Configure Secure Email Gateway Outbound MTA-STS

Contents

Introduction

This document describes steps to configure the Secure Email Gateway (SEG) Outbound Mail Transfer Agent - Strict Transport Security (MTA-STS).

Prerequisites

Requirements

General knowledge of the Cisco Secure Email Gateway (SEG) general settings and configuration.

Components Used

This setup requires:

- Cisco Secure Email Gateway (SEG) AsyncOS 16.0 or newer.
- Destination Control Profiles.

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.

Overview

Mail Transfer Agent - Strict Transport Security (MTA-STS) is a protocol that enforces the use of secure TLS Connections with an added secure protection layer. MTA-STS helps prevent man-in-the-middle attacks and eavesdropping by ensuring emails are sent over secure, encrypted channels.

SEG AsyncOS 16 and newer can perform outbound MTA-STS message delivery to MTA-STS configured receiving domains.

When enabled, the SEG checks the Destination Control Profiles for MTA-STS settings. The SEG initiates the MTA-STS process to fetch, validate, and apply the defined record and policy, ensuring the connection to the receiving MTA is secure over TLSv1.2 or higher.

The receiving domain owners are responsible for creating, publishing, and maintaining the DNS Record and the MTA-STS Policy.

How MTA-STS Works for SEG

- The Receiving Domain maintains the MTA-STS policy and MTA-STS DNS text record.
- The Sending Domain MTA must be MTA-STS capable of resolving and acting upon the destination domain MTA-STS Policy.

The **Receiving Email Domain** owner publishes an MTA-STS txt record via DNS as described here:

- The txt record triggers the SEG to check the MTA-STS policy, hosted on an HTTPS-enabled web server.
- The policy specifies the parameters for communication to the domain.
    - Contains MTA-STS MX hosts to receive.
    - Mode is defined as either Testing Mode or Enforce Mode
    - TLSv1.2 or greater is required.

- MTA-STS uses DNS TXT records for policy discovery. It fetches the MTA-STS policy from an HTTPS host.
- During the TLS handshake, initiated to fetch a new or updated policy from the Policy Host, the HTTPS server must present a valid X.509 certificate for the "MTA-STS" DNS-ID.

The **Sending Email Domain** aspects:

- When an SEG (sending MTA) sends an email to an MTA-STS domain, it first checks for the recipient domain MTA-STS policy.
- If the policy is configured with Enforce Mode, the sending email server attempts to establish a secure, encrypted connection to the receiving email server (receiving MTA). If a secure connection cannot be established (for example, if the TLS certificate is invalid or the connection is downgraded to an insecure protocol), the email fails delivery, and the sender is notified of the failure.

RFC8461

Configure

Preliminary actions are recommended during setup:

1. Verify the destination domain has a properly configured MTA-STS DNS record and policy record, before configuring the SEG Destination Control Profile.

- This is most efficiently performed by accessing MTA-STS checker web pages.
    - Google search "verify MTA-STS domain"
    - Choose a verification website from the search results.
    - Enter the destination domain.
- Only configure domains once the verification check has been completed.

