Guide complet d'installation pour le TLS sur l'ESA

Contenu

Introduction

Ce document décrit comment créer un certificat pour l'usage avec le Transport Layer Security (TLS), lancer le TLS d'arrivée et sortant, et dépanner les questions de base de TLS sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

L'implémentation de TLS sur l'ESA fournit l'intimité pour la transmission point par point des emails par le cryptage. Il permet à un administrateur pour importer un certificat et une clé privée d'un service d'Autorité de certification (CA), ou utilise un certificat auto-signé.

Cisco AsyncOS pour la sécurité du courrier électronique prend en charge l'extension *STARTTLS au* Protocole SMTP (Simple Mail Transfer Protocol) (*SMTP sécurisé au-dessus de TLS*).

> **Conseil** : Pour plus d'informations sur le TLS, référez-vous à RFC 3207.

> **Note**: Ce document décrit comment installer des Certificats au niveau de batterie avec l'utilisation de la *fonctionnalité de gestion centralisée* sur l'ESA. Les Certificats peuvent être appliqués au niveau d'ordinateur aussi bien ; cependant, si l'ordinateur est jamais retiré de la batterie et de retour alors ajouté, les Certificats niveau de l'ordinateur seront perdus.

Présentation fonctionnelle et conditions requises

Un administrateur pourrait désirer créer un certificat auto-signé sur l'appliance pour l'un de ces raisons :

- Afin de chiffrer les conversations de SMTP avec d'autres MTA qui utilisent le TLS (les conversations d'arrivée et sortantes)
- Afin d'activer le service HTTPS sur l'appliance pour l'accès au GUI par l'intermédiaire de HTTPS
- Pour l'usage comme certificat client pour des protocoles LDAP (LDAP), si le serveur LDAP a besoin d'un certificat client
- Afin de permettre la communication protégée entre l'appliance et le gestionnaire d'entreprise de Rivest-Shamir-Addleman (RSA) pour la protection de perte de données (DLP)
- Afin de permettre la communication protégée entre l'appliance et Cisco a avancé l'appliance de grille de menace de protection de malware (AMP)

L'ESA est livré préconfiguré avec un certificat de démonstration qui peut être utilisé afin d'établir des connexions de TLS.

> **Attention** : Tandis que le certificat de démonstration est suffisant pour l'établissement d'une connexion sécurisée de TLS, rendez-vous compte qu'elle ne peut pas offrir une connexion vérifiable.

Cisco recommande que vous obteniez un X.509, ou certificat de l'email amélioré par intimité (PEM) d'un CA. Ceci pourrait également désigné sous le nom d'un certificat d'*Apache*. Le certificat d'un CA est desirable au-dessus du certificat auto-signé parce qu'un certificat auto-signé est semblable au certificat précédemment mentionné de démonstration, qui ne peut pas offrir une connexion vérifiable.

> **Note**: Le format de certificat PEM est encore défini dans RFC 1421 à RFC 1424. Le PEM est un format de conteneur qui peut inclure seulement le certificat public (comme avec Apache installe et fichier */etc/ssl/certs de* certificat de CA) ou une chaîne de certificat entière, pour inclure la clé publique, la clé privée, et les certificats racine. *Le PEM de* nom est d'une méthode défectueuse pour l'email sécurisé, mais le format de conteneur qu'il a utilisé est toujours en activité et est une traduction base-64 des clés X.509 ASN.1.

Apportez votre propre certificat

L'option d'importer votre propre certificat est disponible sur l'ESA ; cependant, la condition requise est que le certificat soit dans le format *PKCS#12*. Ce format inclut la clé privée. Les administrateurs n'ont pas souvent des Certificats qui sont disponibles dans ce format. Pour cette raison, Cisco recommande que vous génériez le certificat sur l'ESA et le fassiez signer correctement par un CA.

Mettez à jour un certificat valable

Si un certificat qui existe déjà a expiré, ignorez la section Auto-*signée la déployant de Certificats de* ces document et re-signe le certificat qui existe.

> **Conseil** : Référez-vous au renouveler un certificat sur un document Cisco d'appareils de sécurité du courrier électronique pour plus de détails.

Déployez les Certificats Auto-signés

Cette section décrit comment générer une demande auto-signée de certificat et de signature de certificat (CSR), fournir le certificat auto-signé à un CA pour signer, télécharger le certificat signé à l'ESA, spécifier le certificat pour l'usage avec les services ESA, et sauvegarder la configuration et les certificats d'appareils.

