Sender Policy Framework in MDaemon 7.1+

Alt-N Technologies, Ltd
2201 East Lamar Blvd, Suite 270
Arlington, TX 76006
Tel: (817) 525-2005

Contents

Abstract

Spoofing of email addresses causes huge problems for Internet communications. Spoofing is the unauthorized use of an email address. It is one of the main tactics used to spread messages containing spam, viruses and other types of scams. It enables email senders to hide their true identities. Anyone can easily spoof an email address by simply modifying the return address in their email client configuration. Sender Policy Framework (SPF) is an open standard security protocol designed to detect spoofed email addresses. It is an important part of any email security policy. SPF verifies the identities of email servers for incoming messages. It compares the FROM email address of a message against a list of all computers authorized to send email as that address. Using the results of an SPF lookup, an email server (or other software) working with SPF can take appropriate action. Beginning with version 7.1, MDaemon offers SPF as one of its security options.

SPF Concepts

Address Spoofing Background

Email address spoofing enables the widespread proliferation of spam and viruses while hiding the true identities of those responsible.

Spoofers use email addresses of other people without their permission or knowledge. In this way anyone can send email pretending to be anyone else. For example, someone might send messages while masquerading as:
`frodo@shire.net`,
`mars@solarsystem.org`, or
`billgates@microsoft.com`.

The Origins of Flexible Email Sending

Email address spoofing is possible because of the flexibility, openness and trusting nature of the current electronic mail communications standards. The idea is simple—allow users to send mail from multiple servers while receiving mail at one consolidated address.

In practice, this design concept is still very useful for some email users. For example, consider the road warriors:

> A lot of people travel as part of their jobs. For a variety of reasons—mostly security—their home email servers may not be available for sending messages from remote locations.
>
> As alternatives, the road warriors may send their email by using public services such as Hotmail or Yahoo!, Internet Service Providers such as Earthlink or personal email servers on their notebook computers. They may also use a combination of these, depending on their needs, preferences and the availability of services in different parts of the world.
>
> In any case, whatever method they choose to send their messages, traveling workers typically plug in their home email information as their return addresses. In this way they can receive all of their incoming messages through single email accounts.

Every day, thousands of email users employ the ability of electronic mail to send messages from one domain and receive them at another, all for legitimate reasons. Even more often, spammers, virus writers and thieves misuse the openness of email for inappropriate and illegal purposes.

The Fallout of Spoofing

Email address spoofing assists in the rapid expansion of spam, viruses and information theft.

Spammers often hide behind spoofed return addresses. Replying to or bouncing the messages almost always results in “Returned mail: User unknown” messages. The cost of spam is billions annually in lost time, stolen bandwidth and wasted computer resources. Spam offers little or no benefit to anyone but the spammers. Because of this, spam is well known for its economy to the senders and high cost to everyone else.

Viruses often spread by using real, but spoofed, addresses collected from their victim machines. Many viruses send messages by using their own built-in email senders. They mail themselves to all addresses found on infected machines. Also, they randomly spoof the same addresses as the message senders. Besides spreading the viruses, this methodology generates a flood of “virus-found” messages back to the spoofed addresses. This confuses some users who send angry denials, wasting more time and resources. Viruses can also infect machines with software designed to launch denial of service attacks.

Cyber thieves often use spoofing to disguise themselves as people with legitimate needs to know personal information. For example, an email requesting account information may appear to come from a system administrator. Instead, the address is spoofed and any response goes to vandals looking for unauthorized access. In another type of scam, an email requests the user to update account information for online financial services. While the email credentials may look authentic, the updated information helps the efforts of identity thieves.

Because of the power of spoofing, the forging of email addresses is on the rise. Over 50 percent of all email messages now use spoofed return addresses. In fact, the volume of unwanted and illegal messages is now high enough to threaten the legitimate use of email.

Making address spoofing more difficult forces spammers to use their own email addresses. Stopping forging of addresses also removes one of the primary means of spreading viruses. When spammers and virus writers can no longer spoof addresses their unwanted messages will be easier to detect and block using other security measures.

Security Measures and Spoofing

Until recently there have been no strong measures to prevent the spoofing of email sender addresses.

To be sure, email security experts—including Alt-N Technologies—have developed numerous means of detecting and suppressing unwanted and harmful messages. These techniques consist mostly of preventing unauthorized use of email servers and blocking illegitimate messages.

