Configurer la passerelle de messagerie sécurisée pour les messages sortants MTA-STS

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Aperçu](#)

- [Fonctionnement de MTA-STS pour SEG](#)

[Configurer](#)

- [Configuration WebUI](#)
- [Configuration CLI](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes pour configurer l'agent de transfert de courrier sortant Secure Email Gateway (SEG) - Strict Transport Security (MTA-STS).

Conditions préalables

Exigences

Connaissance générale des paramètres généraux et de la configuration de Cisco Secure Email Gateway (SEG).

Composants utilisés

Cette configuration nécessite :

- Cisco Secure Email Gateway (SEG) AsyncOS 16.0 ou version ultérieure.
- Profils de contrôle de destination.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

MTA-STS (Mail Transfer Agent - Strict Transport Security) est un protocole qui impose l'utilisation de connexions TLS sécurisées avec une couche de protection sécurisée supplémentaire. MTA-STS permet d'empêcher les attaques de l'homme du milieu et les écoutes en garantissant que les e-mails sont envoyés sur des canaux cryptés sécurisés.

SEG AsyncOS 16 et versions ultérieures peuvent effectuer la remise de messages MTA-STS sortants aux domaines récepteurs configurés MTA-STS.

Lorsque cette option est activée, le SEG recherche les paramètres MTA-STS dans les profils de contrôle de destination. Le SEG lance le processus MTA-STS pour récupérer, valider et appliquer l'enregistrement et la politique définis, en s'assurant que la connexion au MTA de réception est sécurisée sur TLSv1.2 ou supérieur.

Les propriétaires du domaine récepteur sont responsables de la création, de la publication et de la maintenance de l'enregistrement DNS et de la stratégie MTA-STS.

Fonctionnement de MTA-STS pour SEG

- Le domaine récepteur gère la stratégie MTA-STS et l'enregistrement de texte DNS MTA-STS.
- Le MTA du domaine expéditeur doit être MTA-STS capable de résoudre et d'agir sur la politique MTA-STS du domaine de destination.

Le propriétaire du domaine de réception des e-mails publie un enregistrement MTA-STS txt via DNS comme décrit ici :

- L'enregistrement de texte déclenche le SEG pour vérifier la stratégie MTA-STS, hébergée sur un serveur Web compatible HTTPS.
- La stratégie spécifie les paramètres de communication avec le domaine.
    - Contient les hôtes MTA-STS MX à recevoir.
    - Le mode est défini comme le mode de test ou le mode d'application
    - TLSv1.2 ou supérieur est requis.

- MTA-STS utilise les enregistrements DNS TXT pour la détection des stratégies. Il récupère la stratégie MTA-STS à partir d'un hôte HTTPS.
- Lors de la connexion TLS, initiée pour récupérer une stratégie nouvelle ou mise à jour à partir de l'hôte de stratégie, le serveur HTTPS doit présenter un certificat X.509 valide pour l'ID DNS « MTA-STS ».

Aspects du domaine de messagerie d'envoi :

- Lorsqu'un SEG (MTA expéditeur) envoie un e-mail à un domaine MTA-STS, il vérifie d'abord la stratégie MTA-STS du domaine destinataire.
- Si la stratégie est configurée avec le mode d'application, le serveur de messagerie expéditeur tente d'établir une connexion sécurisée et chiffrée avec le serveur de messagerie destinataire (MTA destinataire). Si une connexion sécurisée ne peut pas être établie (par exemple, si le certificat TLS n'est pas valide ou si la connexion est rétrogradée à un protocole non sécurisé), l'e-mail ne parvient pas à être remis et l'expéditeur est averti de

l'échec.

RFC8461

Configurer

Des actions préliminaires sont recommandées lors de la configuration :

1. Vérifiez que le domaine de destination dispose d'un enregistrement DNS et d'un enregistrement de stratégie MTA-STS correctement configurés, avant de configurer le profil de contrôle de destination SEG.

- Pour ce faire, accédez plus efficacement aux pages Web du vérificateur MTA-STS.
  - Recherche google "vérifier le domaine MTA-STS"
  - Sélectionnez un site Web de vérification dans les résultats de la recherche.
  - Entrez le domaine de destination.
- Ne configurez les domaines qu'une fois la vérification terminée.

