

IMSV 9.0/9.1 Sender Policy Framework

Best Practice Guide

1. Introduction

SPF (Sender Policy Framework) is an open standard which provides solutions to resist sender address forgery. Organizations who want to adopt SPF are required to publish DNS records for the hosts that are used in "MAIL FROM" and "HELO" identities so that recipients can identify whether a host is authorized to send email messages for the domain by querying these records. The complete specifications of SPF are documented in RFC 4408. For a simple introduction, visit <http://www.openspf.org/Introduction>.

This document guides you on how to integrate SPF checking for IMSV 9.0/9.1. This solution makes use of the Postfix SMTP access policy delegation mechanism. A script will be used to do SPF checking and report specific actions to Postfix. Postfix then takes the appropriate action. For further details, visit http://www.postfix.org/SMTPD_POLICY_README.html.

2. Configuration

The file *config.ini*, /opt/trend/imss/postfix/etc/postfix/SPFPolicyd/, is the main configuration file. The format for the file is as follows:

```
# Comments...  
[section1]  
Key1 = value1  
  
[section2]  
Key2 = value1, value2
```

To modify this configuration file, you should SSH to IMSV with root credential first. Please always backup the file before making any modification to it

```
#cp /opt/trend/imss/postfix/etc/postfix/SPFPolicyd/config.ini config.ini.default
```

2.1. Basic Configuration

Add your internal mail server's IPs to `white_ip`, or just add all private IP ranges. Separate multiple items with comma. Below is an example to exclude all private IP ranges:

```
# White list of IP and domains, client from these IPs and domains will not do SPF check and the mail will be bypassed.  
white_ip=127.0.0.1,10.0.0.0/8,172.16.0.0/16,192.168.0.0/16
```

In case certain domain is trusted but experiencing SPF problem, you may add the domain to `white_domain` like below:

```
# White list of IP and domains, client from these IPs and domains will not do SPF check and the mail will be bypassed.  
white_ip=127.0.0.1, 10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16  
white_domain= sample1.com, sample2.com
```

2.2. Using SPF with Cloud Pre-Filter

If you are using Cloud Pre-Filter, a little more configuration is needed. Cloud Pre-Filter actually works as a proxy, so messages passed from Cloud Pre-Filter may not pass an SPF check. You have to add the IP addresses of Cloud Pre-Filter to the approved list. If you enabled Cloud Pre-Filter, open the file `"/opt/trend/imss/postfix/etc/postfix/NRSAllowAccessList"`, and add the IP addresses in this file to `"white_ip"`, so messages from Cloud Pre-Filter will not be subjected to an SPF check. There may be many IP addresses for Cloud Pre-Filter, so you can make use of the subnet format (`<IP address>/<subnet mask length>`) to save time.

2.3. Configure Domain-Specific Actions

Sometimes you may want to apply specific actions to some domains. For example, the domain `example.com` has a published SPF record and never sends messages using hosts not in the SPF record. So you want to block messages if they do not come from the hosts in the SPF record. You can add a section in `config.ini` to block those messages.

```
[<domain>.com]  
none=block
```

Now if the SPF query result is none, the message will be blocked. Actions for other query results are kept the same as the global actions. You can also override actions for other query results if needed.

Wildcards are supported. For example, you can use `"*.example.com"` to define actions for `example.com` and all its sub-domains. The SPF check automatically searches for the best matched

domains. If the sender is “postmaster@example.com”, the SPF check will first look for “[example.com]”, if this section does not exist, it will look for “[*.example.com]” next. The priority of this section is lower than approved list and enforcement list.

Refer to **Appendix I** for all the configuration items in config.ini.

3. Enable/Disable

● To Enable SPF

1. Modify your Postfix settings to inject SPF checking to the Postfix email message flow.
 - 1). SSH to IMSVA with root credential.
 - 2). Backup `/opt/trend/imss/postfix/etc/postfix/master.cf` and then modify it with VIM command:

```
#cp /opt/trend/imss/postfix/etc/postfix/master.cf master.cf.b4spf  
#vi /opt/trend/imss/postfix/etc/postfix/master.cf
```

Remove the comments for the following so that the SPF script will be launched by Postfix when needed.

```
SPFPolicyd    unix    -      n      n      -      0      spawn  
              user=imss  argv=/opt/trend/imss/postfix/etc/postfix/SPFPolicyd/SPFPolicyd.py
```

- 3.) Backup `/opt/trend/imss/postfix/etc/postfix/main.cf` and then modify it with VIM command:

```
#cp /opt/trend/imss/postfix/etc/postfix/master.cf main.cf.b4spf  
#vi /opt/trend/imss/postfix/etc/postfix/main.cf
```

Locate `smtpd_sender_restrictions` key, which looks like below:

```
smtpd_sender_restrictions =  
check_policy_service inet:127.0.0.1:999
```

Change it as below:

```
smtpd_sender_restrictions =  
check_policy_service inet:127.0.0.1:999, check_policy_service unix:private/SPFPolicyd
```

Locate `SPFPolicyd_time_limit` key, remove the comment before it like below:

```
SPFPolicyd_time_limit = 3600
```

Save the changes.

