Konfigurieren von Secure Email Gateway Outbound MTA-STS

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren des Secure Email Gateway (SEG) Outbound Mail Transfer Agent - Strict Transport Security (MTA-STS) beschrieben.

Voraussetzungen

Anforderungen

Allgemeine Kenntnisse der allgemeinen Einstellungen und Konfiguration des Cisco Secure Email Gateway (SEG)

Verwendete Komponenten

Diese Einrichtung erfordert Folgendes:

- Cisco Secure Email Gateway (SEG) AsyncOS 16.0 oder höher
- Zielsteuerelementprofile.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Mail Transfer Agent - Strict Transport Security (MTA-STS) ist ein Protokoll, das die Verwendung sicherer TLS-Verbindungen mit einer zusätzlichen sicheren Schutzschicht erzwingt. MTA-STS verhindert Man-in-the-Middle-Angriffe und Lauschangriffe, indem es sicherstellt, dass E-Mails über sichere, verschlüsselte Kanäle gesendet werden.

SEG AsyncOS 16 und neuere Versionen können ausgehende MTA-STS-Nachrichten an MTA-STS-konfigurierte Empfangsdomänen senden.

Wenn diese Funktion aktiviert ist, überprüft die SEG die Zielsteuerungsprofile auf MTA-STS-Einstellungen. Die SEG initiiert den MTA-STS-Prozess zum Abrufen, Validieren und Anwenden der definierten Datensätze und Richtlinien. So wird sichergestellt, dass die Verbindung zur empfangenden MTA über TLSv1.2 oder höher sicher ist.

Die Inhaber der empfangenden Domäne sind für die Erstellung, Veröffentlichung und Wartung der DNS-Datensätze und der MTA-STS-Richtlinie verantwortlich.

So funktioniert MTA-STS für SEG

- Die empfangende Domäne pflegt die MTA-STS-Richtlinie und den MTA-STS-DNS-Textdatensatz.
- Die sendende MTA-Domäne muss MTA-STS sein, die die MTA-STS-Richtlinie der Zieldomäne auflösen und auf diese reagieren kann.

Der Eigentümer der empfangenden E-Mail-Domäne veröffentlicht einen MTA-STS-Textdatensatz über DNS wie hier beschrieben:

- Der Textdatensatz veranlasst die SEG, die MTA-STS-Richtlinie zu überprüfen, die auf einem HTTPS-fähigen Webserver gehostet wird.
- Die Richtlinie legt die Parameter für die Kommunikation mit der Domäne fest.
    - Enthält zu empfangende MTA-STS MX Hosts.
    - Modus ist entweder als Testmodus oder als Erzwingungsmodus definiert.
    - TLSv1.2 oder höher ist erforderlich.

- MTA-STS verwendet DNS-TXT-Datensätze für die Richtlinienerkennung. Es ruft die MTA-STS-Richtlinie von einem HTTPS-Host ab.
- Beim TLS-Handshake, der initiiert wird, um eine neue oder aktualisierte Richtlinie vom Policy Host abzurufen, muss der HTTPS-Server ein gültiges X.509-Zertifikat für die DNS-ID "MTA-STS" präsentieren.

Die Aspekte der E-Mail-Domäne:

- Wenn ein SEG (eine MTA sendende) eine E-Mail an eine MTA-STS-Domäne sendet, sucht er zunächst nach der MTA-STS-Richtlinie der Empfängerdomäne.
- Wenn die Richtlinie mit Erzwingungsmodus konfiguriert ist, versucht der sendende E-Mail-Server, eine sichere, verschlüsselte Verbindung zum empfangenden E-Mail-Server

(empfangende MTA) herzustellen. Wenn keine sichere Verbindung hergestellt werden kann (z. B. wenn das TLS-Zertifikat ungültig ist oder die Verbindung auf ein unsicheres Protokoll herabgestuft wird), schlägt die Zustellung der E-Mail fehl, und der Absender wird über den Fehler informiert.