Some of these methods require regular human intervention, such as reviewing feedback from email users and reading system logs. Other approaches rely on software for analysis, detection and preventative intervention. Some users have also implemented encrypted digital signatures for positive user identification

MDaemon—an industry leader in protecting both the email server and its account holders—employs multiple security methods including:

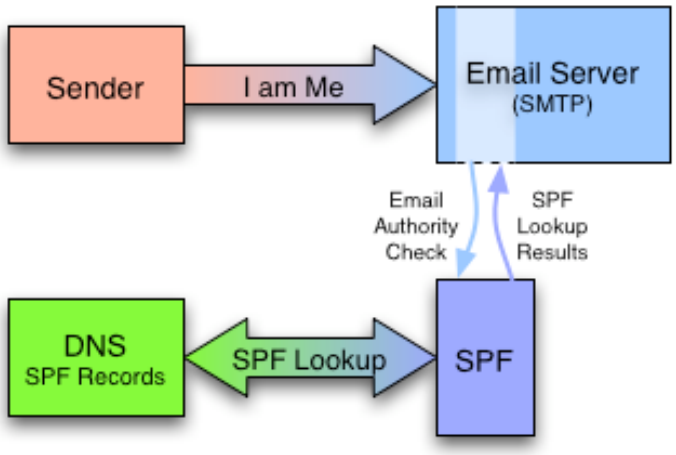
Anti Virus	Restricted Attachments	Address Suppression
Content Filter	Relay Control	IP Screening
Spam Blocker	Trusted IPs	Host Screening
Spam Filter	Tarpitting	IP Shielding
SSL	Reverse Lookups	AUTH
TLS	Trusted Domains	POP Before SMTP

While all of these security options address both general and specific issues, none directly handle the problem of email address spoofing,

That is where the Sender Policy Framework applies.

The Fundamentals of SPF

The Sender Policy Framework detects spoofed addresses in email. It does this by checking the validity of sender addresses in message envelopes. If an envelope contains a spoofed sender address, the message can be rejected. This saves processing time and bandwidth because the server does not download the message. However, even if an address is spoofed, its message can optionally be downloaded for additional processing, and, perhaps, delivery.



The email server pauses processing of a message while SPF validates the sender address against authorized email servers for a domain. Wide adoption of SPF will help reduce the amount of spam, viruses and email scams by stopping email address spoofing.

The concepts behind SPF originated in the late 1990's. SPF is a simplified spinoff of the RMX proposal by Hadmut Danisch. RMX traces its origins to Paul Vixie's *Repudiating Mail-From* paper. Vixie's paper was the result of a suggestion by Jim Miller in 1998.

SPF Records

The information in this section highlights the concepts of the SPF record. To gain a full understanding see the SPF RFC at: http://spf.pobox.com/rfcs.html

SPF uses special DNS records. These records identify authorized SMTP servers for each domain. They can also specify other domains used by local email account holders.

An SPF record consists of the SPF version number followed by statements comprised of mechanisms, prefixes and modifiers. This is the generic format:

```
version ([prefix] mechanisms) (modifiers)
```

An example entry may look like this:

```
"v=spf1 +a +mx +ptr include: exampleisp.net exp=spf-err ~all"
```

In the example:

`v=spf1`	is the version number. There is one of these.
`a, mx, ptr and include`	are mechanisms. There can be one or more mechanisms
`+ and ~`	are prefixes. Prefixes precede mechanisms—if none are specified + is implied.
`exp`	is a modifier. There can be zero, one or two modifiers.

Version Number

An SPF record always begins with a version number, such as

```
v=spf1
```

Subsequent versions could be:

```
v=spf2
v=spf3
```

The version designates the level of SPF supported by the record.

Mechanisms

Mechanisms identify the IP addresses authorized to send email from a domain. Two *basic* mechanisms—`all` and `include`—generally relate to broad categories of IPs, both internal and external to a domain. The remaining mechanisms—such as `ip4`, `a` and `mx`—authorize the IP addresses of designated senders. The mechanisms specify:

`all`	all IPs, both local and remote.
`include`	external domains used by local mail senders, typically when they are traveling.
`a`	all IPs in the DNS A record.
`mx`	all A records for each MX record host.
`ptr`	all A records for the PTR record hosts.
`ip4`	one or more specified domains using IPv4 Ips.
`exists`	one or more specified domains normally singled out as exceptions to the SPF definitions.

Prefixes

While mechanisms identify the IP addresses, prefixes designate whether or not the IP addresses pass or fail the lookup tests.

A frequently used application of the prefix is the `all` mechanism. When `-all` appears in an SPF record, it means no IP's pass the test[1].

[1] Practically speaking, `-all` means no more IPs pass the test. SPF clients, such as MDaemon, read and process the elements of SPF records from left to right. The SPF standards recommend ending most SPF records with `-all`. This stops the processing of the SPF record because no more IPs need to be checked.

The prefixes designate whether or not an IP address passes the lookup tests. For example:

+	the address passed the test. Example: `+all`
-	the address failed the test. Example: `-all`
~	the address failed the test but the result is not definitive. Example: `~all`
?	the address did not pass or fail the test. Example: `?all`

The + prefix is the default for all mechanisms. For example, `all` is the same as `+all`.

Modifiers

Modifiers provide additional information. They also can branch the SPF processing.

