Crear guía de configuración de certificados para TLS en ESA

Contenido

Introducción

Este documento describe cómo crear un certificado para su uso con TLS, activar TLS entrante / saliente y solucionar problemas en Cisco ESA.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La implementación de TLS en el ESA proporciona privacidad para la transmisión punto a punto de correos electrónicos a través del cifrado. Permite a un administrador importar un certificado y una clave privada de un servicio de Autoridad de certificados (CA) o utilizar un certificado autofirmado.

Cisco AsyncOS para Email Security admite la extensión *STARTTLS* para el protocolo simple de transferencia de correo (SMTP) (*SMTP seguro sobre TLS*).

> **Sugerencia**: para obtener más información sobre TLS, consulte RFC 3207.

> **Nota**: Este documento describe cómo instalar certificados en el nivel de agrupamiento con el uso de la función *Administración centralizada* en el ESA. Los certificados también se pueden aplicar en el nivel de equipo; sin embargo, si la máquina se quita del clúster y después se vuelve a agregar, los certificados de nivel de equipo se pierden.

Descripción general funcional y requisitos

Un administrador desea crear un certificado autofirmado en el dispositivo por cualquiera de estos motivos:

- Para cifrar las conversaciones SMTP con otros MTAs que utilizan TLS (conversaciones entrantes y salientes).
- Para habilitar el servicio HTTPS en el dispositivo para el acceso a la GUI a través de HTTPS.
- Para su uso como certificado de cliente para protocolos ligeros de acceso a directorios (LDAP), si el servidor LDAP requiere un certificado de cliente.
- Para permitir una comunicación segura entre el dispositivo y Rivest-Shamir-Addleman (RSA) Enterprise Manager for Data Loss Protection (DLP).
- Para permitir una comunicación segura entre el dispositivo y un appliance de Threat Grid de

protección frente a malware avanzado (AMP) de Cisco.

El ESA viene preconfigurado con un certificado de demostración que se puede utilizar para establecer conexiones TLS.

> **Precaución**: aunque el certificado de demostración es suficiente para establecer una conexión TLS segura, tenga en cuenta que no puede ofrecer una conexión verificable.

Cisco recomienda que obtenga un certificado X.509, o correo electrónico de privacidad mejorada (PEM) de una CA. Esto también se conoce como un certificado *Apache*. El certificado de una CA es deseable sobre el certificado autofirmado porque un certificado autofirmado es similar al certificado de demostración mencionado anteriormente, que no puede ofrecer una conexión verificable.

> **Nota**: El formato de certificado PEM se define con más detalle en RFC 1421 a través de RFC 1424. PEM es un formato de contenedor que puede incluir sólo el certificado público (como con instalaciones de Apache y archivos de certificado de CA */etc/ssl/certs*) o una cadena de certificados completa, para incluir certificados de clave pública, clave privada y raíz. El nombre *PEM* proviene de un método fallido para correo electrónico seguro, pero el formato de contenedor que utilizó sigue activo y es una traducción en base 64 de las claves ASN.1 X.509.

Traiga su propio certificado

La opción para importar su propio certificado está disponible en el ESA; sin embargo, el requisito es que el certificado esté en el formato *PKCS#12*. Este formato incluye la clave privada. Los administradores no suelen tener certificados disponibles en este formato. Por este motivo, Cisco recomienda que genere el certificado en el ESA y que una CA lo firme correctamente.

Actualizar un certificado actual

Si un certificado que ya existe ha caducado, omita la sección *Implementación de Certificados Autofirmados* de este documento y vuelva a firmar el certificado que existe.

> **Sugerencia**: consulte el documento Renovación de un certificado en un dispositivo de seguridad de correo electrónico de Cisco para obtener más detalles.

Implementar certificados autofirmados

En esta sección se describe cómo generar un certificado autofirmado y una solicitud de firma de certificado (CSR), proporcionar el certificado autofirmado a una CA para su firma, cargar el certificado firmado en el ESA, especificar el certificado para su uso con los servicios ESA y realizar una copia de seguridad de la configuración del dispositivo y de los certificados.

Generar un certificado autofirmado y CSR

Para crear un certificado autofirmado a través de la CLI, ingrese el comando **certconfig**.

