst bei oder nach Gabe des Befehls MAIL durchgeführt werden. Der zweite Parameter kann "pass", "fail" oder "error" sein.
  - **pass**—Wahr, falls für den Absender das SPF-Ergebnis pass, lautet; falsch, bei Ergebnis neutral oder fail.
  - **fail**—Wahr, falls die SPF-Prüfung für den Absender fehlschlägt; falsch bei Ergebnis neutral oder pass.
  - **error**—Wahr, falls bei der Verarbeitung ein Fehler aufgetreten ist (meist ein Fehler in der DNS-Abfrage).

- **rblip**—Ist dies der erste Parameter, so kann die Prüfung `lookup` jederzeit durchgeführt werden. Der zweite Parameter kann "all", "any oder "error" sein.
  - **all**—Wahr, falls die IP-Adresse des Clients alle Abfragen von Schwarzen Listen für DNS bestanden hat.
  - **any**—Wahr, falls die IP-Adresse des Clients mindestens eine Abfrage einer Schwarzen Liste für DNS bestanden hat.
  - **error**—Wahr, falls bei der Verarbeitung ein Fehler aufgetreten ist (meist ein Fehler in der DNS-Abfrage).

- **rblhdr**—Ist dies der erste Parameter, so kann die Prüfung `lookup` erst bei oder nach Gabe des Befehls DATA durchgeführt werden. Der zweite Parameter kann "all", "any oder "error" sein.
  - **all**—Wahr, falls die Received-Kopfzeilen alle Abfragen von Schwarzen Listen für DNS bestanden haben.
  - **any**—Wahr, falls die Received-Kopfzeilen mindestens eine Abfrage einer Schwarzen Liste für DNS bestanden haben.
  - **error**—Wahr, falls bei der Verarbeitung ein Fehler aufgetreten ist (meist ein Fehler in der DNS-Abfrage).

port

Die Prüfung `port` kann jederzeit durchgeführt werden. Der einzige Parameter ist die Port-Nummer, die mit dem Port verglichen wird, zu dem der Client tatsächlich eine Verbindung hergestellt hat.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Beispiel-Kode: `if port 25 { greylist; }`

auth

Es hängt vom ersten Parameter ab, wann die Prüfung `auth` aufgerufen werden kann:

- **succeeded**—Wahr, falls die Echtheitsbestätigung erfolgreich war. Ist dies der erste Parameter, so kann die Prüfung `auth` bei Gabe des Befehls AUTH oder später durchgeführt werden.
- **match**—Wahr, falls die Echtheitsbestätigung erfolgreich ist und die Adresse aus MAIL FROM mit dem Benutzerkonto übereinstimmt, das sich angemeldet hat. Ist dies der erste Parameter, so kann die Prüfung `auth` bei Gabe des Befehls MAIL oder später durchgeführt werden.

verify

Die Prüfung `verify` prüft Adressen auf Gültigkeit (vgl. Datenquellen für Benutzerprüfung 63). Anders als die anderen Prüfungen wir diese Prüfung immer durchgeführt, selbst dann, wenn sie nicht in einem Sieve-Filter enthalten ist. Es wird jede Adresse aus einem Befehl MAIL FROM und RCPT TO geprüft, und die Ergebnisse werden zwischengespeichert. Es hängt vom ersten Parameter ab, wann die Prüfung `verify` aufgerufen werden kann:

- **from**—Wahr, falls die Adresse aus MAIL FROM eine gültige lokale Adresse ist. Ist dies der erste Parameter, so kann die Prüfung `verify` bei oder nach Gabe des Befehls MAIL durchgeführt werden.
- **fromdomain**—Wahr, falls die Adresse aus MAIL FROM zu einer gültigen lokalen Domäne gehört. Ist dies der erste Parameter, so kann die Prüfung `verify` bei oder nach Gabe des Befehls MAIL durchgeführt werden.
- **fail_from**—Wahr, falls bei der Prüfung der Adresse aus MAIL FROM ein Fehler aufgetreten ist. Ist dies der erste Parameter, so kann die Prüfung `verify` bei oder nach Gabe des Befehls MAIL durchgeführt werden.
- **to**—Wahr, falls die Adresse aus RCPT TO eine gültige lokale Adresse ist. Ist dies der erste Parameter, so kann die Prüfung `verify` bei oder nach Gabe des Befehls RCPT durchgeführt werden.
- **todomain**—Wahr, falls die Adresse aus RCPT TO zu einer gültigen lokalen Domäne gehört. Ist dies der erste Parameter, so kann die Prüfung `verify` bei oder nach Gabe des Befehls RCPT durchgeführt werden.
- **fail_to**—Wahr, falls bei der Prüfung der Adresse aus RCPT TO ein Fehler aufgetreten ist. Ist dies der erste Parameter, so kann die Prüfung `verify` bei oder nach Gabe des Befehls RCPT durchgeführt werden.

dkim

Die Prüfung `dkim` vergleicht die Ergebnisse der Prüfung über DomainKeys Identified Mail (DKIM) 197 und kann erst bei Gabe des Befehls DATA durchgeführt werden.

- **pass**—Wahr, falls die Nachricht mithilfe von DKIM signiert ist und die Signatur erfolgreich geprüft wurde.
- **fail**—Wahr, falls die Prüfung über DKIM das Ergebnis hard fail erbringt (ADSP-Option muss aktiv sein).

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **error**—Wahr, falls bei der Verarbeitung der DKIM-Signatur ein Fehler aufgetreten ist.

cbv

Die Prüfung `cbv` kann bei Gabe des Befehls MAIL oder danach durchgeführt werden. Ohne Parameter ergibt sie das Ergebnis wahr, falls die Adresse aus MAIL FROM die Prüfung durch Rückruf 217 besteht.

- **error**—Wahr, falls bei der Prüfung durch Rückruf ein Fehler aufgetreten ist.

spamtotal

Die Prüfung `spamtotal` vergleicht die Nachrichten-Bewertung 185 und kann während jeder Ereignisgruppe durchgeführt werden. Sie soll in den meisten Fällen jedoch als letzter Filter in der Ereignisgruppe DATA eingesetzt werden, damit alle anderen Filter bereits abgearbeitet und ihre Ergebnisse in die Nachrichten-Bewertung eingeflossen sind.

Die Prüfung `spamtotal` hat nur einen Parameter, den Schwellwert. Ist die Nachrichten-Bewertung größer oder gleich dem Schwellwert, ergibt sie das Ergebnis wahr, ansonsten falsch.

OutbreakProtection

Die Prüfung `OutbreakProtection` kann nur in der Ereignisgruppe DATA durchgeführt werden. Ohne Parameter ergibt sie das Ergebnis wanr, falls die Outbreak Protection 157 eine Nachricht als Spam, vireninfiziert oder Massennachricht einstuft.

- **spam**—Wahr, falls die Outbreak Protection die Nachricht als Spam einstuft.
- **virus**—Wahr, falls die Outbreak Protection die Nachricht als vireninfiziert einstuft.
- **phish**—Wahr, falls die Outbreak Protection die Nachricht als Phishing-Nachricht einstuft.
- **suspect**—Wahr, falls die Outbreak Protection die Nachricht als spamverdächtig einstuft.
- **bulk**—Wahr, falls die Outbreak Protection die Nachricht als Massennachricht einstuft.
- **error**—Wahr, falls während der Verarbeitung durch die Outbreak Protection ein Fehler aufgetreten ist.

whitelisted

Diese Prüfung hat aus Gründen der Abwärtskompatibilität einen Alias: `exempt`. Es hängt vom ersten Parameter ab, wann diese Prüfung durchgeführt werden kann:

- **all**—Vorgehensweise wie ohne Parameter; ergibt wahr, falls der Client in einer Weißen Liste 275 eingetragen ist. Diese Prüfung kann jederzeit aufgerufen werden und greift auf die jeweils verfügbaren Informationen zurück. Wird sie etwa in der Ereignisgruppe IP (der ersten Ereignisgruppe) aufgerufen, so werden nur IPs auf der Weißen Liste und Hosts, deren PTR-Eintrag übereinstimmt, verglichen.
- **ip**—Wahr, falls der Client in der Weißen Liste für IPs 281 eingetragen ist. Kann jederzeit durchgeführt werden.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **host**—Wahr, falls der Client in der Weißen Liste für Hosts[278] eingetragen ist. Prüfung kann anhand von HELO-Parameter oder PTR-Host durchgeführt werden. Kann in Ereignisgruppe HELO oder später aufgerufen werden.
- **mail**—Wahr, falls MAIL FROM in der Weißen Liste für Adressen[276] eingetragen ist. Kann in Ereignisgruppe MAIL oder später aufgerufen werden.
- **from**—Wahr, falls Kopfzeile From: in der Weißen Liste für Adressen[276] eingetragen ist. Kann nur in Ereignisgruppe DATA aufgerufen werden.

blacklisted

Diese Prüfung hat aus Gründen der Abwärtskompatibilität einen Alias: `blocklist`. Parameter und Funktionsweise entsprechen der Prüfung `whitelist`, jedoch werden die Vergleiche mit den Schwarzen Listen[265] vorgenommen.

vbr

Die Prüfung `vbr` (vgl. Zertifizierung von Nachrichten[179]) hat nur einen Parameter:

- *kommagetrennte Liste der vertrauten Zertifizierungsdienstleister*—Wahr, falls die Nachricht zertifiziert ist.
- **error**—Wahr, falls bei der Prüfung der Zertifizierung ein Fehler aufgetreten ist.

Aktions-Befehle

error

Der Befehl `error` entspricht dem Befehl "reject", der in RFC-3028 definiert ist, hat jedoch zwei Parameter. Der erste Parameter ist der SMTP-Fehlerkode, und der zweite Parameter ist eine Textmeldung. Beide werden als Antwort auf den jeweils vom Client empfangenen Befehl gesendet.

disconnect

Der Befehl `disconnect` entspricht dem Befehl "error", er trennt schließt jedoch außerdem den TCP/IP-Socket. Die Vorgehensweise gleicht der Option zum Trennen der Verbindung in MD.

greylist

Der Befehl `greylist` aktiviert die Graue Liste[176].

dynamicscreen

Der Befehl `dynamicscreen` aktiviert den Dynamischen Filter[229].

tarpit

Der Befehl `tarpit` aktiviert die Teergrube[231].