Générez un certificat et un CSR Auto-signés

Afin de créer un certificat auto-signé par l'intermédiaire du CLI, sélectionnez la commande de **certconfig**.

Terminez-vous ces étapes afin de créer un certificat auto-signé du GUI :

1. Naviguez vers le **réseau > les Certificats > ajoutent le certificat du** GUI d'appareils.

2. Cliquez sur le menu déroulant de **certificat Auto-signé par création**.

   Quand vous créez le certificat, assurez-vous que le *nom commun* apparie l'adresse Internet de l'interface de écoute, ou qu'il apparie l'adresse Internet de l'interface de la livraison.

   L'interface de *écoute* est l'interface qui est liée à l'auditeur qui est configuré sous le **réseau > les auditeurs**.

   L'interface de la *livraison* est automatiquement sélectionnée, à moins qu'explicitement configuré du CLI avec la commande de **deliveryconfig**.
3. Pour une connexion entrante vérifiable, validez que ces trois éléments s'assortissent :

   MX Record (adresse Internet de Système de noms de domaine (DNS))

   Nom commun

   Adresse Internet d'interface

   Note: L'adresse Internet de système n'affecte pas les connexions de TLS en vue d'être vérifiable. L'adresse Internet de système est affichée dans l'angle supérieur droit du GUI d'appareils, ou de la sortie de commande de **sethostname** CLI.

   Attention : Souvenez-vous **pour soumettre** et **commettre** vos modifications avant que vous exportiez le CSR. Si ces étapes ne sont pas terminées, le nouveau certificat ne sera pas commis à la configuration d'appareils, et le certificat signé du CA ne peut pas signer, ou soit appliqué à, un certificat qui existe déjà.

Fournissez le certificat Auto-signé à un CA

Terminez-vous ces étapes afin de soumettre le certificat auto-signé à un CA pour la signature :

1. Sauvegardez le CSR à un ordinateur local dans le format PEM (**réseau > Certificats > *demande de signature de certificat de* nom > de *téléchargement de* certificat**).

2. Envoyez le certificat généré à un CA identifié pour la signature.

3. Demandez par X.509/PEM/Apache un certificat formaté, aussi bien que le certificat intermédiaire.

Le CA génère alors un certificat dans le format PEM.

Note: Pour une liste de fournisseurs CA, référez-vous à l'article de Wikipedia d'autorité de certification.

Téléchargez le certificat signé à l'ESA

Après que le CA renvoie le certificat public de confiance qui est signé par une clé privée, vous devez télécharger le certificat signé à l'ESA. Le certificat peut alors être utilisé avec un auditeur public ou privé, un service de l'interface IP HTTPS, l'interface de LDAP, ou toutes les connexions sortantes de TLS aux domaines de destination.

Terminez-vous ces étapes afin de télécharger le certificat signé à l'ESA :

1. Assurez-vous que le certificat public de confiance qui est format reçu PEM d'utilisations, ou un format qui peut être converti en PEM avant que vous le téléchargiez à l'appliance. **Conseil** : Vous pouvez employer l'OpenSSLtoolkit, un programme de logiciel gratuit, afin de convertir le format.
2. Téléchargez le certificat signé :

   Naviguez vers le **réseau > les Certificats**.

   Cliquez sur le nom du certificat qui a été envoyé au CA pour la signature.

   Entrez dans le chemin au fichier sur le volume d'ordinateur local ou de réseau.

   Note: Quand vous téléchargez le nouveau certificat, il remplace le certificat valable. Un certificat intermédiaire qui est lié au certificat auto-signé peut également être téléchargé.

   Attention : Souvenez-vous **pour soumettre** et **commettre les** modifications après que vous téléchargiez le certificat signé.

Spécifiez le certificat pour l'usage avec des services ESA

Maintenant que le certificat est créé, signé, et téléchargé à l'ESA, il peut être utilisé pour les services qui exigent l'utilisation de certificat.

TLS d'arrivée

Terminez-vous ces étapes afin d'utiliser le certificat pour les services d'arrivée de TLS :

1. Naviguez vers le **réseau > les auditeurs**.
2. Cliquez sur le nom d'auditeur.
3. Sélectionnez le nom de certificat du menu déroulant de *certificat*.
4. Cliquez sur **Submit**.
5. Répétez les étapes 1 à 4 comme nécessaire pour tous les auditeurs supplémentaires.
6. **Commettez les** modifications.

