Guide
Cisco public

Cisco Email Security How-to Guide
How to Enable Spoof Protection

'Spoofed' emails are messages that have been altered by a sender to appear as if another party is sending them. An organization may permit email spoofing by third parties such as healthcare providers, marketing firms, and travel agencies, which send email to certain users on behalf of that organization. But malicious spam distributors or other unauthorized parties can use spoofing to dupe recipients into opening an email solicitation and then taking some action. Often, recipients are told to click a link that sends them to a malware-laden site and asks for banking or credit card information.

This guide shows you how to enable spoof protection with Cisco® Email Security to help you prevent unauthorized parties from spoofing your email.

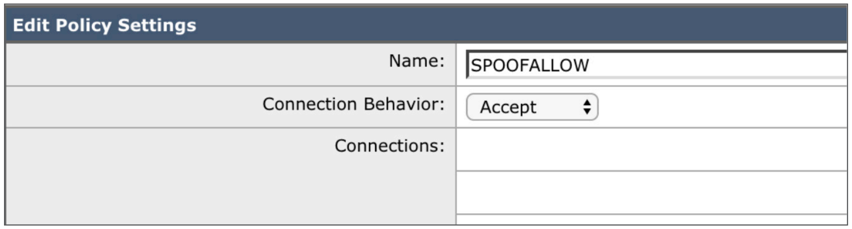
© 2018 Cisco and/or its affiliates. All rights reserved.

Contents

Step 1: Configure a new ‘Mail Flow Policy’

Create a new ‘Mail Flow Policy’ using a relevant name such as **SPOOFALLOW**, and choose **Accept** as the connection behavior.

Figure 1. ‘Mail Flow Policy’ settings

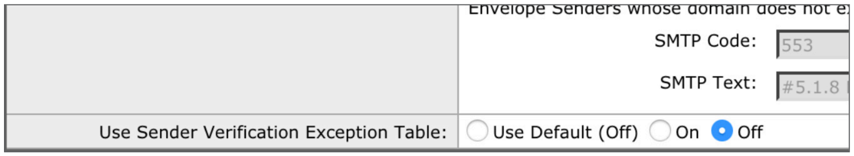


Edit Policy Settings

Name:	SPOOFALLOW
Connection Behavior:	Accept
Connections:	

At the very end of the **‘Sender Verification’** section, in the **‘Use Sender Verification Exception Table’**, change the default to **Off**. Submit the change.

Figure 2. ‘Sender Verification Exception Table’ setting



Envelope Senders whose domain does not e

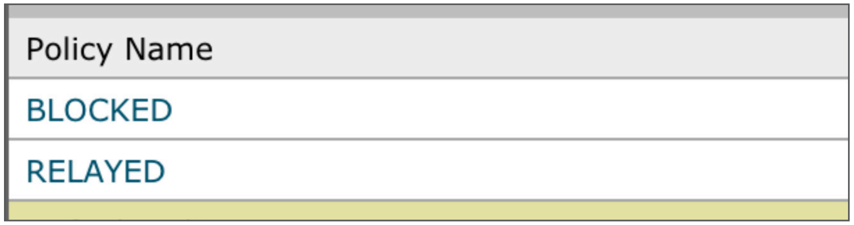
SMTP Code: 553

SMTP Text: #5.1.8

Use Sender Verification Exception Table: ○ Use Default (Off) ○ On ● Off

Edit the **RELAYED** ‘Mail Flow Policy’. Look for **‘Use Sender Verification Exception Table’** and change the default to **Off** as well.

Figure 3. Relayed ‘Mail Flow Policy’

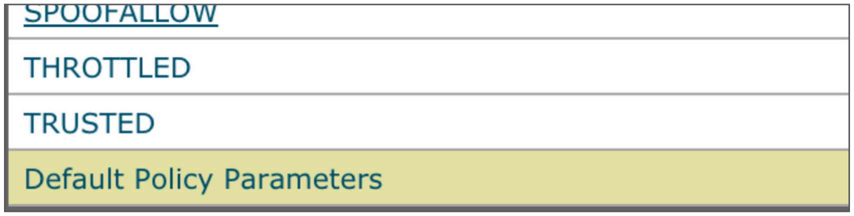


Policy Name
BLOCKED
RELAYED

Next, navigate to the **‘Default Policy Parameters’** in ‘Mail Flow Policies’ page.

