Spoof Protection using Sender Verification

Contents

[Introduction](#)
[Spoof Protection using Sender Verification](#)
[Configure HAT](#)
[Configure Exception Table](#)
[Verify](#)
[Related Information](#)

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 ALLOWLIST and BLOCKLIST 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:

```
$ telnet example.com 25
Trying 192.168.0.189...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP
helo example.com
250 example.com
mail from: <test@example.com>
553 Envelope sender <test@example.com> rejected
```

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:

```
Wed Aug 5 21:16:51 2015 Info: New SMTP ICID 2692 interface Management (192.168.0.189) address
192.168.0.9 reverse dns host my.host.com verified no
Wed Aug 5 21:16:51 2015 Info: ICID 2692 RELAY SG RELAY_SG match 192.168.0.0/24 SBRS not enabled
Wed Aug 5 21:17:02 2015 Info: ICID 2692 Address: <test@example.com> sender rejected, envelope
sender matched domain exception
```

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

```
Wed Aug 5 21:38:19 2015 Info: New SMTP ICID 2694 interface Management (192.168.0.189) address
192.168.0.15 reverse dns host unknown verified no
Wed Aug 5 21:38:19 2015 Info: ICID 2694 ACCEPT SG SPOOF_ALLOW match 192.168.0.15 SBRS not
enabled
Wed Aug 5 21:38:29 2015 Info: Start MID 3877 ICID 2694
Wed Aug 5 21:38:29 2015 Info: MID 3877 ICID 2694 From: <test@example.com>
Wed Aug 5 21:38:36 2015 Info: MID 3877 ICID 2694 RID 0 To: <robert@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 Subject 'This is an allowed IP and email'
Wed Aug 5 21:38:50 2015 Info: MID 3877 ready 170 bytes from <test@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim verdict using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim AV verdict using Sophos CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 antivirus negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 AMP file reputation verdict : CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 Outbreak Filters: verdict negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 queued for delivery
Wed Aug 5 21:38:51 2015 Info: New SMTP DCID 354 interface 192.168.0.189 address 192.168.0.15
port 25
Wed Aug 5 21:38:51 2015 Info: Delivery start DCID 354 MID 3877 to RID [0]
Wed Aug 5 21:38:51 2015 Info: Message done DCID 354 MID 3877 to RID [0] [('X-IPAS-Result',
'A0GJMwA8usJV/w8AqMBbGQSEFRqFGKUygmUBkV2GMAKBcQEBAgEBAQOBB4QbKIEIhxuCQbxmoDcRAYNPAYE0AQSqSZB5gXA
BAQgCAYQjgT8DAgE'), ('X-IronPort-AV', 'E=Sophos;i="5.15,620,1432612800"; \r\n
d="scan\'";a="3877"')]
Wed Aug 5 21:38:51 2015 Info: MID 3877 RID [0] Response '2.0.0 Ok: queued as 1D74E1002A8'
Wed Aug 5 21:38:51 2015 Info: Message finished MID 3877 done
Wed Aug 5 21:38:56 2015 Info: DCID 354 close
```

Related Information

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