TLS-onderhandelingen over levering op het ESA

Inhoud

Inleiding

In dit document wordt beschreven hoe u de onderhandeling over Transport Layer Security (TLS) bij levering op de e-mail security applicatie (ESA) kunt controleren.

Zoals gedefinieerd in RFC 3207, is "TLS een uitbreiding naar de MTP-service die een MTP-server en -client toestaat om de beveiliging van de transportlaag te gebruiken om privé, geauthentiseerde communicatie via het internet te verstrekken. TLS is een populair mechanisme voor het verbeteren van TCP-communicatie met privacy en authenticatie."

TLS op levering inschakelen

U kunt STARTTLS nodig hebben voor e-maillevering aan specifieke domeinen met een van deze methoden die in dit document worden beschreven:

- Gebruik de CLI **deconfiguratie** opdracht.
- Kies in de GUI het **postbeleid** > **Bestemmingscontroles**.

De pagina Besturing doelmap of het opdracht deconfiguratie heeft u in staat om vijf verschillende instellingen voor TLS voor een bepaald domein te specificeren wanneer u een domein toevoegt. Daarnaast kunt u bepalen of validering van het domein noodzakelijk is.

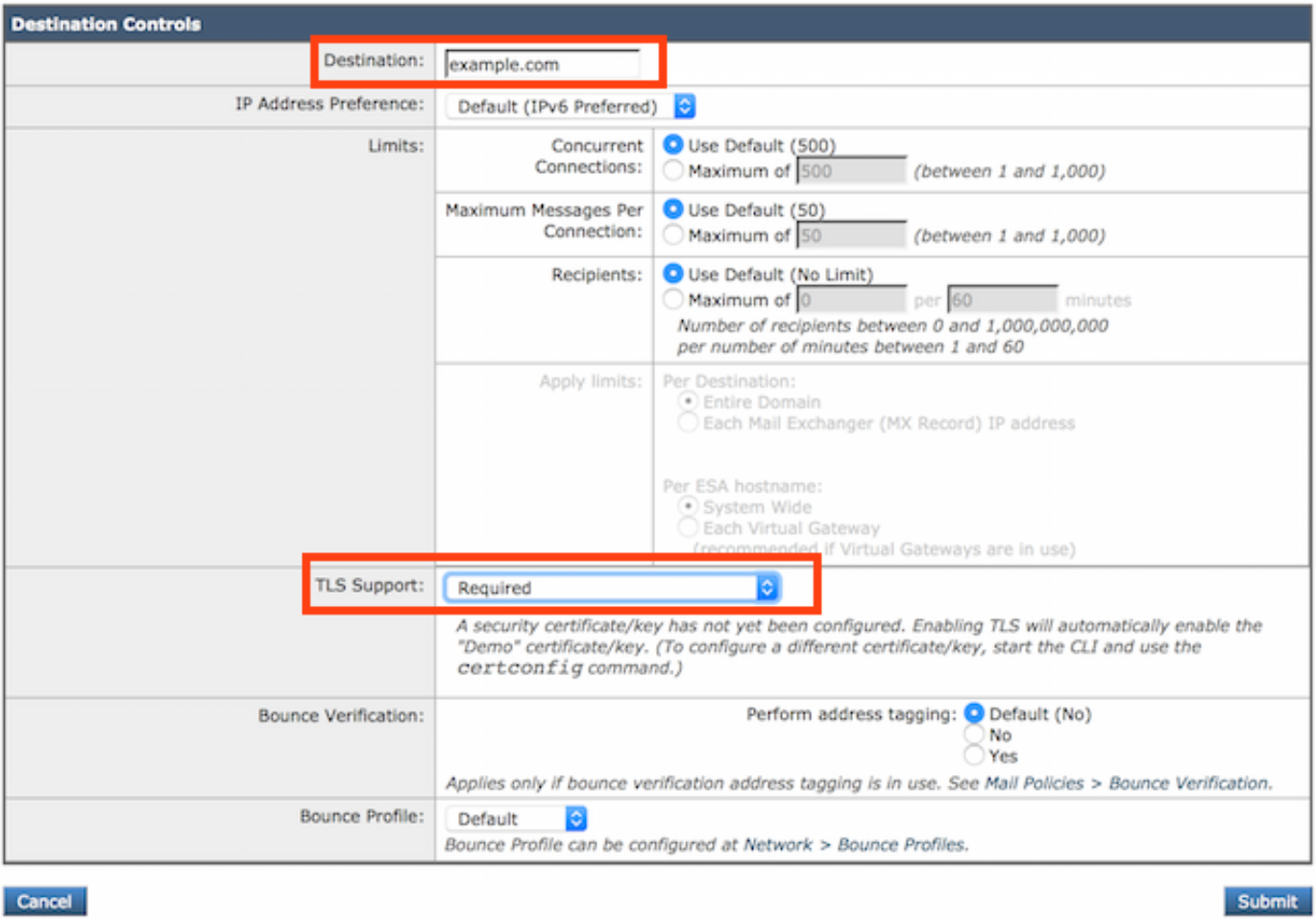
TLS-instellingsdefinities

TLS-instelling	Betekenis
Standaard	Standaard TLS-instelling die wordt ingesteld wanneer u de pagina Bestandscontrole op bestemming of de **deconfiguratie ->standaard** subopdracht gebruikt voor uitgaande verbindingen van de luisteraar naar de Message Transfer Agent (MTA) voor het domein. D waarde "Standaard" wordt ingesteld als u **op** de vraag nee antwoordt: "Wilt u een specifiek instelling voor TLS voor dit domein toepassen?"
1. Nr.	TLS is niet overeengekomen voor uitgaande verbindingen van de interface naar de MTA voor het domein.
2. Voorkeuren	Voor TLS wordt via onderhandelingen van de ESA-interface naar de MTA(s) voor het domein onderhandeld. Als de TLS-onderhandeling echter mislukt (vóór het ontvangen van een 220-respons), blijft de mtp-transactie "in de duidelijke" (niet versleuteld) doorgaan. Er wordt niet geprobeerd na te gaan of het certificaat afkomstig is van een vertrouwde certificeringsinstantie. Als er een fout optreedt nadat de 220-respons is ontvangen, valt de partij niet terug in de duidelijke tekst.
3. Vereiste	Voor het domein wordt via onderhandelingen tussen de ESA-interface en de MTA(s) over

	TLS onderhandeld. Er wordt niet geprobeerd het certificaat van het domein te verifiëren. Al de onderhandeling mislukt, wordt er geen e-mail verstuurd via de verbinding. Als de onderhandelingen slagen, wordt de post geleverd via een versleutelde sessie.
4. Voorkeuren (Verifiëren)	De TLS wordt via onderhandelingen van het ESA aan de MTA(s) voor het domein onderhandeld. Het apparaat probeert het certificaat van het domein te verifiëren.Er zijn drie uitkomsten mogelijk: • Het TLS wordt onderhandeld en het certificaat wordt geverifieerd. De post wordt afgeleverd via een versleutelde sessie. • Het TLS wordt onderhandeld, maar het certificaat wordt niet geverifieerd. De post word afgeleverd via een versleutelde sessie. • Er wordt geen TLS-verbinding gemaakt en vervolgens wordt het certificaat niet geverifieerd. Het e-mailbericht wordt in onbewerkte tekst verzonden.
