Configurare il servizio MTA-STS in uscita del gateway di posta elettronica sicuro

Sommario

Introduzione

In questo documento viene descritto come configurare il servizio Agente di trasferimento posta in uscita SEG (Secure Email Gateway) - Strict Transport Security (MTA-STS).

Prerequisiti

Requisiti

Conoscenze generali delle impostazioni generali e della configurazione di Cisco Secure Email Gateway (SEG).

Componenti usati

L'installazione richiede:

- Cisco Secure Email Gateway (SEG) AsyncOS 16.0 o versione successiva.
- Profili di controllo di destinazione.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Mail Transfer Agent - Strict Transport Security (MTA-STS) è un protocollo che impone l'uso di connessioni TLS sicure con un livello di protezione sicuro aggiunto. MTA-STS aiuta a prevenire gli attacchi man-in-the-middle e le intercettazioni assicurando che le e-mail vengano inviate su canali protetti e crittografati.

SEG AsyncOS 16 e versioni successive può eseguire il recapito dei messaggi MTA-STS in uscita ai domini di ricezione configurati per MTA-STS.

Quando è abilitato, SEG controlla i profili di controllo di destinazione per individuare le impostazioni MTA-STS. Il SEG avvia il processo MTA-STS per recuperare, convalidare e applicare il record e il criterio definiti, garantendo che la connessione all'MTA ricevente sia protetta su TLSv1.2 o versioni successive.

I proprietari del dominio ricevente sono responsabili della creazione, della pubblicazione e della gestione del record DNS e del criterio MTA-STS.

Funzionamento di MTA-STS per SEG

- Il dominio ricevente mantiene il criterio MTA-STS e il record di testo DNS MTA-STS.
- L'MTA del dominio di invio deve essere in grado di risolvere e di agire in base al criterio MTA-STS del dominio di destinazione.

Il proprietario del dominio di posta elettronica di ricezione pubblica un record di testo MTA-STS tramite DNS come descritto di seguito:

- Il record di testo attiva il SEG per controllare il criterio MTA-STS ospitato in un server Web abilitato per HTTPS.
- Il criterio specifica i parametri per la comunicazione al dominio.
    - Contiene gli host MTA-STS MX da ricevere.
    - La modalità è definita come modalità di prova o modalità di applicazione
    - TLSv1.2 o superiore.

- MTA-STS utilizza i record TXT DNS per l'individuazione dei criteri. Recupera il criterio MTA-STS da un host HTTPS.
- Durante l'handshake TLS, avviato per recuperare un criterio nuovo o aggiornato dall'host criteri, il server HTTPS deve presentare un certificato X.509 valido per l'ID DNS "MTA-STS".

Aspetti del dominio di posta elettronica di invio:

- Quando un SEG (MTA di invio) invia un messaggio di posta elettronica a un dominio MTA-STS, verifica innanzitutto la presenza del criterio MTA-STS del dominio del destinatario.
- Se il criterio è configurato con la modalità di imposizione, il server e-mail di invio tenta di stabilire una connessione protetta e crittografata al server e-mail ricevente (MTA ricevente). Se non è possibile stabilire una connessione protetta (ad esempio, se il certificato TLS non è valido o se la connessione viene declassata a un protocollo non protetto), il messaggio di

posta elettronica non viene recapitato e il mittente viene informato dell'errore.

RFC 8461

Configurazione

Durante l'installazione sono consigliate azioni preliminari:

1. Verificare che il dominio di destinazione disponga di un record DNS MTA-STS e di un record dei criteri configurati correttamente, prima di configurare il profilo di controllo della destinazione SEG.

- Questa operazione viene eseguita in modo più efficiente accedendo alle pagine Web del controllo MTA-STS.
  - Ricerca Google "verifica dominio MTA-STS"
  - Scegli un sito Web di verifica dai risultati della ricerca.
  - Immettere il dominio di destinazione.
- Configurare i domini solo dopo il completamento della verifica.

