配置安全邮件网关出站MTA-STS

目录

简介

本文档介绍配置安全邮件网关(SEG)出站邮件传输代理 — 严格传输安全(MTA-STS)的步骤。

先决条件

要求

思科安全邮件网关(SEG)常规设置和配置的一般知识。

使用的组件

此设置要求：

- 思科安全邮件网关(SEG)AsyncOS 16.0或更高版本。
- 目标控制配置文件。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

邮件传输代理 — 严格传输安全(MTA-STS)是一种通过增加的安全保护层强制使用安全TLS连接的协议。MTA-STS通过确保邮件通过安全的加密通道发送，帮助防止中间人攻击和窃听。

SEG AsyncOS 16和更新版本可以执行出站MTA-STS消息传送至已配置的MTA-STS接收域。

启用时，SEG会检查目标控制配置文件的MTA-STS设置。SEG启动MTA-STS进程以获取、验证和应用定义的记录和策略，从而确保通过TLSv1.2或更高版本安全地连接到接收MTA。

接收域所有者负责创建、发布和维护DNS记录和MTA-STS策略。

MTA-STS如何为SEG工作

- 接收域维护MTA-STS策略和MTA-STS DNS文本记录。
- 发送域MTA必须是能够根据目标域MTA-STS策略进行解析和操作的MTA-STS。

接收邮件域所有者通过DNS发布MTA-STS文本记录，如下所述：

- txt记录触发SEG检查托管在启用HTTPS的Web服务器上的MTA-STS策略。
- 策略指定用于与域通信的参数。
    - 包含要接收的MTA-STS MX主机。
    - 模式定义为测试模式或实施模式
    - 需要TLSv1.2或更高版本。

- MTA-STS使用DNS TXT记录进行策略发现。它从HTTPS主机获取MTA-STS策略。
- 在TLS握手期间，HTTPS服务器必须针对“MTA-STS”DNS-ID提供有效的X.509证书。

发送邮件域方面：

- 当SEG（发送MTA）向MTA-STS域发送邮件时，它首先检查收件人域MTA-STS策略。
- 如果策略配置为Enforce Mode，则发送邮件服务器会尝试与接收邮件服务器（接收MTA）建立安全的加密连接。 如果无法建立安全连接（例如，如果TLS证书无效或连接降级为不安全的协议），邮件将无法传送，发件人将收到失败通知。

RFC8461

配置

安装过程中建议采取初步措施：

1.在配置SEG目标控制配置文件之前，验证目标域是否具有正确配置的MTA-STS DNS记录和策略记录。

- 通过访问MTA-STS检查器网页最有效地执行此任务。
    - Google搜索“验证MTA-STS域”
    - 从搜索结果中选择验证网站。
    - 输入目标域。
- 只有验证检查完成后才能配置域。

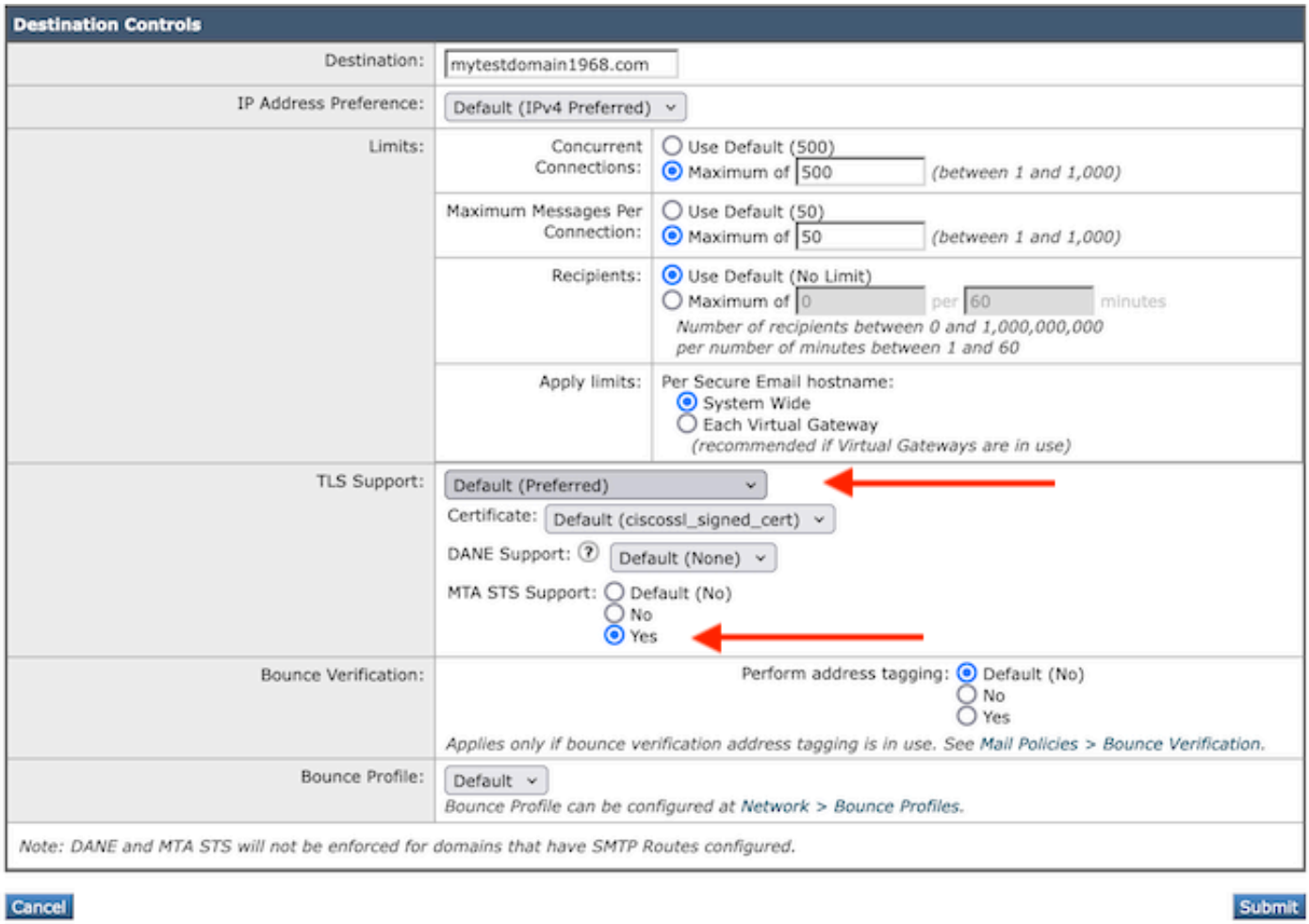
2. 不在Destination Controls Default Policy上使用MTA-STS。