SPF has two current modifiers:

`redirect`	sends the SPF inquiry to another domain. Example: `redirect=example.net`
`exp`	set s up an explanation in the SPF record. Example: `exp=spf-error`

SPF Record Examples

Here are some simple examples of possible SPF records.

`"v=spf1 -all"`	Specifies no addresses pass the test
`"v=spf1 +all"`	Specifies all addresses pass the test.
`"v=spf1 a -all"`	Specifies addresses listed in the DNS A record pass the test.
`"v=spf1 a mx -all"`	Specifies addresses listed in the DNS A record and MX A record pass the test.
`"v=spf1 a mx ptr -all"`	Specifies addresses listed in the DNS, MX and PTR A records pass the test.
`"v=spf1 ip4:192.168.0.1/16 -all"`	Specifies a single IP or a range of IP addresses pass the test.

To view an SPF record, use the `nslookup` command from a terminal window. For example, to see the Alt-N SPF record type `nslookup -type=txt altn.com` and press **Enter**:

```
$ nslookup -type=txt altn.com
Server: 204.127.202.4
Address: 204.127.202.4# 53
altn.com text = "v=spf1 a mx a:lists.altn.com mx:helpdesk.altn.com
ip4:65.240.66.100/30 ip4: 65.240.66.104/29 ip4:65.240.66.112/28
ip4:65.240.66.128/28 ip4:65.240.66.144/30 ip4:65.240.66.148/31
ip4:65.240.66.150 exp=spf-err.% {d}?all"
```

Voluntary Deployment

Recording SPF information in DNS records is new and voluntary for email senders. Numerous large organizations including Amazon, AOL, Earthlink, Google and Symantec use SPF. SPF is the most widely-deployed of several methods of validating message senders. The more domains using SPF, the better it works.

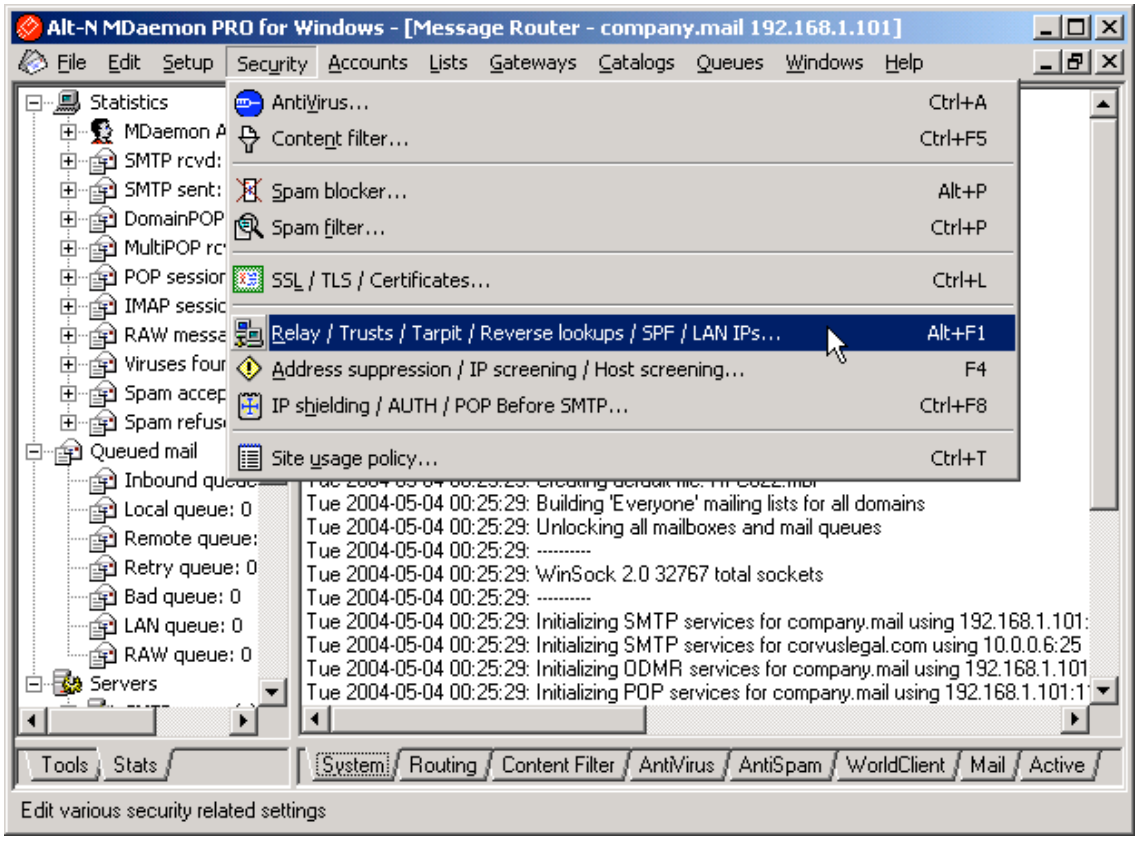
SPF Implementation in MDaemon

SPF Client

Beginning with Version 7.1, MDaemon can serve as an SPF client. This means it can check SPF information. Depending on the SPF lookup result, MDaemon can reject a message, saving bandwidth and disk space. It can also pass the message to the content filter or spam filter, for example, for further analysis. SPF results can also set spam probability values for each message.

