Prevent Negotiations for Null or Anonymous Ciphers on the ESA and SMA

Contents

Introduction

This document describes how to alter the Cisco Email Security Appliance (ESA) and Cisco Security Management Appliance (SMA) cipher settings in order to prevent negotiations for null or anonymous ciphers. This document applies to both hardware based and virtual based appliances.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ESA
- Cisco SMA

Components Used

The information in this document is based on all versions of the Cisco ESA and Cisco SMA.

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.

Prevent Negotiations for Null or Anonymous Ciphers

This section describes how to prevent negotiations for null or anonymous ciphers on the Cisco ESA that runs AsyncOS for Email Security Versions 9.1 and later, and also on the Cisco SMA.

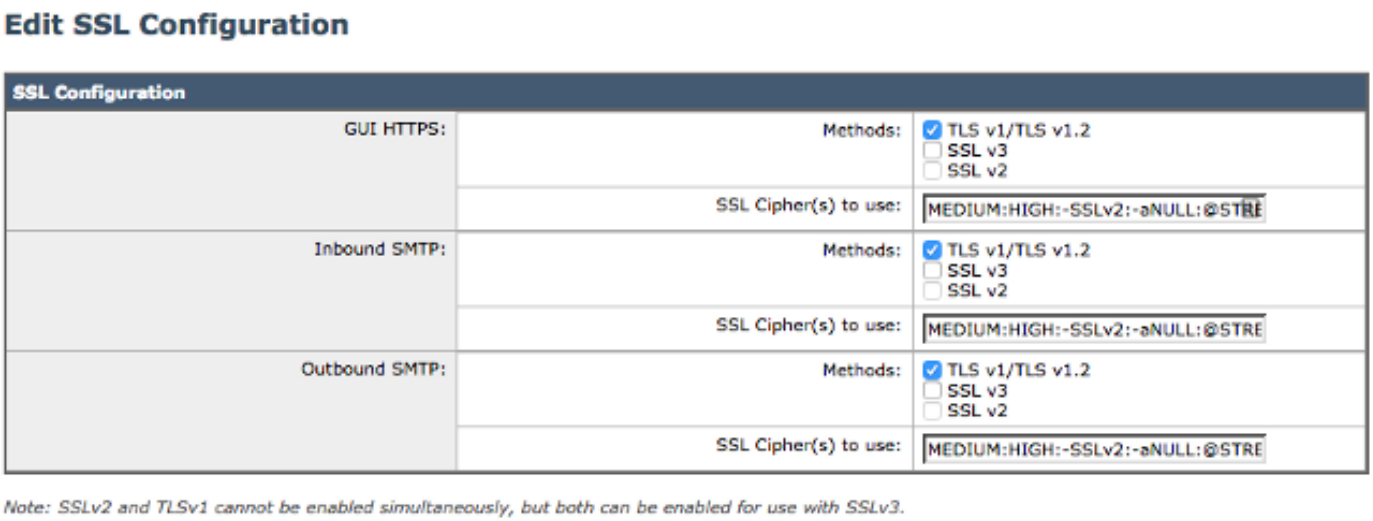
ESAs that Run AsyncOS for Email Security Version 9.5 or newer

With the introduction of AsyncOS for Email Security Version 9.5, TLS v1.2 is now supported. The commands that are described in the previous section still work; however, you will see the updates for TLS v1.2 included in the outputs.

Here is an example output from the CLI:

```
> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH

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.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>
```

In order to reach these settings from the GUI, navigate to **System Administration > SSL Configuration > Edit Settings...**:



> **Tip**: For complete information, refer to the appropriate ESA End-User Guide for Version 9.5 or later.

