Contrôlez la négociation de TLS sur la livraison sur l'ESA

Contenu

Introduction

Ce document décrit comment contrôler la négociation de Transport Layer Security (TLS) sur la livraison sur l'appliance de sécurité du courrier électronique (ESA).

Comme défini dans RFC 3207, le « TLS est une extension au service smtp qui permet à un serveur SMTP et à un client pour employer le degré de sécurité de couche transport pour fournir la transmission privée et authentifiée au-dessus de l'Internet. Le TLS est un mécanisme populaire pour améliorer des transmissions de TCP avec l'intimité et l'authentification. »

TLS d'enable sur la livraison

Vous pouvez avoir besoin de STARTTLS pour la livraison d'email aux domaines spécifiques avec l'un ou l'autre une de ces méthodes décrites dans ce document :

- Utilisez la commande de **destconfig** CLI.
- Du GUI choisissez les **stratégies de messagerie** > les **contrôles de destination**.

La destination contrôle la page ou la commande de **destconfig** te permet pour spécifier cinq configurations différentes pour le TLS pour un domaine donné quand vous incluez un domaine. En outre, vous pouvez dicter si la validation du domaine est nécessaire.

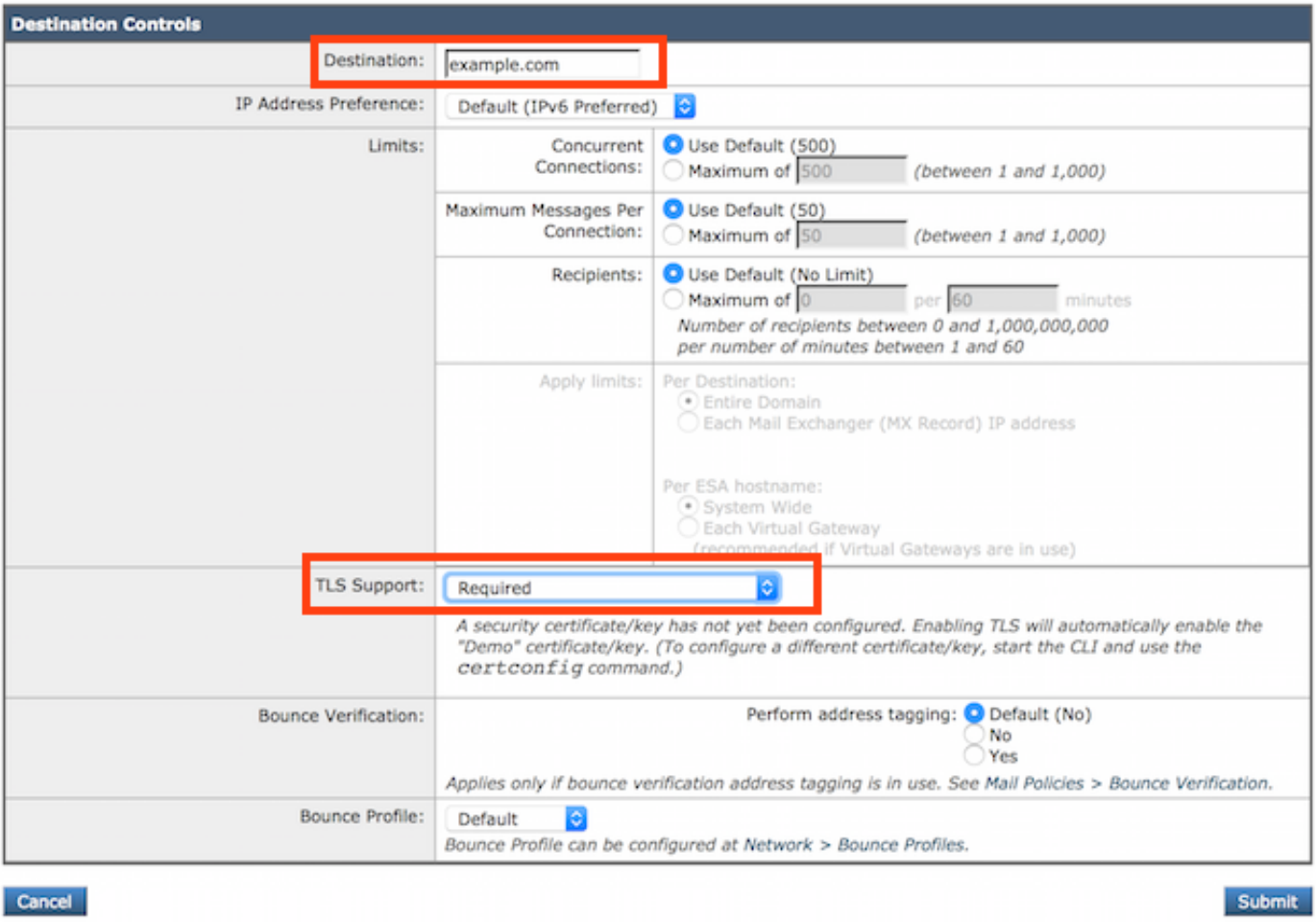
TLS plaçant des définitions

Établissement de TLS	Signification
Par défaut	L'établissement par défaut de TLS qui est placé quand vous utilisez la page de contrôles de destination ou le **destconfig - >** commande secondaire de **par défaut** utilisée pour les connexions sortantes de l'auditeur au message transfer agent (MTA) pour le domaine. La valeur « par défaut » est placée si vous répondez **non à la** question : « Vous souhaitez appliquer le TLS spécifique plaçant pour ce domaine ? »
1. **Non**	Le TLS n'est pas négocié pour les connexions sortantes de l'interface au MTA pour le domaine.
2. **Préféré**	Le TLS est négocié de l'interface ESA au MTA pour le domaine. Cependant, si la négociation de TLS échoue (avant de recevoir une réponse 220), la transaction de SMTP continue « en clair » (non chiffré). Aucune tentative n'est faite pour vérifier si le certificat provient d'une autorité de certification de confiance. Si une erreur se produit après que la

	réponse 220 soit reçue, la transaction de SMTP ne retombe pas au texte clair.
3. **Requis**	Le TLS est négocié de l'interface ESA au MTA pour le domaine. Aucune tentative n'est faite pour vérifier le certificat du domaine. Si la négociation échoue, aucun email n'est envoyé par la connexion. Si la négociation réussit, la messagerie est fournie par l'intermédiaire d'une session chiffrée.
4. **Préféré (vérifiez)**	Le TLS est négocié de l'ESA au MTA pour le domaine. Les tentatives d'appareils de vérifier le certificat du domaine. 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, ultérieurement le certificat n'est pas vérifié. Le message électronique est fourni en texte brut.
5. **Requis (vérifiez)**	Le TLS est négocié de l'ESA au MTA pour le domaine. La vérification du certificat de domaine est exigée. 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 une autorité de confiance de Cerfificate (CA). La messagerie n'est pas fournie. • Une connexion de TLS n'est pas négociée. La messagerie n'est pas fournie. La différence entre le **TLS exigé - Vérifiez** et **TLS requis - Vérifiez les** options **hébergées de domaine** s'étend dans le processus de vérification d'identité. La manière comment l'identité présentée est traitée et quel type d'identifiants de référence sont permis pour être utilisés font une différence au sujet d'un résultat final.