RFC 8461

Konfigurieren

Vorläufige Maßnahmen werden während der Einrichtung empfohlen:

1. Überprüfen Sie, ob die Zieldomäne über einen ordnungsgemäß konfigurierten MTA-STS-DNS-Eintrag und -Richtlinieneintrag verfügt, bevor Sie das SEG-Zielsteuerungsprofil konfigurieren.

- Dies wird am effizientesten durch den Zugriff auf MTA-STS-Checker-Webseiten durchgeführt.
  - Google search "verify MTA-STS domain"
  - Wählen Sie aus den Suchergebnissen eine Überprüfungswebsite aus.
  - Geben Sie die Zieldomäne ein.
- Konfigurieren Sie Domänen erst, nachdem die Verifizierungsprüfung abgeschlossen wurde.

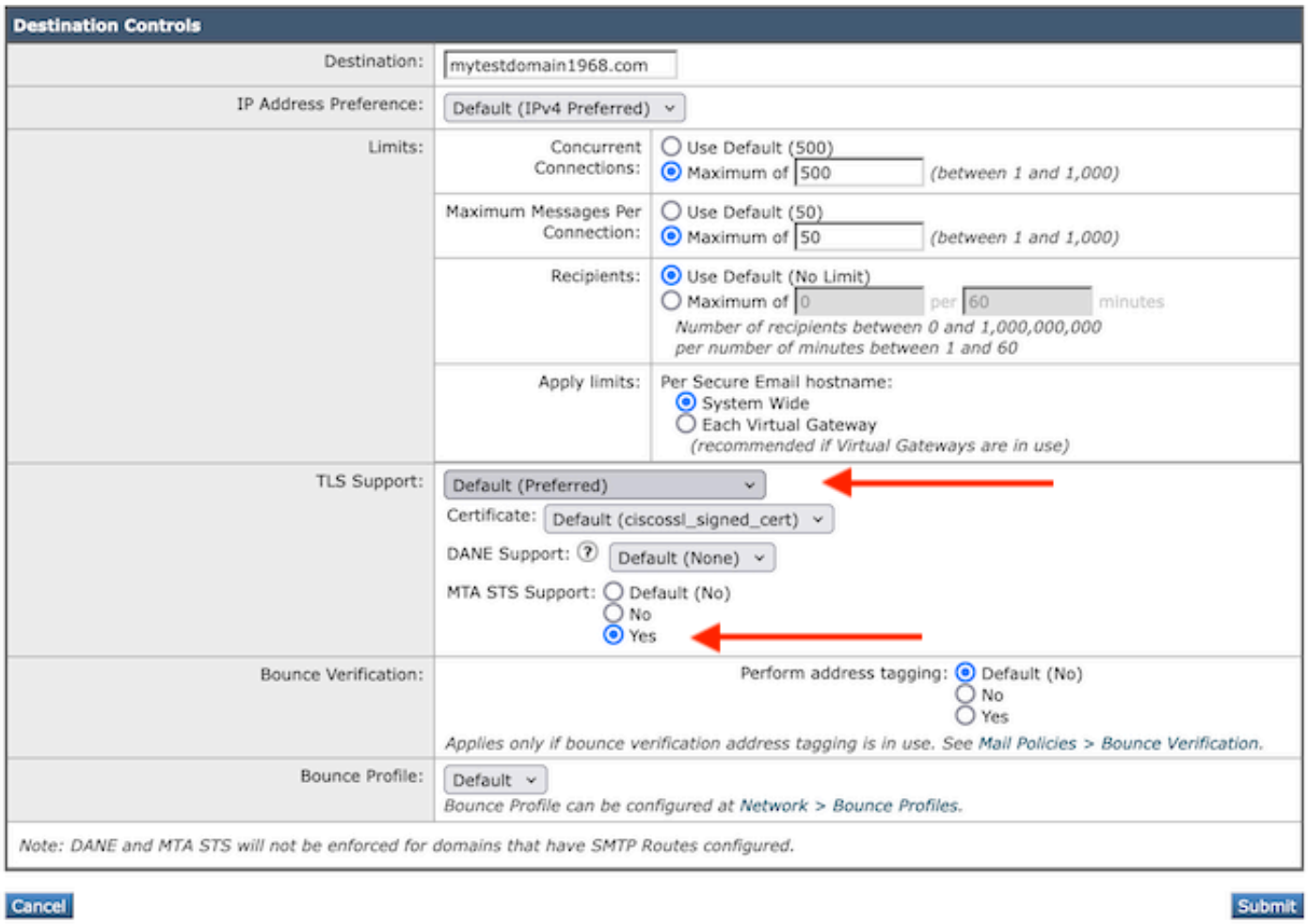
2. Verwenden Sie MTA-STS nicht in der Standardrichtlinie der Zielsteuerelemente.

