Configurar MTA-STS de saída do Secure Email Gateway

Contents

Introdução

Este documento descreve as etapas para configurar o Agente de Transferência de Correio de Saída do Secure Email Gateway (SEG) - Segurança de Transporte Estrita (MTA-STS).

Pré-requisitos

Requisitos

Conhecimento geral das configurações gerais do Cisco Secure Email Gateway (SEG).

Componentes Utilizados

Esta instalação requer:

- Cisco Secure Email Gateway (SEG) AsyncOS 16.0 ou mais recente.
- Perfis de controle de destino.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Agente de transferência de e-mail - O MTA-STS (Strict Transport Security) é um protocolo que impõe o uso de conexões TLS seguras com uma camada de proteção segura adicional. O MTA-STS ajuda a evitar ataques de intermediários e espionagem, garantindo que os e-mails sejam enviados por canais seguros e criptografados.

O SEG AsyncOS 16 e mais recente pode executar a entrega de mensagens MTA-STS de saída para domínios de recebimento configurados MTA-STS.

Quando ativado, o SEG verifica os perfis de controle de destino quanto às configurações de MTA-STS. O SEG inicia o processo MTA-STS para buscar, validar e aplicar o registro e a política definidos, garantindo que a conexão com o MTA receptor seja segura por TLSv1.2 ou superior.

Os proprietários de domínio de recebimento são responsáveis por criar, publicar e manter o Registro DNS e a Política MTA-STS.

Como o MTA-STS funciona para o SEG

- O domínio de recebimento mantém a política MTA-STS e o registro de texto MTA-STS DNS.
- O MTA do Domínio de Envio deve ser um MTA-STS capaz de resolver e agir sobre a Política MTA-STS do domínio de destino.

O proprietário do domínio de e-mail de recebimento publica um registro de texto MTA-STS via DNS conforme descrito aqui:

- O registro de texto aciona o SEG para verificar a política MTA-STS, hospedada em um servidor Web habilitado para HTTPS.
- A política especifica os parâmetros para comunicação com o domínio.
    - Contém hosts MX MTA-STS a serem recebidos.
    - O modo é definido como Modo de teste ou Modo de aplicação
    - TLSv1.2 ou superior é necessário.

- O MTA-STS usa registros TXT DNS para descoberta de política. Ele busca a política MTA-STS de um host HTTPS.
- Durante o handshake TLS, iniciado para buscar uma política nova ou atualizada do host de política, o servidor HTTPS deve apresentar um certificado X.509 válido para o DNS-ID "MTA-STS".

Os aspectos do domínio de envio de e-mail :

- Quando um SEG (MTA de envio) envia um e-mail para um domínio MTA-STS, ele primeiro verifica a política MTA-STS do domínio do destinatário.
- Se a política estiver configurada com o Modo de imposição, o servidor de e-mail de envio tentará estabelecer uma conexão segura e criptografada com o servidor de e-mail de recebimento (MTA de recebimento). Se uma conexão segura não puder ser estabelecida (por exemplo, se o certificado TLS for inválido ou a conexão for submetida a downgrade para um protocolo não seguro), o e-mail falhará na entrega e o remetente será notificado da falha.

RFC8461

Configurar

As ações preliminares são recomendadas durante a configuração:

1. Verifique se o domínio de destino tem um registro DNS MTA-STS e um registro de política configurados corretamente, antes de configurar o Perfil de Controle de Destino SEG.

- Isso é executado com mais eficiência acessando as páginas da Web do verificador MTA-STS.
  - Pesquisa do Google "verificar domínio MTA-STS"
  - Escolha um site de verificação nos resultados da pesquisa.
  - Digite o domínio de destino.
- Configure domínios somente depois que a verificação de verificação tiver sido concluída.

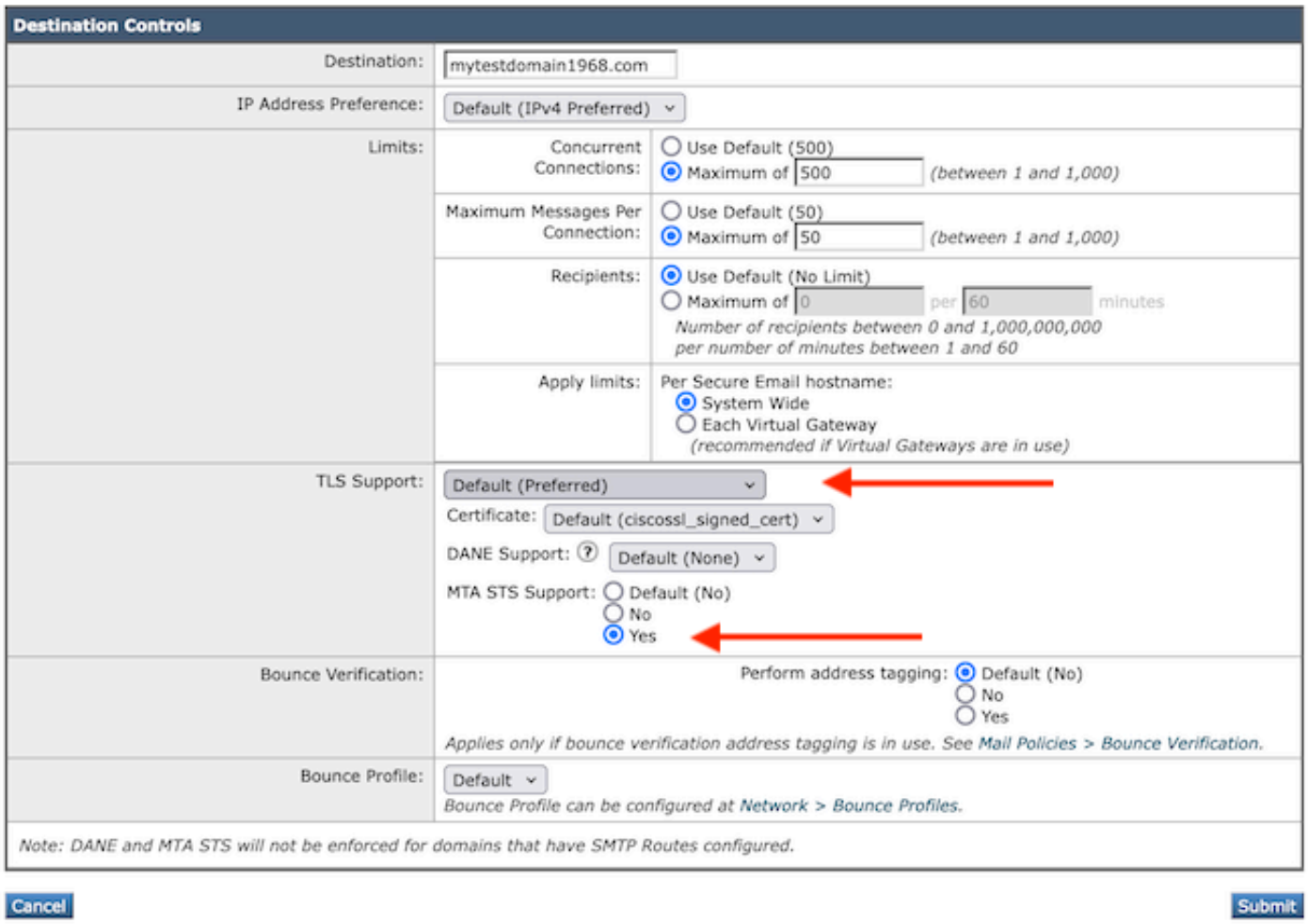
2. Não use MTA-STS na Política Padrão de Controles de Destino.

- Cada Perfil de Controle de Destino configurado para utilizar MTA-STS adiciona uma pequena carga ao SEG. Se a política de controle de destino padrão tivesse MTA-STS configurado, sem verificar o domínio, ela poderia afetar o serviço SEG.

Configuração de WebUI

- Navegue até Políticas de e-mail > Página Controles de destino.
- Selecione Add Destination Controls ou edite um Destination Control Profile existente.
  - As configurações de suporte TLS permitem qualquer configuração, exceto Nenhum, acomodando várias opções de suporte TLS.
  - O submenu DANE Support Options inclui Mandatory, Opportunistic ou None.
  - Configuração de suporte a MTA-STS = Sim
- Selecione Submit seguido de Commit para aplicar as alterações.

Note: Se o MTA de recebimento residir em um ambiente hospedado como Gsuite ou O365, configure o TLS de controles de destino para TLS necessário - Verificar domínios hospedados.



Perfil de Controle de Destino

Avisos de interoperabilidade:

O Suporte DANE tem precedência sobre o MTA STS e pode afetar as ações tomadas:

- Se o DANE tiver êxito, o MTA-STS será ignorado e o correio será entregue.
- Se o DANE obrigatório falhar, o e-mail não será entregue.
- Se o DANE Opportunistic falhar, e o MTA-STS for ignorado devido a erros de configuração, o SEG tentará entregar usando a configuração TLS configurada.
- O MTA-STS não será aplicado se uma rota SMTP estiver configurada para o domínio.

Configuração de CLI

- desconfig
  - novo/editar
    - Insira as opções preferidas até que o item de menu de opções de TLS seja apresentado.
    - As opções 2-6 para TLS suportam MTA-STS.

