Detect Spoofed Email Messages on the ESA and Create Exceptions For Senders That Are Allowed to Spoof

Contents

Introduction

This document describes how to control email spoofing on the Cisco Email Security Appliance (ESA) and how to create exceptions for the users allowed to send spoofed emails.

Prerequisites

Requirements

Your ESA should be processing both incoming and outgoing mails, and should use a standard configuration of RELAYLIST to flag messages as outgoing.

Components Used

The information in this document is based on the ESA with any AsyncOS version. The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Specific components used include:

- Dictionary: used to store all your internal domains.

- Message Filter : used to handle the logic of detecting spoofed email and inserting a header that content filters can act on.
- Policy Quarantine: used to store duplicartes of spoofed emails temporarily. Consider adding the IP address of released messages to the MY_TRUSTED_SPOOF_HOSTS to prevent future messages from this sender from entering the policy quarantine.
- MY_TRUSTED_SPOOF_HOSTS: list for referencing your trusted sending IP addresses. Adding an IP address of a sender to this list will skip the quarantine and allow the sender to spoof. We are placing trusted senders in your MY_TRUSTED_SPOOF_HOSTS sender group so that spoofed messages from these senders are not quarantined.
- RELAYLIST: list for authenticating IP addresses that are allowed to relay, or send outbound email. If the email is being delivered via this sender group the assumption is that the message is not a spoofed message.

  Note: If either sender group is called something different than MY_TRUSTED_SPOOF_HOSTS or RELAYLIST, you will have to modify the filter with the corresponding sender group name. Also, if you have multiple listeners, you may also have more than one MY_TRUSTED_SPOOF_HOSTS.

Background Information

Spoofing is enabled by default on the Cisco ESA. There are several, valid reasons for allowing other domains to send on your behalf. One common example, ESA Administrator may want to controlling spoofed emails by quarantining spoofed messages before they are delivered.

To take a specific action such as quarantine on spoofed email, you must first detect spoofed email.

What is Email Spoofing?

Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source.

How to Detect Spoofed Email?

You will want to filter any messages that have an envelope sender (Mail-From) and "friendly from" (From) header that contain one of your own incoming domains in the email address.

How to allow Spoofing for Specific Senders?

When implementing the message filter provided with-in this article, spoofed messages are tagged with a header, and the content filter is used to take action on the header . To add an exception, simply add the sender IP to MY_TRUSTED_SPOOF_HOSTS.