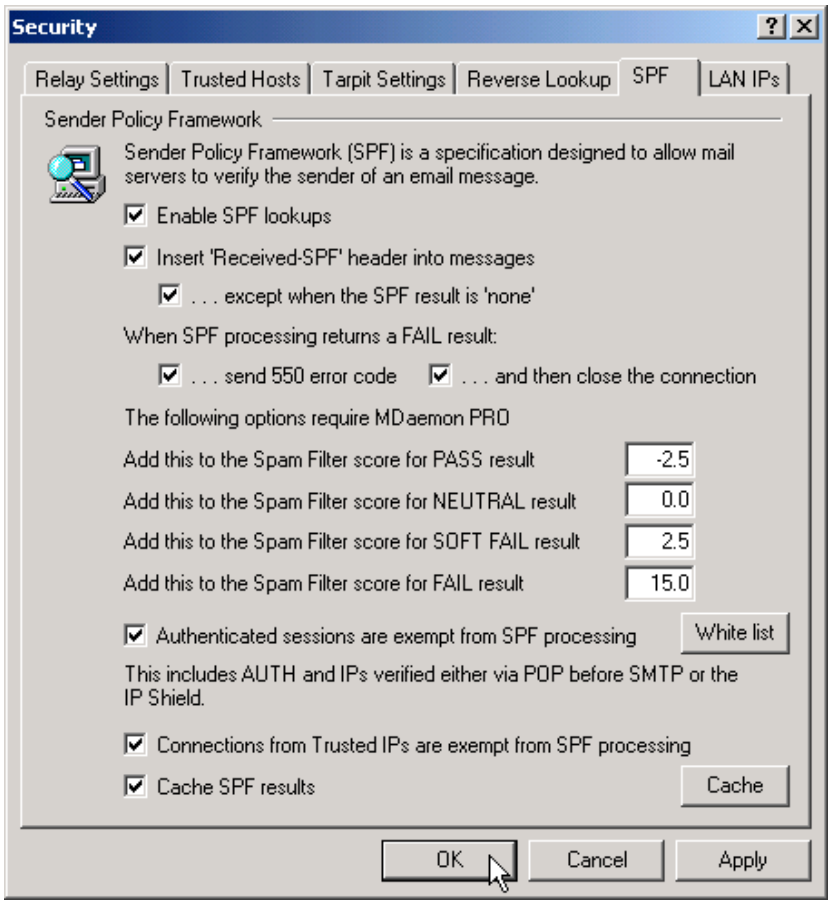
SPF Command

You access the SPF options through the **Security > Relay / Trusts...** command.



SPF Options

The options for SPF are on the **SPF** tab of the Security dialog.



The options on this dialog are:

Enable SPF Lookups
Activate this to enable MDaemon to check SPF records.

Insert 'Received-SPF' header into messages
Activate this to insert SPF headers into the incoming messages. The headers describe the results of SPF lookups.

For example, this is a header for a message from a domain without an SPF record:

```
Received-SPF: none (smtp.altn.com: me@asample.com does not
      designate permitted sender hosts)
      x-spf-client=MDaemon.PRO.v7.1.0.R
      receiver=smtp.altn.com
      client-ip=192.168.1.101
      envelope-from=<me@asample.com>
      helo= whoami.asample.com
```

This header is from a message from a domain with an SPF record:

```
Received-SPF: pass (example.mail: domain of robin@altn.com
      designates 65.240.66.16 as permitted sender)
      x-spf-client=MDaemon.PRO.v7.1.0.R
      receiver=example.net
      client-ip=65.240.66.16
      envelope-from=<robin@altn.com>
      helo=smtp.altn.com
```