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

sign

Der Befehl `sign` fügt der Nachricht eine Signatur[199]-Kopfzeile hinzu. Der erste Parameter kann sein:

- **dkim**—Nachricht über DKIM[199] signieren. Der zweite Parameter ist der Name des zu verwendenden Selektors.
- **vbr**—Kopfzeile VBR-Info: einfügen (für die Zertifizierung von Nachrichten[179]). Der zweite Parameter ist die Liste der vertrauten Zertifizierungsdienstleister, die in den Parameter mv= übernommen werden sollen.

throttle

Der Befehl `throttle` aktiviert die Bandbreitenbegrenzung[233]. Der erste Parameter ist die Bandbreitenbegrenzung in Zeichen pro Sekunde.

ipshield

Der Befehl `ipshield` aktiviert die IP-Abschirmung[227].

spamscore

Der Befehl `spamscore` rechnet der Nachrichten-Bewertung[185] der Nachricht den als ersten Parameter übergebenen Wert hinzu. Vgl. auch die Prüfung `spamtotal`.

tagheader

Der Befehl `tagheader` stellt einer Kopfzeile der Nachricht eine Kennzeichnung voran. Der erste Parameter ist die zu ändernde Kopfzeile. Der zweite Parameter ist der Text, der in den Wert der Kopfzeile eingefügt werden soll.

addheader

Der Befehl `addheader` fügt der Nachricht eine neue Kopfzeile hinzu. Der erste Parameter ist der Name der neuen Kopfzeile. Der zweite Parameter ist ihr Wert.

removeheader

Der Befehl `removeheader` entfernt eine Kopfzeile aus der Nachricht. Der erste Befehl ist die zu entfernende Kopfzeile.

alert

Der Befehl `alert` sendet eine Nachricht. Der einzige Parameter ist ein Nachrichtentext, einschließlich der Kopfzeilen für Absender, Empfänger, Betreff und sonstiger etwa benötigter Kopfzeilen. In dem gesamten Text werden Makros ausgewertet und umgesetzt.

changesender

Der Befehl `changesender` wird verwendet, um den Inhalt des Befehls `SMTP MAIL FROM` zu ändern, den SecurityGateway bei Zustellung einer Nachricht verwendet. Dieser Befehl kann beispielsweise eingesetzt werden, wenn Domänennamen

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

verwendet werden, die nur intern gültig sind und für den Versand von Nachrichten an Empfänger außerhalb dieser internen Domäne geändert werden müssen.

Ein Beispiel:

```
require ["securitygateway", "envelope"];
if envelope :matches "From" "frank@interne.mail"
{
changesender "frank@example.com";
}
```

execute

- Das Skript muss im Verzeichnis "Ausführbare Dateien für Sieve-Skripte" abgelegt sein. Dieses Verzeichnis kann auf der Seite Einstellungen » System » Verzeichnisse 134 konfiguriert werden. Das Sieve-Schlüsselwort "execute" kann sowohl als Aktions-Befehl als auch als Test-Befehl verwendet werden.
- Der erste Parameter ist der Name des Skripts. Dateien der Typen .bat, .exe und PowerShell werden unterstützt.
- Der zweite Parameter sind die Argumente, die dem Prozess übergeben werden. Die Sieve-Variable `message_filename` wird durch den vollständigen Pfad zur RFC822-Quelle der jeweils gerade verarbeiteten Nachricht ersetzt.

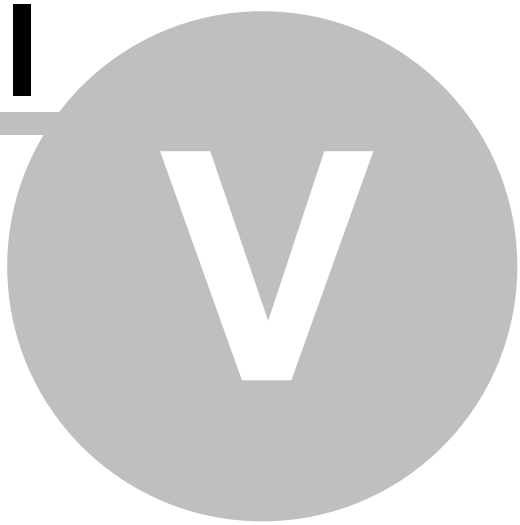
Ein Beispiel:

```
require ["securitygateway","relational","comparator-i;ascii-
numeric"];
execute "Test.ps1" "-msg '${message_filename}'";

Der Text des PowerShell-Skripts, das den Dateinamen jeder
verarbeiteten Datei protokolliert, lautet...
param
(
    [string]$msg = ""
)

Add-Content -Path "c:\verarbeitete_dateien.txt" -Value $msg
Write-Host $msg
```

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kapitel



5 Nachrichten/Warteschlangen

Der Abschnitt Nachrichten/Warteschlangen im linken Fensterbereich gibt Ihnen Zugriff auf zwei Abschnitte: Nachrichten-Protokoll und Nachrichten-Warteschlangen.

Nachrichten-Protokoll 307

Das Nachrichten-Protokoll enthält zu jeder Nachricht, die Ihre Benutzer senden und empfangen, einen eigenen Eintrag. Darin sind Datum und Uhrzeit, zu denen die Nachricht verarbeitet wurde, Absender und Empfänger, sowie der Betreff der Nachricht vermerkt. Das Protokoll gibt außerdem Aufschluss über die Ergebnisse der Zustellversuche, insbesondere, ob die Nachricht zugestellt oder nicht zugestellt wurde. Wurde eine Nachricht nicht zugestellt, so ist auch der Grund aufgeführt, etwa, dass der Absender in einer Schwarzen Liste erfasst war, dass die Nachricht eine gesperrte Dateianlage enthielt, oder ähnliches. Auch die Größe der Nachricht und die Bewertung der Nachricht 185 werden erfasst.

Über das Nachrichten-Protokoll können Sie Einzelheiten zu allen Nachrichten einsehen. Hierzu gehören ein Verbindungsmitschnitt für die Verbindung, in der die Nachricht übermittelt wurde, der Inhalt der Nachricht und der Quelltext (soweit verfügbar). Sie können im Nachrichten-Protokoll Nachrichten als Spam und als normale Nachrichten kennzeichnen und so das Bayes'sche Lernverfahren 164 von SecurityGateway verfeinern helfen, um so Nachrichten genauer zu kategorisieren.

Sie können das Nachrichten-Protokoll auch über das Menü Protokollierung 316 erreichen.

Nachrichten-Warteschlangen

In diesem Abschnitt finden Sie Verknüpfungen zu vier Nachrichten-Warteschlangen: Benutzer-Quarantäne 308, Administrative Quarantäne 310, Nachrichten, die auf Zustellung warten 311 und defekte Nachrichten 312.

- Die **Benutzer-Quarantäne** 308 ist eine Warteschlange für eingehende Nachrichten. Diese werden darin festgehalten, wenn sie die Prüfung durch die verschiedenen Sicherheitsfunktionen 154 von SecurityGateway nicht bestehen und diese Funktionen so konfiguriert sind, dass die Nachrichten in Quarantäne gegeben und nicht abgewiesen oder nur gekennzeichnet werden. Die Benutzer können sich an SecurityGateway anmelden und die Inhalte ihrer Quarantäne-Warteschlangen einsehen. Sie können von dort einzelne Nachrichten einsehen, sie löschen oder aus der Quarantäne zur normalen Zustellung freigeben.
- Die **Administrative Quarantäne** 310 arbeitet ähnlich wie die Benutzer-Quarantäne. Sie ist aber eine Warteschlange für abgehende Nachrichten und Nachrichten, die Viren enthalten. Auf die Administrative Quarantäne haben nur Administratoren 60 Zugriff.
- **Die Warteschlange für Nachrichten, die auf Zustellung warten** 311, ist eine Warteschlange für alle Nachrichten, die noch auf ihre Zustellung warten. Dazu gehören auch Nachrichten, die unzustellbar waren, und deren Zustellung erneut versucht werden wird 92. Von dieser Seite aus

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

können Sie alle Nachrichten in der Warteschlange betrachten, Nachrichten an den Absender zurücksenden, die Zustellung einer Nachricht anhalten und veranlassen, dass die erneute Zustellung einzelner oder aller Nachrichten sofort versucht wird.

- Die **Defekt-Warteschlange** 312 ist eine Warteschlange für Nachrichten, die aufgrund eines nicht behebbaren Fehlers bei der Verarbeitung nicht zugestellt werden können. Hierzu gehören Nachrichten, bei deren Zustellung eine Endlosschleife aufgetreten ist, und die daher die *Höchstzahl der Zwischenstationen* 95 erreicht haben. Von dieser Seite aus können Sie alle Nachrichten in der Warteschlange betrachten, Nachrichten an den Absender zurückzusenden versuchen, Nachrichten löschen und veranlassen, dass die erneute Zustellung einzelner oder aller Nachrichten sofort versucht wird.

5.1 Nachrichten-Protokoll

Um das Nachrichten-Protokoll aufzurufen, klicken Sie auf "Alle Nachrichten". Das Nachrichten-Protokoll enthält zu jeder Nachricht, die Ihre Benutzer senden und empfangen, einen eigenen Eintrag. Darin sind Datum und Uhrzeit, zu denen die Nachricht verarbeitet wurde, Absender und Empfänger, sowie der Betreff der Nachricht vermerkt. Das Protokoll gibt außerdem Aufschluss über die Ergebnisse der Zustellversuche, insbesondere, ob die Nachricht zugestellt oder nicht zugestellt wurde. Wurde eine Nachricht nicht zugestellt, so ist auch der Grund aufgeführt, etwa, dass der Absender in einer Schwarzen Liste erfasst war, dass die Nachricht eine gesperrte Dateianlage enthielt, oder ähnliches. Auch die Größe der Nachricht und die Bewertung der Nachricht 185 werden erfasst.

In der Symbolleiste am oberen Rand des Nachrichten-Protokolls stehen Ihnen mehrere Steuerelemente zur Verfügung, mit denen Sie die nachfolgend beschriebenen Aufgaben erledigen können:

- **Aktualisieren**—Klicken Sie auf dieses Steuerelement, um die Darstellung des Nachrichten-Protokolls zu aktualisieren. Es werden dann auch Einträge angezeigt, die in das Protokoll eingetragen wurden, nachdem Sie das Protokoll aufgerufen haben.
- **Suche**—Über dieses Steuerelement erhalten Sie Zugriff auf umfassende Such-Funktionen, mit deren Hilfe Sie das Nachrichten-Protokoll filtern können, sodass nur bestimmte Nachrichten angezeigt werden. Sie können das Protokoll nach ein- und abgehenden Nachrichten filtern, bestimmten Text in beliebigen Kopfzeilen suchen, den Zeitrahmen für die Suche einschränken, und vieles mehr. Um das Nachrichten-Protokoll zu durchsuchen, öffnen Sie die Such-Maske durch einen Klick auf *Suche* in der Symbolleiste. Legen Sie dann die Suchkriterien fest, und klicken Sie schließlich in der Such-Maske auf das Steuerelement Suche. Die Suche wird dann durchgeführt, und die Ergebnisse erscheinen im Nachrichten-Protokoll. Sie können durch erneutes Anklicken von *Suche* in der Symbolleiste die Such-Maske ausblenden und die Ergebnisse der Suche im Nachrichten-Protokoll angezeigt lassen. Um zur vollständigen Anzeige des Nachrichten-Protokolls zurückzukehren, klicken Sie in der Such-Maske auf *Abbrechen*.
- **Details**—Wählen Sie eine Nachricht aus, und klicken Sie dann auf dieses Steuerelement, um die Nachrichten-Informationen einzublenden. Sie sind in drei Registerkarten unterteilt: Mitschnitt, Nachricht und Quelltext. Die

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Registerkarte Mitschnitt enthält den Mitschnitt des eigentlichen Zustellvorgangs und insbesondere die SMTP-Verbindung und interne Verarbeitung. Die Registerkarte Nachricht enthält den Inhalt der Nachricht selbst. Ob der Nachrichten-Inhalt im Einzelfall verfügbar ist, hängt vom Alter der Nachricht und davon ab, ob die Nachricht erfolgreich zugestellt wurde und welche Optionen im Abschnitt Datenhaltung 144 aktiv sind. Die Registerkarte Quelltext enthält den Quelltext der Nachricht einschließlich der Kopfzeilen, des HTML-Kodes und sonstiger Komponenten. Der Quelltext ist unter Umständen nicht verfügbar, etwa, wenn die Nachricht alt ist oder die Optionen zur Datenhaltung 144 von SecurityGateway eine Speicherung dieser Daten nicht vorsehen.