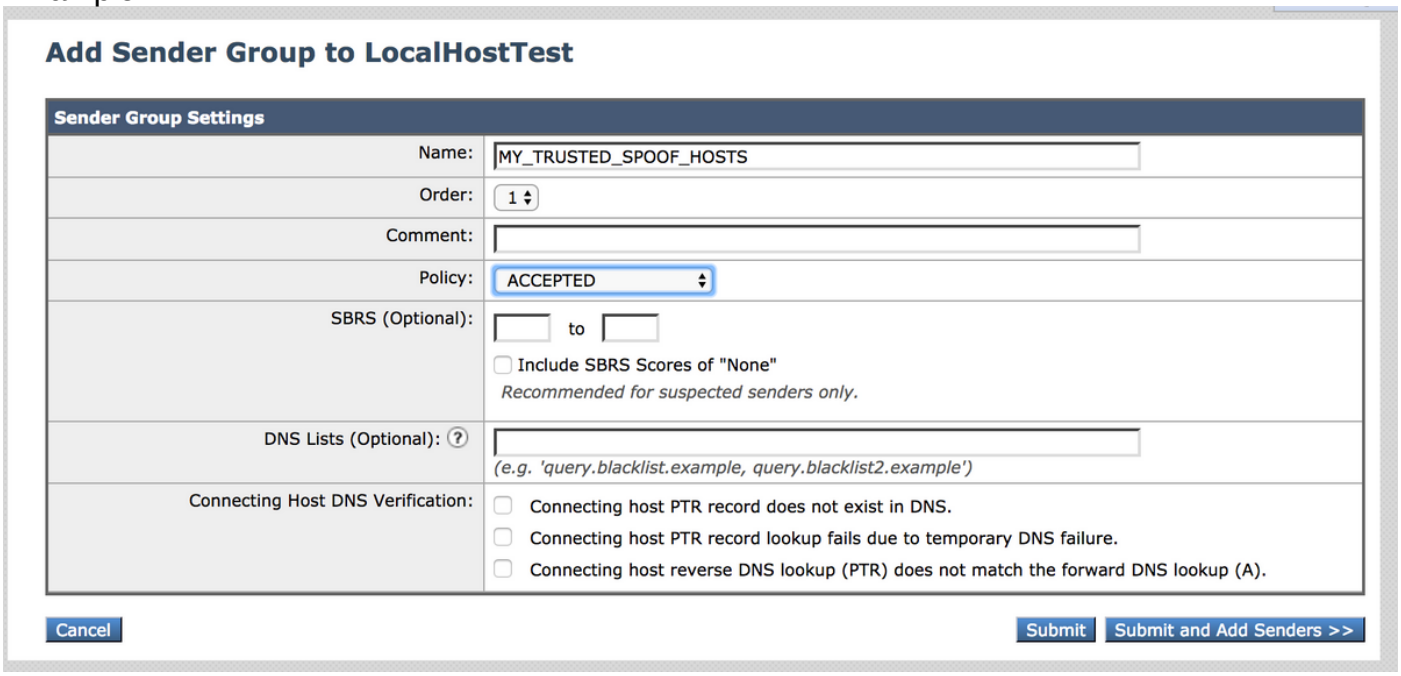
Configure

Create a Sendergroup

Create a dictionary for all domains which you want to disable spoofing for on the ESA:

1. From the ESA GUI, navigate to **Mail Policies > HAT Overview**
2. Click **Add.**
3. In the "Name" field specify **MY_TRUSTED_SPOOF_HOSTS**
4. In the "Order" field specify **1**
5. For "Policy" field, specify **ACCEPTED**
6. Click **Submit** to save changes.
7. Finally, click **Commit Changes** to save the configuration

Example:

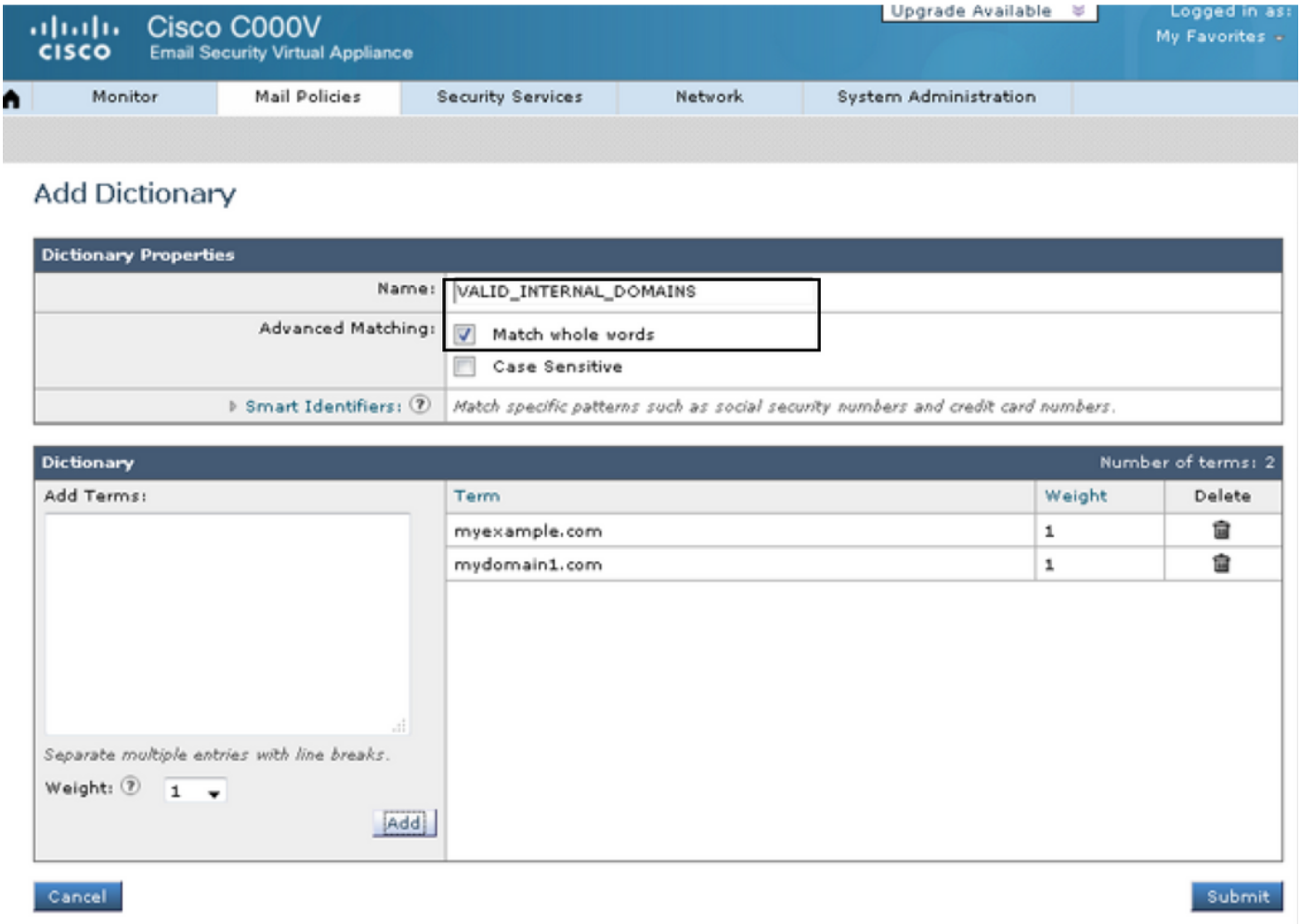


Create a Dictionary

Create a dictionary for all domains which you want to disable spoofing for on the ESA:

1. From the ESA GUI, navigate to **Mail Policies > Dictionaries.**
2. Click **Add Dictionary.**
3. In the "Name" field specify 'VALID_INTERNAL_DOMAINS', for example.
4. Under "add terms", add all domains which you want to detect spoofing.
5. Click **Submit** to save the dictionary changes.
6. Finally, click **Commit Changes** to save the configuration

Example:



Create a Message Filter

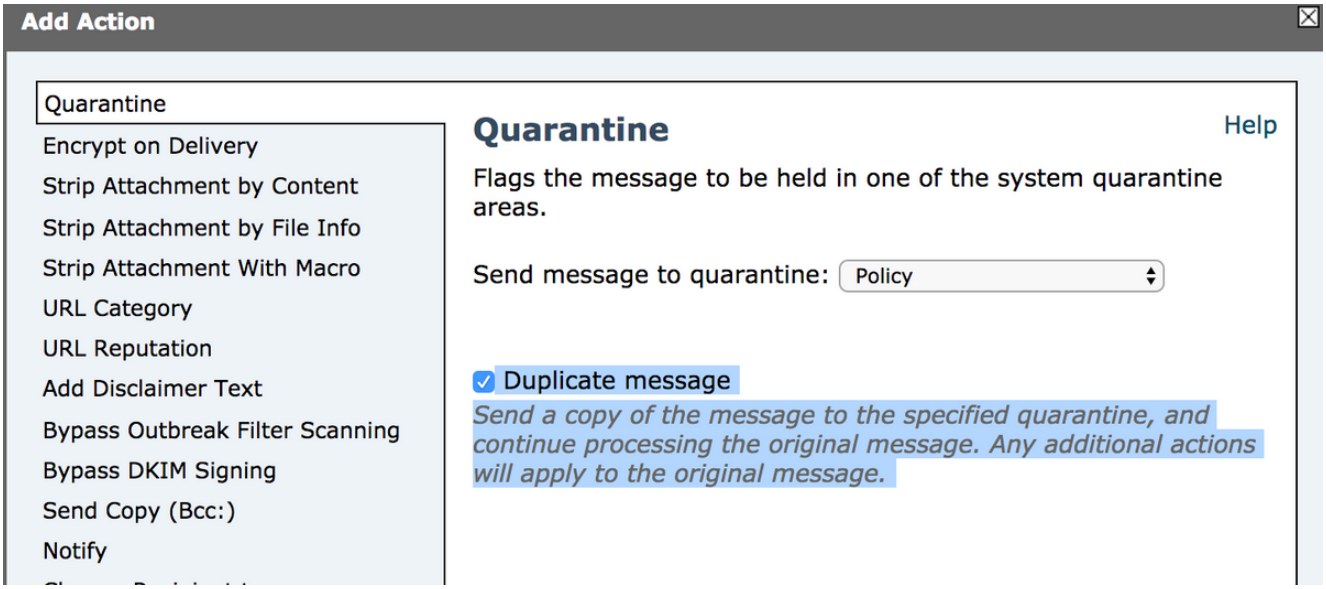
Next, you will need to create a message filter in order to leverage the dictionary just created, "VALID_INTERNAL_DOMAINS"**:**

