Controle a negociação TLS na entrega no ESA

Índice

Introdução

Este documento descreve como controlar a negociação do Transport Layer Security (TLS) na entrega na ferramenta de segurança do email (ESA).

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.”

Permita o TLS na entrega

Você pode exigir STARTTLS para a entrega do email aos domínios específicos com qualquer um um destes métodos descritos neste documento:

- Use o comando do **destconfig** CLI.
- Do GUI escolha **políticas do correio > controles do destino**.

O destino controla a página ou o comando do **destconfig** permite que você especifique cinco ajustes diferentes para o TLS para um domínio dado quando você inclui um domínio. Além, você pode ditar se a validação do domínio é necessária.

Definições do ajuste TLS

Ajuste TLS	Significado
Padrão	O ajuste do padrão TLS que está ajustado quando você usar a página dos controles do desti ou o **destconfig - >** subcommand do **padrão** usado para conexões de saída do ouvinte ao agente de transferência de mensagem (MTA) para o domínio. O valor “padrão” é ajustado se você responde **não à** pergunta: “Você deseja aplicar um ajuste específico TLS para este domínio?”
1. **Não**	O TLS não é negociado para conexões de saída da relação ao MTA para o domínio.
2. **Preferido**	O TLS é negociado da relação ESA ao MTA para o domínio. Contudo, se a negociação TLS falha (antes de receber uma resposta 220), a transação de SMTP continua “na claro” (não cifrado). Nenhuma tentativa está feita para verificar se o certificado origina de um Certificate

	Authority confiado. Se um erro ocorre depois que a resposta 220 está recebida, a transação d SMTP não cai de volta ao texto claro.
3. **Necessário**	O TLS é negociado da relação ESA ao MTA para o domínio. Nenhuma tentativa é feita para verificar o certificado do domínio. Se a negociação falha, nenhum email está enviado através conexão. Se a negociação sucede, o correio está entregado através de uma sessão de criptografia.
4. **Preferido (verifique)**	O TLS é negociado do ESA ao MTA para o domínio. O dispositivo tenta verificar o certificado do domínio. Três resultados são possíveis: • O TLS é negociado e o certificado é verificado. O correio é entregado através de uma sessão de criptografia. • O TLS é negociado, mas o certificado não é verificado. O correio é entregado através de uma sessão de criptografia. • Nenhuma conexão TLS é feita e, o certificado não é verificado subseqüentemente. O mensagem de Email é entregado no texto simples.
5. **Exigido (verifique)**	O TLS é negociado do ESA ao MTA para o domínio. A verificação do certificado do domínio é exigida. Três resultados são possíveis: • Uma conexão TLS é negociada e o certificado é verificado. O mensagem de Email é entregado através de uma sessão de criptografia. • Uma conexão TLS é negociada, mas o certificado não é verificado por uma autoridade confiada de Cerfificate (CA). O correio não é entregado. • Uma conexão TLS não é negociada. O correio não é entregado.

Permita o TLS no GUI

1. Escolha **Montior > controles do destino**.
2. O clique **adiciona o destino**.
3. Adicionar o domínio do destino no campo de destino.
4. Selecione o método do apoio TLS da lista de drop-down do apoio TLS.
5. O clique **submete-se** a fim submeter as mudanças.

Permita o TLS no CLI

Este exemplo usa o comando do **destconfig** a fim exigir conexões TLS e conversações cifradas para o domínio *example.com*. Note que este exemplo mostra que o TLS está exigido para um domínio que use o certificado da demonstração 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.

O valor “padrão” é ajustado se você responde **não à** pergunta: “Você deseja aplicar um ajuste específico TLS para este domínio?” Se você responde **sim**, escolha o **nenhum**, **preferido**, ou **exigido**.

```
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
```