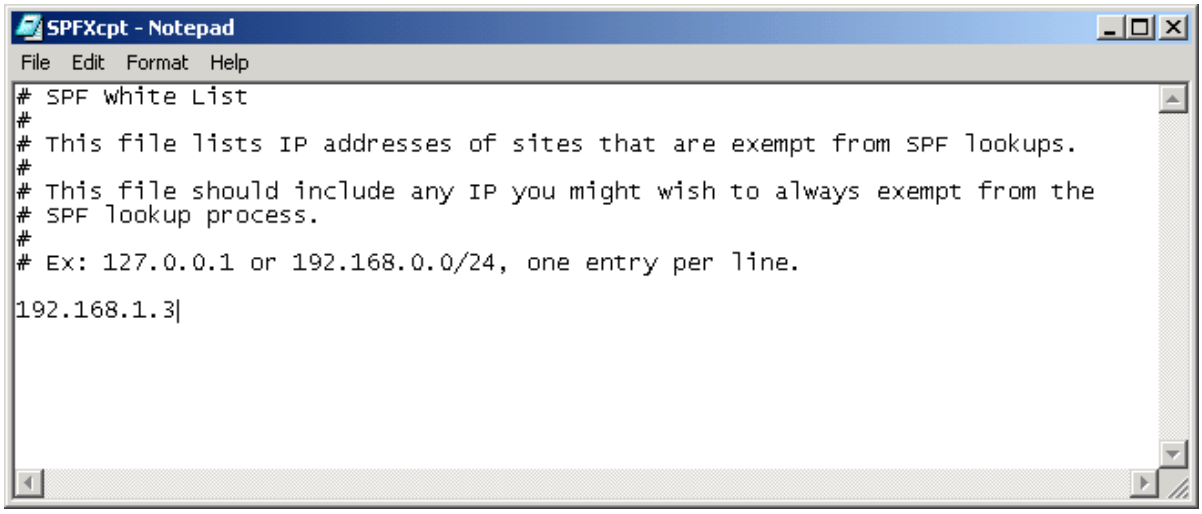
Activating ...**except when the SPF result is 'none'** keeps MDaemon from adding the header to messages from domains without SPF records.

When SPF processing returns a FAIL result:
Activate **send 550 error code** to return a 'no such account' response to the sender. Activate **and then close the connection** to terminate the session. This blocks the message from ever entering your server.

Add this to the Spam Filter score...
These options set the amount of Spam Filter score to add and subtract, depending on the SPF results.

Authenticated sessions are exempt from SPF processing
Activate this to skip SPF processing for messages from authenticated sessions.

White List
Select this command to open an editing window for entering white list IP addresses. These are exempt from SPF processing.

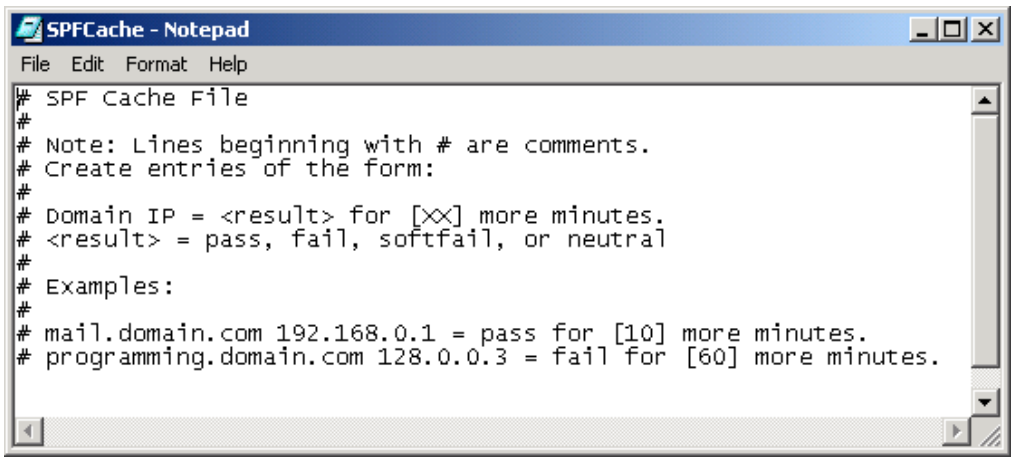


Connections from Trusted IPs are exempt from SPF processing
Activate this to skip SPF processing for messages from trusted IPs.

Cache SPF results
Activate this to keep the results of SPF processing for a specified amount of time.

Cache

Select this command to open an editing window for the SPF cache information.