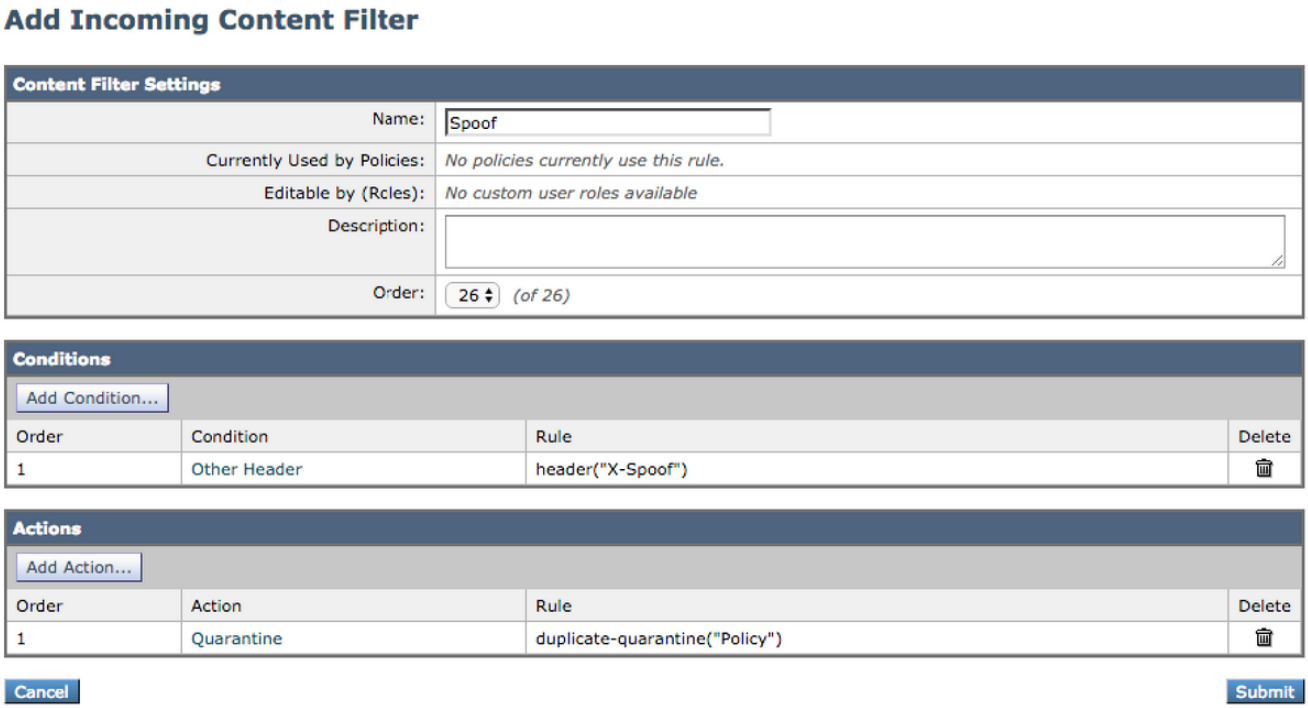
1. Connect to the Command Line Interface (CLI) of the ESA.
2. Run the command **Filters.**
3. Run the command **New** to create a new message filter.
4. Copy and paste the following filter example, making edits for your actual sender group names if needed:

```
mark_spoofed_messages:
if(
(mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
OR (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
AND ((sendergroup != "RELAYLIST")
AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
)
{
insert-header("X-Spoof", "");
}
```

5. Return to the main CLI prompt and run **Commit** to save the configuration.

6. Navigate to the GUI > Mail Policies > Incoming Content Filters
7. Create Incoming Content Filter that takes action on the spoof header X-Spoof: Add action: duplicate-quarantine("Policy").
   Note: The Duplicate message feature shown here will keep a copy of the message, and continue to send the original message to the recipient.