TLS sortant

Terminez-vous ces étapes afin d'utiliser le certificat pour les services sortants de TLS :

1. Naviguez **pour envoyer par mail des stratégies > des contrôles de destination**.
2. Cliquez sur Edit les **paramètres généraux…** dans la section de *paramètres généraux*.
3. Sélectionnez le nom de certificat du menu déroulant de *certificat*.
4. Cliquez sur **Submit**.
5. **Commettez les** modifications.

HTTPS

Terminez-vous ces étapes afin d'utiliser le certificat pour les services HTTPS :

1. Naviguez vers le **réseau > les interfaces IP**.
2. Cliquez sur le nom d'interface.
3. Sélectionnez le nom de certificat du menu déroulant de *certificat HTTPS*.
4. Cliquez sur **Submit**.
5. Répétez les étapes 1 à 4 comme nécessaire pour toutes les interfaces supplémentaires.
6. **Commettez les** modifications.

LDAP

Terminez-vous ces étapes afin d'utiliser le certificat pour les LDAP :

1. Naviguez vers l'**administration système > le LDAP**.
2. Cliquez sur Edit les **configurations…** dans la section de *paramètres généraux de LDAP*.
3. Sélectionnez le nom de certificat du menu déroulant de *certificat*.
4. Cliquez sur **Submit**.
5. **Commettez les** modifications.

Filtrage des URL

Terminez-vous ces étapes afin d'utiliser le certificat pour le Filtrage URL :

1. Sélectionnez la commande de **websecurityconfig** dans le CLI.

2. Poursuivez par les invites de commande. Assurez-vous que vous sélectionnez **Y** quand vous atteignez cette demande :

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. Sélectionnez le nombre qui est associé avec le certificat.

4. Sélectionnez la commande de **validation** afin de commettre les modifications de configuration.

Sauvegardez la configuration et les certificats d'appareils

Assurez-vous que la configuration d'appareils est enregistrée à ce moment. La configuration d'appareils contient le travail terminé de certificat qui a été appliqué par l'intermédiaire des processus précédemment décrits.

Terminez-vous ces étapes afin de sauvegarder le fichier de configuration d'appareils :

1. Naviguez vers l'**administration système > le fichier de configuration > le fichier téléchargé vers l'ordinateur local à visualiser ou sauvegarder**.

2. Exportez le certificat :

   Naviguez vers le **réseau > les Certificats**.

   Certificat d'exportation de clic.

   Sélectionnez le certificat pour exporter.

   Écrivez le nom du fichier du certificat.

   Entrez un mot de passe pour le fichier du certificat.

   Exportation de clic.

   Sauvegardez le fichier à des gens du pays ou à un ordinateur du réseau.

   Des Certificats supplémentaires peuvent être exportés à ce moment, ou l'**annulation de** clic afin de retourner au **réseau > délivre un certificat l'**emplacement.

   Note: Ce processus enregistre le certificat dans le format PKCS#12, qui crée et enregistre le fichier avec la protection par mot de passe.

Lancez le TLS d'arrivée

Afin de lancer le TLS pour toutes les sessions d'arrivée, connectez au GUI de Web, choisissez les **stratégies de messagerie > les stratégies de flux de courrier** pour l'auditeur d'arrivée configuré, et puis terminez-vous ces étapes :

1. Choisissez un auditeur pour lequel les stratégies doivent être modifiées.

2. Cliquez sur le lien pour le nom de la stratégie afin de l'éditer.

3. Dans les *fonctionnalités de sécurité* sectionnez, choisissez un de ces des options de *cryptage et d'authentification* afin de placer le niveau du TLS qui est exigé pour ces auditeur et stratégie de flux de courrier :

   Outre de – Quand cette option est choisie, le TLS n'est pas utilisé.

   Préféré – Quand cette option est choisie, le TLS peut négocier du distant MTA à l'ESA. Cependant, si le distant MTA ne négocie pas (avant la réception d'une réponse *220*), la transaction de SMTP continue *en clair* (non chiffré). Aucune tentative n'est faite afin de vérifier si le certificat provient d'une autorité de certification de confiance. Si une erreur se produit après que la réponse 220 soit reçue, alors la transaction de SMTP ne retombe pas au texte clair.

   Requis – Quand cette option est choisie, le TLS peut être négocié du distant MTA à l'ESA. Aucune tentative n'est faite afin de vérifier le certificat du domaine. Si la négociation échoue, aucun email n'est envoyé par la connexion. Si la négociation réussit, alors la messagerie est fournie par l'intermédiaire d'une session chiffrée.
4. Cliquez sur **Submit**.