- Jedes Zielsteuerungsprofil, das für die Verwendung von MTA-STS konfiguriert wurde, stellt eine kleine Belastung für die SEG dar. Wenn für die standardmäßige Zielsteuerungsrichtlinie MTA-STS konfiguriert wurde, ohne die Domäne zu überprüfen, kann dies sich auf den SEG-Dienst auswirken.

WebUI-Konfiguration

- Navigieren Sie zu Mail-Policys > Zielsteuerelemente.
- Wählen Sie Zielsteuerelemente hinzufügen aus, oder bearbeiten Sie ein vorhandenes Zielsteuerelementprofil.
  - Die TLS-Supporteinstellungen lassen jede Einstellung außer Keine zu, sodass verschiedene TLS-Supportoptionen berücksichtigt werden können.
  - Das Untermenü DANE Support Optionen umfasst Obligatorisch, Opportunistisch oder Keine.
  - MTA-STS Support-Einstellung = Ja
- Wählen Sie Senden und anschließend Übernehmen aus, um die Änderungen zu übernehmen.

Anmerkung: Wenn sich die empfangende MTA in einer gehosteten Umgebung wie Gsuite oder O365 befindet, konfigurieren Sie die Zielsteuerelemente TLS in TLS Required-Verify Hosted Domains.



Zielsteuerungsprofil

Hinweise zur Interoperabilität:

DANE Support hat Vorrang vor MTA STS und könnte sich auf die getroffenen Maßnahmen auswirken:

- Wenn DANE erfolgreich ist, wird MTA-STS übersprungen und die Post zugestellt.
- Wenn DANE erforderlich fehlschlägt, werden die E-Mails nicht zugestellt.
- Wenn DANE Opportunistic fehlschlägt und MTA-STS aufgrund von Konfigurationsfehlern übersprungen wird, versucht die SEG, mithilfe der konfigurierten TLS-Einstellung eine Übermittlung zu ermöglichen.
- MTA-STS wird nicht angewendet, wenn eine SMTP-Route für die Domäne konfiguriert ist.

CLI-Konfiguration

- Destconfig
  - Neu/Bearbeiten
    - Geben Sie die gewünschten Optionen ein, bis der Menüpunkt "TLS-Optionen" angezeigt wird.
    - Die Optionen 2-6 für TLS unterstützen MTA-STS.

Möchten Sie eine bestimmte TLS-Einstellung für diese Domäne übernehmen? [N]> J

Möchten Sie die TLS-Unterstützung nutzen?
1. Nein
2. Bevorzugt
3. Erforderlich
4. Bevorzugt - Verifizieren
5. Erforderlich - Verifizieren
6. Erforderlich - Gehostete Domänen überprüfen
[2]>2

Sie haben sich entschieden, TLS zu aktivieren. Verwenden Sie den Befehl certconfig, um sicherzustellen, dass ein gültiges Zertifikat konfiguriert ist.
Möchten Sie den DANE-Support konfigurieren? [N]>

Möchten Sie den MTA STS-Support konfigurieren? [N]> J

Möchten Sie den MTA STS-Support nutzen?
1. Aus
2. Am
[1]> 2

MTA STS wird nicht für Domänen erzwungen, für die SMTP-Routen konfiguriert sind:

1. Füllen Sie die verbleibenden Optionen aus, um das spezifische Zielsteuerungsprofil fertigzustellen.
2. Wenden Sie die Änderungen an, indem Sie Senden > Übernehmen wählen.

