Configurar Secure Email Gateway Outbound MTA-STS

Contenido

Introducción

Este documento describe los pasos para configurar el Agente de transferencia de correo saliente de Secure Email Gateway (SEG) - Seguridad de transporte estricta (MTA-STS).

Prerequisites

Requirements

Conocimiento general de los parámetros y la configuración generales de Cisco Secure Email Gateway (SEG).

Componentes Utilizados

Esta configuración requiere:

- Cisco Secure Email Gateway (SEG) AsyncOS 16.0 o posterior.
- Perfiles de control de destino.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Agente de transferencia de correo: seguridad de transporte estricta (MTA-STS) es un protocolo que aplica el uso de conexiones TLS seguras con una capa de protección segura agregada. MTA-STS ayuda a prevenir los ataques de intrusos y las escuchas asegurándose de que los correos electrónicos se envían a través de canales seguros y cifrados.

SEG AsyncOS 16 y versiones posteriores pueden realizar la entrega de mensajes MTA-STS salientes a los dominios de recepción configurados MTA-STS.

Cuando está habilitado, el SEG verifica los Perfiles de control de destino para la configuración de MTA-STS. El SEG inicia el proceso MTA-STS para obtener, validar y aplicar el registro y la política definidos, asegurándose de que la conexión al MTA receptor sea segura a través de TLSv1.2 o superior.

Los propietarios del dominio receptor son responsables de crear, publicar y mantener el registro DNS y la política MTA-STS.

Cómo funciona MTA-STS para SEG

- El dominio de recepción mantiene la política MTA-STS y el registro de texto DNS MTA-STS.
- El MTA del dominio de envío debe ser MTA-STS capaz de resolver y actuar sobre la política MTA-STS del dominio de destino.

El propietario del dominio de correo electrónico de recepción publica un registro de texto MTA-STS a través de DNS como se describe aquí:

- El registro txt hace que el SEG compruebe la política MTA-STS, alojada en un servidor web habilitado para HTTPS.
- La directiva especifica los parámetros para la comunicación con el dominio.
    - Contiene hosts MTA-STS MX para recibir.
    - El modo se define como modo de prueba o modo de aplicación
    - Se requiere TLSv1.2 o superior.

- MTA-STS utiliza registros DNS TXT para la detección de políticas. Obtiene la política MTA-STS de un host HTTPS.
- Durante el intercambio de señales de TLS, iniciado para obtener una política nueva o actualizada del host de políticas, el servidor HTTPS debe presentar un certificado X.509 válido para el ID de DNS "MTA-STS".

Aspectos de Sending Email Domain:

- Cuando un SEG (que envía MTA) envía un correo electrónico a un dominio MTA-STS, primero verifica la política MTA-STS del dominio de destinatario.
- Si la directiva se configura con el modo de aplicación, el servidor de correo electrónico de envío intenta establecer una conexión segura y cifrada con el servidor de correo electrónico de recepción (MTA de recepción). Si no se puede establecer una conexión segura (por

ejemplo, si el certificado TLS no es válido o la conexión se ha degradado a un protocolo no seguro), el correo electrónico no se entrega correctamente y se notifica al remitente del error.

RFC8461

Configurar

Se recomiendan acciones preliminares durante la configuración:

1. Verifique que el dominio de destino tenga un registro de DNS MTA-STS y un registro de política correctamente configurados, antes de configurar el perfil de control de destino SEG.

- Esto se realiza de la manera más eficiente al acceder a las páginas web del verificador MTA-STS.
  - Búsqueda de Google "verify MTA-STS domain"
  - Elija un sitio web de verificación de los resultados de búsqueda.
  - Introduzca el dominio de destino.
- Configure los dominios solamente una vez que se haya completado la verificación.

