Troubleshoot Older Exchange Server Connectivity to SEG AsyncOS 15.0 after Upgrade

Contents

Introduction

This document describes the steps to fix Exchange 2013 (or older) connectivity issue with Secure Email Gateway (SEG) after upgrade to version 15.0.

Components Used

Exchange 2013 or older.

SEG version 15.0.

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, ensure that you understand the potential impact of any command.

Problem

After upgrading the SEG to version 15.0, the connectivity between Exchange servers older than 2013 is not established. If you check **tophosts** from CLI, you can see that the domain is marked as down **(*)**

```
mx1.cisco.com > tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]> 1

Status as of:                  Sun Sep 03 11:44:11 2023 -03
Hosts marked with '*' were down as of the last delivery attempt.

                         Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host       Recip.    Out     Recip.    Bounced    Bounced
```

```
1*  cisco.com        118      0          0          0     507
2*  alt.cisco.com    94       0        226          0     64
3*  prod.cisco.com   89       0          0          0     546
```

From the Mail_logs, you can see connection failures to the domain with the reason of **network error**.

```
Thu Aug 29 08:16:21 2023 Info: Connection Error: DCID 4664840 domain: cisco.com IP: 10.0.0.1 port: 25 d
```

In Packet capture, you can see the Exchange server closes the connection with FIN packet, immediately after TLS Negotiation.

Solution

Confirm the Exchange server is on version 2013 or older, then you can use this cipher string as a workaround to allow the SEG to connect to those older servers. This allows mail to deliver until exchange can be upgraded to a currently supported version.

```
ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!eNULL:!DES:!3DE
```

You can input this either through the Command Line Interface (CLI) or the Web Graphical User Interface (GUI).

In the CLI:

```
mx1.cisco.com> sslconfig

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, Outbound SMTP, updater
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, Outbound SMTP, updater
[]> outbound

Enter the outbound SMTP ssl method you want to use.
1. TLS v1.1
2. TLS v1.2
3. TLS v1.0
[2]>

Enter the outbound SMTP ssl cipher you want to use.
[!aNULL:!eNULL]> ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL

.....
Hit enter until you are back to the default command line.


mx1.cisco.com> commit
```

In the GUI:

Step 1. Choose on **System Administration** tab.
Step 2. Choose on **SSL Configuration.**
Step 3. Select the **Edit Settings** button**.**
Step 4. Change the **Outbound SMTP SSL Cipher(s) to use** the string provided in this article.
Step 5. **Submit** and **commit** the changes.

Related Information

User Guide for AsyncOS 15.0: System Administration

Alter the Methods and Ciphers Used with SSL/TLS on the ESA

Cisco bug ID CSCwh48138 - ESA 15.0 Email delivery failure over TLS with Exchange 2013