5. Cliquez sur le bouton de **modifications de validation**. Vous pouvez ajouter un commentaire facultatif à ce moment, si désiré.

6. **Modifications de validation de** clic afin de sauvegarder les modifications.

La stratégie de flux de courrier pour l'auditeur est maintenant mise à jour avec les configurations de TLS que vous avez choisies.

Terminez-vous ces étapes afin de lancer le TLS pour les sessions d'arrivée qui arrivent d'un ensemble choisi de domaines :

1. Connectez au GUI de Web et choisissez les **stratégies de messagerie > l'aperçu de CHAPEAU**.

2. Ajoutez les expéditeurs au groupe approprié d'expéditeur.

3. Éditez les configurations de TLS de la stratégie de flux de courrier qui est associée avec le groupe d'expéditeur que vous avez modifié dans l'étape précédente.

4. Cliquez sur **Submit**.

5. Cliquez sur le bouton de **modifications de validation**. Vous pouvez ajouter un commentaire facultatif à ce moment, si désiré.

6. **Modifications de validation de** clic afin de sauvegarder les modifications.

La stratégie de flux de courrier pour le groupe d'expéditeur est maintenant mise à jour avec les

configurations de TLS que vous avez choisies.

> **Conseil** : Référez-vous à l'article suivant pour plus d'informations sur la façon dont l'ESA manipule la vérification de TLS : Quel est l'algorithme pour la vérification de certificat sur l'ESA ?

Lancez le TLS sortant

Afin de lancer le TLS pour des sessions sortantes, connectez au GUI de Web, choisissez les **stratégies de messagerie > les contrôles de destination**, et puis terminez-vous ces étapes :

1. Cliquez sur Add la **destination….**

2. Ajoutez le domaine de destination (tel que *domain.com*).

3. Dans la section de *support de TLS*, cliquez sur le menu déroulant et choisissez une de ces options afin d'activer le type de TLS qui doit être configuré :

   Aucun – Quand cette option est choisie, le TLS n'est pas négocié pour les connexions sortantes de l'interface au MTA pour le domaine.

   Préféré – Quand cette option est choisie, le TLS est négocié de l'interface ESA au MTA pour le domaine. Cependant, si la négociation de TLS échoue (avant la réception d'une réponse 220), la transaction de SMTP continue *en clair* (non chiffré). Aucune tentative n'est faite afin de vérifier si le certificat provient d'un CA de confiance. Si une erreur se produit après que la réponse 220 soit reçue, alors la transaction de SMTP ne retombe pas au texte clair.

   Requis – Quand cette option est choisie, le TLS est négocié de l'interface ESA au MTA pour le domaine. Aucune tentative n'est faite afin de vérifier le certificat du domaine. Si la négociation échoue, aucun email n'est envoyé par la connexion. Si la négociation réussit, alors la messagerie est fournie par l'intermédiaire d'une session chiffrée.

   Préférer-vérifiez – Quand cette option est choisie, le TLS est négocié de l'ESA au MTA pour le domaine, et des tentatives d'appareils de vérifier le certificat de domaine. Dans ce cas, ces trois résultats sont possibles :

   Le TLS est négocié et le certificat est vérifié. La messagerie est fournie par l'intermédiaire d'une session chiffrée.

   Le TLS est négocié, mais le certificat n'est pas vérifié. La messagerie est fournie par l'intermédiaire d'une session chiffrée.

   Aucun rapport de TLS n'est établi, et le certificat n'est pas vérifié. Le message électronique est fourni en texte brut.**Exiger-vérifiez** – Quand cette option est choisie, le TLS est négocié de l'ESA au MTA pour le domaine, et la vérification du certificat de domaine est exigée. Dans ce cas, ces trois résultats sont possibles :

Une connexion de TLS est négociée, et le certificat est vérifié. Le message électronique est fourni par l'intermédiaire d'une session chiffrée.

Une connexion de TLS est négociée, mais le certificat n'est pas vérifié par un CA de confiance. La messagerie n'est pas fournie.

Une connexion de TLS n'est pas négociée, mais la messagerie n'est pas fournie.

4. Apportez pas plus les modifications qui sont nécessaires les *contrôles de destination* pour le domaine de destination.

5. Cliquez sur **Submit**.

6. Cliquez sur le bouton de **modifications de validation**. Vous pouvez ajouter un commentaire facultatif à ce moment, si désiré.

7. **Modifications de validation de** clic afin de sauvegarder les modifications.