© 2018 Cisco and/or its affiliates. All rights reserved.

Figure 4. Default Policy Parameters



SPOOFALLOW

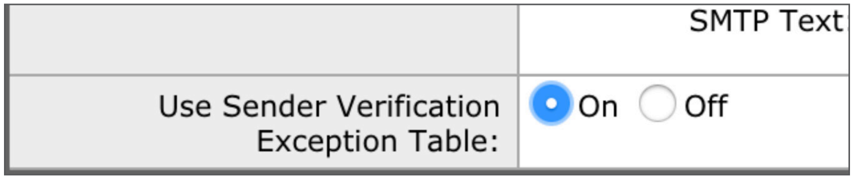
THROTTLED

TRUSTED

Default Policy Parameters

Set **‘Use Sender Verification Exception Table’** as **On**.

Figure 5. Sender verification exception table setting

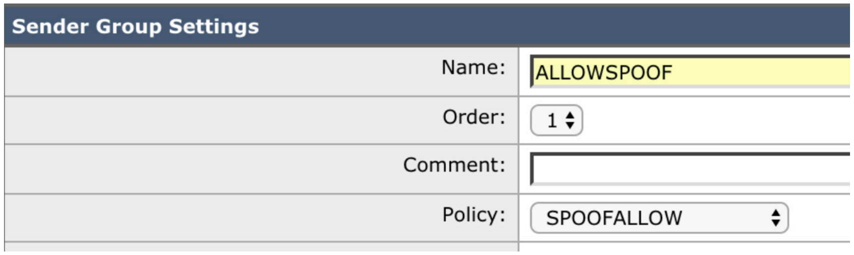


	SMTP Text
Use Sender Verification Exception Table:	● On ○ Off

Step 2: Configure the ‘Host Access Table’ (HAT)

Create a new ‘Sender Group’ named **ALLOWSPOOF**. Choose 1 as the order to place it above whitelists and blacklists. Then assign the **SPOOFALLOW** ‘Mail Flow Policy’ to this ‘Sender Group’.

Figure 6. ‘Sender Group’ setting



Sender Group Settings

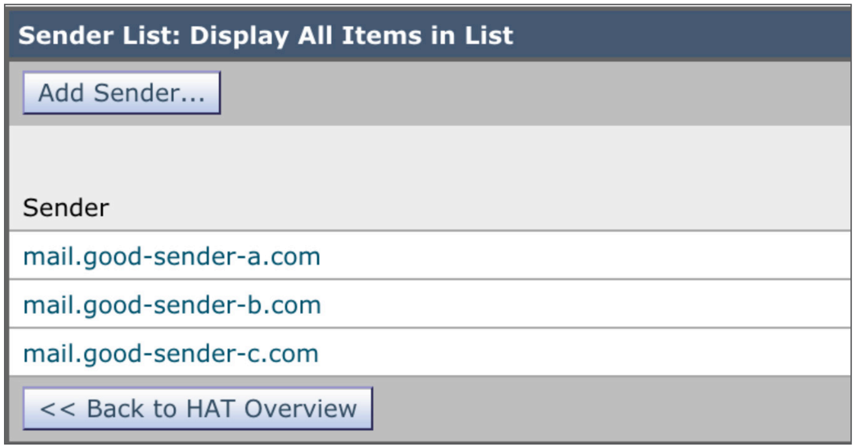
Name:	ALLOWSPOOF
Order:	1
Comment:	
Policy:	SPOOFALLOW

Add domains from external parties that you want to **allow** to spoof email to the internal domain. Note: These are the DNS domains of sending hosts, not their email domains.