- 配置为使用MTA-STS的每个目标控制配置文件会为SEG增加较小的负担。如果默认目标控制策略配置了MTA-STS，而不验证域，可能会影响SEG服务。

WebUI配置

- 导航到邮件策略>目标控制页面。
- 选择Add Destination Controls或编辑现有目标控制配置文件。
  - TLS支持设置允许除None之外的任何设置，以适应各种TLS支持选项。
  - 子菜单DANE Support Options包括Mandatory、Opportunistic或None。
  - MTA-STS支持设置=是
- 选择Submit，然后选择Commit以应用更改。

注意：如果接收MTA驻留在Gsuite或O365等托管环境中，请将目标控制TLS配置为TLS必需验证托管域。



目标控制配置文件

互操作性注意事项：

DANE支持优先于MTA STS，并可能影响所采取的操作：

- 如果DANE成功，则会跳过MTA-STS并发送邮件。
- 如果DANE强制失败，则不传送邮件。
- 如果DANE Opportunity失败，并且由于配置错误而跳过MTA-STS，则SEG会尝试使用配置的TLS设置进行传送。
- 如果为域配置了SMTP路由，则不会应用MTA-STS。

CLI 配置

- destconfig
  - 新建/编辑
    - 输入首选选项，直到显示TLS选项菜单项。
    - TLS选项2-6支持MTA-STS。

是否要为此域应用特定TLS设置？[N]> y

是否要使用TLS支持？
1.否
2.首选
3.必填
4.首选 — 验证
5.必需 — 验证
6.必需 — 验证托管域
[2]>2

您已选择启用TLS。请使用certconfig命令确保配置了有效的证书。
是否要配置DANE支持？[N]>

是否要配置MTA STS支持？[N]> y

是否要使用MTA STS支持？
1.关闭
2.打开
[1]> 2

对于配置了SMTP路由的域，不实施MTA STS:

1. 完成其余选项以完成特定目标控制配置文件。
2. 使用Submit > Commit应用更改。

验证

信息级别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 su
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
```

接收支持SEG的TLS v1.3:

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

2024年9月24日星期二09:13:52 2024调试：DNS查询：Q(_mta-sts.domain.com, 'TXT')
2024年9月24日星期二09:13:52 2024调试：DNS查询：QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
2024年9月24日星期二09:13:52 2024调试：DNS查询：QIP(_mta-sts.domain.com,'TXT','10.10.5.61',15)
2024年9月24日星期二09:13:52 2024调试：DNS缓存(_mta-sts.domain.com, TXT，[(13136652570158050 8L， 0, 'insecure',('v=STSv1;id=12345678598Z;',)])
2024年9月24日星期二09:13:52 2024信息：已成功获取域(domain.com)的MTA-STS TXT记录
2024年9月24日星期二09:13:52 2024调试：获取域的MTA-STS策略(domain.com)
2024年9月24日星期二09:13:52 2024调试：通过代理请求MTA-STS策略获取
2024年9月24日星期二09:13:52 2024调试：由于连接超时，请求获取STS策略失败。对于域domain.com
2024年9月24日星期二09:13:52 2024信息：获取域的MTA-STS策略时遇到故障(domain.com)

2024年9月19日周四13:04:50信息：已成功获取域(domain.com)的MTA-STS TXT记录
2024年9月19日周四13:04:50调试：获取域的MTA-STS策略(domain.com)
2024年9月19日周四13:04:50调试：通过代理请求MTA-STS策略获取
2024年9月19日周四13:04:50调试：由于连接超时，请求获取STS策略失败。对于域domain.com
2024年9月19日周四13:04:50信息：获取域的MTA-STS策略时遇到故障(domain.com)

2024年9月19日周四13:04:50信息：MID 5411已排队等待交付

故障排除

1.如果SEG传送失败，并出现“peer cert does not match domain.com”错误。

这表示目标为托管服务，例如G Suite或M365。请更改目标控制配置文件TLS设置>需要TLS — 验证托管域:

```
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.如果发送或接收证书配置不正确或过期，通信将失败。

3. SEG需要验证证书颁发机构列表中是否存在正确的目标中间证书和根证书。

4.从SEG cli执行简单的Telnet测试，以验证DNS文本记录和对策略Web服务器的基本响应测试。

- 从cli > dig _mta-sts.domain.com txt执行DNS查询：

;；答案部分：
_mta-sts.domain.com。0，以TXT“v=STSv1;id=12345678598Z;"

- 通过Telnet从cli > telnet mta-sts.domain.com 443验证基本Web服务器的可访问性：
- 使用常规的Web浏览器查看MTA-STS策略。
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

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

相关信息

- 支持指南的思科安全邮件网关发布页面

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。