Perguntas mais frequentes da configuração TLS para o ESA

Índice

Introdução

Este documento descreve perguntas mais frequentes sobre a configuração do Transport Layer Security (TLS) na ferramenta de segurança do email (ESA).

Que é TLS?

Como definido no RFC 3207, o “TLS é uma extensão ao serviço S TP que permite que um servidor SMTP e um cliente usem o Transport Layer Security para fornecer uma comunicação privada, autenticada sobre o Internet. O TLS é um mecanismo popular para aumentar comunicações TCP com privacidade e autenticação.” A aplicação STARTTLS no ESA fornece a privacidade com a criptografia. Permite que você importe um certificado X.509 e uma chave privada de um serviço do Certificate Authority, ou usa um certificado auto-assinado.

Que é exigido para permitir o TLS no ESA?

As seguintes etapas são necessárias para permitir o TLS:

> Nota: O ESA inclui um certificado da demonstração para propósitos testando. O certificado do programa demonstrativo não é seguro e não é recomendado para o uso geral.

Para mais informação refira exigências da instalação certificada ESA.

Como permitir o TLS para receber?

As seguintes etapas são necessárias para exigir o TLS dos host remotos que comunicam-se com

seu ouvinte público ESA (recepção). Permita o TLS na tabela do acesso host (CHAPÉU) do ouvinte que se comunica com os host remotos:

1. Vá ao GUI: Envie políticas > políticas do fluxo de correio
2. Selecione o ouvinte a que os host remotos conectarão do ouvinte deixam cair para baixo o menu na página das políticas do fluxo de correio.
3. Permita o TLS em umas ou várias políticas do fluxo de correio clicando o nome da política e verificando a caixa de verificação do uso TLS na parte inferior da página da política da edição.

Para mais informação, refira como permitir o TLS para a criptografia da conexão de entrada no ouvinte ESA?

Como permitir o TLS para a entrega?

As seguintes etapas são necessárias para permitir o TLS para a entrega aos anfitriões nos domínios remotos.

1. Vá ao GUI: Envie políticas > controles do destino
2. Adicionar um destino novo para o domínio a que você estará usando o TLS
3. Ajuste o limite da concorrência, o limite destinatário, e o perfil do salto, ou aceite os valores padrão.
4. Aplique um ajuste TLS para o domínio (`não`, `preferido`, ou `exigido`)

Para mais informação, refira como faz a negociação do controle TLS I na entrega?

Como posso eu determinar se o ESA está usando o TLS?

Os logs do correio ESA contêm entradas para conexões TLS bem sucedidas e falhadas. Você pode usar ferramentas da linha de comando tais como o **grep** para procurar por entradas de registro específicas. Você pode igualmente configurar alertas do sistema quando as conexões TLS falham através do GUI: A administração do sistema > alerta a página ou o comando do alertconfig CLI.

Para mais informação, consulte para determinar se o ESA está usando o TLS para a entrega ou a recepção

Para mais informação veja Cisco AsyncOS para uma comunicação de criptografia do capítulo do Guia do Usuário do email com o outro MTAs.

Informações Relacionadas

- O utilizador final guia AsyncOS para o email