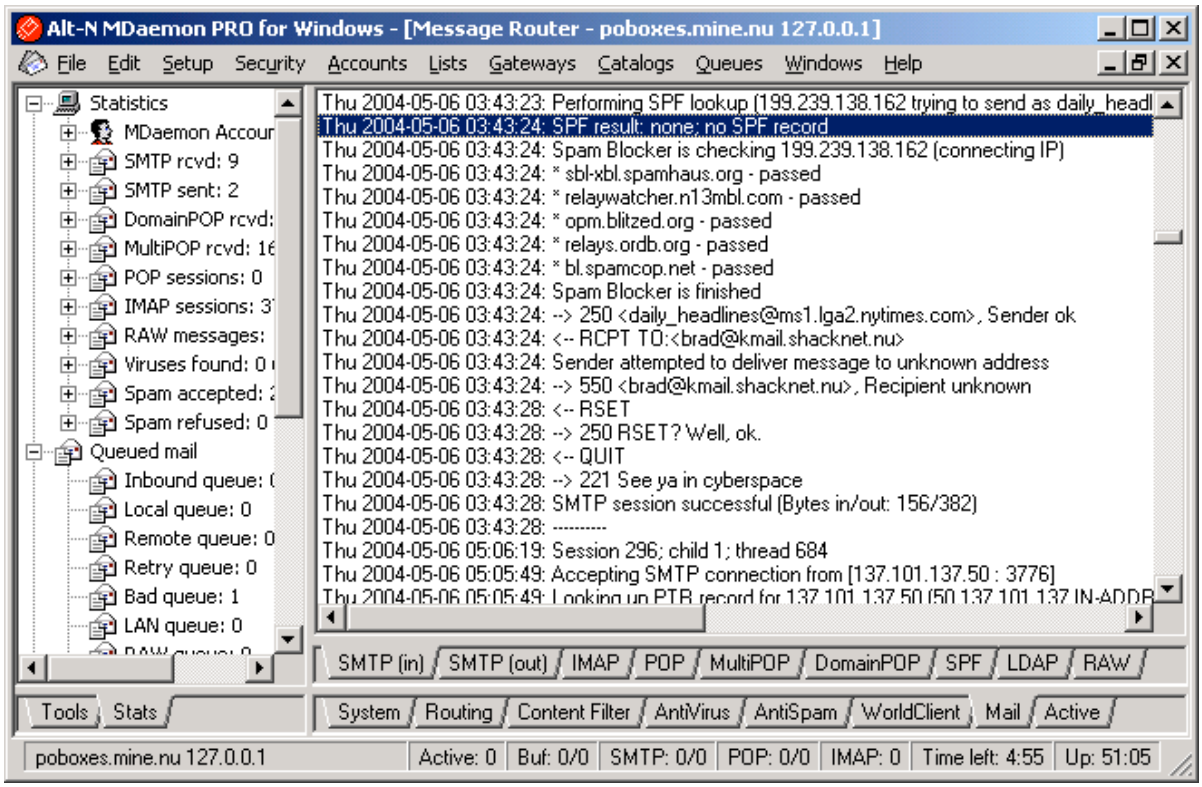


SPF Tracking

You can track SPF activity through the **SMTP (In)** tab, the **SPF** tab and the `MDaemon-SPF.log` file.

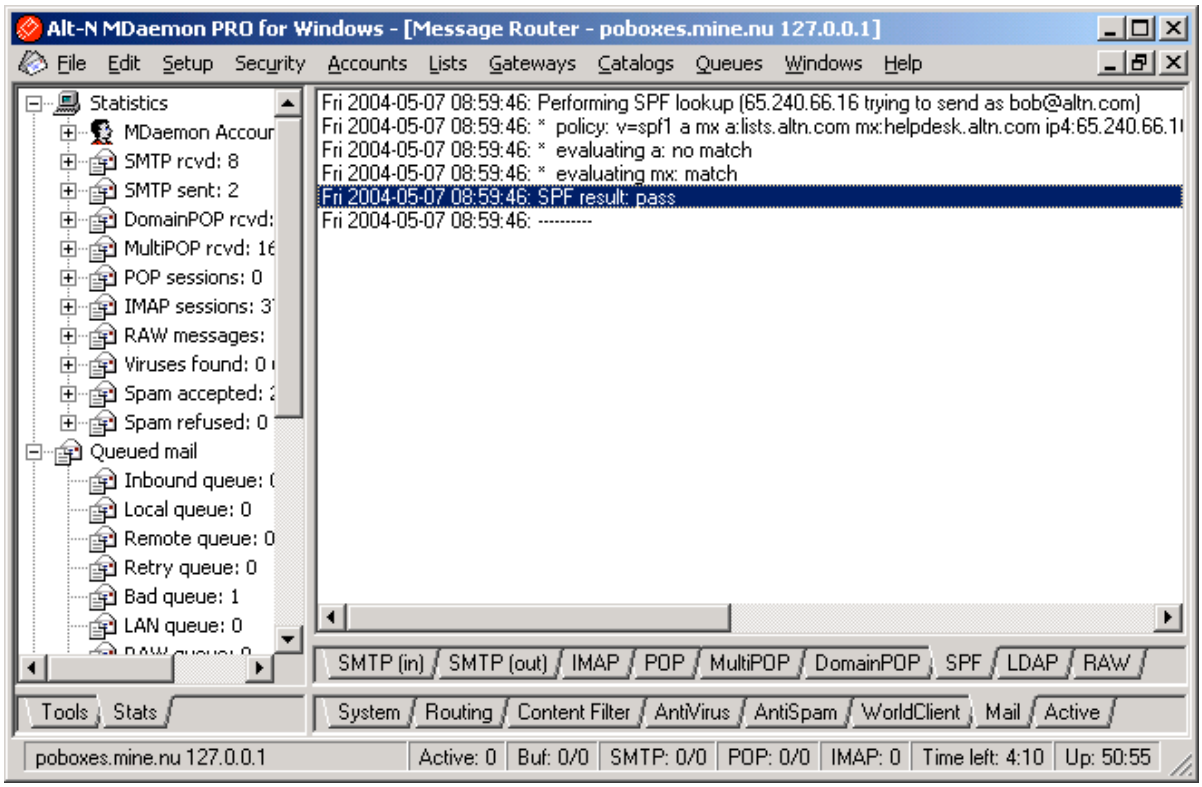
SMTP (In) Tab

On the **SMTP (In)** tab, MDaemon shows the results of SPF activity.