- **Erneut zustellen**—Um eine Nachricht oder mehrere Nachrichten erneut zuzustellen, wählen Sie sie aus der Liste aus, und klicken Sie dann auf dieses Steuerelement. Sie können mehrere Nachrichten auswählen, indem Sie die Strg- oder Hochschalttaste gedrückt halten. Die erneute Zustellung ist nur möglich, solange die Inhalte der Nachrichten noch nicht aus der Datenbank gelöscht wurden.
- **Spam**—Um eine Nachricht als Spam zu kennzeichnen, wählen Sie die Nachricht aus, und klicken Sie dann auf dieses Steuerelement. Sie können SecurityGateway dadurch helfen, Spam-Nachrichten in Zukunft noch sicherer zu erkennen. Diese Option ist nur verfügbar, wenn die Funktionen für das Bayes'sche Lernverfahren 164 aktiv sind.
- **Kein Spam**—Um eine Nachricht als normale Nachricht zu kennzeichnen, wählen Sie die Nachricht aus, und klicken Sie dann auf dieses Steuerelement. Sie können SecurityGateway dadurch helfen, legitime Nachrichten in Zukunft nicht irrtümlich als Spam zu erkennen. Diese Option ist nur verfügbar, wenn die Funktionen für das Bayes'sche Lernverfahren 164 aktiv sind.
- **Weiße Liste/Schwarze Liste**—Um einen Eintrag in einer Weißen Liste 276 oder einer Schwarzen Liste 266 zu erstellen, klicken Sie die Nachricht an, und klicken Sie danach auf Weiße Liste oder Schwarze Liste. Klicken Sie anschließend auf die Adressliste, der Sie den Absender oder die Domäne des Absenders hinzufügen wollen. Es stehen dafür zur Verfügung die Liste des Benutzers, die Liste der Domäne sowie die globale Liste.

5.2 Nachrichten-Warteschlangen

5.2.1 In Quarantäne (Benutzer)

Die Benutzer-Quarantäne ist eine Warteschlange für eingehende Nachrichten. Diese werden darin festgehalten, wenn sie die Prüfung durch die verschiedenen Sicherheitsfunktionen 154 von SecurityGateway nicht bestehen und diese Funktionen so konfiguriert sind, dass die Nachrichten in Quarantäne gegeben und nicht abgewiesen oder nur gekennzeichnet werden. Die Benutzer können sich an SecurityGateway anmelden und die Inhalte ihrer Quarantäne-Warteschlangen einsehen. Sie können von dort einzelne Nachrichten einsehen, sie löschen oder aus der Quarantäne zur normalen Zustellung freigeben.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Abgehende Nachrichten, die in Quarantäne gegeben werden, und Nachrichten, die Viren enthalten, werden in die Administrative Quarantäne 310 gegeben. Auf diese Nachrichten haben nur Administratoren 60 Zugriff.

Für jeden Eintrag in der Quarantäne bestehen mehrere Spalten, in denen folgende Daten aufgeführt sind: Datum und Uhrzeit, zu denen die Nachricht in Quarantäne gegeben wurde, Absender, Empfänger und Betreffzeile, Grund, warum die Nachricht in Quarantäne gegeben wurde, Größe der Nachricht und Nachrichten-Bewertung 185.

Die Symbolleiste am oberen Rand der Quarantäne-Übersicht enthält eine Reihe von Schaltflächen, mit deren Hilfe Sie die folgenden Aufgaben ausführen können:

- **Aktualisieren**—Durch Anklicken dieser Schaltfläche wird die Übersicht aktualisiert. Es erscheinen dann auch Nachrichten, die seit dem Aufruf der Übersicht etwa neu hinzugekommen sind.
- **Suche**—Es stehen umfangreiche Suchfunktionen zur Verfügung, mit denen Sie die Benutzer-Quarantäne filtern und sich nur bestimmte Nachrichten anzeigen lassen können. Sie können nach eingehenden und abgehenden Nachrichten suchen, Sie können nach Texten in beliebigen Kopfzeilen suchen, Sie können Nachrichten jedes Datums und jeder Uhrzeit oder aus bestimmten Datumsbereichen suchen, und vieles mehr. Um die Quarantäne-Übersicht zu durchsuchen, gehen Sie folgendermaßen vor: Klicken Sie in der Symbolleiste auf *Suche*, um das Suchfenster zu öffnen. Wählen Sie dann die gewünschten Suchkriterien aus, und klicken Sie danach im Suchfenster auf die Schaltfläche *Suche*, um die Suche auszuführen. Die Ergebnisse der Suche erscheinen unter dem Suchfenster. Die Quarantäne-Übersicht wird so gefiltert, dass nur die Nachrichten angezeigt werden, die den Suchkriterien entsprechen. Um das Suchfenster auszublenden und die Suche dennoch wirksam bleiben zu lassen, klicken Sie in der Symbolleiste erneut auf *Suche*. Um die Suche zu beenden und zur normalen Übersicht über die Quarantäne zurückzukehren, klicken Sie im Suchfenster auf *Abbrechen*.
- **Anzeigen**—Um Informationen zu einer bestimmten Nachricht einzusehen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. Es erscheint eine Übersicht, die drei Registerkarten enthält: Mitschnitt, Nachricht und Quelltext. Die Registerkarte Mitschnitt enthält einen Mitschnitt des Übermittlungsvorgangs einschließlich der SMTP-Verbindung und der Übersicht über die internen Verarbeitungabläufe. Die Registerkarte Nachricht enthält den eigentlichen Inhalt der Nachricht. Die Registerkarte Quelltext enthält den Quelltext der Nachricht einschließlich der Kopfzeilen, des HTML-Kodes und weiterer Elemente.
- **Freigeben**—Um eine Nachricht aus der Quarantäne zur Zustellung freizugeben, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche.
- **Löschen**—Um eine Nachricht zu löschen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche.
- **Alle löschen**—Um alle Nachrichten aus der Quarantäne zu löschen, klicken Sie auf diese Schaltfläche.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

5.2.2 In Quarantäne (Admin)

Die Administrative Quarantäne arbeitet ähnlich wie die Benutzer-Quarantäne 308. Sie ist aber eine Warteschlange für abgehende Nachrichten und Nachrichten, die Viren enthalten. Diese Nachrichten werden darin festgehalten, wenn sie die Prüfung durch die verschiedenen Sicherheitsfunktionen 154 von SecurityGateway nicht bestehen und diese Funktionen so konfiguriert sind, dass die Nachrichten in Quarantäne gegeben und nicht abgewiesen oder nur gekennzeichnet werden. Anders als die Benutzer-Quarantäne ist die Administrative Quarantäne nur für Administratoren zugänglich. Sie können von dort einzelne Nachrichten einsehen, sie löschen oder aus der Quarantäne zur normalen Zustellung freigeben.

Für jeden Eintrag in der Administrativen Quarantäne bestehen mehrere Spalten, in denen folgende Daten aufgeführt sind: Datum und Uhrzeit, zu denen die Nachricht in Quarantäne gegeben wurde, Absender, Empfänger und Betreffzeile, Grund, warum die Nachricht in Quarantäne gegeben wurde, Größe der Nachricht und Nachrichten-Bewertung 185.

Die Symbolleiste am oberen Rand der Quarantäne-Übersicht enthält eine Reihe von Schaltflächen, mit deren Hilfe Sie die folgenden Aufgaben ausführen können:

- **Aktualisieren**—Durch Anklicken dieser Schaltfläche wird die Übersicht aktualisiert. Es erscheinen dann auch Nachrichten, die seit dem Aufruf der Übersicht etwa neu hinzugekommen sind.
- **Suche**—Es stehen umfangreiche Suchfunktionen zur Verfügung, mit denen Sie die Administrative Quarantäne filtern und sich nur bestimmte Nachrichten anzeigen lassen können. Sie können nach eingehenden und abgehenden Nachrichten suchen, Sie können nach Texten in beliebigen Kopfzeilen suchen, Sie können Nachrichten jedes Datums und jeder Uhrzeit oder aus bestimmten Datumsbereichen suchen, und vieles mehr. Um die Quarantäne-Übersicht zu durchsuchen, gehen Sie folgendermaßen vor: Klicken Sie in der Symbolleiste auf *Suche*, um das Suchfenster zu öffnen. Wählen Sie dann die gewünschten Suchkriterien aus, und klicken Sie danach im Suchfenster auf die Schaltfläche *Suche*, um die Suche auszuführen. Die Ergebnisse der Suche erscheinen unter dem Suchfenster. Die Quarantäne-Übersicht wird so gefiltert, dass nur die Nachrichten angezeigt werden, die den Suchkriterien entsprechen. Um das Suchfenster auszublenden und die Suche dennoch wirksam bleiben zu lassen, klicken Sie in der Symbolleiste erneut auf *Suche*. Um die Suche zu beenden und zur normalen Übersicht über die Quarantäne zurückzukehren, klicken Sie im Suchfenster auf *Abbrechen*.
- **Anzeigen**—Um Informationen zu einer bestimmten Nachricht einzusehen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. Es erscheint eine Übersicht, die drei Registerkarten enthält: Mitschnitt, Nachricht und Quelltext. Die Registerkarte Mitschnitt enthält einen Mitschnitt des Übermittlungsvorgangs einschließlich der SMTP-Verbindung und der Übersicht über die internen Verarbeitungabläufe. Die Registerkarte Nachricht enthält den eigentlichen Inhalt der Nachricht. Die Registerkarte Quelltext enthält den Quelltext der Nachricht einschließlich der Kopfzeilen, des HTML-Kodes und weiterer Elemente.
- **Freigeben**—Um eine Nachricht aus der Quarantäne zur Zustellung freizugeben, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **Löschen**—Um eine Nachricht zu löschen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche.
- **Alle löschen**—Um alle Nachrichten aus der Quarantäne zu löschen, klicken Sie auf diese Schaltfläche.

