Configurar o TLS para a criptografia da conexão de entrada em um ouvinte ESA

Índice

Introdução

Este documento descreve como permitir o Transport Layer Security (TLS) em um ouvinte na ferramenta de segurança do email (ESA).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no ESA com toda a versão de AsyncOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Você deve permitir o TLS para todos os ouvintes onde você exige a criptografia para conexões de entrada. Você pôde querer permitir o TLS nos ouvintes que enfrentam o Internet (ouvintes públicos), mas não para ouvintes para sistemas internos (ouvintes privados). Ou, você pôde querer ao Enable Encryption para todos os ouvintes. À revelia, nem os ouvintes privados nem públicos permitem conexões TLS. Você deve permitir o TLS na tabela do acesso host de um ouvinte (CHAPÉU) a fim permitir o TLS para o email (de emissão) de entrada (recebendo) ou de partida. Além, os ajustes da política do fluxo de correio para ouvintes privados e públicos têm "OFF" girado TLS à revelia.

Configurar

Você pode especificar três ajustes diferentes para o TLS em um ouvinte:

Configuração	Significado
No	O TLS não é permitido conexões recebidas. As conexões ao ouvinte não exigem conversa cifradas do Simple Mail Transfer Protocol (SMTP). Esta é a configuração padrão para todos ouvintes que você configura no dispositivo.
Preferido	O TLS é permitido conexões recebidas ao ouvinte dos agentes de transferência de mensag (MTAs).
Necessário	O TLS é permitido conexões recebidas ao ouvinte de MTAs, e até STARTTLS um comando recebido, o ESA responde com um Mensagem de Erro a cada comando a não ser nenhum opção (NOOP), EHLO, ou PARA. Se o TLS “é exigido” significa que esse email que o reme não quer cifrado com TLS estará recusado pelo ESA antes que esteja enviado, de que o im desse modo esteja transmitido na claro.

Permita o TLS em uma política do fluxo de correio do CHAPÉU para um ouvinte através do GUI

Conclua estes passos:

1. Das políticas do fluxo de correio pagine, escolha um ouvinte cujas políticas você queira alterar e clique então o link para o nome da política para editar. (Você pode igualmente editar os parâmetros da política padrão.) A página das políticas do fluxo de correio da edição é indicada.
2. Na “criptografia e na autenticação” seção, para o “uso TLS: o” campo, escolhe o nível do TLS que você quer para o ouvinte.
3. Clique em Submit.
4. O clique **compromete mudanças**, adiciona um comentário opcional caso necessário, e clica-o então **compromete mudanças** a fim salvar as mudanças.

Note: Você pode atribuir um certificado específico para conexões TLS aos ouvintes públicos individuais quando você cria um ouvinte.

Permita o TLS em uma política do fluxo de correio do CHAPÉU para um ouvinte

através do CLI

1. Use o **listenerconfig > editam o** comando a fim escolher um ouvinte que você quer configurar.
2. Use os **hostaccess > o comando default** a fim editar os ajustes do CHAPÉU do padrão do ouvinte.
3. Incorpore uma destas escolhas a fim mudar o ajuste TLS quando você é alertado:
   ```
   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.
   ```
   Note que este exemplo pede que você use o comando do **certconfig** a fim se assegurar de que haja um certificado válido que possa ser usado com o ouvinte. Se você não criou nenhuns Certificados, o ouvinte usa o certificado da demonstração que é instalado no dispositivo. Você pode permitir o TLS com o certificado da demonstração para propósitos testando, mas não é seguro e não é recomendado para o uso geral. Use o **listenerconfig > editam > comando certificate** a fim atribuir um certificado ao ouvinte.Uma vez que você configurou o TLS, o ajuste está refletido no sumário do ouvinte no 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. Inscreva o **comando commit** a fim permitir a mudança.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- Use o arquivo de registro do correio de texto e veja este documento: Determine se o ESA está usando o TLS para a entrega ou a recepção
- Rastreamento de mensagem do uso: GUI: Monitor > rastreamento de mensagem
- Relatório do uso: GUI: Monitor > conexões TLS
- Use um Web site da terceira parte tal como checktls.com

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Você pode especificar se o ESA envia um alerta se a negociação TLS falha quando as mensagens estão entregadas a um domínio que exija uma conexão TLS. O mensagem de alerta contém o nome do domínio do destino para a negociação falhada TLS. O ESA envia o mensagem

de alerta a todos os receptores ajustados para receber alertas de advertência do nível de seriedade para tipos do alerta do sistema. Você pode controlar receptores alertas através da página da administração do sistema > dos alertas no GUI (ou através do comando do **alertconfig no** CLI).

Informações Relacionadas

- O utilizador final guia AsyncOS para o email
- Suporte Técnico e Documentação - Cisco Systems