SPF Tab

The **SPF** tab shows details of SPF lookups:



MDaemon-SPF.log File

MDaemon keeps a record of SPF activity in the `MDaemon-SPF.log` file:

```
START Event Log / MDaemon PRO v7.1.0rc1 R, SPF log information

--------------------------------------------------------------------------------

Event Time/Date             Event Description

--------------------------------------------------------------------------------

Fri 2004-05-07 08:59:46: Performing SPF lookup (65.240.66.16 trying to send as
bob@altn.com)

Fri 2004-05-07 08:59:46: *  policy: v=spf1 a mx a:lists.altn.com mx:helpdesk.altn.com
ip4:65.240.66.100/30 ip4:65.240.66.104/29 ip4:65.240.66.112/28 ip4:65.240.66.128/28
ip4:65.240.66.144/30 ip4:65.240.66.148/31 ip4:65.240.66.150 exp=spf-err.\%\{d\} ?all

Fri 2004-05-07 08:59:46: *  evaluating a: no match

Fri 2004-05-07 08:59:46: *  evaluating mx: match

Fri 2004-05-07 08:59:46: SPF result: pass

Fri 2004-05-07 08:59:46: ----------
```

Setting Up SPF Records

Information from the SPF Web Site

For details about setting up your SPF record, visit the SPF web site at: http://spf.pobox.com/

The RFC is at: http://spf.pobox.com/rfcs.html

There is also an online wizard for helping define your SPF record at: http://spf.pobox.com/wizard.html

What You Need to Know

To setup SPF records you need to know the contents of your DNS record, the public IP addresses of all additional machines authorized to send mail and the domain names of any ISPs your traveling account holders can use while on the road.

Specifically you need to know if your domain sends email from:

- addresses listed in your DNS A record.
- addresses listed in the A record of your DNS MX entry.
- addresses listed in the A record of your DNS PTR entry.
- other machines, including personal computers running SMTP servers.
- addresses of any ISPs.

A Sample Session with the Wizard

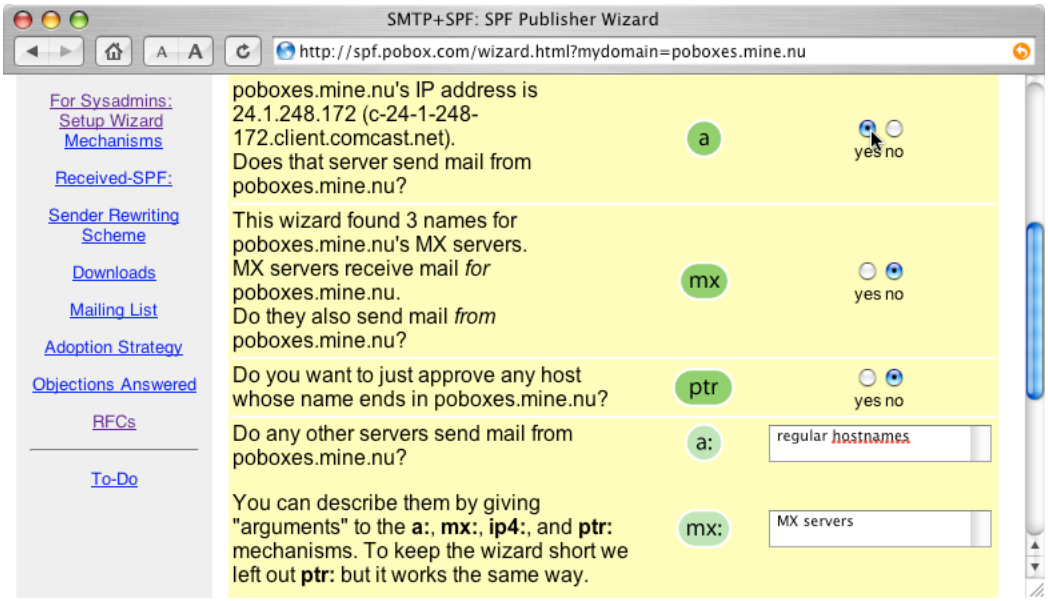
This is a brief and simple example showing how to use the SPF record wizard at: http://spf.pobox.com/wizard.html

The wizard is helpful for getting started. In many cases it can create the entire contents of your SPF record.