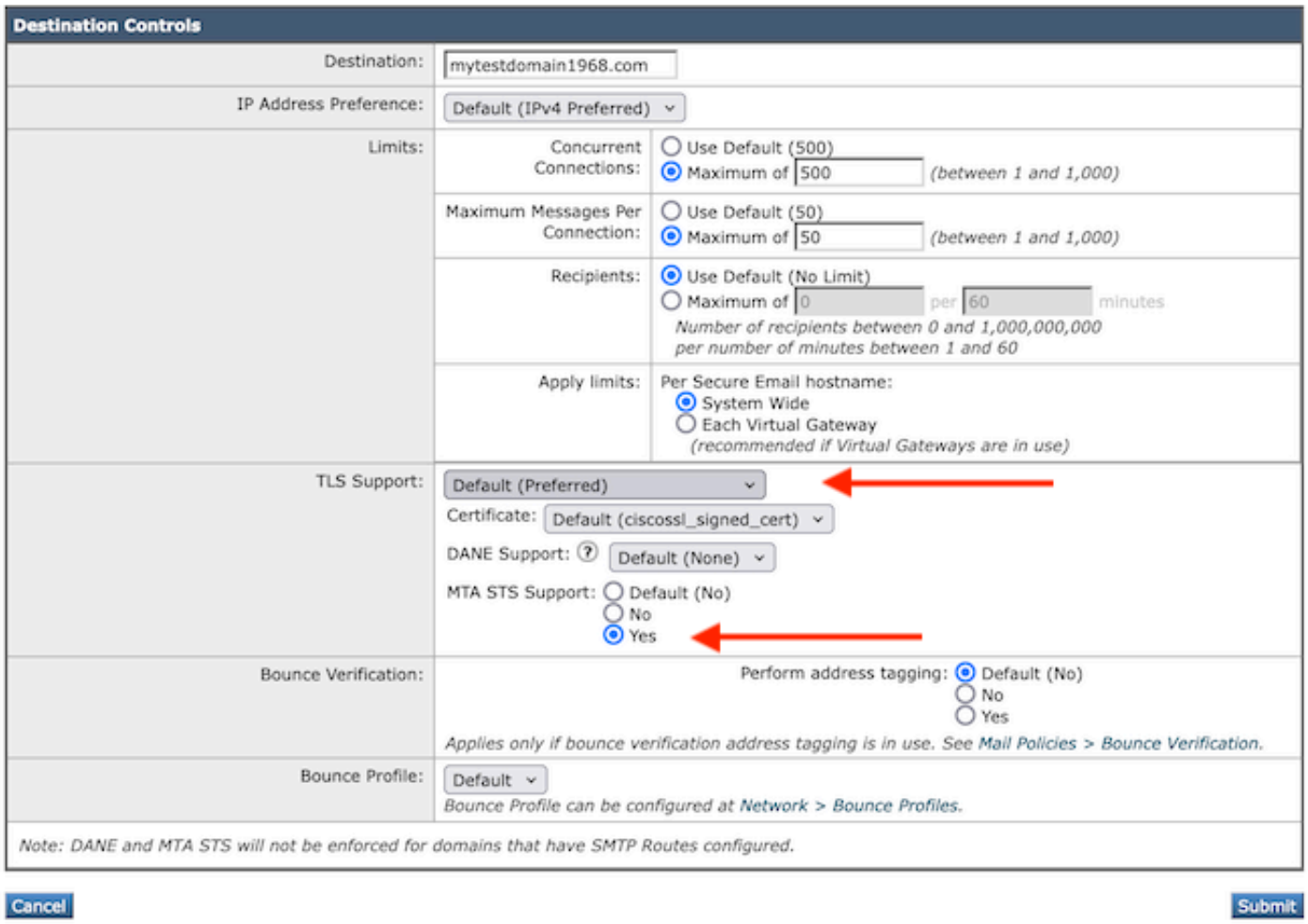
2. N'utilisez pas MTA-STS sur la stratégie par défaut des contrôles de destination.

- Chaque profil de contrôle de la destination configuré pour utiliser MTA-STS ajoute une petite charge au SEG. Si la stratégie de contrôle de la destination par défaut avait MTA-STS configuré, sans vérifier le domaine, cela pourrait avoir un impact sur le service SEG.

Configuration WebUI

- Accédez à Politiques de messagerie > Page Contrôles de destination.
- Sélectionnez Ajouter des contrôles de destination ou modifier un profil de contrôle de destination existant.
  - Les paramètres de prise en charge TLS autorisent tous les paramètres sauf None, acceptant diverses options de prise en charge TLS.
  - Le sous-menu Options de support DANE comprend Obligatoire, Opportuniste ou Aucune.
  - Paramètre de prise en charge MTA-STS = Oui
- Sélectionnez Submit, puis Commit pour appliquer les modifications.

Remarque : Si le MTA de réception réside dans un environnement hébergé tel que Gsuite ou O365, configurez le TLS des contrôles de destination sur TLS Required-Verify Hosted Domains.



