Controllo della negoziazione TLS sulla consegna sull'ESA

Sommario

Introduzione

In questo documento viene descritto come controllare la negoziazione TLS (Transport Layer Security) sulla consegna in Email Security Appliance (ESA).

Come definito nella RFC 3207, "TLS è un'estensione del servizio SMTP che consente a un server e a un client SMTP di utilizzare la protezione a livello di trasporto per fornire comunicazioni private autenticate su Internet. TLS è un meccanismo molto diffuso per migliorare le comunicazioni TCP con la privacy e l'autenticazione."

Abilita TLS alla consegna

Èpossibile richiedere STARTTLS per il recapito della posta elettronica a domini specifici con uno dei metodi descritti di seguito:

- Usare il comando CLI **destconfig**.
- Dalla GUI, selezionare **Mail Policies > Destination Controls** (Policy di posta > Controlli **destinazione)**.

La pagina Controlli destinazione o il comando **destconfig** consente di specificare cinque diverse impostazioni per TLS per un determinato dominio quando si include un dominio. È inoltre possibile stabilire se è necessaria la convalida del dominio.

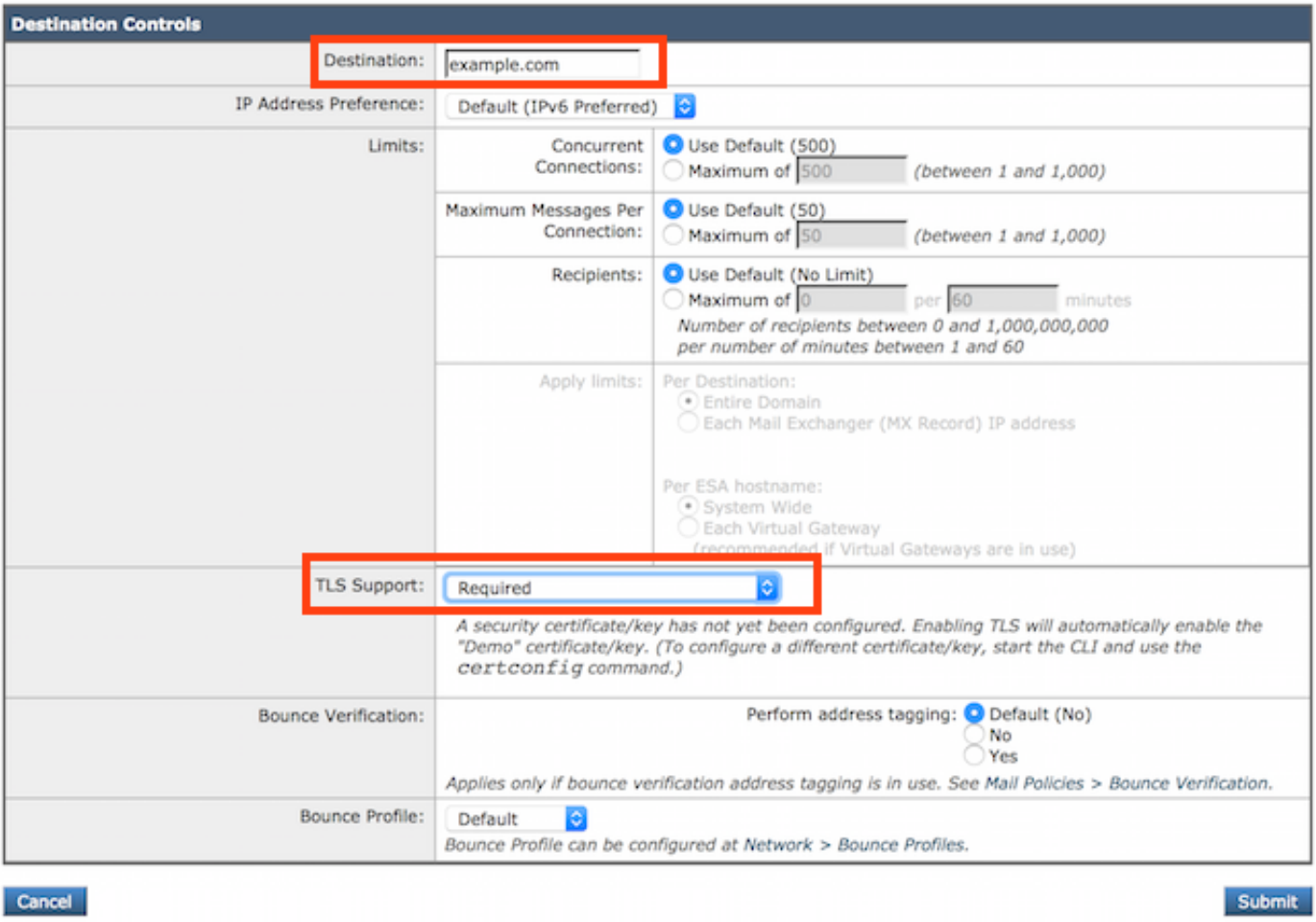
Definizioni impostazioni TLS

Impostazione TLS	Significato
Predefinito	Impostazione TLS predefinita impostata quando si utilizza la pagina Controlli di destinazione o il sottocomando **destconfig ->default** utilizzato per le connessioni in uscita dal listener all'agente di trasferimento messaggi (MTA) per il dominio. Il valore "Default" viene impostato se si risponde **no** alla domanda: "Applicare un'impostazione TLS specifica per questo dominio?"
1. No	Il protocollo TLS non viene negoziato per le connessioni in uscita dall'interfaccia all'agente di trasferimento messaggi per il dominio.
2. Preferenziale	Il TLS viene negoziato dall'interfaccia ESA con gli MTA del dominio. Tuttavia, se la negoziazione TLS non riesce (prima di ricevere una risposta 220), la transazione SMTP continua "in chiaro" (non crittografata). Non viene eseguito alcun tentativo di verificare se il

	certificato proviene da un'autorità di certificazione attendibile. Se si verifica un errore dopo la ricezione della risposta 220, la transazione SMTP non restituirà testo non crittografato.
3. Obbligatorio	Il TLS viene negoziato dall'interfaccia ESA agli MTA per il dominio. Nessun tentativo di verifica del certificato del dominio. Se la negoziazione ha esito negativo, non verrà inviato alcun messaggio di posta elettronica tramite la connessione. Se la negoziazione ha esito positivo, la posta viene recapitata tramite una sessione crittografata.