© 2018 Cisco and/or its affiliates. All rights reserved.

Contents

Figure 7. ‘Sender Group’ setting



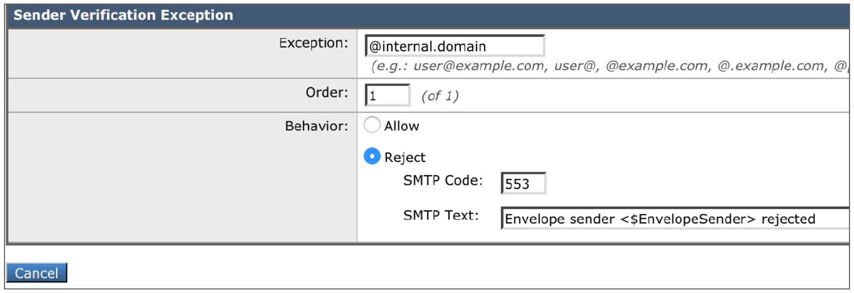
Sender List: Display All Items in List

Sender
mail.good-sender-a.com
mail.good-sender-b.com
mail.good-sender-c.com

Step 3: Configure the ‘Sender Verification Exception Table’

Add the local domain(s) to the **Exception** (as a comma-separated list), and set the behavior to **Reject**.

Figure 8. ‘Sender Verification Exception Table’ setting



Sender Verification Exception

Exception:	@internal.domain *(e.g.: user@example.com, user@, @example.com, @.example.com, @*
Order:	1 *(of 1)*
Behavior:	○ Allow ● Reject SMTP Code: 553 SMTP Text: Envelope sender <$EnvelopeSender> rejected

At this point, the configuration is finished. Click **‘Submit’** and then **‘Commit Changes’** to save the configuration.

Note: Mail coming from @internal.domain(s) to @internal.domain(s) will be rejected unless the sender is listed in the ‘Sender Group’ **ALLOWSPOOF**, because it is tied to a ‘Mail Flow Policy’ that does not use the ‘Sender Verification Exception Table’.

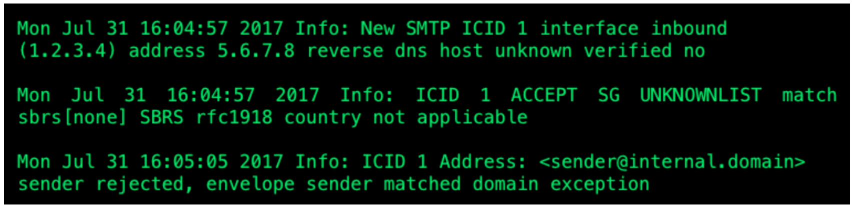
© 2018 Cisco and/or its affiliates. All rights reserved.

Contents

Sender Domain Verification in action

We are showing the event (ICID 1) recorded in mail_logs. The incoming message was delivered from a sending domain that is found to be identical to the internal domain. Hence email has been rejected as instructed in the ‘Sender Domain Verification Exception Table’ setting.

Figure 9. mail_logs



```
Mon Jul 31 16:04:57 2017 Info: New SMTP ICID 1 interface inbound
(1.2.3.4) address 5.6.7.8 reverse dns host unknown verified no

Mon  Jul  31  16:04:57  2017  Info:  ICID  1  ACCEPT  SG  UNKNOWNLIST  match
sbrs[none] SBRS rfc1918 country not applicable

Mon Jul 31 16:05:05 2017 Info: ICID 1 Address: <sender@internal.domain>
sender rejected, envelope sender matched domain exception
```

Conclusion

By taking a few simple steps to configure your ‘Mail- Flow Policy’, the ‘Host Access Table’, and the ‘Sender Verification Exception Table’, you can configure Cisco Email Security to empower trusted third parties to send authorized email on behalf of your organization, while closing a frequent avenue for spoofed emails by unauthorized actors.

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)