Profil de contrôle de destination

Avertissements d'interopérabilité :

L'assistance DANE a priorité sur MTA STS et peut affecter les actions entreprises :

- Si DANE réussit, MTA-STS est ignoré et le courrier est remis.
- Si le DANE obligatoire échoue, le courrier n'est pas remis.
- Si DANE Opportunistic échoue et que MTA-STS est ignoré en raison d'erreurs de configuration, le SEG tente d'effectuer la livraison en utilisant le paramètre TLS configuré.
- MTA-STS ne doit pas être appliqué si une route SMTP est configurée pour le domaine.

Configuration CLI

- destconfig
  - nouveau/modifier
    - Saisissez les choix préférés jusqu'à ce que l'option de menu Options TLS soit affichée.
    - Les options 2 à 6 pour TLS prennent en charge MTA-STS.

Voulez-vous appliquer un paramètre TLS spécifique pour ce domaine ? [N]> o

Voulez-vous utiliser la prise en charge TLS ?
1. Non

2. Préféré
3. Obligatoire
4. Préféré - Vérifier
5. Obligatoire - Vérifier
6. Obligatoire - Vérifier les domaines hébergés
[2]>2

Vous avez choisi d'activer TLS. Utilisez la commande certconfig pour vous assurer qu'un certificat valide est configuré.
Souhaitez-vous configurer l'assistance DANE ? [N]>

Voulez-vous configurer la prise en charge MTA STS ? [N]> o

Voulez-vous utiliser la prise en charge MTA STS ?
1. Désactivé
2. Le
[1]> 2

MTA STS n'est pas appliqué aux domaines pour lesquels des routes SMTP sont configurées :

1. Complétez les options restantes pour terminer le profil de contrôle de la destination spécifique.
2. Appliquez les modifications en utilisant Soumettre > Valider.

Vérifier

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
```

Réception de TLS v1.3 pris en charge par SEG :

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

Mar Sep 24 09:13:52 2024 Débogage : Requête DNS : Q(_mta-sts.domain.com, 'TXT')
Mar Sep 24 09:13:52 2024 Débogage : Requête DNS : QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
Mar Sep 24 09:13:52 2024 Débogage : Requête DNS : QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Mar Sep 24 09:13:52 2024 Débogage : Encadrement DNS (_mta-sts.domain.com, TXT, [(131366525701580508L, 0, 'non sécurisé', ('v=STSv1 ; id=12345678598Z ;',))])
Mar Sep 24 09:13:52 2024 Info : Enregistrement MTA-STS TXT récupéré pour le domaine (domain.com)
Mar Sep 24 09:13:52 2024 Débogage : Récupérer la stratégie MTA-STS pour le domaine (domain.com)
Mar Sep 24 09:13:52 2024 Débogage : Demande de récupération de stratégie MTA-STS via le proxy
Mar Sep 24 09:13:52 2024 Débogage : La demande de récupération de la stratégie STS a échoué en raison d'un délai d'attente de connexion., pour le domaine domain.com
Mar Sep 24 09:13:52 2024 Info : Échec rencontré lors de l'extraction de la stratégie MTA-STS pour le domaine (domain.com)

Jeu Sept 19 13:04:50 2024 Info : Enregistrement MTA-STS TXT récupéré pour le domaine (domain.com)
Jeu Sept 19 13:04:50 2024 Débogage : Récupérer la stratégie MTA-STS pour le domaine (domain.com)
Jeu Sept 19 13:04:50 2024 Débogage : Demande de récupération de stratégie MTA-STS via le proxy
Jeu Sept 19 13:04:50 2024 Débogage : La demande de récupération de la stratégie STS a échoué en raison d'un délai d'attente de connexion., pour le domaine domain.com
Jeu Sept 19 13:04:50 2024 Info : Échec rencontré lors de l'extraction de la stratégie MTA-STS pour le domaine (domain.com)

Jeu Sept 19 13:04:50 2024 Info : MID 5411 en attente de livraison

Dépannage

1. Si SEG ne parvient pas à remettre avec l'erreur "le certificat de l'homologue ne correspond pas

au domaine domain.com".

Cela indique que la destination est un service hébergé tel que G Suite ou M365. Modifiez le paramètre TLS du profil des contrôles de destination > 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. La communication échoue si les certificats d'envoi ou de réception ne sont pas correctement configurés ou ont expiré.

3. Le SEG doit vérifier que les certificats intermédiaires et racine de destination appropriés figurent dans les listes des autorités de certification.

4. Tests Telnet simples à partir de l'interface de ligne de commande SEG pour vérifier l'enregistrement de texte DNS et un test de réponse de base au serveur Web Policy.

- Requête DNS à partir de cli > dig _mta-sts.domain.com txt :

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

- Telnet pour vérifier l'accessibilité du serveur Web de base à partir de cli > telnet mta-sts.domain.com 443 :
- Utilisez un navigateur Web standard pour afficher la politique MTA-STS.
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

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

Informations connexes

- Guides d'assistance de la page de lancement de Cisco Secure Email Gateway

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.