Configuración TLS para el cifrado de la conexión hacia adentro en un módulo de escucha ESA

Contenido

Introducción

Este documento describe cómo habilitar Transport Layer Security (TLS) en un módulo de escucha en el dispositivo de seguridad del correo electrónico (ESA).

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el ESA con cualquier versión de AsyncOS.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Usted debe habilitar TLS para cualquier módulo de escucha donde usted requiere el cifrado para las conexiones hacia adentro. Usted puede ser que quiera habilitar TLS en los módulos de escucha que hacen frente a Internet (módulos de escucha públicos), pero no para los módulos de escucha para los sistemas internos (módulos de escucha privados). O, usted puede ser que quiera al Enable Encryption para todos los módulos de escucha. Por abandono, ni los módulos de escucha privados ni públicos permiten las conexiones TLS. Usted debe permitir a TLS en la tabla del acceso del host de un módulo de escucha (SOMBRERO) para habilitar TLS para el correo electrónico (de envío) entrante (recibiendo) o saliente. Además, las configuraciones de la directiva del flujo de correo para los módulos de escucha privados y públicos tienen "OFF" dado vuelta TLS por abandono.

Configurar

Usted puede especificar tres diversas configuraciones para TLS en un módulo de escucha:

Configuración	Significado
No	TLS no se permite para las conexiones entrantes. Las conexiones al módulo de escucha n requieren las conversaciones cifradas del Simple Mail Transfer Protocol (SMTP). Ésta es l configuración predeterminada para todos los módulos de escucha que usted configura en dispositivo.
Preferido	TLS se permite para las conexiones entrantes al módulo de escucha de los Agentes de transferencia de mensajes (MTAs).
Necesario	TLS se permite para las conexiones entrantes al módulo de escucha de MTAs, y hasta STARTTLS se recibe un comando, el ESA responde con un mensaje de error a cada coma con excepción de ninguna opción (NOOP), EHLO, o SALIÓ. Si “se requiere” TLS significa ese correo electrónico que el remitente no quiere cifrado con TLS será rechazado por el E antes de que se envíe, del cual de tal modo lo previene se transmita en el claro.

Permiso TLS en una directiva del flujo de correo del SOMBRERO para un módulo de escucha vía el GUI

Complete estos pasos:

1. De las directivas del flujo de correo pagine, elija a un módulo de escucha cuyas directivas usted quiera modificar y después haga clic el link para el nombre de la directiva para editar. (Usted puede también editar los parámetros de la política predeterminada.) Se visualiza la página de las directivas del flujo de correo del editar.
2. En el “cifrado y la autenticación” sección, para el “uso TLS: el” campo, elige el nivel de TLS que usted quiere para el módulo de escucha.
3. Haga clic en Submit (Enviar).
4. **Los cambios del cometer del** tecleo, agregan un comentario opcional en caso necesario, y después hacen clic los **cambios del cometer** para salvar los cambios.

Note: Usted puede asignar un certificado específico para las conexiones TLS a los módulos de escucha públicos individuales cuando usted crea a un módulo de escucha.

Permiso TLS en una directiva del flujo de correo del SOMBRERO para un módulo de escucha vía el CLI

1. Utilice el **listenerconfig > editan el** comando para elegir a un módulo de escucha que usted quiere configurar.
2. Utilice los **hostaccess > el comando default** para editar las configuraciones predeterminadas del SOMBRERO del módulo de escucha.
3. Ingrese una de estas opciones para cambiar la configuración TLS cuando le indican:
```
Do you want to allow encrypted TLS connections?

   1. No
   2. Preferred
   3. Required
 [1]>3

You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.
```
   Observe que este ejemplo pide que usted utilice el comando del **certconfig** para asegurarse de que hay un certificado válido que se puede utilizar con el módulo de escucha. Si usted no ha creado ningunos Certificados, el módulo de escucha utiliza el certificado de la demostración que se instala 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. Utilice el **listenerconfig > editan > comando certificate** para asignar un certificado al módulo de escucha.Una vez que usted ha configurado TLS, la configuración se refleja en el resumen del módulo de escucha en el CLI:
```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: Required
```
4. Ingrese el **comando commit** para habilitar el cambio.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

- Utilice el archivo del registro del correo de texto y vea este documento: Determine si el ESA está utilizando el TLS para la salida o recibir
- Uso Seguimiento de mensajes: GUI: Monitor > Seguimiento de mensajes
- El señalar del uso: GUI: Monitor > conexiones TLS
- Utilice un sitio web del otro vendedor tal como checktls.com

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Usted puede especificar si el ESA envía una alerta si la negociación de TLS falla cuando los

mensajes se entregan a un dominio que requiera una conexión TLS. El mensaje de alerta contiene el nombre del dominio del destino para la negociación fallada de TLS. El ESA envía el mensaje de alerta a todos los beneficiarios fijados para recibir las alertas amonestadoras del nivel de gravedad para los tipos de la alerta del sistema. Usted puede manejar a los beneficiarios alertas vía la página de la administración del sistema > de las alertas en el GUI (o vía el comando del **alertconfig** en el CLI).

Información Relacionada

- Guías del usuario final AsyncOS para el correo electrónico
- Soporte Técnico y Documentación - Cisco Systems