Dépannez

Cette section décrit comment dépanner les questions de base de TLS sur l'ESA.

Certificats intermédiaires

Vous devriez rechercher les Certificats intermédiaires en double, particulièrement quand les certificats valables sont mis à jour au lieu d'une nouvelle création de certificat. Les certificats intermédiaires pourraient avoir changé, ou pourraient avoir été incorrectement enchaînés, et le certificat pourrait avoir téléchargé de plusieurs Certificats intermédiaires. Ceci peut introduire des questions d'enchaînement et de vérification de certificat.

Notifications d'enable pour des pannes requises de connexion de TLS

Vous pouvez configurer l'ESA afin d'envoyer une alerte si la négociation de TLS échoue quand des messages sont fournis à un domaine qui exige une connexion de TLS. Le message d'alerte contient le nom du domaine de destination pour la négociation défectueuse de TLS. L'ESA envoie le message d'alerte à tous les destinataires qui sont placés pour recevoir des alertes d'avertissement de niveau d'importance pour des types d'*alerte système*.

Note: C'est un paramètre général, ainsi il ne peut pas être placé sur une base de par-domaine.

Terminez-vous ces étapes afin d'activer des alertes de connexion de TLS :

1. Naviguez **pour envoyer par mail des stratégies > des contrôles de destination**.

2. Cliquez sur Edit les **paramètres généraux**.

3. Cochez l'**envoi une alerte quand une connexion exigée de TLS échoue** case.

Conseil : Vous pouvez également configurer cette configuration avec le **destconfig >** commande **installée** CLI.

L'ESA également se connecte les exemples pour lesquels le TLS est exigé pour un domaine mais ne pourrait pas être utilisé dans les logs de messagerie d'appareils. Ceci se produit quand l'un de ces conditions sont remplies :

- Le distant MTA ne prend en charge pas ESMTP (par exemple, il n'a pas compris la commande *EHLO de l'*ESA).
- Le distant MTA prend en charge ESMTP, mais la commande *STARTTLS* n'était pas dans la liste d'extensions qu'elle a annoncées dans sa réponse *EHLO*.
- Le distant MTA a annoncé l'extension *STARTTLS* mais a répondu avec une erreur quand l'ESA a envoyé la commande *STARTTLS*.

Localisez les sessions de communication réussies de TLS dans les logs de messagerie

Les connexions de TLS sont enregistrées dans les logs de messagerie, avec d'autres actions significatives qui sont liées aux messages, tels que les actions de filtre, l'antivirus et les verdicts d'anti-Spam, et tentatives de la livraison. S'il y a une connexion réussie de TLS, il y aura une entrée de *succès de* TLS dans les logs de messagerie. De même, le TLS défectueux que la connexion produit TLS *a manqué* entrée. Si un message n'a pas une entrée associée de TLS dans le fichier journal, ce message n'a pas été fourni au-dessus d'une connexion de TLS.

Conseil : Afin de comprendre les logs de messagerie, référez-vous au document Cisco de détermination de disposition de message ESA.

Voici un exemple d'une connexion réussie de TLS du serveur distant (réception) :

```
Wed Jul 20 19:47:40 2005 Info: New smtp ICID 282204970 interface mail.example.com
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 ACCEPT SG None match SBRS None
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 TLS success
Wed Jul 20 19:47:40 2005 Info: Start MID 200257070 ICID 282204970
```

Voici un exemple d'une connexion défectueuse de TLS du serveur distant (réception) :

```
Tue Jun 28 19:08:49 2005 Info: New SMTP ICID 282204971 interface Management
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 ACCEPT SG None match SBRS None
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS failed
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 lost
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS was required but remote host did
not initiate it
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 close
```

Voici un exemple d'une connexion réussie de TLS au serveur distant (la livraison) :

```
Tue Jun 28 19:28:31 2005 Info: New SMTP DCID 834 interface 10.10.10.100 address
```

```
192.168.1.25 port 25
Tue Jun 28 19:28:31 2005 Info: DCID 834 TLS success protocol TLSv1 cipher
DHE-RSA-AES256-SHA
Tue Jun 28 19:28:31 2005 Info: Delivery start DCID 834 MID 1074 to RID [0]
```

Voici un exemple d'une connexion défectueuse de TLS au serveur distant (la livraison) :

```
Fri Jul 22 22:00:05 2005 Info: DCID 2386070 IP 10.3.4.5 TLS failed: STARTTLS
unexpected response
```

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Appliance de Gestion de sécurité du contenu de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems