Controle la negociación de TLS en la salida en el ESA

Contenido

Introducción

Este documento describe cómo controlar la negociación de Transport Layer Security (TLS) en la salida en el dispositivo de seguridad del correo electrónico (ESA).

Según lo definido en el RFC 3207, “TLS es una extensión al servicio SMTP que permite que un servidor SMTP y un cliente utilicen el Transport Layer Security para proporcionar la comunicación privada, autenticada sobre Internet. TLS es un mecanismo popular para aumentar las comunicaciones TCP con la aislamiento y la autenticación.”

Permiso TLS en la salida

Usted puede requerir STARTTLS para la salida del correo electrónico a los dominios específicos con cualquiera uno de estos métodos descritos en este documento:

- Utilice el comando del **destconfig** CLI.
- Del GUI elija las **directivas del correo** > los **controles del destino**.

Los controles del destino paginan o el comando del **destconfig** permite que usted especifique cinco diversas configuraciones para TLS para un dominio dado cuando usted incluye un dominio. Además, usted puede dictar si la validación del dominio es necesaria.

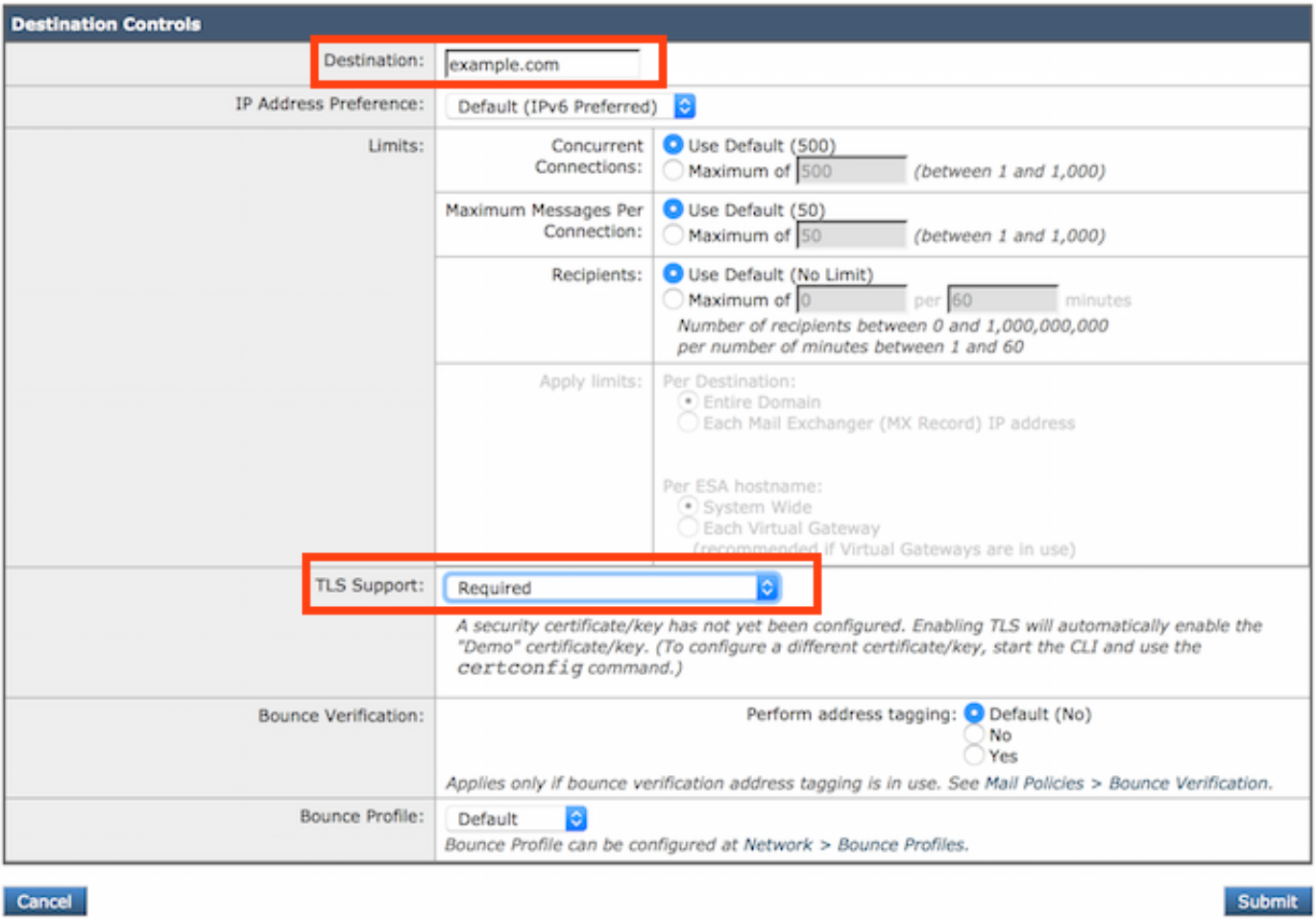
TLS que fija las definiciones

Determinación de TLS	Significado
Predeterminado	La determinación predeterminada de TLS se fija que cuando usted utiliza la página de los controles del destino o el **destconfig - >** submandato del **valor por defecto** usado para las conexiones salientes del módulo de escucha al agente de transferencia de mensajes (MTA) para el dominio. Se fija el valor “valor por defecto” si usted contesta **no a la** pregunta: “Usted desea aplicar TLS específico que fija para este dominio?”
1. **No**	TLS no se negocia para las conexiones salientes de la interfaz al MTA para el dominio.
2. **Preferido**	TLS se negocia de la interfaz ESA al MTA para el dominio. Sin embargo, si la negociación de TLS falla (antes de recibir una respuesta 220), la transacción SMTP continúa “en el claro” (no cifrado). No se hace ninguna tentativa para verificar si el certificado origina de un Certificate Authority de confianza. Si ocurre un error después de que se reciba la respuesta 220, la transacción SMTP no recurre al texto claro.

3. **Necesario**	TLS se negocia de la interfaz ESA al MTA para el dominio. No se hace ninguna tentativa para verificar el certificado del dominio. Si la negociación falla, no se envía ningún correo electrónico a través de la conexión. Si la negociación tiene éxito, el correo se entrega vía una sesión encriptada.