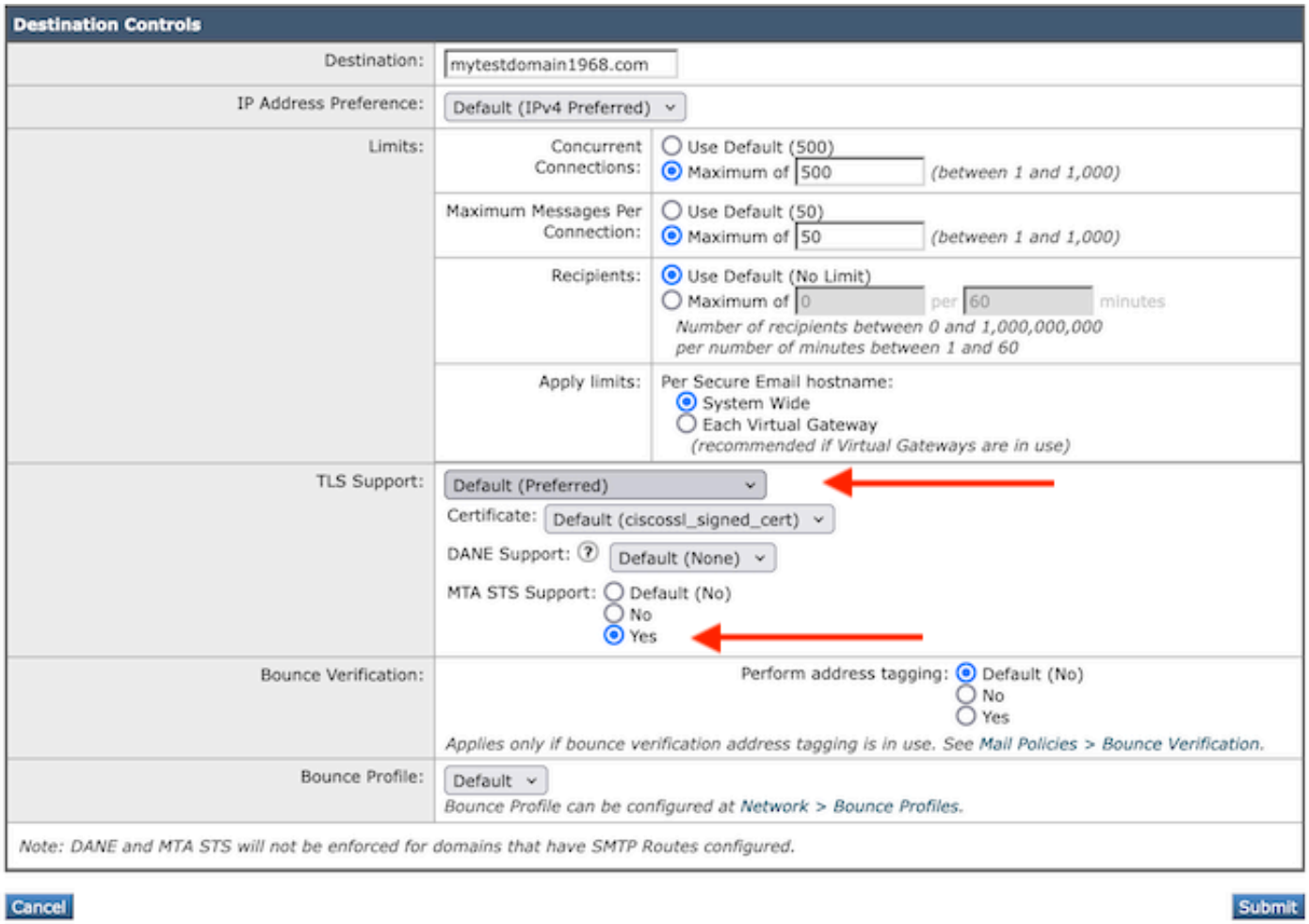
2. Do **not** use MTA-STS on the Destination Controls **Default Policy**.

- Each Destination Control Profile configured to utilize MTA-STS adds a small burden to the SEG. If the default Destination Control Policy had MTA-STS configured, without verifying the domain, it could impact the SEG service.

WebUI Configuration

- Navigate to **Mail Policies > Destination Controls Page**.
- Select **Add Destination Controls** or edit an existing **Destination Control Profile**.
  - TLS Support settings permit any setting except **None**, accommodating various TLS Support Options.
  - The sub-menu **DANE Support Options** include **Mandatory**, **Opportunistic**, or **None**.
  - MTA-STS Support setting = Yes
- Select **Submit** followed by **Commit** to apply the changes.

Note: If the Receiving MTA resides in a hosted environment such as Gsuite or O365, configure the Destination Controls TLS to **TLS Required-Verify Hosted Domains**.



Destination Control Profile

Interoperability Caveats:

DANE Support takes precedence over MTA STS and could affect the actions taken:

- If DANE succeeds, MTA-STS is skipped and mail is delivered.

- If DANE mandatory fails, mail is not delivered.
- If DANE Opportunistic fails, and MTA-STS is skipped due to configuration errors, the SEG attempts to deliver using the configured TLS setting.
- MTA-STS is not be applied if an SMTP Route is configured for the domain.

CLI Configuration

- **destconfig**
  - **new/edit**
    - Enter the preferred choices until the TLS options menu item is presented.
    - Options 2-6 for TLS supports MTA-STS.