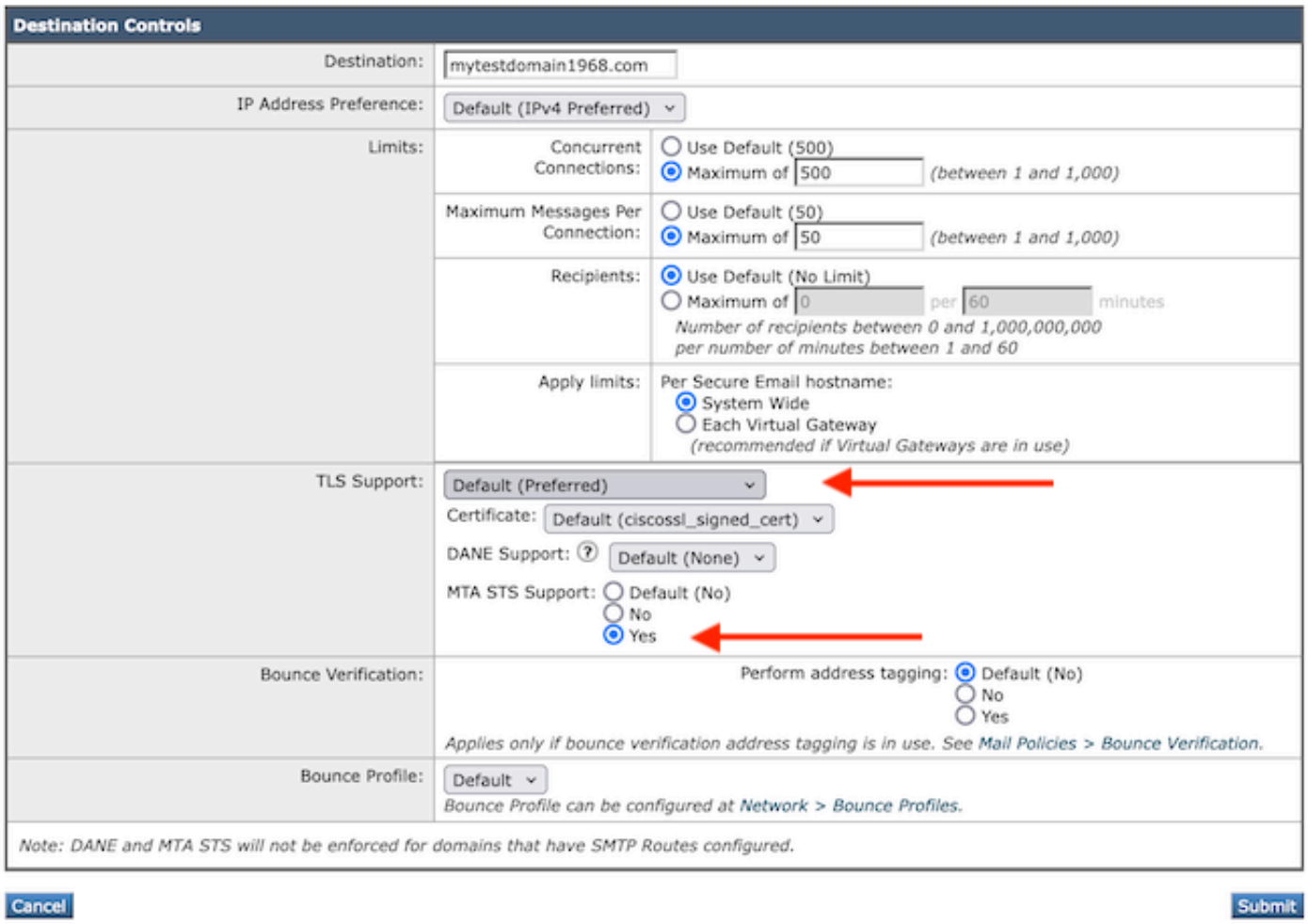
2. No utilice MTA-STS en la política predeterminada de controles de destino.

- Cada perfil de control de destino configurado para utilizar MTA-STS agrega una pequeña carga al SEG. Si la política de control de destino predeterminada tuviera MTA-STS configurado, sin verificar el dominio, podría afectar el servicio SEG.

Configuración de WebUI

- Vaya a Políticas de Correo > Página Controles de Destino.
- Seleccione Agregar controles de destino o edite un perfil de control de destino existente.
  - La configuración de compatibilidad con TLS permite cualquier configuración excepto None, que incluye varias opciones de compatibilidad con TLS.
  - El submenú Opciones de soporte de DANE incluye Obligatorio, Oportunista o Ninguno.
  - Configuración de soporte de MTA-STS = Sí
- Seleccione Submit seguido de Commit para aplicar los cambios.

Nota: Si el MTA de recepción reside en un entorno alojado como Gsuite o O365, configure los controles de destino de TLS en TLS Required-Verify Hosted Domains.



Perfil de control de destino

Advertencias de interoperabilidad:

El soporte del DANE tiene prioridad sobre el MTA STS y podría afectar las acciones tomadas:

- Si DANE tiene éxito, se omite MTA-STS y se entrega el correo.
- Si el DANE obligatorio falla, el correo no se entrega.
- Si DANE Opportunistic falla y MTA-STS se salta debido a errores de configuración, SEG intenta realizar la entrega utilizando la configuración de TLS configurada.
- MTA-STS no se aplicará si se ha configurado una ruta SMTP para el dominio.