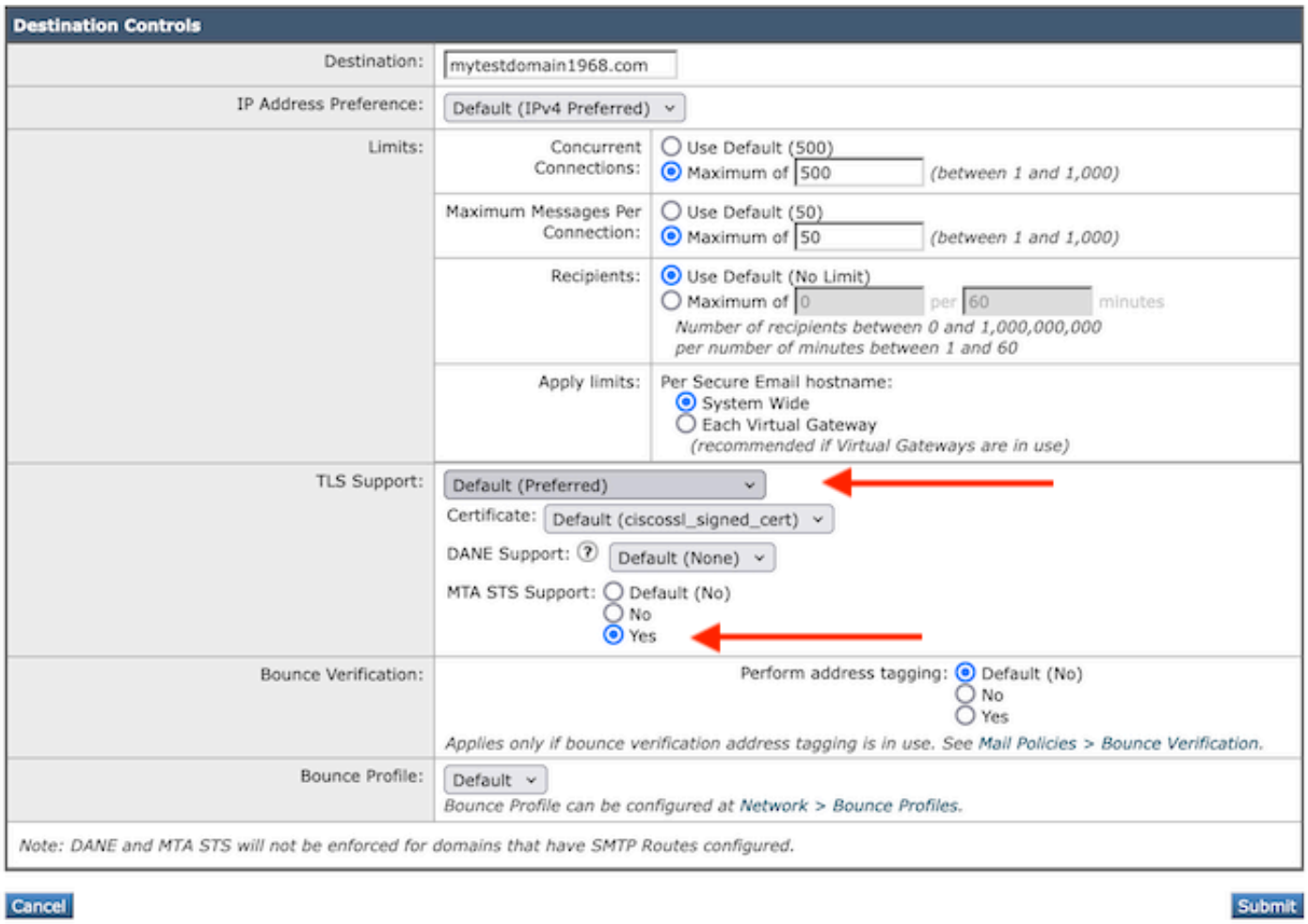
2. Non utilizzare MTA-STS nel criterio predefinito dei controlli di destinazione.

- Ogni profilo di controllo della destinazione configurato per l'utilizzo di MTA-STS aggiunge un carico minimo al SEG. Se per i criteri di controllo di destinazione predefiniti è stato configurato il servizio MTA-STS, senza verificare il dominio, il problema potrebbe riguardare il servizio SEG.

Configurazione WebUI

- Passare a Policy di posta > Pagina Controlli di destinazione.
- Selezionare Aggiungi controlli destinazione o modificare un profilo di controllo destinazione esistente.
  - Le impostazioni del supporto TLS consentono qualsiasi impostazione eccetto None, che supporta varie opzioni di supporto TLS.
  - Il sottomenu Opzioni di supporto DANE include Obbligatorio, Opportunistico o Nessuno.
  - Impostazione supporto MTA-STS = Sì
- Selezionare Sottometti seguito da Conferma per applicare le modifiche.

Nota: Se l'agente di trasferimento messaggi ricevente risiede in un ambiente host come Gsuite o O365, configurare il controllo della destinazione TLS su TLS Required-Verify Hosted Domains.