5.2.3 Warten auf Zustellung

Die Warteschlange für Nachrichten, die auf Zustellung warten,

ist eine Warteschlange für alle Nachrichten, die noch auf ihre Zustellung warten. Dazu gehören auch Nachrichten, die unzustellbar waren, und deren Zustellung erneut versucht werden wird 92. Von dieser Seite aus können Sie alle Nachrichten in der Warteschlange betrachten, Nachrichten an den Absender zurücksenden, die Zustellung einer Nachricht anhalten und veranlassen, dass die erneute Zustellung einzelner oder aller Nachrichten sofort versucht wird.

Für jeden Eintrag in der Warteschlange bestehen mehrere Spalten, in denen folgende Daten aufgeführt sind: Richtung der Nachricht (eingehend oder abgehend), Datum und Uhrzeit, zu denen die Nachricht in die Warteschlange verschoben wurde, Absender, Empfänger und Betreffzeile, Grund, warum die Nachricht in die Warteschlange verschoben wurde, Größe der Nachricht und Ergebnis des Zustellversuchs.

Die Symbolleiste am oberen Rand der Übersicht über die auf Zustellung wartenden Nachrichten enthält eine Reihe von Schaltflächen, mit deren Hilfe Sie die folgenden Aufgaben ausführen können:

- **Aktualisieren**—Durch Anklicken dieser Schaltfläche wird die Übersicht aktualisiert. Es erscheinen dann auch Nachrichten, die seit dem Aufruf der Übersicht etwa neu hinzugekommen sind.
- **Suche**—Es stehen umfangreiche Suchfunktionen zur Verfügung, mit denen Sie die Übersicht filtern und sich nur bestimmte Nachrichten anzeigen lassen können. Sie können nach eingehenden und abgehenden Nachrichten suchen, Sie können nach Texten in beliebigen Kopfzeilen suchen, Sie können Nachrichten jedes Datums und jeder Uhrzeit oder aus bestimmten Datumsbereichen suchen, und vieles mehr. Um die Übersicht zu durchsuchen, gehen Sie folgendermaßen vor: Klicken Sie in der Symbolleiste auf *Suche*, um das Suchfenster zu öffnen. Wählen Sie dann die gewünschten Suchkriterien aus, und klicken Sie danach im Suchfenster auf die Schaltfläche *Suche*, um die Suche auszuführen. Die Ergebnisse der Suche erscheinen unter dem Suchfenster. Die Übersicht wird so gefiltert, dass nur die Nachrichten angezeigt werden, die den Suchkriterien entsprechen. Um das Suchfenster auszublenden und die Suche dennoch wirksam bleiben zu lassen, klicken Sie in der Symbolleiste erneut auf *Suche*. Um die Suche zu beenden und zur normalen Übersicht über die auf Zustellung wartenden Nachrichten zurückzukehren, klicken Sie im Suchfenster auf *Abbrechen*.
- **Anzeigen**—Um Informationen zu einer bestimmten Nachricht einzusehen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. Es erscheint eine Übersicht, die drei Registerkarten enthält: Mitschnitt, Nachricht und Quelltext. Die Registerkarte Mitschnitt enthält einen Mitschnitt des Übermittlungsvorgangs einschließlich der SMTP-Verbindung und der Übersicht über die internen Verarbeitungabläufe. Die Registerkarte Nachricht

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

enthält den eigentlichen Inhalt der Nachricht. Die Registerkarte Quelltext enthält den Quelltext der Nachricht einschließlich der Kopfzeilen, des HTML-Kodes und weiterer Elemente.

- **Abweisen**—Um eine Nachricht an den Absender zurückzuleiten, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. Hierdurch werden alle weiteren Versuche unterbunden, die Nachricht an den gewünschten Empfänger zuzustellen.
- **Zustellung anhalten**—Durch Auswählen einer Nachricht oder mehrerer Nachrichten und Anklicken dieser Schaltfläche erhalten die ausgewählten Nachrichten den Status "Zustellung fehlgeschlagen". Weitere Zustellversuche finden dann nicht mehr statt. Wird eine Nachricht aber gerade zugestellt, während die Schaltfläche angeklickt wird, so wird diese laufende Zustellung nicht unterbunden.
- **Alle stoppen**—Diese Option ähnelt der Option *Zustellung anhalten* weiter oben; sie wirkt jedoch auf alle Nachrichten in der Warteschlange. Falls die Warteschlange mithilfe der Suche gefiltert wurde, wirkt die Option nur auf die Nachrichten, die gerade als Suchergebnis angezeigt werden.
- **Erneute Zustellung**—Um die Zustellung einer Nachricht sofort erneut zu versuchen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. SecurityGateway versucht dann sofort, die Nachricht erneut zuzustellen, und wartet nicht erst den nächsten turnusgemäßen Versuch zur erneuten Zustellung 92 ab.
- **Alle erneut versuchen**—Um SecurityGateway zu veranlassen, die Zustellung für alle Nachrichten in der Warteschlange sofort zu versuchen, klicken Sie auf diese Schaltfläche. SecurityGateway versucht dann sofort, die Nachrichten erneut zuzustellen, und wartet nicht erst den nächsten turnusgemäßen Versuch zur erneuten Zustellung 92 ab.

5.2.4 Defekte Nachrichten

Die Defekt-Warteschlange ist eine Warteschlange für Nachrichten, die aufgrund eines nicht behebbaren Fehlers bei der Verarbeitung nicht zugestellt werden können. Hierzu gehören Nachrichten, bei deren Zustellung eine Endlosschleife aufgetreten ist, und die daher die *Höchstzahl der Zwischenstationen* 95 erreicht haben. Von dieser Seite aus können Sie alle Nachrichten in der Warteschlange betrachten, Nachrichten an den Absender zurückzusenden versuchen, Nachrichten löschen und veranlassen, dass die erneute Zustellung einzelner oder aller Nachrichten sofort versucht wird.

Für jeden Eintrag in der Warteschlange bestehen mehrere Spalten, in denen folgende Daten aufgeführt sind: Richtung der Nachricht (eingehend oder abgehend), Datum und Uhrzeit, zu denen die Nachricht in die Warteschlange verschoben wurde, Absender, Empfänger und Betreffzeile und Größe der Nachricht.

Die Symbolleiste am oberen Rand der Übersicht über die auf Zustellung wartenden Nachrichten enthält eine Reihe von Schaltflächen, mit deren Hilfe Sie die folgenden Aufgaben ausführen können:

- **Aktualisieren**—Durch Anklicken dieser Schaltfläche wird die Übersicht aktualisiert. Es erscheinen dann auch Nachrichten, die seit dem Aufruf der Übersicht etwa neu hinzugekommen sind.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **Suche**—Es stehen umfangreiche Suchfunktionen zur Verfügung, mit denen Sie die Übersicht filtern und sich nur bestimmte Nachrichten anzeigen lassen können. Sie können nach eingehenden und abgehenden Nachrichten suchen, Sie können nach Texten in beliebigen Kopfzeilen suchen, Sie können Nachrichten jedes Datums und jeder Uhrzeit oder aus bestimmten Datumsbereichen suchen, und vieles mehr. Um die Übersicht zu durchsuchen, gehen Sie folgendermaßen vor: Klicken Sie in der Symbolleiste auf *Suche*, um das Suchfenster zu öffnen. Wählen Sie dann die gewünschten Suchkriterien aus, und klicken Sie danach im Suchfenster auf die Schaltfläche *Suche*, um die Suche auszuführen. Die Ergebnisse der Suche erscheinen unter dem Suchfenster. Die Übersicht wird so gefiltert, dass nur die Nachrichten angezeigt werden, die den Suchkriterien entsprechen. Um das Suchfenster auszublenden und die Suche dennoch wirksam bleiben zu lassen, klicken Sie in der Symbolleiste erneut auf *Suche*. Um die Suche zu beenden und zur normalen Übersicht über die auf Zustellung wartenden Nachrichten zurückzukehren, klicken Sie im Suchfenster auf *Abbrechen*.
- **Anzeigen**—Um Informationen zu einer bestimmten Nachricht einzusehen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. Es erscheint eine Übersicht, die drei Registerkarten enthält: Mitschnitt, Nachricht und Quelltext. Die Registerkarte Mitschnitt enthält einen Mitschnitt des Übermittlungsvorgangs einschließlich der SMTP-Verbindung und der Übersicht über die internen Verarbeitungabläufe. Die Registerkarte Nachricht enthält den eigentlichen Inhalt der Nachricht. Die Registerkarte Quelltext enthält den Quelltext der Nachricht einschließlich der Kopfzeilen, des HTML-Kodes und weiterer Elemente.
- **Abweisen**—Um eine Nachricht an den Absender zurückzuleiten, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. Hierdurch werden alle weiteren Versuche unterbunden, die Nachricht an den gewünschten Empfänger zuzustellen.
- **Löschen**—Um eine Nachricht zu löschen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. Für diese Schaltfläche steht eine Dropdown-Liste mit Optionen zur Verfügung, über die Sie nur die ausgewählten und wahlweise auch alle Nachrichten in der Übersicht löschen können.
- **Erneute Zustellung**—Um die Zustellung einer Nachricht sofort erneut zu versuchen, wählen Sie die Nachricht aus, und klicken Sie dann auf diese Schaltfläche. SecurityGateway versucht dann sofort, die Nachricht erneut zuzustellen, und wartet nicht erst den nächsten turnusgemäßen Versuch zur erneuten Zustellung 92 ab.
- **Alle erneut versuchen**—Um SecurityGateway zu veranlassen, die Zustellung für alle Nachrichten in der Warteschlange sofort zu versuchen, klicken Sie auf diese Schaltfläche. SecurityGateway versucht dann sofort, die Nachrichten erneut zuzustellen, und wartet nicht erst den nächsten turnusgemäßen Versuch zur erneuten Zustellung 92 ab.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kapitel VI

6 Protokollierung

Der Menüpunkt Protokollierung im linken Bereich des Fensters erlaubt den Zugriff auf drei Abschnitte: Nachrichten-Protokoll, Protokolldateien und Konfiguration.

Nachrichten-Protokoll 307

Das Nachrichten-Protokoll enthält zu jeder Nachricht, die Ihre Benutzer senden und empfangen, einen eigenen Eintrag. Darin sind Datum und Uhrzeit, zu denen die Nachricht verarbeitet wurde, Absender und Empfänger, sowie der Betreff der Nachricht vermerkt. Das Protokoll gibt außerdem Aufschluss über die Ergebnisse der Zustellversuche, insbesondere, ob die Nachricht zugestellt oder nicht zugestellt wurde. Wurde eine Nachricht nicht zugestellt, so ist auch der Grund aufgeführt, etwa, dass der Absender in einer Schwarzen Liste erfasst war, dass die Nachricht eine gesperrte Dateianlage enthielt, oder ähnliches. Auch die Größe der Nachricht und die Bewertung der Nachricht 185 werden erfasst.

Sie können sich zu jeder Nachricht aus dem Nachrichten-Protokoll detaillierte Informationen anzeigen lassen, insbesondere den Mitschnitt der Übermittlung der Nachricht, ihren Inhalt und ihre Quelle (soweit verfügbar). Sie können Nachrichten als Spam oder als normale Nachrichten kennzeichnen und damit die Bayes'schen Lernverfahren 164 von SecurityGateway verfeinern helfen, sodass Nachrichten genauer bewertet werden können.