- Restart the Postfix service. To make all the modifications take effect, using the following command:

```
# postfix restart
```

The logs of the SPF check script are written to `/var/log/maillog`, with a leading “SPFPolicyd” in front of each line in the log.

To verify that SPF checking works, send an email message that can pass an IMSVA scan. If the message contains “Received-SPF” in the header, the SPF check script is working correctly.

● To Disable SPF

To disable SPF checking, rollback all the above changes, then restart the Postfix service.

Appendix I

The table below describes detailed uses of all keys in `config.ini`. We recommend to keep them with default values, except for the items discussed in other sections of this document.

NOTE: Possible values are separated by pipes “|”. Underlined values are default values. For parameters that can have multiple values, use a comma or space to separate them. For example: example.com, example2.com.

Section	Parameter	Value	Description
globals	block_res	<text> <u>550 Service unavailable; SPF check unsuccessful and transaction closed due to the organization's policy.</u>	The SMTP response code if email messages are blocked. Both the response code “550” and message can be customized. The response code can be any valid 3 digits starting with 5. Do not forget the blank space between the response

			code and the message.
	check_helo	<u>yes</u> no	Specifies if the HELO/EHLO identity needs to do a SPF check. The HELO/EHLO identity will be checked if the MAILFROM identity is empty or invalid.
	enforce_domain	<comma or space separated list of domains>	Specifies an enforcement list of domains. Email messages from these domains will have actions applied to them defined in "enforce_actions" section. You can add domains that are frequently forged by spammers and apply stricter actions, to better protect your mail system.
	enforce_ip	<comma or space separated list of IPs>	Specifies an enforcement list of IP addresses. The usage is similar to "enforce_domain". Currently only IP v4 is supported. You can use a specific format <x.x.x.x> to exactly match an IP address or the subnet mask pattern <x.x.x.x>/<subnet mask length> to match a series of IP addresses.
	log_level	0 <u>1</u> 2 3 4	Defines the log level. There are 5 log levels. 0: no log > no log will be generated. 1: normal > provides basic information for administration and maintenance. 2: detailed > detailed information, including original SPF check results. 3: diagnostic > all information of level 1 and 2 logs, plus configurations in use. 4: debug > most detailed, only recommended when trouble shooting.
	pass	<u>bypass</u> tempblock block	SPF queries can return 7 kinds of results: pass, neutral, softfail, fail, none, temperror and permerror. The parameters with the same names define the corresponding actions. The available actions are:

			<p>bypass, tempblock and block.</p> <p>Bypass: means the SPF check is not performed</p> <p>Tempblock: returns a 4XX SMTP response to temporarily block the mail.</p> <p>Block: returns a 5XX response to block the mail.</p> <p>Pass: means the host is allowed to send messages for this domain.</p>
	neutral	<u>bypass</u> tempblock block	Neutral means the validity of this host is not specified.
	softfail	bypass <u>tempblock</u> block	Softfail means the host is not allowed to send messages but is in transition.
	fail	bypass tempblock <u>block</u>	Fail means the host is not allowed to send messages.
	none	<u>bypass</u> tempblock block	None means the domain does not have an SPF record or the SPF record does not have a result.
	temperror	<u>bypass</u> tempblock block	Temperror means a temporary error has occurred. For example: network connections lost.
	permerror	<u>bypass</u> tempblock block	Permerror means a permanent error has occurred For example: SPF record invalid format.
	prepend_header	<u>yes</u> no	<p>Specify whether to insert a "Received-SPF" header in your messages.</p> <p>Trend Micro recommends adding this header for further administration or analysis of messages.</p>
	tempblock_res	<text> <u>451 Service temporarily unavailable; SPF check unsuccessful and transaction closed due to the organization's policy.</u>	The SMTP response code if temporarily blocking the messages. Both the response code "451" and message can be customized. The response code can be any valid 3 digits starting with 4. Do forget the blank space between the response code and message.
	white_domain	<comma or space separated list of	Specify an approved list of domains. Messages from these domains will

		domains>	bypass the SPF check. You can add trusted domains to this list.
	white_ip	<comma or space separated list of IPs> <u>127.0.0.1</u>	Specify an approved list of domains. Messages from these addresses will bypass the SPF check. You can add trusted domains to this list.
enforce_actions	pass	<u>bypass</u> tempblock block	Parameters under the “enforce_actions” section define the actions for domains and IP addresses in the enforcement list. Follows the same behavior as global actions.
	neutral	<u>bypass</u> tempblock block	Same as above.
	softfail	bypass <u>tempblock</u> block	Same as above.
	fail	bypass tempblock <u>block</u>	Same as above.
	none	<u>bypass</u> tempblock block	Same as above.
	temperror	bypass <u>tempblock</u> block	Same as above.
	permerror	bypass <u>tempblock</u> block	Same as above.