4. Preferito (Verifica)	Il TLS viene negoziato tra l'ESA e gli MTA del dominio. L'accessorio tenta di verificare il certificato del dominio.Sono possibili tre risultati: • TLS viene negoziato e il certificato verificato. La posta viene recapitata tramite una sessione crittografata. • TLS viene negoziato, ma il certificato non viene verificato. La posta viene recapitata tramite una sessione crittografata. • Non viene stabilita alcuna connessione TLS e, di conseguenza, il certificato non viene verificato. Il messaggio e-mail viene recapitato in formato testo normale.
5. Obbligatorio (verifica)	Il TLS viene negoziato tra l'ESA e gli MTA del dominio. Verifica del certificato di dominio obbligatoria. Sono possibili tre risultati: • Una connessione TLS viene negoziata e il certificato verificato. Il messaggio e-mail viene recapitato tramite una sessione crittografata. • Una connessione TLS viene negoziata, ma il certificato non viene verificato da un'Autorità di certificazione (CA) attendibile. La posta non viene recapitata. • Connessione TLS non negoziata. La posta non viene recapitata.
6. Obbligatorio - Verifica domini ospitati	La differenza tra le opzioni **TLS Required - Verify** e **TLS Required - Verify Hosted Domain** risiede nel processo di verifica dell'identità. Il modo in cui viene elaborata l'identità presentata e il tipo di identificativi di riferimento che è consentito utilizzare fanno la differenza per il risultato finale. L'identità presentata deriva innanzitutto dall'estensione subjectAltName di tipo dNSName. Se non c'è corrispondenza tra dNSName e una delle identità di riferimento accettate (REF-ID), la verifica non riesce indipendentemente dal fatto che nel campo dell'oggetto esista un CN e potrebbe superare un'ulteriore verifica dell'identità. Il CN derivato dal campo del soggetto viene convalidato solo quando il certificato non contiene estensioni subjectAltName di tipo dNSName. Per ulteriori informazioni, esaminare il processo di verifica TLS per Cisco Email Security.

Abilitare TLS sulla GUI

1. Scegliere **Monitor > Controlli destinazione**.
2. Fare clic su **Aggiungi destinazione**.
3. Aggiungere il dominio di destinazione nel campo Destinazione.
4. Selezionare il metodo di supporto TLS dall'elenco a discesa Supporto TLS.
5. Per inviare le modifiche, fare clic su **Submit** (Invia).



Abilitazione di TLS sulla CLI

In questo esempio viene utilizzato il comando **destconfig** per richiedere connessioni TLS e conversazioni crittografate per il dominio *example.com*. Nell'esempio riportato di seguito viene indicato che per un dominio in cui viene utilizzato il certificato dimostrativo preinstallato sull'accessorio è necessario disporre di TLS. È possibile attivare TLS con il certificato dimostrativo a scopo di test, ma non è sicuro e non è consigliato per un uso generico.

Il valore "Default" viene impostato se si risponde **no** alla domanda: "Applicare un'impostazione TLS specifica per questo dominio?" Se si risponde **sì**, scegliere **No**, **Preferito** o **Obbligatorio**.

```
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
```