Profilo di controllo destinazione

Note sull'interoperabilità:

Il supporto DANE ha la precedenza sul servizio token di sicurezza MTA e potrebbe influire sulle azioni intraprese:

- Se DANE ha esito positivo, MTA-STS viene ignorato e la posta viene recapitata.
- Se l'operazione DANE obbligatoria non riesce, la posta non viene recapitata.
- Se DANE Opportunistic non riesce e MTA-STS viene ignorato a causa di errori di configurazione, SEG tenta di eseguire il recapito utilizzando l'impostazione TLS configurata.
- MTA-STS non viene applicato se per il dominio è configurata una route SMTP.

Configurazione dalla CLI

- destconfig
  - nuovo/modifica
    - Immettere le scelte preferite fino a quando non viene visualizzata la voce di menu Opzioni TLS.
    - Le opzioni 2-6 per TLS supportano MTA-STS.

Applicare un'impostazione TLS specifica per questo dominio? [N]> s

Utilizzare il supporto TLS?

1. No
2. Preferenziale
3. Obbligatorio
4. Preferito - Verifica
5. Obbligatorio - Verifica
6. Obbligatorio - Verifica domini ospitati
[2]>2

Si è scelto di abilitare TLS. Utilizzare il comando certconfig per verificare che sia configurato un certificato valido.
Configurare il supporto DANE? [N]>

Configurare il supporto del servizio token di sicurezza MTA? [N]> s

Utilizzare il supporto MTA STS?
1. Disattivato
2. Il
[1]> 2

Il servizio token di sicurezza MTA non viene applicato per i domini con route SMTP configurate:

1. Completare le altre opzioni per completare il profilo di controllo della destinazione specifico.
2. Applicate le modifiche utilizzando Sottometti (Submit) > Conferma (Commit).

Verifica

mail_logs livello informazioni:

```
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
```

mail_logs livello di debug:

```
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
```

Ricezione di TLS supportate da SEG v1.3:

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

mar 24 set 09:13:52 2024 Debug: Query DNS: Q(_mta-sts.domain.com, 'TXT')
mar 24 set 09:13:52 2024 Debug: Query DNS: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
mar 24 set 09:13:52 2024 Debug: Query DNS: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
mar 24 set 09:13:52 2024 Debug: Cache DNS (_mta-sts.domain.com, TXT, [(13136652570158050 8L, 0, 'non sicuro', ('v=STSv1; id=12345678598Z;',)])
mar 24 set 09:13:52 2024 Info: Recupero del record TXT MTA-STS per il dominio completato (domain.com)
mar 24 set 09:13:52 2024 Debug: Recupero del criterio MTA-STS per il dominio(domain.com)
mar 24 set 09:13:52 2024 Debug: Richiesta recupero criteri MTA-STS tramite proxy
mar 24 set 09:13:52 2024 Debug: Richiesta di recupero del criterio STS non riuscita a causa di un timeout di connessione., per il dominio domain.com
mar 24 set 09:13:52 2024 Info: Errore durante il recupero del criterio MTA-STS per il dominio(domain.com)

—

Thu Sep 19 13:04:50 2024 Info: Recupero del record TXT MTA-STS per il dominio completato (domain.com)
Thu Sep 19 13:04:50 2024 Debug: Recupero del criterio MTA-STS per il dominio(domain.com)
Thu Sep 19 13:04:50 2024 Debug: Richiesta recupero criteri MTA-STS tramite proxy
Thu Sep 19 13:04:50 2024 Debug: Richiesta di recupero del criterio STS non riuscita a causa di un timeout di connessione., per il dominio domain.com
Thu Sep 19 13:04:50 2024 Info: Errore durante il recupero del criterio MTA-STS per il dominio(domain.com)

Thu Sep 19 13:04:50 2024 Info: MID 5411 in coda per la consegna

Risoluzione dei problemi

1. Se SEG non riesce a eseguire il recapito con l'errore "il certificato peer non corrisponde a domain.com".

Ciò indica che la destinazione è un servizio ospitato come G Suite o M365. Modificare l'impostazione TLS profilo controlli destinazione > TLS richiesto - Verifica domini ospitati:

```
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 comunicazione non riesce se i certificati di invio o di ricezione non sono configurati correttamente o sono scaduti.

3. Il SEG deve verificare che i certificati intermedi e i certificati radice di destinazione siano corretti negli elenchi dell'autorità di certificazione.

4. Test Telnet semplici dalla CLI SEG per verificare il record di testo DNS e un test di risposta di base al server Web dei criteri.

- Query DNS da cli > dig _mta-sts.domain.com txt:

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

- Telnet per verificare la raggiungibilità del server Web di base da cli > telnet mta-sts.domain.com 443:
- Utilizzare un normale browser Web per visualizzare il criterio MTA-STS.
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

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

Informazioni correlate

- Pagina di avvio di Cisco Secure Email Gateway per il supporto delle guide

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).