Para crear un certificado autofirmado desde la GUI:

1. Vaya a **Red > Certificados > Agregar certificado** desde la GUI del dispositivo.

2. Haga clic en el menú desplegable **Create Self-Signed Certificate**.

   Cuando cree el certificado, asegúrese de que el *Nombre Común* coincida con el nombre de host de la interfaz de escucha, o que coincida con el nombre de host de la interfaz de entrega.
   La interfaz de *escucha* es la interfaz que está vinculada al receptor que se configura en **Red > Receptores**.La interfaz *delivery* se selecciona automáticamente, a menos que se configure explícitamente desde la CLI con el comando **delivery config**.
3. Para una conexión entrante verificable, compruebe que estos tres elementos coinciden:

   Registro MX (nombre de host del sistema de nombres de dominio (DNS))

   Nombre común

   Nombre de host de interfaz

   Nota: El nombre de host del sistema no afecta a las conexiones TLS en lo que respecta a ser verificable. El nombre de host del sistema se muestra en la esquina superior derecha de la GUI del dispositivo o en la salida del comando CLI **sethostname**.

   Precaución: no olvide **enviar** y **confirmar** los cambios antes de exportar el CSR. Si no se completan estos pasos, el nuevo certificado no se confirma en la configuración del dispositivo y el certificado firmado de la CA no puede firmar un certificado que ya existe ni aplicarlo a él.

Proporcionar el certificado autofirmado a una CA

Para enviar el certificado autofirmado a una CA para su firma:

1. Guarde el CSR en un equipo local en formato PEM **Red > Certificados > Nombre del certificado > Descargar solicitud de firma de certificado**.

2. Envíe el certificado generado a una CA reconocida para su firma.

3. Solicite un certificado con formato X.509/PEM/Apache, así como el certificado intermedio.

A continuación, la CA genera un certificado en formato PEM.

Nota: Para obtener una lista de proveedores de CA, consulte el artículo de Wikipedia Certificate authority.

Cargar el certificado firmado en el ESA

Después de que la CA devuelva el certificado público de confianza firmado por una clave privada,

cargue el certificado firmado en el ESA.

El certificado se puede utilizar con un receptor público o privado, un servicio HTTPS de interfaz IP, la interfaz LDAP o todas las conexiones TLS salientes a los dominios de destino.

Para cargar el certificado firmado en el ESA:

1. Asegúrese de que el certificado público de confianza que se recibe utiliza el formato PEM o un formato que se pueda convertir en PEM antes de cargarlo en el dispositivo. **Sugerencia**: Puede utilizar el OpenSSL toolkit, un programa de software libre, para convertir el formato.
2. Cargue el certificado firmado:

   Vaya a **Red > Certificados**.

   Haga clic en el nombre del certificado que se envió a la CA para su firma.

   Introduzca la ruta del archivo en el equipo local o volumen de red.

   Nota: Al cargar el nuevo certificado, se sobrescribe el certificado actual. También se puede cargar un certificado intermedio relacionado con el certificado autofirmado.

   Precaución: recuerde **enviar** y **registrar** los cambios después de cargar el certificado firmado.

Especifique el certificado para su uso con los servicios ESA

Ahora que el certificado se ha creado, firmado y cargado en el ESA, se puede utilizar para los servicios que requieren el uso de certificados.

TLS entrante

Complete estos pasos para utilizar el certificado para los servicios TLS entrantes:

1. Vaya a **Red > Receptores**.
2. Haga clic en el nombre del listener.
3. Seleccione el nombre del certificado en el menú desplegable *Certificate*.
4. Haga clic en Submit (Enviar).
5. Repita los pasos 1 a 4 según sea necesario para los receptores adicionales.
6. **Realice** los cambios.

TLS saliente

Complete estos pasos para utilizar el certificado para los servicios TLS salientes:

1. Vaya a **Políticas de correo > Controles de destino**.
2. Haga clic en **Edit Global Settings...** en la sección *Global Settings*.
3. Seleccione el nombre del certificado en el menú desplegable *Certificate*.
4. Haga clic en Submit (Enviar).
5. **Realice** los cambios.

HTTPS

Complete estos pasos para utilizar el certificado para los servicios HTTPS:

1. Vaya a **Red > Interfaces IP**.
2. Haga clic en el nombre de la interfaz.
3. Seleccione el nombre del certificado en el menú desplegable *HTTPS Certificate*.
4. Haga clic en Submit (Enviar).
5. Repita los pasos 1 a 4 según sea necesario para cualquier interfaz adicional.
6. **Realice** los cambios.

LDAP

Complete estos pasos para utilizar el certificado para los LDAP:

1. Vaya a **Administración del sistema > LDAP**.
2. Haga clic en **Edit Settings...** en la sección *LDAP Global Settings*.
3. Seleccione el nombre del certificado en el menú desplegable *Certificate*.
4. Haga clic en Submit (Enviar).
5. **Realice** los cambios.

Filtrado de URL

Para utilizar el certificado para el filtrado de URL:

1. Ingrese el comando **websecurityconfig** en la CLI.
2. Continúe con las indicaciones de comandos. Asegúrese de seleccionar **Y** cuando llegue a este mensaje:

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

3. Seleccione el número asociado al certificado.

4. Ingrese el comando **commit** para confirmar los cambios de configuración.

Copia de seguridad de la configuración y los certificados del dispositivo

Asegúrese de que la configuración del dispositivo está guardada en este momento. La configuración del dispositivo contiene el trabajo de certificado completado que se ha aplicado a través de los procesos descritos anteriormente.

Complete estos pasos para guardar el archivo de configuración del dispositivo:

1. Vaya a **Administración del sistema > Archivo de configuración > Descargar archivo al equipo local para verlo o guardarlo**.

2. Exportar el certificado:

   Vaya a **Red > Certificados**.

   Haga clic en **Exportar certificado**.

   Seleccione el certificado que desea exportar.

   Introduzca el nombre de archivo del certificado.

   Introduzca una contraseña para el archivo de certificado.

   Haga clic en **Exportar**.

   Guarde el archivo en un equipo local o de red.

   Se pueden exportar certificados adicionales en este momento, o haga clic en **Cancel** para volver a la ubicación **Network > Certificates**.

   Nota: Este proceso guarda el certificado en formato PKCS#12, que crea y guarda el archivo con protección por contraseña.

Activar TLS entrante

Para activar TLS para todas las sesiones entrantes, conéctese a la GUI web, elija **Políticas de correo > Políticas de flujo de correo** para el receptor entrante configurado y luego complete estos pasos:

1. Elija un receptor para el que se deben modificar las políticas.

2. Haga clic en el enlace del nombre de la política para editarla.

3. En la sección *Funciones de Seguridad*, elija una de estas opciones de *Cifrado y Autenticación* para establecer el nivel de TLS que se requiere para ese receptor y la política de flujo de correo:

   Apagado: cuando se elige esta opción, no se utiliza TLS.

   Preferido: cuando se elige esta opción, TLS puede negociar desde el MTA remoto al ESA. Sin embargo, si el MTA remoto no negocia (antes de la recepción de una respuesta *220*), la transacción SMTP continúa *en modo sin cifrar* (no cifrada). No se realiza ningún intento para comprobar si el certificado proviene de una entidad emisora de certificados de confianza. Si se produce un error después de que se reciba la respuesta 220, la transacción SMTP no vuelve al texto sin cifrar.

   Requerido: cuando se elige esta opción, TLS se puede negociar desde el MTA remoto al ESA. No se realiza ningún intento para verificar el certificado del dominio. Si la negociación falla, no se envía ningún correo electrónico a través de la conexión. Si la negociación se realiza correctamente, el correo se entrega a través de una sesión cifrada.
4. Haga clic en Submit (Enviar).

5. Haga clic en el botón **Registrar cambios**. Si lo desea, puede agregar un comentario opcional en este momento.

6. Haga clic en **Registrar Cambios** para guardar los cambios.

La política de flujo de correo para el receptor se actualiza ahora con la configuración de TLS que ha elegido.

Complete estos pasos para activar TLS para las sesiones entrantes que llegan desde un conjunto seleccionado de dominios:

1. Conéctese a la GUI web y elija **Políticas de correo > Descripción general de HAT**.

2. Agregue los remitentes IP/FQDN al grupo de remitentes apropiado.

3. Edite la configuración de TLS de la política de flujo de correo asociada con el Grupo de remitentes que modificó en el paso anterior.

4. Haga clic en Submit (Enviar).

5. Haga clic en el botón **Registrar cambios**. Si lo desea, puede agregar un comentario opcional en este momento.

6. Haga clic en **Registrar Cambios** para guardar los cambios.

La política de flujo de correo para el grupo de remitentes se actualiza ahora con la configuración de TLS que ha elegido.

Consejo: Consulte este artículo para obtener más información sobre cómo maneja el ESA la

verificación de TLS: ¿Cuál es el algoritmo para la verificación de certificados en el ESA?