8. Link content filter to incoming mail policies at GUI > Mail Policies> Incoming Mail Policies
9. Submit and Commit Changes

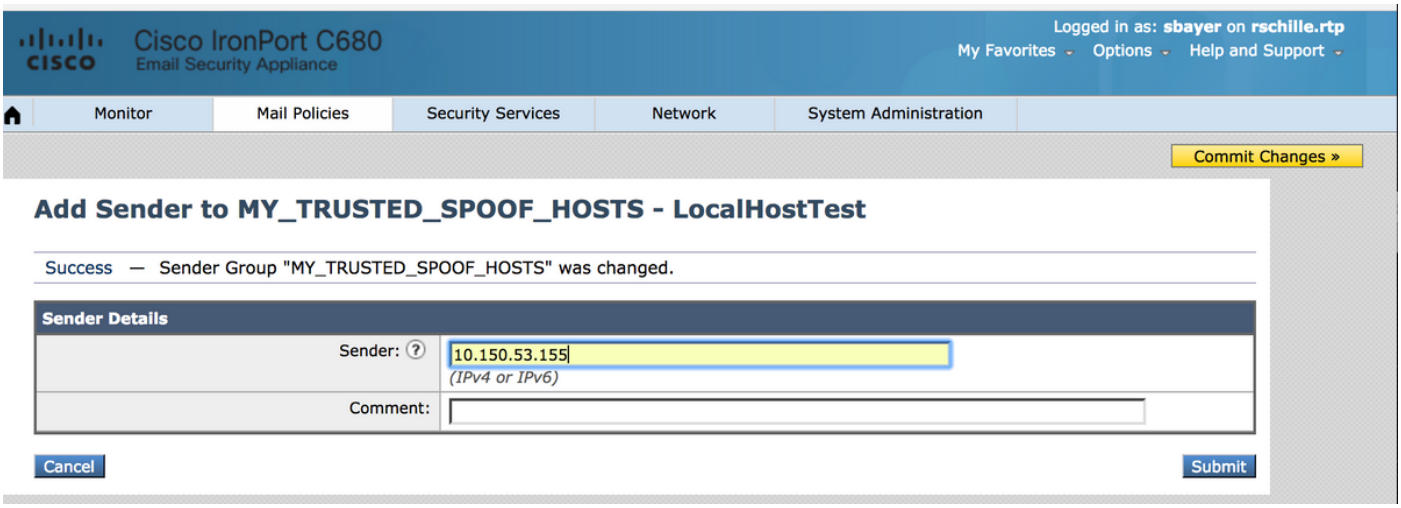
Add Spoof-Exceptions to MY_TRUSTED_SPOOF_HOSTS

Finally, you will need to add spoof-exceptions (IP addresses or hostnames) to the MY_TRUSTED_SPOOF_HOSTS sendergroup.

1. Navigate via the web GUI: **Mail Policies > HAT Overview**
2. Click and open the MY_TRUSTED_SPOOF_HOSTS sender group.

3. Click on "Add Sender..." to add an IP address, range, host name, or partial host name.
4. Click **Submit** to save the sender changes.
5. Finally, click **Commit Changes** to save the configuration.

Example:



Verify

Verify Spoofed Messages are being Quarantined

Send a test message specifying one of your domains as the envelope sender. Validate the filter is working as expected by performing a message track on that message. The expected result is that the message will get quarantined because we have not created any exceptions yet for those senders who are allowed to spoof.

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message
filter:quarantine_spoofed_messages)
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Verify Spoof-Exception Messages are being delivered

"Spoof-Exception" senders are IP addresses in your sender group(s) referenced in the filter above.

RELAYLIST is referenced because it is used by the ESA to send outbound mail. Messages being sent by RELAYLIST are typically outbound mail, and not including this would create false positives, or outbound messages being quarantined by the filter above.

Message tracking example of a "Spoof-Exception" IP address that was added to MY_TRUSTED_SPOOF_HOSTS. The expected action is deliver and not quarantine. (This IP is allowed to spoof).

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
```

```
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598 Message accepted
for delivery'
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

Related Information

- ESA Spoofed Mail Filtering
- Spoof Protection using Sender Verification