5. Vereiste (controle)	De TLS wordt via onderhandelingen van het ESA aan de MTA(s) voor het domein onderhandeld. Verificatie van het domeincertificaat is vereist. Er zijn drie uitkomsten mogelijk: • Er wordt onderhandeld over een TLS-verbinding en het certificaat wordt geverifieerd. Het e-mailbericht wordt afgeleverd via een versleutelde sessie. • Er is onderhandeld over een TLS-verbinding, maar het certificaat is niet geverifieerd door een vertrouwde certificeringsinstantie (CA). De post is niet afgeleverd. • Een TLS-verbinding is niet onderhandeld. De post is niet afgeleverd.
6. Vereist - controleer Hosted velden	Het verschil tussen **TLS vereist - Controleer** en **TLS vereist - Controleer de** opties van de **Hosted Domain** in het proces van identiteitscontrole. De wijze waarop de gepresenteerde identiteit wordt verwerkt en het type referentienummers dat mag worden gebruikt, maken een verschil over het eindresultaat. De gepresenteerde identiteit is voor het eerst afgeleid van de subjectAltName extensie van type dNSName. Indien de naam van de NSN en een van de aanvaarde referentie-identiteiten (REF-ID) niet met elkaar overeenkomen, geeft de controle geen aanleiding tot het ontbreken van GN in het onderwerpveld en kan zij een verdere identiteitscontrole ondergaan. De van het onderwerpveld afgeleide GN wordt alleen gevalideerd indien het certificaat geen enkele van de onderwerpregel of naam van het type dNSName bevat. Controleer het TLS-verificatieproces voor Cisco e-mail security voor meer informatie.

TLS op GUI inschakelen

1. Kies **monitor** > **Bestemmingscontroles**.
2. Klik op **Bestanden toevoegen**.
3. Voeg het doeldomein toe in het veld Bestemming.
4. Selecteer de TLS-ondersteuningsmethode in de vervolgkeuzelijst TLS-ondersteuning.
5. Klik op **Inzenden** om de wijzigingen voor te leggen.



TLS op CLI inschakelen

Dit voorbeeld gebruikt het bevel **deconfiguratie** om TLS verbindingen en gecodeerde gesprekken voor het domein *voorbeeld.com* te vereisen. Dit voorbeeld toont aan dat TLS vereist is voor een domein dat gebruik maakt van het demonstratiecertificaat dat vooraf op het apparaat is geïnstalleerd. U kunt TLS met het demonstratiecertificaat inschakelen voor testdoeleinden, maar dit is niet veilig en wordt niet aanbevolen voor algemeen gebruik.

De waarde "Standaard" wordt ingesteld als u **op** de vraag nee antwoordt: "Wilt u een specifieke instelling voor TLS voor dit domein toepassen?" Als u **ja** antwoordt, kiest u **Nee**, **Voorkeuren** of **Vereist**.

```
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
```