6. **Requis - Vérifiez les domaines hébergés**	L'identité présentée est d'abord dérivée de l'extension de subjectAltName du dNSName de type. S'il n'y a aucune correspondance entre le dNSName et celui d'identités reçues de référence (REF-ID), la vérification échoue aucune matière si la NC existent dans le domaine et pourraient passer davantage de vérification d'identité. La NC dérivée du domaine est validée seulement quand le certificat ne contient pas d'extension de subjectAltName de dNSName de type. Veuillez passer en revue le processus de vérification de TLS pour le pour en savoir plus de sécurité du courrier électronique de Cisco.

TLS d'enable sur le GUI

1. Choisissez **Montior > contrôles de destination**.
2. Cliquez sur Add la **destination**.
3. Ajoutez le domaine de destination dans le champ de destination.
4. Sélectionnez la méthode de support de TLS de la liste déroulante de support de TLS.
5. Cliquez sur Submit afin de soumettre les modifications.



TLS d'enable sur le CLI

Cet exemple emploie la commande de **destconfig** afin d'exiger des connexions de TLS et des conversations chiffrées pour le domaine *example.com*. Notez que cet exemple prouve que le TLS est exigé pour un domaine qui utilise le certificat de démonstration préinstallé sur l'appliance. Vous pouvez activer le TLS avec le certificat de démonstration afin de tester, mais il n'est pas sécurisé et n'est pas recommandé pour l'usage général.

La valeur « par défaut » est placée si vous répondez **non à la** question : « Vous souhaitez appliquer le TLS spécifique plaçant pour ce domaine ? » Si vous répondez **oui**, choisissez l'**aucun**, **préféré**, ou **requis**.

```
ESA> destconfig

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.
```

```
[]> example.com
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to configure.
[]> example.com

Do you wish to configure a concurrency limit for example.com? [Y]> N

Do you wish to apply a messages-per-connection limit to this domain? [N]> N

Do you wish to apply a recipient limit to this domain? [N]> N

Do you wish to apply a specific TLS setting for this domain? [N]> Y

Do you want to use TLS support?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
6. Required - Verify Hosted Domains
[1]> 3

You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.

Do you wish to apply a specific bounce verification
address tagging setting for this domain? [N]> N

Do you wish to apply a specific bounce profile to this domain? [N]> N

Do you wish to apply a specific IP sort preference to this domain? [N]> N

There are currently 3 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> list

            Rate               Bounce        Bounce     IP Version
Domain      Limiting  TLS      Verification  Profile    Preference
==========  ========  =======  ============  =========  ============
example.com Default   On       Default       Default    Default
(Default)   On        Off      Off           (Default)  Prefer IPv6
```