Sie können das Nachrichten-Protokoll auch aus dem Menü Nachrichten/Warteschlangen 306 erreichen.

Protokolldateien 318

Im Abschnitt Protokolldateien erhalten Sie Zugriff auf die verschiedenen Protokolldateien, die SecurityGateway im Verzeichnis für Protokolle 134 ablegt. Im Gegensatz zum Nachrichten-Protokoll werden diese Protokolle nicht in der Datenbank abgelegt. Sie können daher nicht als sortierfähige Listen angezeigt werden, und ihre Einträge sind nicht nach Ereignissen gruppiert oder getrennt. Sie liegen vielmehr als Nur-Text-Dateien vor, in denen die Mitschnitte der verschiedenen SMTP-Verbindungen und der anderen Aktionen verzeichnet sind, die SecurityGateway bearbeitet. Die Seite Alle Protokolldateien im Abschnitt Protokolldateien macht alle Protokolldateien zugänglich, die im Ordner "logs" (Protokolle) enthalten sind. Dazu gehören die aktuellen Protokolldateien und frühere 320 Protokolldateien, die archiviert wurden. Von dieser Seite aus können Sie alle dort aufgeführten Dateien einsehen. Die anderen Seiten im Abschnitt Protokolldateien enthalten Verknüpfungen mit den jeweils aktuellen Protokolldateien, die SecurityGateway führt; dazu gehören das System-Protokoll, die Eingangs- und Ausgangs-Protokolle und Protokolle über die AntiVirus-Aktualisierung.

Konfiguration 320

Der Abschnitt Konfiguration enthält eine Verknüpfung mit der Seite für die Konfiguration des Protokolls 320, auf der die Einstellungen und Optionen für die Protokollierung eingerichtet werden. Auf dieser Seite können Sie festlegen, in

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

welchem Detaillierungsgrad die Eingangs-, Ausgangs- und HTTP-Protokolle geführt werden. Sie können auch wählen, in welcher Weise die Protokolldateien angelegt werden sollen: Zur Auswahl stehen ein Standardsatz Protokolldateien, ein neuer Satz Protokolldateien für jeden Tag, deren Dateinamen das Erstellungsdatum enthält, und ein neuer Satz Protokolldateien, der nach Wochentagen getrennt angelegt wird, und dessen Dateinamen die Namen der Wochentage enthalten. Schließlich können Sie auch verschiedene Einstellungen zur Pflege der Protokolle festlegen; hierzu gehören eine Größenbegrenzung, bei deren Erreichen eine Protokolldatei archiviert und eine neue Datei begonnen werden, die Anzahl solcher archivierter Protokolldateien, die auf dem System höchstens verbleiben sollen, und die Zeit, für die ein Protokoll höchstens bestehen kann, bevor es in jedem Falle archiviert wird.

6.1 Nachrichten-Protokoll

Um das Nachrichten-Protokoll aufzurufen, klicken Sie auf "Alle Nachrichten". Das Nachrichten-Protokoll enthält zu jeder Nachricht, die Ihre Benutzer senden und empfangen, einen eigenen Eintrag. Darin sind Datum und Uhrzeit, zu denen die Nachricht verarbeitet wurde, Absender und Empfänger, sowie der Betreff der Nachricht vermerkt. Das Protokoll gibt außerdem Aufschluss über die Ergebnisse der Zustellversuche, insbesondere, ob die Nachricht zugestellt oder nicht zugestellt wurde. Wurde eine Nachricht nicht zugestellt, so ist auch der Grund aufgeführt, etwa, dass der Absender in einer Schwarzen Liste erfasst war, dass die Nachricht eine gesperrte Dateianlage enthielt, oder ähnliches. Auch die Größe der Nachricht und die Bewertung der Nachricht 185 werden erfasst.

In der Symbolleiste am oberen Rand des Nachrichten-Protokolls stehen Ihnen mehrere Steuerelemente zur Verfügung, mit denen Sie die nachfolgend beschriebenen Aufgaben erledigen können:

- **Aktualisieren**—Klicken Sie auf dieses Steuerelement, um die Darstellung des Nachrichten-Protokolls zu aktualisieren. Es werden dann auch Einträge angezeigt, die in das Protokoll eingetragen wurden, nachdem Sie das Protokoll aufgerufen haben.
- **Suche**—Über dieses Steuerelement erhalten Sie Zugriff auf umfassende Such-Funktionen, mit deren Hilfe Sie das Nachrichten-Protokoll filtern können, sodass nur bestimmte Nachrichten angezeigt werden. Sie können das Protokoll nach ein- und abgehenden Nachrichten filtern, bestimmten Text in beliebigen Kopfzeilen suchen, den Zeitrahmen für die Suche einschränken, und vieles mehr. Um das Nachrichten-Protokoll zu durchsuchen, öffnen Sie die Such-Maske durch einen Klick auf *Suche* in der Symbolleiste. Legen Sie dann die Suchkriterien fest, und klicken Sie schließlich in der Such-Maske auf das Steuerelement Suche. Die Suche wird dann durchgeführt, und die Ergebnisse erscheinen im Nachrichten-Protokoll. Sie können durch erneutes Anklicken von *Suche* in der Symbolleiste die Such-Maske ausblenden und die Ergebnisse der Suche im Nachrichten-Protokoll angezeigt lassen. Um zur vollständigen Anzeige des Nachrichten-Protokolls zurückzukehren, klicken Sie in der Such-Maske auf *Abbrechen*.
- **Details**—Wählen Sie eine Nachricht aus, und klicken Sie dann auf dieses Steuerelement, um die Nachrichten-Informationen einzublenden. Sie sind in drei Registerkarten unterteilt: Mitschnitt, Nachricht und Quelltext. Die Registerkarte Mitschnitt enthält den Mitschnitt des eigentlichen

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Zustellvorgangs und insbesondere die SMTP-Verbindung und interne Verarbeitung. Die Registerkarte Nachricht enthält den Inhalt der Nachricht selbst. Ob der Nachrichten-Inhalt im Einzelfall verfügbar ist, hängt vom Alter der Nachricht und davon ab, ob die Nachricht erfolgreich zugestellt wurde und welche Optionen im Abschnitt Datenhaltung 144 aktiv sind. Die Registerkarte Quelltext enthält den Quelltext der Nachricht einschließlich der Kopfzeilen, des HTML-Kodes und sonstiger Komponenten. Der Quelltext ist unter Umständen nicht verfügbar, etwa, wenn die Nachricht alt ist oder die Optionen zur Datenhaltung 144 von SecurityGateway eine Speicherung dieser Daten nicht vorsehen.

- **Erneut zustellen**—Um eine Nachricht oder mehrere Nachrichten erneut zuzustellen, wählen Sie sie aus der Liste aus, und klicken Sie dann auf dieses Steuerelement. Sie können mehrere Nachrichten auswählen, indem Sie die Strg- oder Hochschalttaste gedrückt halten. Die erneute Zustellung ist nur möglich, solange die Inhalte der Nachrichten noch nicht aus der Datenbank gelöscht wurden.
- **Spam**—Um eine Nachricht als Spam zu kennzeichnen, wählen Sie die Nachricht aus, und klicken Sie dann auf dieses Steuerelement. Sie können SecurityGateway dadurch helfen, Spam-Nachrichten in Zukunft noch sicherer zu erkennen. Diese Option ist nur verfügbar, wenn die Funktionen für das Bayes'sche Lernverfahren 164 aktiv sind.
- **Kein Spam**—Um eine Nachricht als normale Nachricht zu kennzeichnen, wählen Sie die Nachricht aus, und klicken Sie dann auf dieses Steuerelement. Sie können SecurityGateway dadurch helfen, legitime Nachrichten in Zukunft nicht irrtümlich als Spam zu erkennen. Diese Option ist nur verfügbar, wenn die Funktionen für das Bayes'sche Lernverfahren 164 aktiv sind.
- **Weiße Liste/Schwarze Liste**—Um einen Eintrag in einer Weißen Liste 276 oder einer Schwarzen Liste 266 zu erstellen, klicken Sie die Nachricht an, und klicken Sie danach auf Weiße Liste oder Schwarze Liste. Klicken Sie anschließend auf die Adressliste, der Sie den Absender oder die Domäne des Absenders hinzufügen wollen. Es stehen dafür zur Verfügung die Liste des Benutzers, die Liste der Domäne sowie die globale Liste.

6.2 Protokolldateien

Im Abschnitt Protokolldateien erhalten Sie Zugriff auf die verschiedenen Protokolldateien, die SecurityGateway im Verzeichnis für Protokolle 134 ablegt. Im Gegensatz zum Nachrichten-Protokoll werden diese Protokolle nicht in der Datenbank abgelegt. Sie können daher nicht als sortierfähige Listen angezeigt werden, und ihre Einträge sind nicht nach Ereignissen gruppiert oder getrennt. Sie liegen vielmehr als Nur-Text-Dateien vor, in denen die Mitschnitte der verschiedenen SMTP-Verbindungen und der anderen Aktionen verzeichnet sind, die SecurityGateway bearbeitet. Die Seite Alle Protokolldateien im Abschnitt Protokolldateien macht alle Protokolldateien zugänglich, die im Ordner "logs" (Protokolle) enthalten sind. Dazu gehören die aktuellen Protokolldateien und frühere 320 Protokolldateien, die archiviert wurden. Von dieser Seite aus können Sie alle dort aufgeführten Dateien einsehen. Die anderen Seiten im Abschnitt Protokolldateien enthalten Verknüpfungen mit den jeweils aktuellen Protokolldateien, die SecurityGateway führt; dazu gehören das System-Protokoll, die Eingangs- und Ausgangs-Protokolle und Protokolle über die AntiVirus-Aktualisierung.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

SecurityGateway sichert die Protokolldateien nicht im Rahmen der internen Datensicherung[146]. Sie können jedoch die Optionen zur Archivierung in der Konfiguration der Protokollierung[320] dazu nutzen, diese Dateien zu archivieren. Falls Sie die Protokolldateien statt in das Protokollverzeichnis[134] in ein anderes Verzeichnis archivieren oder sichern möchten, müssen Sie hierfür eine bestehende Datensicherungs-Lösung oder eine andere externe Methode einsetzen.

Alle Protokolldateien

Auf der Seite Alle Protokolldateien wird eine Übersicht über alle Dateien angezeigt, die in Ihrem im Abschnitt Verzeichnisse[134] bestimmten Protokollverzeichnis gespeichert sind. Die Übersicht umfasst die aktuellen Dateien, in die SecurityGateway laufend Ereignisse einträgt, und die früheren[320] Protokolldateien. In jedem Eintrag sind der Dateiname, die Dateigröße sowie Datum und Uhrzeit der letzten Änderung vermerkt. Um eine Datei aus der Liste anzeigen zu lassen, klicken Sie doppelt auf ihren Eintrag, oder wählen Sie den Eintrag durch einfachen Klick, und klicken Sie dann in der Symbolleiste auf *Anzeigen*. Um eine Datei aus der Liste herunterzuladen, wählen Sie die Datei aus, und klicken Sie dann auf *Herunterladen*. Um eine Datei zu löschen, wählen Sie die Datei aus, und klicken Sie dann auf *Löschen*.

Aktuelle Protokolldateien

Die weiteren Verknüpfungen im Abschnitt Protokolldateien führen Sie direkt zu den aktuellen Protokollen, in die SecurityGateway laufend Ereignisse einträgt. Folgende aktuelle Protokolldateien können mithilfe der Verknüpfungen direkt angezeigt werden:

- **System**—Das System-Protokoll enthält unter anderem die Ereignisse Starten und Beenden des SecurityGateway-Dienstes, Initialisierung von SMTP-, SSL-, HTTP- und sonstigen Diensten, sowie bestimmte Systemfehler.
- **Eingang**—Das Eingangs-Protokoll von SecurityGateway enthält die Verbindungs-Mitschnitte für alle eingehenden Nachrichten.
- **Ausgang**—Dieses Protokoll enthält die Verbindungs-Mitschnitte für alle abgehenden Nachrichten.
- **Routing**—Das Routing-Protokoll erfasst alle Aktionen, die SecurityGateway durchführt, um eingehende Nachrichten an Ihre Benutzer und Server zu leiten.
- **Änderung**—Das Änderungsprotokoll erfasst alle Änderungen, die an der Konfiguration von SecurityGateway vorgenommen wurden, und die Benutzer, die sie vorgenommen haben.
- **Archivierung**—Dieses-Protokoll erfasst alle Aktionen im Zusammenhang mit der Archivierung[105].
- **POP**—Dieses Protokolle enthält die Informationen und Mitschnitte über alle Aktivitäten für etwa konfigurierte POP-Benutzerkonten[82].
- **HTTP**—Dieses Protokoll enthält alle Daten und Ereignisse im Zusammenhang mit dem HTTP-Dienst.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- **ClamAV-Aktualisierung**—Das Aktualisierungs-Protokoll für ClamAV erfasst alle Daten über die Aktualisierung der Viren-Signaturen für ClamAV.
- **IKARUS Anti-Virus Protokolldateien**—Es gibt drei Protokolldateien, die sich auf IKARUS-Virensignatur-Updates, den Motorstatus und das Scannen beziehen.

6.3 Konfiguration der Protokollierung

Der Abschnitt Konfiguration enthält eine Verknüpfung mit der Seite für die Konfiguration des Protokolls, auf der die Einstellungen und Optionen für die Protokollierung eingerichtet werden. Um diese Seite aufzurufen, klicken Sie im linken Bereich auf *Protokollierung»Konfiguration»Protokollierung konfigurieren*. Auf dieser Seite können Sie festlegen, in welchem Detaillierungsgrad die Eingangs-, Ausgangs- und HTTP-Protokolle geführt werden. Sie können auch wählen, in welcher Weise die Protokolldateien angelegt werden sollen: Zur Auswahl stehen ein Standardsatz Protokolldateien, ein neuer Satz Protokolldateien für jeden Tag, deren Dateinamen das Erstellungsdatum enthält, und ein neuer Satz Protokolldateien, der nach Wochentagen getrennt angelegt wird, und dessen Dateinamen die Namen der Wochentage enthalten. Schließlich können Sie auch verschiedene Einstellungen zur Pflege der Protokolle festlegen; hierzu gehören eine Größenbegrenzung, bei deren Erreichen eine Protokolldatei archiviert und eine neue Datei begonnen werden, die Anzahl solcher archivierter Protokolldateien, die auf dem System höchstens verbleiben sollen, und die Zeit, für die ein Protokoll höchstens bestehen kann, bevor es in jedem Falle archiviert wird. Alle Protokolldateien werden in dem Verzeichnis für Protokolle abgelegt, das auf der Seite Verzeichnisse 134 festgelegt wird.

Detailgrad

Die Optionen dieses Abschnitts bestimmen Umfang und Detailgrad der Protokolldateien 318 für eingehende und abgehende SMTP-Verbindungen und den HTTP-Dienst. Sie wirken nicht auf die anderen Protokolldateien, insbesondere System und Routing.

Debug
Diese Option erzeugt in den Protokolldateien für Eingang, Ausgang und HTTP den höchsten Detailgrad und erfasst die umfangreichsten Informationen. Da diese Option zu sehr großen Protokolldateien führen kann, kann sie auch die Systemleistung beeinträchtigen. Sie soll daher nur im Bedarfsfall ausgewählt werden, wenn etwa ein bestimmtes Problem zu diagnostizieren und zu beheben ist. Als allgemeine Betriebsart soll sie nicht ausgewählt werden.

Information
Dies ist der Standard-Detailgrad, der für die meisten Anwendungsfälle empfohlen wird. Die Protokollierung erreicht zwar nicht den Detailgrad der Option Debug, das Protokoll enthält dennoch Einträge für erfolgreiche und fehlgeschlagene Vorgänge.

Warnung
Diese Option bewirkt, dass nur fehlgeschlagene Vorgänge und Informationen über mögliche Probleme in das Protokoll eingetragen werden.

Fehler
Diese Option bewirkt, dass nur fehlgeschlagene Vorgänge in das Protokoll eingetragen werden. Die Auswahl dieser Option kann die Systemleistung erhöhen.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

keine
Diese Option bewirkt, dass für Eingang, Ausgang und HTTP kein Protokoll geführt wird. Von der Nutzung dieser Option wird abgeraten.

Betriebsart des Protokolls

Die folgenden Optionen bestimmen, wie die Protokolldateien benannt werden.

Standardsatz Protokolldateien anlegen
Diese Option bewirkt, dass SecurityGateway einen Standardsatz Protokolldateien nach folgendem Namensschema anlegt: `SecurityGateway-Inbound.log`, `SecurityGateway-Outbound.log`, `SecurityGateway-System.log` usw. Aus technischen Gründen vergibt SecurityGateway englische Dateinamen.

Jeden Tag einen neuen Satz Protokolldateien anlegen
Dies ist die Standardeinstellung. Sie bewirkt, dass jeden Tag um Mitternacht ein neuer Satz Protokolldateien angelegt wird, und dass dabei das Datum in die Dateinamen aufgenommen wird. Ein Beispiel hierzu: `SecurityGateway-20080315-Inbound.log` ist das Protokoll über eingehende SMTP-Verbindungen, das am 15. März 2008 angelegt wurde.

Computernamen in Dateinamen der Protokolldateien aufnehmen
Diese Option bewirkt, dass der Computername in die Dateinamen der Protokolldateien aufgenommen wird. Falls das Verzeichnis für die Speicherung der Protokolldateien durch einen UNC-Pfad bezeichnet ist, muss diese Option aktiviert sein. Die Option ermöglicht es mehreren Servern in einem Cluster[137], die Protokolle im selben Verzeichnis zu speichern.

SMTP- und HTTP-Verbindungen von folgenden IP-Adressen nicht protokollieren
Mithilfe dieser Option können Sie eine Ausschlussliste für IP-Adressen konfigurieren. SMTP- und HTTP-Verbindungen, die von den IP-Adressen auf dieser Liste ausgehen, werden nicht protokolliert. Unvollständige und abgewiesene Nachrichten, die von einer hier erfassten IP-Adresse über SMTP übermittelt werden sollten, werden nicht in die Datenbank aufgenommen. Wird eine Nachricht zur Zustellung entgegengenommen, so wird sie der Datenbank hinzugefügt.

Pflege der Protokolle

Die Optionen in diesem Abschnitt bestimmen die Größe der Protokolldateien, die Anzahl alter Protokolldateien, die nach der Umstellung noch beibehalten werden, das Überschreiben bestehender Protokolldateien und das Intervall, in dem alte Protokolldateien archiviert werden.

Größenbegrenzung für Protokolldateien: [xx] KB (0 = keine Größenbegrenzung)
Diese Option bestimmt die höchstzulässige Größe (in KB) für jede Protokolldatei. Erreicht eine Protokolldatei diesen Schwellwert, so wird sie in `*.OLD` umbenannt, und eine neue Datei wird angelegt und weitergeführt. Die Option *Höchstzahl der Dateien nach Protokoll-Umstellung* weiter unten bestimmt, wie viele dieser alten Protokolldateien nach der Umstellung beibehalten werden.

Höchstzahl der Dateien nach Protokoll-Umstellung:
Diese Option bestimmt, wie viele alte Protokolldateien für jedes Protokoll beibehalten werden. Eine alte Protokolldatei entsteht immer dann, wenn ein Protokoll die oben festgelegte *Größenbegrenzung für Protokolldateien* überschreitet. Solche Dateien werden nach folgendem Schema benannt:

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

"Dateiname(1).old", "Dateiname(2).old", "Dateiname(3).old" usw. Sobald eine neue Datei nach diesem Schema angelegt wird, werden alle anderen alten Dateien so umbenannt, dass die zuletzt umgestellte Protokolldatei an erster Stelle steht. Daraus ergibt sich, dass "Dateiname(1).old" immer die jüngste umgestellte Datei ist, dann folgt "Dateiname(2).old" usw. Wird die Höchstzahl der Dateien erreicht, so wird die älteste Datei gelöscht, und die übrigen Dateien werden nach dem bekannten Schema umbenannt. Die Voreinstellung für diesen Wert beträgt 10.

Bestehende Protokolldateien beim Namenswechsel um Mitternacht überschreiben
Ist die Option *Protokolldateien nach Wochentagen getrennt anlegen* aktiv, so erstellt SecurityGateway jeden Tag um Mitternacht einen neuen Satz Protokolldateien und nimmt in die Dateinamen den Namen des Wochentags auf. Diese Option bestimmt, ob bestehende Dateien gleichen Namens dabei überschrieben werden, oder ob SecurityGateway die neuen Daten an das Ende der bestehenden Dateien anfügen soll. Ist diese Option aktiv, und erkennt SecurityGateway beispielsweise am Sonntag, dass die Datei "SecurityGateway-Sunday-Inbound.log" bereits besteht, so wird diese Datei überschrieben und enthält folglich nur noch Informationen über den aktuellen Tag. Ist die Option nicht aktiv, so werden die Informationen aus dem aktuellen Tag an das Ende der bestehenden Datei angefügt. Die Option ist per Voreinstellung abgeschaltet.