1. Go to **http://spf.pobox.com/wizard.html**

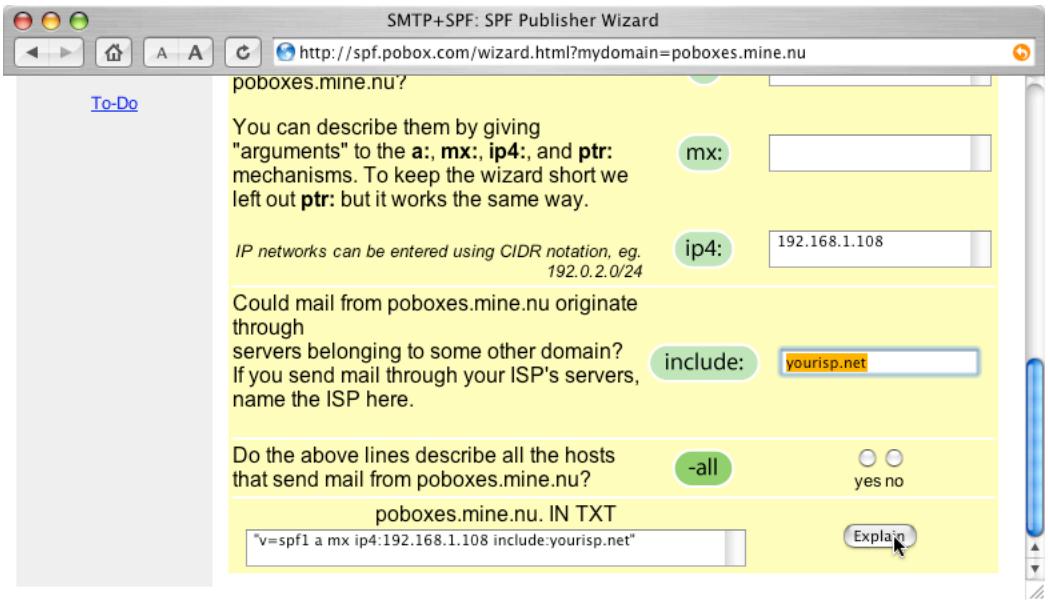
2. Enter your *domain name* and use the **Begin** button.

   The wizard responds with information about your domain.

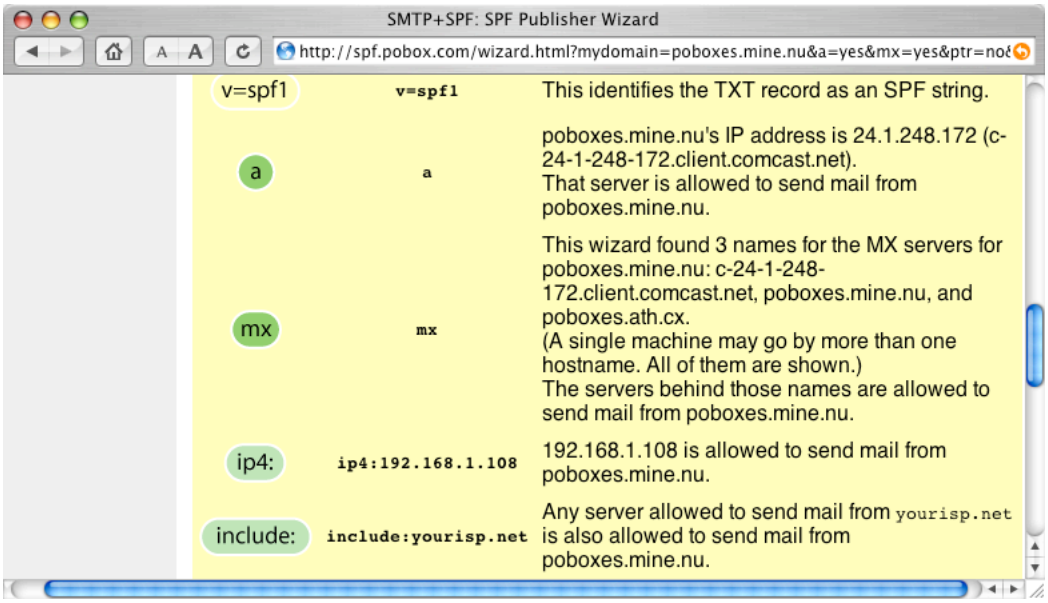


3. Scroll down through the wizard and enter the requested information. It asks about such things as your DNS `a` and `mx` records.

   As you enter the information the wizard creates the contents of an SPF record. You can edit the information.



4. Use the **Explain** button to see details about your record.



5. You can use the resulting string as the contents of your SPF record. The wizard gives you guidelines for doing that with some DNS servers.