Deseja aplicar uma configuração TLS específica para este domínio? [N]> y

Deseja usar o suporte TLS?
1. Não

2. Preferido
3. Obrigatório
4. Preferencial - Verificar
5. Obrigatório - Verificar
6. Obrigatório - Verificar Domínios Hospedados
[2]>2

Você optou por habilitar o TLS. Use o comando certconfig para garantir que haja um certificado válido configurado.
Deseja configurar o suporte DANE? [N]>

Deseja configurar o Suporte MTA STS? [N]> y

Deseja usar o suporte MTA STS?
1. Desligado
2. Em
[1]> 2

O MTA STS não é imposto para domínios que têm Rotas SMTP configuradas:

1. Preencha as opções restantes para finalizar o Perfil de Controle de Destino específico.
2. Aplique as alterações usando Enviar > Confirmar.

Verificar

info level mail_logs:

```
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(mta-test.domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

debug level mail_logs:

```
Thu Sep 26 15:23:39 2024 Debug: DNS query: Q(_mta-sts.domain.com, 'TXT')
Thu Sep 26 15:23:39 2024 Debug: DNS query: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Debug: DNS encache (_mta-sts.domain.com, TXT, [(131794459543073830L, 0, 'insec
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(domain.com)
Thu Sep 26 15:23:39 2024 Debug: Valid cache entry found for the domain (domain.com).Thu Sep 26 15:23:39
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (domain.com,'MX','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Info: Applying MTA-STS policy for the domain (domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Debug: DNS query: Q(domain.com, 'MX')
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
```

```
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

Recebendo TLS v1.3 suportado por SEG:

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

Ter Set 24 09:13:52 2024 Depuração: Consulta DNS: P(_mta-sts.domain.com, 'TXT')
Ter Set 24 09:13:52 2024 Depuração: Consulta DNS: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
Ter Set 24 09:13:52 2024 Depuração: Consulta DNS: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Ter Set 24 09:13:52 2024 Depuração: Cache DNS (_mta-sts.domain.com, TXT, [(1313665257015805O8L, 0, 'inseguro', ('v=STSv1; id=12345678598Z;',)])
Ter Set 24 09:13:52 2024 Informações: Êxito ao buscar registro TXT MTA-STS para o domínio (domain.com)
Ter Set 24 09:13:52 2024 Depuração: Buscar política MTA-STS para o domínio(domain.com)
Ter Set 24 09:13:52 2024 Depuração: Solicitando busca de política MTA-STS via proxy
Ter Set 24 09:13:52 2024 Depuração: Falha na solicitação de busca da política STS devido a um tempo limite de conexão., para o domínio domain.com
Ter Set 24 09:13:52 2024 Informações: Falha ao buscar a política MTA-STS para o domínio (domain.com)

Qui Set 19 13:04:50 2024 Informações: Êxito ao buscar registro TXT MTA-STS para o domínio (domain.com)
Qui Set 19 13:04:50 2024 Depuração: Buscar política MTA-STS para o domínio(domain.com)
Qui Set 19 13:04:50 2024 Depuração: Solicitando busca de política MTA-STS via proxy
Qui Set 19 13:04:50 2024 Depuração: Falha na solicitação de busca da política STS devido a um tempo limite de conexão., para o domínio domain.com
Qui Set 19 13:04:50 2024 Informações: Falha ao buscar a política MTA-STS para o domínio (domain.com)

Qui Set 19 13:04:50 2024 Informações: MID 5411 na fila para entrega

Troubleshooting

1. Se o SEG falhar ao entregar com o erro "peer cert does not match domain.com".

Indica que o destino é um serviço hospedado, como G Suite ou M365. Altere a configuração TLS do Perfil de Controles de Destino > TLS Necessário - Verificar Domínios Hospedados:

```
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS deferring: verify error: peer cert does not match domain
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS was required but could not be successfully negotiated
```

2. A comunicação falhará se os certificados de envio ou de recebimento não estiverem configurados corretamente ou tiverem expirado.

3. O SEG precisa verificar se os certificados raiz e intermediários de destino adequados estão nas Listas de autoridades de certificação.

4. Testes simples de Telnet do SEG cli para verificar o Registro de texto DNS e um teste básico de resposta para o servidor Web de políticas.

- Consulta DNS da cli > dig _mta-sts.domain.com txt:

;; SEÇÃO DE RESPOSTA:
_mta-sts.domain.com. 0 IN TXT "v=STSv1; id=12345678598Z;"

- Faça Telnet para verificar a acessibilidade do servidor web básico a partir de cli > telnet mta-sts.domain.com 443:
- Use um navegador da Web regular para exibir a Política MTA-STS.
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

```
version: STSv1
mode: enforce
mx: *.mail123.domain.com
max_age: 604800
```

Informações Relacionadas

- Página inicial do Cisco Secure Email Gateway para guias de suporte

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.