Configuración de CLI

- destconfig
  - nuevo/editar
    - Introduzca las opciones preferidas hasta que se muestre el elemento de menú Opciones de TLS.
    - Las opciones 2-6 para TLS admiten MTA-STS.

¿Desea aplicar una configuración de TLS específica para este dominio? [N]> y

¿Desea utilizar la compatibilidad con TLS?
1. No

2. Preferible
3. Obligatorio
4. Preferido - Verificar
5. Obligatorio - Verificar
6. Necesario - Verificar dominios alojados
[2]>2

Ha elegido habilitar TLS. Utilice el comando certconfig para asegurarse de que haya un certificado válido configurado.
¿Desea configurar el soporte de DANE? [N]>

¿Desea configurar el soporte STS de MTA? [N]> y

¿Desea utilizar la compatibilidad con MTA STS?
1. Apagado
2. Activado
[1]> 2

MTA STS no se aplica para dominios que tienen rutas SMTP configuradas:

1. Complete las opciones restantes para finalizar el perfil de control de destino específico.
2. Aplique los cambios mediante Enviar > Confirmar.

Verificación

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
```

Recepción de TLS v1.3 compatible con SEG:

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

Mar 24 Sep 09:13:52 2024 Depuración: Consulta DNS: P(_mta-sts.domain.com, 'TXT')
Mar 24 Sep 09:13:52 2024 Depuración: Consulta DNS: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
Mar 24 Sep 09:13:52 2024 Depuración: Consulta DNS: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Mar 24 Sep 09:13:52 2024 Depuración: Caché DNS (_mta-sts.domain.com, TXT, [(13136652570158050 8L, 0, 'insecure', ('v=STSv1; id=12345678598Z;',)])
Mar Sep 24 09:13:52 2024 Info: Registro TXT MTA-STS obtenido correctamente para el dominio (domain.com)
Mar 24 Sep 09:13:52 2024 Depuración: Obtener directiva MTA-STS para el dominio (domain.com)
Mar 24 Sep 09:13:52 2024 Depuración: Solicitando captura de política MTA-STS mediante proxy
Mar 24 Sep 09:13:52 2024 Depuración: Error en la solicitud para obtener la directiva STS debido a un tiempo de espera de conexión., para el dominio domain.com
Mar Sep 24 09:13:52 2024 Info: Error al recuperar la directiva MTA-STS para el dominio (domain.com)

Jueves 19 de septiembre 13:04:50 2024 Info: Registro TXT MTA-STS obtenido correctamente para el dominio (domain.com)
Jueves 19 de septiembre 13:04:50 2024 Depuración: Obtener directiva MTA-STS para el dominio (domain.com)
Jueves 19 de septiembre 13:04:50 2024 Depuración: Solicitando captura de política MTA-STS mediante proxy
Jueves 19 de septiembre 13:04:50 2024 Depuración: Error en la solicitud para obtener la directiva STS debido a un tiempo de espera de conexión., para el dominio domain.com
Jueves 19 de septiembre 13:04:50 2024 Info: Error al recuperar la directiva MTA-STS para el dominio (domain.com)

Jueves 19 de septiembre 13:04:50 2024 Info: MID 5411 en cola para entrega

Troubleshoot

1. Si SEG no puede entregar con el error "el certificado de peer no coincide con el dominio domain.com".

Esto indica que el destino es un servicio alojado como G Suite o M365. Cambie la configuración

TLS del perfil de controles de destino > TLS requerido - Verificar dominios alojados:

```
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. La comunicación falla si los certificados de envío o recepción no están configurados correctamente o han caducado.

3. El SEG debe verificar que los certificados raíz e intermedio de destino adecuados se encuentran en las listas de autoridades certificadoras.

4. Pruebas Telnet simples de la CLI de SEG para verificar el registro de texto DNS y una prueba de respuesta básica al servidor web de políticas.

- Consulta DNS de cli > dig _mta-sts.domain.com txt:

;; SECCIÓN DE RESPUESTA:
_mta-sts.domain.com. 0 IN TXT "v=STSv1; id=12345678598Z;"

- Telnet para verificar el alcance básico del servidor web desde cli > telnet mta-sts.domain.com 443:
- Utilice un navegador web normal para ver la política MTA-STS.
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

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

Información Relacionada

- Página de inicio de Cisco Secure Email Gateway para las guías de asistencia

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).