Activar TLS saliente

Para activar TLS para las sesiones salientes, conéctese a la GUI web, elija **Políticas de correo > Controles de destino**, y luego complete estos pasos:

1. Haga clic en **Agregar destino...**.

2. Agregue el dominio de destino.

3. En la sección *Soporte de TLS*, haga clic en el menú desplegable y elija una de estas opciones para habilitar el tipo de TLS que se va a configurar:

   Ninguno: cuando se elige esta opción, TLS no se negocia para las conexiones salientes de la interfaz al MTA para el dominio.

   Preferido: cuando se elige esta opción, TLS se negocia desde la interfaz ESA a los MTA para el dominio. Sin embargo, si la negociación TLS falla (antes de la recepción de una respuesta 220), la transacción SMTP continúa *en modo despejado* (no encriptado). No se realiza ningún intento para comprobar si el certificado proviene de una CA de confianza. Si se produce un error después de que se reciba la respuesta 220, la transacción SMTP no vuelve al texto sin cifrar.

   Requerido: cuando se elige esta opción, TLS se negocia desde la interfaz ESA a los MTA para el dominio. No se realiza ningún intento para verificar el certificado del dominio. Si la negociación falla, no se envía ningún correo electrónico a través de la conexión. Si la negociación se realiza correctamente, el correo se entrega a través de una sesión cifrada.

   Preferred-Verify: cuando se elige esta opción, TLS se negocia desde el ESA a los MTA para el dominio y el dispositivo intenta verificar el certificado de dominio. En este caso, estos tres resultados son posibles:

   Se negocia la TLS y se verifica el certificado. El correo se envía a través de una sesión cifrada.

   TLS se negocia, pero el certificado no se verifica. El correo se envía a través de una sesión cifrada.

   No se realiza ninguna conexión TLS y el certificado no se verifica. El mensaje de correo electrónico se envía como texto sin formato.**Required-Verify**: cuando se elige esta opción, TLS se negocia desde el ESA a los MTA para el dominio y se requiere la verificación del certificado del dominio. En este caso, estos tres resultados son posibles:

   Se negocia una conexión TLS y se verifica el certificado. El mensaje de correo electrónico se envía mediante una sesión cifrada.

Se negocia una conexión TLS, pero una CA de confianza no verifica el certificado. El correo no se entrega.

Una conexión TLS no se negocia, pero el correo no se entrega.

4. Realice los cambios necesarios en los *controles de destino* para el dominio de destino.

5. Haga clic en Submit (Enviar).

6. Haga clic en el botón **Registrar cambios**. Si lo desea, puede agregar un comentario opcional en este momento.

7. Haga clic en **Registrar Cambios** para guardar los cambios.

Síntomas de configuración incorrecta del certificado ESA

TLS funciona con un certificado autofirmado; sin embargo, si el remitente requiere la verificación de TLS, se deberá instalar un certificado firmado por CA.

La verificación de TLS puede fallar aunque se haya instalado un certificado firmado por la CA en el ESA.

En estos casos, se recomienda verificar el certificado a través de los pasos de la sección Verificar.

Verificación

Verificar TLS con un Navegador Web

Para verificar el certificado firmado por la CA, aplique el certificado al servicio HTTPS de ESA GUI.

A continuación, vaya a la GUI del ESA en el navegador web. Si hay advertencias cuando navega a https://youresa, es probable que el certificado esté incorrectamente encadenado, como si faltara un certificado intermedio.