Überprüfung

Mail_Protokolle auf Informationsebene:

```
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-Ebene 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
```

Empfangen von SEG-unterstütztem TLS v1.3:

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

Dienstag, 24. September 2024, 09:13:52 Uhr Debug: DNS-Abfrage: Q(_mta-sts.domain.com, 'TXT')
Dienstag, 24. September 2024, 09:13:52 Uhr Debug: DNS-Abfrage: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
Dienstag, 24. September 2024, 09:13:52 Uhr Debug: DNS-Abfrage: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Dienstag, 24. September 2024, 09:13:52 Uhr Debug: DNS encache (_mta-sts.domain.com, TXT, [(13136652570158050 8L, 0, 'unsecure', ('v=STSv1; id=12345678598Z;',))])
Dienstag, 24. September 2024, 09:13:52 Uhr, Info: MTA-STS TXT-Datensatz für Domäne erfolgreich abgerufen (domain.com)
Dienstag, 24. September 2024, 09:13:52 Uhr Debug: Abrufen der MTA-STS-Richtlinie für die Domäne (domain.com)
Dienstag, 24. September 2024, 09:13:52 Uhr Debug: Anfordern des MTA-STS-Richtlinienabrufs über Proxy
Dienstag, 24. September 2024, 09:13:52 Uhr Debug: Fehler bei der Anforderung zum Abrufen der STS-Richtlinie aufgrund eines Verbindungs-Timeouts für die Domäne domain.com.
Dienstag, 24. September 2024, 09:13:52 Uhr, Info: Fehler beim Abrufen der MTA-STS-Richtlinie für die Domäne (domain.com)

Do, 19. September 2024, 13:04:50 Uhr, Info: MTA-STS TXT-Datensatz für Domäne erfolgreich abgerufen (domain.com)
Do, 19. Sept. 13:04:50 2024 Fehlerbehebung: Abrufen der MTA-STS-Richtlinie für die Domäne (domain.com)
Do, 19. Sept. 13:04:50 2024 Fehlerbehebung: Anfordern des MTA-STS-Richtlinienabrufs über Proxy
Do, 19. Sept. 13:04:50 2024 Fehlerbehebung: Fehler bei der Anforderung zum Abrufen der STS-Richtlinie aufgrund eines Verbindungs-Timeouts für die Domäne domain.com.
Do, 19. September 2024, 13:04:50 Uhr, Info: Fehler beim Abrufen der MTA-STS-Richtlinie für die Domäne (domain.com)

Do, 19. September 2024, 13:04:50 Uhr, Info: MID 5411 in Warteschlange für Zustellung

Fehlerbehebung

1. Wenn SEG die Fehlermeldung "peer cert does not match domain.com" (Peer-Zertifikat stimmt nicht mit domäne.com überein) nicht liefert.

Zeigt an, dass es sich bei dem Ziel um einen gehosteten Service wie G Suite oder M365 handelt. Ändern Sie die TLS-Einstellung für das Zielsteuerelementprofil > TLS erforderlich - Gehostete Domänen überprüfen:

```
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. Die Kommunikation schlägt fehl, wenn das sendende oder empfangende Zertifikat nicht ordnungsgemäß konfiguriert ist oder abgelaufen ist.

3. Die SEG muss überprüfen, ob die geeigneten Zwischen- und Stammzertifikate für das Ziel in den Zertifizierungsstellenlisten enthalten sind.

4. Einfache Telnet-Tests von der SEG-CLI zur Verifizierung des DNS-TXT-Datensatzes und eines grundlegenden Reaktionstests für den Policy-Webserver.

- DNS-Abfrage aus CLI > dig _mta-sts.domain.com txt:

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

- Telnet, um die Erreichbarkeit der grundlegenden Webserver über CLI > Telnet mta-sts.domain.com 443 zu überprüfen:
- Verwenden Sie einen normalen Webbrowser, um die MTA-STS-Richtlinie anzuzeigen.
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

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

Zugehörige Informationen

- Cisco Secure Email Gateway Launch-Website für Support-Leitfäden

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.