Protokolldateien in ZIP-Archiv packen und archivieren nach [xx] Tagen (0 = nie)
SecurityGateway kann jeden Tag um Mitternacht alle Protokolldateien, die das hier angegebene Alter überschritten haben, komprimieren und in das Verzeichnis 134 \Logs\OldLogs\ verschieben. Die Voreinstellung für diese Option beträgt 14 Tage.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Kapitel

7 Berichte

Im Abschnitt Berichte stehen interaktive, detailreiche grafische Berichte über die Aktivität von SecurityGateway zur Verfügung. Sie können Berichte erstellen, die die Anzahl der eingehenden im Vergleich zu den abgehenden Nachrichten zeigen, eine Übersicht über die Arten von Spam- oder Junk-Nachrichten geben, die Bandbreitennutzung aufschlüsseln, die aktivsten Absender nach Gesamt-Nachrichtengröße zeigen, Übersichten über erkannte Viren geben, und viele weitere Angaben enthalten. Jeder Bericht kann außerdem mithilfe besonderer Optionen konfiguriert werden. So kann ein Bericht etwa Daten nur für eine bestimmte Domäne oder für alle Domänen enthalten, der Maßstab der Daten lässt sich nach Stunden, Tagen und Monaten auflösen, und der Bericht kann sich wahlweise auf festgelegte Zeiträume beziehen, etwa einen Tag, eine Woche, einen Monat, oder den Zeitraum zwischen zwei Daten. Unterhalb jedes Berichts wird ihr Inhalt tabellarisch dargestellt. Diese Darstellung enthält Verknüpfungen mit dem Nachrichten-Protokoll 317, die eine Anzeige nur derjenigen Daten aus dem Protokoll bewirken, die sich auf die Daten aus dem Bericht beziehen. Eine solche Verknüpfung kann beispielsweise alle eingehenden Nachrichten anzeigen, die zu einer bestimmten Stunde empfangen wurden, die auch im Bericht dargestellt wird, alle Nachrichten, die einen Virus enthielten und an einem bestimmten Tag eingingen, und alle Nachrichten, die durch den aktivsten Empfänger in einer Domäne empfangen wurden. Um einen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.

Das Menü Berichte ist in sechs Abschnitte untergliedert:

Zeitplangesteuerte Berichte

Dieser Abschnitt enthält die Option zur Erstellung des Statistik-Berichts:

- **Statistik-Bericht**—Dieser Bericht enthält Statistiken über das System. Er gibt einen schnellen Überblick über den Zustand des Systems und die Effizienz der Filter des Servers. Er kann täglich oder wöchentlich an die globalen Administratoren, die Domänen-Administratoren und an eine manuell erstellte Empfängerliste versandt werden. Die Berichte für Domänen-Administratoren enthalten dabei nur Statistiken der Domänen, für die diese Administratorrechte haben.

  Im Konfigurationsdialog für den Statistik-Bericht bestimmen Sie durch Auswahl der Option *Täglich* oder *Wöchentlich* im Abschnitt Zeitplanung, wie oft der Bericht versandt werden soll. Sodann legen Sie im Abschnitt Empfänger durch Auswahl der Option *An alle globalen Administratoren senden* oder *An alle Domänen-Administratoren senden* fest, ob der Bericht an alle globalen oder alle Domänen-Administratoren versandt werden soll. Außerdem können Sie im Abschnitt Ausschlüsse einzelne Administratoren als Empfänger ausschließen; diese erhalten den Bericht nicht. Schließlich können Sie im Abschnitt *Zusätzliche Empfänger* die E-Mail-Adressen erfassen, die den Bericht ebenfalls erhalten sollen, obwohl sie nicht Teil der Administratorgruppen sind.

Zusammenfassung

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Die Berichte im Abschnitt Zusammenfassung geben einen allgemeinen Überblick über die Zahl der eingehenden und abgehenden Nachrichten, die SecurityGateway verarbeitet, die Zahl und die Arten der normalen und der Spam- oder Junk-Nachrichten, und die durch die E-Mail-Übermittlung beanspruchte Bandbreite.

- **Eingehende/Abgehende Nachrichten**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die Gesamtzahl der eingehenden und der abgehenden Nachrichten dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für eingehende und abgehende Nachrichten; dabei entspricht jede Zeile einer Einheit der *(zeitlichen) Auflösung,* in der der Bericht erstellt wurde (Stunden, Tage oder Monate). Sie können sich durch einen Klick auf die Verknüpfungen in der Tabelle das Nachrichten-Protokoll für die eingehenden und abgehenden Nachrichten anzeigen lassen, die während des Zeitraums verarbeitet wurden, zu dem die Verknüpfung gehört. Die Zahl der Einträge im Bericht wird durch die Einstellung *Max. Einträge* begrenzt. SecurityGateway beginnt mit der Erstellung des Berichts am Beginn des *Zeitraums* und fügt dem Bericht so lange Daten hinzu, bis der eingestellte Wert *Max. Einträge* erreicht ist. Falls der Wert *Max. Einträge* zu niedrig gesetzt ist, deckt der Bericht unter Umständen nicht den gesamten eingestellten *Zeitraum* ab. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.
- **Normale/Spam-Nachrichten**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die Gesamtzahl der normalen und der Spam-Nachrichten dar. Als Spam-Nachrichten werden dabei solche Nachrichten bezeichnet, bei denen festgestellt wurde, dass sie Spam, gefälschte Absenderadressen, Viren und ähnliches enthalten. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für normale und Spam-Nachrichten; dabei entspricht jede Zeile einer Einheit der *(zeitlichen) Auflösung,* in der der Bericht erstellt wurde (Stunden, Tage oder Monate). Sie können sich durch einen Klick auf die Verknüpfungen in der Tabelle das Nachrichten-Protokoll für die normalen und Spam-Nachrichten anzeigen lassen, die während des Zeitraums verarbeitet wurden, zu dem die Verknüpfung gehört. Die Zahl der Einträge im Bericht wird durch die Einstellung *Max. Einträge* begrenzt. SecurityGateway beginnt mit der Erstellung des Berichts am Beginn des *Zeitraums* und fügt dem Bericht so lange Daten hinzu, bis der eingestellte Wert *Max. Einträge* erreicht ist. Falls der Wert *Max. Einträge* zu niedrig gesetzt ist, deckt der Bericht unter Umständen nicht den gesamten eingestellten *Zeitraum* ab. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.
- **Aufschlüsselung der Spam-Nachrichten**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* einen Überblick über alle Spam-Nachrichten dar, der in sechs Kategorien aufgeschlüsselt ist: Spam 155, Virus 187, Spoofing 190, Abuse 222, unvollständig und Benutzer. Die Kategorie *unvollständig* erfasst alle Verbindungen, in denen eine Zeitüberschreitung auftritt oder in denen die Gegenstelle die Socket-Verbindung beendet oder einen Befehl zum Abbruch der Verbindung sendet, bevor Nutzdaten übertragen wurden. In diese Kategorie gehören auch SMTP-Sondierungen. Die Kategorie *Benutzer* umfasst Schwarze Listen 265, Regeln des Inhaltsfilters 252,

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Filterung von Dateianlagen[263] und benutzerdefinierte Sieve-Skripte[284]. Die verbleibenden Kategorien beziehen sich auf die zugehörigen Abschnitte im Bereich Sicherheit[154]. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für die einzelnen Kategorien; dabei entspricht jede Zeile einer Einheit der *(zeitlichen) Auflösung,* in der der Bericht erstellt wurde (Stunden, Tage oder Monate). Sie können sich durch einen Klick auf die Verknüpfungen in der Tabelle das Nachrichten-Protokoll für die Kategorie der Spam-Nachrichten anzeigen lassen, die während des Zeitraums verarbeitet wurden, zu dem die Verknüpfung gehört. Die Zahl der Einträge im Bericht wird durch die Einstellung *Max. Einträge* begrenzt. SecurityGateway beginnt mit der Erstellung des Berichts am Beginn des *Zeitraums* und fügt dem Bericht so lange Daten hinzu, bis der eingestellte Wert *Max. Einträge* erreicht ist. Falls der Wert *Max. Einträge* zu niedrig gesetzt ist, deckt der Bericht unter Umständen nicht den gesamten eingestellten *Zeitraum* ab. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.

- **Gesamt-Bandbreite für E-Mail**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die gesamte durch E-Mail beanspruchte Bandbreite dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit einer Spalte für die beanspruchte Bandbreite; dabei entspricht jede Zeile einer Einheit der *(zeitlichen) Auflösung,* in der der Bericht erstellt wurde (Stunden, Tage oder Monate). Sie können sich durch einen Klick auf die Verknüpfungen in der Tabelle das Nachrichten-Protokoll für die normalen und Spam-Nachrichten anzeigen lassen, die während des Zeitraums verarbeitet wurden, zu dem die Verknüpfung gehört. Die Zahl der Einträge im Bericht wird durch die Einstellung *Max. Einträge* begrenzt. SecurityGateway beginnt mit der Erstellung des Berichts am Beginn des *Zeitraums* und fügt dem Bericht so lange Daten hinzu, bis der eingestellte Wert *Max. Einträge* erreicht ist. Falls der Wert *Max. Einträge* zu niedrig gesetzt ist, deckt der Bericht unter Umständen nicht den gesamten eingestellten *Zeitraum* ab. Um einen neuen Bericht zu erstellen, wählen Sie, wie bei den anderen Berichten in diesem Abschnitt, zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.

Eingehende E-Mail

Die Berichte im Abschnitt Eingehende E-Mail behandeln nur die eingehenden Nachrichten. Sie können Berichte über alle eingehenden Nachrichten erstellen, die SecurityGateway verarbeitet hat, sowie Berichte über die aktivsten E-Mail-Empfänger nach Anzahl der Nachrichten und nach Gesamt-Nachrichtengröße.

- **Verarbeitete eingehende Nachrichten**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die Gesamtzahl der eingehenden Nachrichten dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit einer Spalte für die Gesamtzahl der eingehenden Nachrichten; dabei entspricht jede Zeile einer Einheit der *(zeitlichen) Auflösung,* in der der Bericht erstellt wurde (Stunden, Tage oder Monate). Sie können sich durch einen Klick auf die Verknüpfungen in der Tabelle das Nachrichten-Protokoll für die eingehenden Nachrichten anzeigen lassen, die während des Berichts-

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Zeitraums verarbeitet wurden, zu dem die Verknüpfung gehört. Die Zahl der Einträge im Bericht wird durch die Einstellung *Max. Einträge* begrenzt. SecurityGateway beginnt mit der Erstellung des Berichts am Beginn des *Zeitraums* und fügt dem Bericht so lange Daten hinzu, bis der eingestellte Wert *Max. Einträge* erreicht ist. Falls der Wert *Max. Einträge* zu niedrig gesetzt ist, deckt der Bericht unter Umständen nicht den gesamten eingestellten *Zeitraum* ab. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.

- **Aktivste E-Mail-Empfänger**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die aktivsten E-Mail-Empfänger dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für die Empfänger und die Zahl der Nachrichten, die sie empfangen haben. Sie können sich durch einen Klick auf einen Empfänger das Nachrichten-Protokoll für die eingehenden Nachrichten anzeigen lassen, die der Empfänger während des Berichts-Zeitraums empfangen hat. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.
- **Aktivste Empfänger nach Gesamt-Datenvolumen**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die aktivsten E-Mail-Empfänger nach der Gesamt-Nachrichtengröße dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für die Empfänger und die Gesamtgröße der Nachrichten, die sie empfangen haben. Sie können sich durch einen Klick auf einen Empfänger das Nachrichten-Protokoll für die eingehenden Nachrichten anzeigen lassen, die der Empfänger während des Berichts-Zeitraums empfangen hat. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.