Verificar TLS con herramientas de terceros

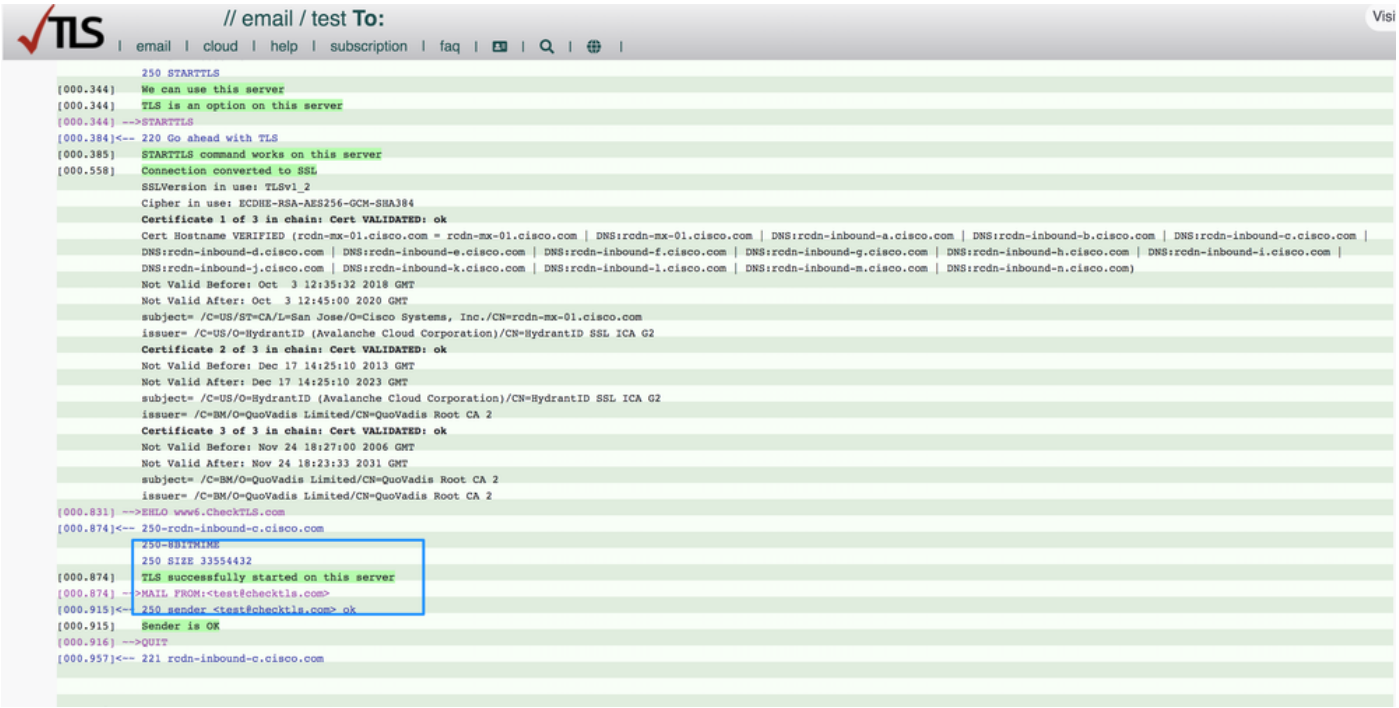
Antes de realizar la prueba, asegúrese de que el certificado que se va a probar se aplica al receptor en el que el dispositivo recibe correo entrante.

Las herramientas de terceros como CheckTLS.com y SSL-Tools.net se pueden utilizar para verificar el encadenamiento correcto del certificado.

Ejemplo de salida CheckTLS.com para TLS-Verify Success

CheckTLS Confidence Factor for "postmaster@cisco.com": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
alln-mx-01.cisco.com [173.37.147.230:25]	10	OK (41ms)	OK (422ms)	OK (50ms)	OK (48ms)	OK (450ms)	OK (58ms)	OK (41ms)
rcdn-mx-01.cisco.com [72.163.7.166:25]	20	OK (41ms)	OK (260ms)	OK (42ms)	OK (41ms)	OK (446ms)	OK (43ms)	OK (42ms)
aer-mx-01.cisco.com [173.38.212.150:25]	30	OK (80ms)	OK (484ms)	OK (81ms)	OK (79ms)	OK (548ms)	OK (80ms)	OK (81ms)
Average		100%	100%	100%	100%	100%	100%	100%



Ejemplo de salida CheckTLS.com para la falla de verificación de TLS

TestReceiver

CheckTLS Confidence Factor for "i[redacted]": 90

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
[redacted]	5	OK (121ms)	OK (683ms)	OK (407ms)	OK (236ms)	FAIL	OK (2,122ms)	OK (122ms)	OK (122ms)
[redacted]	5	OK (125ms)	OK (715ms)	OK (130ms)	OK (125ms)	FAIL	OK (1,608ms)	OK (125ms)	OK (127ms)
Average		100%	100%	100%	100%	0%	100%	100%	100%

El nombre de host del certificado NO ES VERIFICABLE (mailC.example.com != gvsvipa006.example.com)

Resolución

> **Nota:** si se está utilizando un certificado autofirmado, el resultado esperado en la columna "Cert OK" (Certificado correcto) es "FAIL" (Error).