Do you wish to apply a specific TLS setting for this domain? [N]> y

Do you want to use TLS support?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
6. Required - Verify Hosted Domains
[2]>2

You have chosen to enable TLS. Please use the **certconfig** command to ensure that there is a valid certificate configured.
Do you wish to configure DANE Support? [N]>

Do you wish to configure MTA STS Support? [N]> y

Do you want to use MTA STS support?
1. Off
2. On
[1]> 2

MTA STS is not enforced for domains that have SMTP Routes configured:

1. Complete the remaining options to finish the specific Destination Control Profile.
2. Apply the changes using **Submit > Commit**.

Verify

info level mail_logs:

```
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(mta-test.domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

debug level mail_logs:

```
Thu Sep 26 15:23:39 2024 Debug: DNS query: Q(_mta-sts.domain.com, 'TXT')
Thu Sep 26 15:23:39 2024 Debug: DNS query: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Debug: DNS encache (_mta-sts.domain.com, TXT, [(131794459543073830L, 0, 'insec
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(domain.com)
Thu Sep 26 15:23:39 2024 Debug: Valid cache entry found for the domain (domain.com).Thu Sep 26 15:23:39
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (domain.com,'MX','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Info: Applying MTA-STS policy for the domain (domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Debug: DNS query: Q(domain.com, 'MX')
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

Receiving SEG-supported TLS v1.3:

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

Tue Sep 24 09:13:52 2024 Debug: DNS query: Q(_mta-sts.domain.com, 'TXT')
Tue Sep 24 09:13:52 2024 Debug: DNS query: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
Tue Sep 24 09:13:52 2024 Debug: DNS query: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Tue Sep 24 09:13:52 2024 Debug: DNS encache (_mta-sts.domain.com, TXT, [(131366525701580508L, 0, 'insecure', ('v=STSv1; id=12345678598Z;',))])
Tue Sep 24 09:13:52 2024 Info: Successfully fetched MTA-STS TXT record for domain(domain.com)
Tue Sep 24 09:13:52 2024 Debug: Fetch MTA-STS policy for the domain(domain.com)
Tue Sep 24 09:13:52 2024 Debug: Requesting MTA-STS policy fetch via proxy
Tue Sep 24 09:13:52 2024 Debug: Request to fetch STS policy failed due to a connection timeout., for the domain domain.com
Tue Sep 24 09:13:52 2024 Info: Failure encountered while fetching MTA-STS policy for the domain(domain.com)

Thu Sep 19 13:04:50 2024 Info: Successfully fetched MTA-STS TXT record for domain(domain.com)
Thu Sep 19 13:04:50 2024 Debug: Fetch MTA-STS policy for the domain(domain.com)
Thu Sep 19 13:04:50 2024 Debug: Requesting MTA-STS policy fetch via proxy
Thu Sep 19 13:04:50 2024 Debug: Request to fetch STS policy failed due to a connection timeout., for the domain domain.com
Thu Sep 19 13:04:50 2024 Info: Failure encountered while fetching MTA-STS policy for the domain(domain.com)

Thu Sep 19 13:04:50 2024 Info: MID 5411 queued for delivery

Troubleshoot

1. If SEG fails to deliver with the error **"peer cert does not match domain domain.com".**

This indicates the destination is a hosted service such as G Suite or M365. Change the **Destination Controls**

Profile TLS setting > TLS Required - Verify Hosted Domains:

```
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS deferring: verify error: peer cert does not match domain
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS was required but could not be successfully negotiated
```

2. Communication fails if the sending or receiving certificates are not properly configured or expired.

3. The SEG needs to verify the proper destination intermediate and root certificates are in the Certificate Authority Lists.

4. Simple Telnet tests from SEG cli to verify the DNS txt Record and a basic response test to the Policy web server.

- DNS query from **cli > dig _mta-sts.domain.com txt**:

;; ANSWER SECTION:
_mta-sts.domain.com. 0 IN TXT "v=STSv1; id=12345678598Z;"

- Telnet to verify basic web server reachability from **cli > telnet mta-sts.domain.com 443**:
- Use a regular web-browser to view the MTA-STS Policy.
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

```
version: STSv1
mode: enforce
mx: *.mail123.domain.com
max_age: 604800
```

Related Information

- Cisco Secure Email Gateway Launch Page to Support Guides