Contents

Introduction

By default the Cisco Email Security Appliance (ESA) does not prevent the inbound delivery of messages that are addressed “from” the same domain going to the same domain. This allows messages to be “spoofed” by outside companies that do legitimate business with the customer. Some companies rely on 3rd party organization to send email on behalf of the company such as Health Care, Travel Agencies, etc.

Spoof Protection using Sender Verification

Configure Mail Flow Policy (MFP)

1. From the GUI: **Mail Policies > Mail Flow Policies > Add Policy...**
2. Create a new MFP using a name that is relevant like SPOOF_ALLOW
3. In the *Sender Verification* section, change the *Use Sender Verification Exception Table* configuration from **Use Default** to **OFF**.
4. In **Mail Policies > Mail Flow Policies > Default Policy Parameters**, set *Use Sender Verification Exception Table* configuration to **On**.

Configure HAT

1. From the GUI: **Mail Policies > HAT Overview > Add Sender Group...**
2. Set the name accordingly to the MFP created earlier, i.e. SPOOF_ALLOW.
3. Set the order so it is above the WHITELIST and BLACKLIST sender groups.
4. Assign the **SPOOF_ALLOW** policy to this Sender Group settings.
5. Click **Submit and Add Senders...**
6. Add IP(s) or domains for any external parties that you want to allow to spoof the internal domain.

Configure Exception Table

1. From the GUI: **Mail Policies > Exception Table > Add Sender Verification Exception...**
2. Add the local domain to the Sender Verification Exception Table
3. Set the *Behavior* to **Reject**

Verify

At this point, mail coming from *your.domain* to *your.domain* would be rejected unless the sender is

listed in the Sender Group SPOOF_ALLOW, as it would be associated to a MFP that does not use the sender verification exception table.

An example of this would be seen by completing a manual telnet session to the listener:

The 553 SMTP response is a direct response result from the exception table as configured on the ESA from the steps above.

From the mail logs, you can see the IP address of 192.168.0.9 is not in the valid IP address for the correct sender group:

An allowed IP address matching with the configuration sample from the steps above would be seen as follows:

Related Information

- **ESA, SMA, and WSA Grep with Regex to Search Logs**
- **ESA Message Disposition Determination**
- **Technical Support & Documentation - Cisco Systems**