Si un certificado firmado por CA está en uso y TLS-verify aún falla, verifique que estos elementos coincidan:

- Nombre común del certificado.
- Nombre de host (en GUI > Red > Interfaz).
- Nombre de host del registro MX: esta es la columna Servidor MX de la tabla TestReceiver.

Si se instaló un certificado firmado por una CA y aparecen errores, continúe con la siguiente sección para obtener información sobre cómo solucionar el problema.

Troubleshoot

Esta sección describe cómo resolver problemas básicos de TLS en el ESA.

Certificados intermedios

Busque certificados intermedios duplicados, especialmente cuando se actualizan los certificados actuales en lugar de crear un nuevo certificado. Es posible que los certificados intermedios hayan cambiado o se hayan encadenado incorrectamente, y es posible que el certificado haya cargado varios certificados intermedios. Esto puede introducir problemas de encadenamiento y verificación de certificados.

Habilitar notificaciones para errores de conexión TLS requeridos

Puede configurar el ESA para enviar una alerta si la negociación TLS falla cuando se entregan mensajes a un dominio que requiere una conexión TLS. El mensaje de alerta contiene el nombre del dominio de destino para la negociación TLS fallida. El ESA envía el mensaje de alerta a todos los destinatarios que están configurados para recibir alertas de nivel de gravedad de advertencia para los tipos de alerta *Sistema*.

> **Nota**: se trata de una configuración global, por lo que no se puede establecer por dominio.

Complete estos pasos para habilitar las alertas de conexión TLS:

1. Vaya a **Políticas de correo > Controles de destino**.
2. Haga clic en **Edit Global Settings**.
3. Marque la casilla de verificación **Enviar una alerta cuando falle una conexión TLS obligatoria**.

> **Sugerencia**: también puede configurar esta configuración con el comando **destconfig > setup** de la CLI.

El ESA también registra las instancias para las cuales se requiere TLS para un dominio, pero no se pudo utilizar en los registros de correo del dispositivo. Esto ocurre cuando se cumple cualquiera de estas condiciones:

- El MTA remoto no soporta ESMTP (por ejemplo, no entendió el comando *EHLO* del ESA).
- El MTA remoto soporta ESMTP, pero el comando *STARTTLS* no estaba en la lista de extensiones que anunció en su respuesta *EHLO*.
- El MTA remoto anunció la extensión *STARTTLS*, pero respondió con un error cuando el ESA envió el comando *STARTTLS*.

Localizar sesiones de comunicación TLS correctas en los registros de correo

Las conexiones TLS se registran en los registros de correo, junto con otras acciones importantes relacionadas con los mensajes, como acciones de filtrado, veredictos antivirus y antispam e intentos de entrega. Si hay una conexión TLS exitosa, hay una entrada TLS *exitosa* resultante en los registros de correo. Del mismo modo, una conexión TLS fallida produce una entrada *fallida de* TLS. Si un mensaje no tiene una entrada TLS asociada en el archivo de registro, ese mensaje no se entregó a través de una conexión TLS.

> **Sugerencia**: para comprender los registros de correo, consulte el documento de Cisco ESA Message Disposition Determination .

Este es un ejemplo de una conexión TLS exitosa desde el host remoto (recepción):

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS -
1.1
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-
SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

Este es un ejemplo de una conexión TLS fallida desde el host remoto (recepción):

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Mon Apr 16 18:59:13 2018 Info: ICID 590052584 ACCEPT SG UNKNOWNLIST match sbrs[2.1:10.0] SBRS
2.7
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 TLS failed: (336109761, 'error:1408A0C1:SSL
routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

Este es un ejemplo de una conexión TLS exitosa con el host remoto (entrega):

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 10.0.0.1
port 25
```

```
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-
AES256-GCM-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

Este es un ejemplo de una conexión TLS fallida al host remoto (entrega):

```
Mon Apr 16 00:01:34 2018 Info: New SMTP DCID 40986669 interface 192.168.1.1 address 10.0.0.1
port 25
Mon Apr 16 00:01:35 2018 Info: Connection Error: DCID 40986669 domain: domain IP:10.0.0.1 port:
25 details: 454-'TLS not available due to
temporary reason' interface: 192.168.1.1 reason: unexpected SMTP response
Mon Apr 16 00:01:35 2018 Info: DCID 40986669 TLS failed: STARTTLS unexpected response
```

Información Relacionada

- Dispositivo de seguridad Cisco Email Security Appliance: guías del usuario final
- Cisco Content Security Management Appliance: Guías para el usuario final
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).