4. **Preferido (verifique)**	TLS se negocia del ESA al MTA para el dominio. El dispositivo intenta verificar el certificado del dominio. Tres resultados son posibles: • Se negocia TLS y se verifica el certificado. El correo se entrega vía una sesión encriptada. • Se negocia TLS, pero el certificado no se verifica. El correo se entrega vía una sesión encriptada. • No se hace ninguna conexión TLS y, el certificado no se verifica posteriormente. El correo electrónico se entrega en el sólo texto.
5. **Requerido (verifique)**	TLS se negocia del ESA al MTA para el dominio. La verificación del certificado del dominio se requiere. Tres resultados son posibles: • Se negocia una conexión TLS y se verifica el certificado. El correo electrónico se entrega vía una sesión encriptada. • Se negocia una conexión TLS, pero el certificado no es verificado por una autoridad de confianza de Cerfificate (CA). El correo no se entrega. • Una conexión TLS no se negocia. El correo no se entrega.
6. **Requerido - Verifique los dominios recibidos**	La diferencia entre **TLS requirió - Verifique** y **TLS requirió - Verifique las opciones de dominio recibidas** pone en el proceso de verificación de la identidad. La manera cómo se procesa la actual identidad y se permite a qué tipo de identificadores de la referencia ser utilizado diferencia sobre un resultado final. La actual identidad primero se deriva de la extensión del subjectAltName del dNSName del tipo. Si no hay coincidencia entre el dNSName y el que está de las identidades validadas de la referencia (REF-ID), la verificación no falla ninguna materia si el CN existe en el campo Subject y podría pasar la verificación adicional de la identidad. El CN derivado del campo Subject se valida solamente cuando el certificado no contiene ninguna de la extensión del subjectAltName del dNSName del tipo. Revise por favor el proceso de verificación de TLS para la Seguridad del correo electrónico de Cisco para más información.

Habilite TLS en el GUI

1. Elija **Montior** > los **controles del destino**.
2. El tecleo **agrega el destino**.
3. Agregue el dominio del destino en el Campo Destination.
4. Seleccione el método del soporte de TLS de la lista desplegable del soporte de TLS.
5. El tecleo **somete** para someter los cambios.



Permiso TLS en el CLI

Este ejemplo utiliza el comando del **destconfig** para requerir las conexiones TLS y las conversaciones cifradas para el dominio *example.com*. Observe que este ejemplo muestra que TLS está requerido para un dominio que utilice el certificado de la demostración instalado previamente en el dispositivo. Usted puede habilitar TLS con el certificado de la demostración para comprobar, pero no es seguro y no se recomienda para el uso general.

Se fija el valor “valor por defecto” si usted contesta **no a la** pregunta: “Usted desea aplicar TLS específico que fija para este dominio?” Si usted contesta **sí**, elija **ningún**, **preferido**, o **requerido**.

```
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
```