ESAs that Run AsyncOS for Email Security Version 9.1 or older

You can modify the ciphers that are used on the ESA with the **sslconfig** command. In order to prevent the ESA negotiations for null or anonymous ciphers, enter the **sslconfig** command into the ESA CLI and apply these settings:

- Inbound Simple Mail Transfer Protocol (SMTP) method: **sslv3tlsv1**
- Inbound SMTP ciphers: **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**
- Outbound SMTP method: **sslv3tlsv1**
- Outbound SMTP ciphers: **MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**

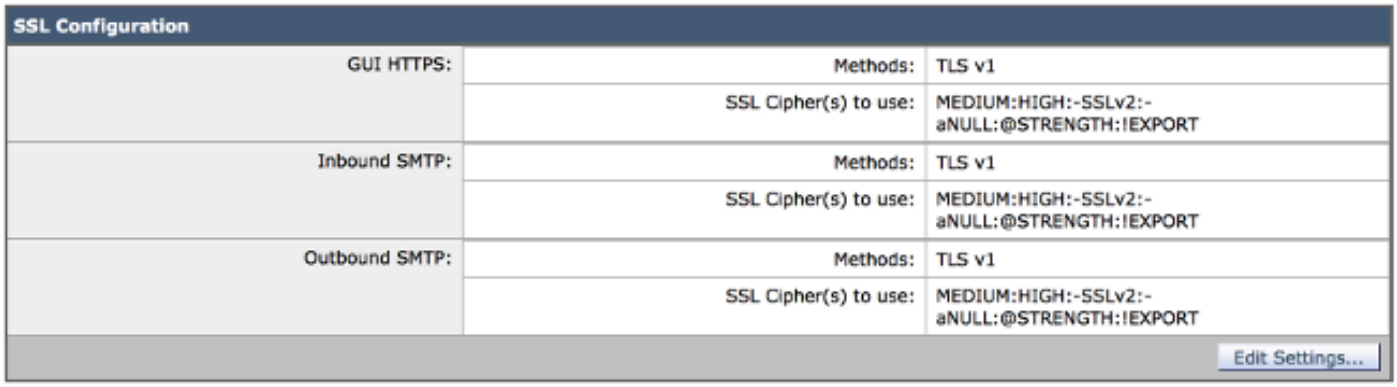
Here is an example configuration for inbound ciphers:

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

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.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
```

```
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

Note: Set the **GUI**, **INBOUND**, and **OUTBOUND** as needed for each cipher.

As of AsyncOS for Email Security Version 8.5, the **sslconfig** command is also available via the GUI. In order to reach these settings from the GUI, navigate to **System Administration > SSL Configurations > Edit Settings**:



Tip: Secure Sockets Laver (SSL) Version 3.0 (RFC-6101) is an obsolete and insecure protocol. There is a vulnerability in SSLv3 CVE-2014-3566 known as *Padding Oracle On Downgraded Legacy Encryption (POODLE) attack*, which is tracked by Cisco bug ID CSCur27131. Cisco recommends that you disable SSLv3 while you change the ciphers, use Transport Layer Security (TLS) only, and select *option 3* (TLS v1). Refer to Cisco bug ID CSCur27131 for complete details.

SMAs that Run AsycnOS for Content Security Management 9.6 or newer

Similar to the ESA, run the **sslconfig** command on the CLI.

SMAs that Run AsyncOS for Content Security Management 9.5 or Later

The **sslconfig** command is not available for old versions of SMA.

Note: Older versions of AsyncOS for SMA only supported TLS v1. Please upgrade to 9.6 or newer on your SMA for up-to-date SSL management.

You must complete these steps from the SMA CLI in order to modify the SSL ciphers:

1. Save the SMA configuration file to your local computer.
2. Open the XML file.
3. Search for the <*ssl*> section in the XML:

```
CLI: > sslconfig
```

```
sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

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.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

4. Modify the ciphers as desired and save the XML:

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

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.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

5. Load the new configuration file onto the SMA.

6. **Submit** and **commit** all changes.

Related Information

- **Cisco ESA - Release Notes**
- **Cisco ESA - User Guides**
- **Cisco SMA - Release Notes**
- **Cisco SMA - User Guides**
- **Technical Support & Documentation - Cisco Systems**