Abgehende E-Mail

Die Berichte im Abschnitt Abgehende E-Mail behandeln nur die abgehenden Nachrichten. Sie können Berichte über alle abgehenden Nachrichten erstellen, die SecurityGateway verarbeitet hat, sowie Berichte über die aktivsten E-Mail-Versender nach Anzahl der Nachrichten und nach Gesamt-Nachrichtengröße.

- **Verarbeitete abgehende Nachrichten**—Dieser Bericht stellt für die jeweils ausgewählte Domäne und den ausgewählten Zeitraum die Gesamtzahl der abgehenden Nachrichten dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit einer Spalte für die Gesamtzahl der abgehenden Nachrichten; dabei entspricht jede Zeile einer Einheit der (zeitlichen) Auflösung, in der der Bericht erstellt wurde (Stunden, Tage oder Monate). Sie können sich durch einen Klick auf die Verknüpfungen in der Tabelle das Nachrichten-Protokoll für die abgehenden Nachrichten anzeigen lassen, die während des Berichts-Zeitraums verarbeitet wurden, zu dem die Verknüpfung gehört. Die Zahl der Einträge im Bericht wird durch die Einstellung Max. Einträge begrenzt. SecurityGateway beginnt mit der Erstellung des Berichts am Beginn des Zeitraums und fügt dem Bericht so lange Daten hinzu, bis der eingestellte Wert Max. Einträge erreicht ist. Falls der Wert Max. Einträge zu niedrig gesetzt ist, deckt der Bericht unter Umständen nicht den gesamten

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

eingestellten Zeitraum ab. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf Anzeigen.

- **Aktivste E-Mail-Versender**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die aktivsten E-Mail-Versender dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für die Adressen der Versender und die Zahl der Nachrichten, die sie versandt haben. Sie können sich durch einen Klick auf die Adresse eines Versenders das Nachrichten-Protokoll für die abgehenden Nachrichten anzeigen lassen, die der Versender während des Berichts-Zeitraums versandt hat. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.
- **Aktivste Versender nach Gesamt-Datenvolumen**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die aktivsten E-Mail-Versender nach der Gesamt-Nachrichtengröße dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für die Adressen der Versender und die Gesamtgröße der Nachrichten, die sie versandt haben. Sie können sich durch einen Klick auf die Adresse eines Versenders das Nachrichten-Protokoll für die abgehenden Nachrichten anzeigen lassen, die der Versender während des Berichts-Zeitraums versandt hat. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.

Anti-Spam

Die Berichte im Abschnitt Anti-Spam verschaffen Ihnen schnell einen Überblick darüber, welche Domänen den meisten Spam an Ihre Benutzer versenden, und welche Benutzer den meisten Spam empfangen.

- **Aktivste Spam-Quellen**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die als Spam-Versender aktivsten Domänen dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für die Domäne, die den Spam versendet, und die Anzahl der Nachrichten, die von dieser Domäne empfangen wurden. Sie können sich durch einen Klick auf eine Domäne aus der Liste das Nachrichten-Protokoll für die Nachrichten anzeigen lassen, die die Domäne während des Berichts-Zeitraums an Ihre Benutzer versandt hat. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.
- **Aktivste Spam-Empfänger**—Dieser Bericht stellt für die jeweils ausgewählte *Domäne* und den ausgewählten *Zeitraum* die am meisten durch eingehenden Spam betroffenen Benutzer dar. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit Spalten für die Adressen der Empfänger und die Zahl der Spam-Nachrichten, die sie empfangen haben. Sie können sich durch einen Klick auf die Adresse eines Empfängers das Nachrichten-Protokoll für die eingehenden Spam-Nachrichten anzeigen lassen, die der Empfänger während des Berichts-Zeitraums erhalten hat. Um einen neuen Bericht zu erstellen, wählen Sie

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf *Anzeigen*.

Anti-Virus

Die Berichte im Abschnitt Anti-Virus verschaffen Ihnen schnell einen Überblick darüber, wie viele Viren SecurityGateway in ein- und abgehenden Nachrichten erkannt und angehalten hat, und um welche Viren es sich dabei genau gehandelt hat.

- **Blockierte eingehende Viren**—Dieser Bericht stellt für die jeweils ausgewählte Domäne und den ausgewählten Zeitraum die Gesamtzahl der eingehenden Nachrichten dar, in denen SecurityGateway Viren erkannt und angehalten hat. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit einer Spalte für die Gesamtzahl der eingehenden Nachrichten mit erkannten und angehaltenen Viren; dabei entspricht jede Zeile einer Einheit der (zeitlichen) Auflösung, in der der Bericht erstellt wurde (Stunden, Tage oder Monate). Sie können sich durch einen Klick auf die Verknüpfungen in der Tabelle das Nachrichten-Protokoll für die eingehenden Nachrichten anzeigen lassen, in denen während des Berichts-Zeitraums Viren erkannt und angehalten wurden. Die Zahl der Einträge im Bericht wird durch die Einstellung Max. Einträge begrenzt. SecurityGateway beginnt mit der Erstellung des Berichts am Beginn des Zeitraums und fügt dem Bericht so lange Daten hinzu, bis der eingestellte Wert Max. Einträge erreicht ist. Falls der Wert Max. Einträge zu niedrig gesetzt ist, deckt der Bericht unter Umständen nicht den gesamten eingestellten Zeitraum ab. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf Anzeigen.
- **Meistgefundene eingehende Viren nach Name**—Dieser Bericht stellt für die jeweils ausgewählte Domäne und den ausgewählten Zeitraum die in eingehenden Nachrichten meistgefundenen Viren dar, die SecurityGateway angehalten hat. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit einer Spalte für die Namen der angehaltenen Viren und die Häufigkeit ihres Auftretens. Sie können sich durch einen Klick auf die Namen der Viren das Nachrichten-Protokoll für die eingehenden Nachrichten anzeigen lassen, in denen während des Berichts-Zeitraums die ausgewählten Viren erkannt und angehalten wurden. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf Anzeigen.
- **Blockierte abgehende Viren**—Dieser Bericht stellt für die jeweils ausgewählte Domäne und den ausgewählten Zeitraum die Gesamtzahl der abgehenden Nachrichten aus der Domäne dar, in denen SecurityGateway Viren erkannt und angehalten hat. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit einer Spalte für die Gesamtzahl der abgehenden Nachrichten mit erkannten und angehaltenen Viren; dabei entspricht jede Zeile einer Einheit der (zeitlichen) Auflösung, in der der Bericht erstellt wurde (Stunden, Tage oder Monate). Sie können sich durch einen Klick auf die Verknüpfungen in der Tabelle das Nachrichten-Protokoll für die abgehenden Nachrichten anzeigen lassen, in denen während des Berichts-Zeitraums Viren erkannt und angehalten wurden, zu dem die Verknüpfung gehört. Die Zahl der Einträge im Bericht wird durch die Einstellung Max. Einträge begrenzt. SecurityGateway beginnt mit der Erstellung des Berichts am Beginn des Zeitraums und fügt dem

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Bericht so lange Daten hinzu, bis der eingestellte Wert Max. Einträge erreicht ist. Falls der Wert Max. Einträge zu niedrig gesetzt ist, deckt der Bericht unter Umständen nicht den gesamten eingestellten Zeitraum ab. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf Anzeigen.

- **Meistgefundene abgehende Viren nach Name**—Dieser Bericht stellt für die jeweils ausgewählte Domäne und den ausgewählten Zeitraum die in abgehenden Nachrichten meistgefundenen Viren dar, die SecurityGateway angehalten hat. Unter der grafischen Darstellung enthält der Bericht eine Tabelle mit einer Spalte für die Namen der angehaltenen Viren und die Häufigkeit ihres Auftretens. Sie können sich durch einen Klick auf die Namen der Viren das Nachrichten-Protokoll für die abgehenden Nachrichten anzeigen lassen, in denen während des Berichts-Zeitraums die ausgewählten Viren erkannt und angehalten wurden. Um einen neuen Bericht zu erstellen, wählen Sie zunächst die Parameter und Kriterien für den Bericht aus, und klicken Sie dann in der Symbolleiste am oberen Rand der Seite auf Anzeigen.

Leistungsindikatoren (Performance Counter) zur Leistungsüberwachung

Neben den hier beschriebenen Auswertungen und Berichten stellt SecurityGateway verschiedene Leistungsindikatoren (sie werden auch als Performance Counter bezeichnet) zur Verfügung, die in der Windows-Leistungsüberwachung (sie wird auch als Windows Performance Monitor bezeichnet) verwendet werden können. Sie können hiermit den Status von SecurityGateway in Echtzeit überwachen. Die zur Verfügung stehenden Leistungsindikatoren sind unter anderem: Zahl der aktiven Verbindungen, Zahl der Nachrichten in den Warteschlangen, Status der Serverdienste als aktiv oder nicht aktiv, Betriebszeit seit Programmstart, Zahl der Domänen und Zahl der Benutzer. **Beachte:** Folgende Leistungsindikatoren werden nur einmal pro Minute aktualisiert: Zustellungs-Warteschlange, administrative Quarantäne und Zahl der Domänen.

Um die Leistungsindikatoren zu nutzen, führen Sie in Microsoft Windows folgende Schritte durch:

1. Rufen Sie aus der Systemsteuerung die Übersicht über die Verwaltungsprogramme auf, und klicken Sie auf **Leistungsüberwachung**. (Stattdessen können Sie auch das Programm **perfmon** ausführen.)
2. Klappen Sie den Abschnitt Überwachungstools aus, und klicken Sie auf **Leistungsüberwachung**. Klicken Sie dann auf der Symbolleiste auf "+" (Hinzufügen), um den Konfigurationsdialog Leistungsindikatoren hinzufügen aufzurufen.
3. Klicken Sie in der Liste im Abschnitt "Verfügbare Indikatoren" auf **SecurityGateway**, und klicken Sie auf **Hinzufügen »**, um alle Indikatoren für SecurityGateway hinzuzufügen. Falls Sie nicht alle Indikatoren hinzufügen wollen, klappen Sie die Gruppe SecurityGateway aus, wählen Sie die gewünschten Indikatoren aus, und klicken Sie dann auf **Hinzufügen»**.
4. Klicken Sie auf **OK.**

Beachte: Um auf Leistungsindikatoren einer SecurityGateway-Installation zuzugreifen, die auf einem anderen Rechner ausgeführt wird, muss der Windows-Dienst "Remoteregistrierung" aktiv sein, und etwa vorhandene Firewalls müssen so konfiguriert sein, dass sie den Zugriff gestatten.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Index

- 2 -

- A -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- B -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- C -

- D -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- E -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- F -

- G -

- H -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- I -

- K -

- L -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- M -

- N -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- O -

- P -

- Q -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- R -

- S -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- T -

- U -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- V -

- W -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.

- Z -

Copyright © 2007-2023. Alle Rechte vorbehalten. MDaemon Technologies, Ltd.