

配置安全邮件网关的TLSv1.3

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[概述](#)

[配置](#)

[WebUI中的配置](#)

[CLI配置：](#)

[验证](#)

[相关信息](#)

简介

本文档介绍思科安全邮件网关(SEG)的TLS v1.3协议的配置。

先决条件

需要具备SEG设置和配置的一般知识。

使用的组件

- 本文档中的信息基于以下软件和硬件版本：
 - 思科安全邮件网关(SEG) AsyncOS 15.5.1及更高版本。
- SEG SSL Configuration Settings。

"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

SEG集成了TLS v1.3协议，可加密SMTP和HTTPS相关服务的通信；传统UI、NGUI和Rest API。

TLS v1.3协议具有更高的通信安全性和更快的协商速度，因为业界正在努力将其用作标准。

SEG使用SSL的SEG WebUI或CLI中的现有SSL配置方法，并突出显示一些重要设置。

- 配置允许的协议时提供预防性建议。
- 密码不能被操纵。
- TLS v1.3可以针对GUI HTTPS、入站邮件和出站邮件进行配置。
- TLS v1.0到TLS v1.3之间的TLS协议复选框选择选项使用本文中更详细地演示的模式。

配置

SEG在AsycOS 15.5中集成了HTTPS和SMTP的TLS v1.3协议。建议选择协议设置以防止HTTPS和电子邮件传送/接收失败。

在撰写本文时，Cisco SEG的先前版本在高端支持TLS v1.2，同时支持TLS v1.2的其他电子邮件提供商（例如MS O365）。

TLS v1.3协议的Cisco SEG实施支持3个默认密码，这些密码不能在其他协议允许的情况下在SEG密码配置设置中更改或排除。

现有SEG SSL配置设置仍允许对密码套件进行TLS v1.0、v1.1、v1.2处理。

TLS 1.3密码：

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

WebUI中的配置

导航到>系统管理> SSL配置

- 升级到15.5 AsyncOS后的默认TLS协议选择仅包括TLS v1.1和TLS v1.2。
- “其他TLS客户端服务”(Other TLS Client Services)的设置使用TLS v1.1和TLS v1.2，并带有选择、仅使用TLS v1.0的选项。

SSL Configuration			
GUI HTTPS:	Methods:	TLS v1.2 TLS v1.1	
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE-RSA- AES256-CCM:!DHE-RSA-AES256-SHA	
	TLS Renegotiation:	Enabled	
Inbound SMTP:	Methods:	TLS v1.2 TLS v1.1	
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:- EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE-RSA- AES256-CCM:!DHE-RSA-AES256-SHA	
	TLS Renegotiation:	Enabled	
Outbound SMTP:	Methods:	TLS v1.2 TLS v1.1	
	SSL Cipher(s) to use:	ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:A ES256:!3DES:!IDEA:!SRP:IAESGCM+DH+aRSA:IAESG CM+RSA:!aNULL:!eNULL:!kRSA:@STRENGTH:- aNULL:-EXPORT:-IDEA:!DHE-RSA-AES128-CCM:!DHE- RSA-AES256-CCM:!ECDHE-ECDSA-CAMELLIA128- SHA256:!ECDHE-RSA-CAMELLIA128-SHA256:!ECDHE- ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA- CAMELLIA256-SHA384:!ECDHE-ECDSA-AES128- CCM:!ECDHE-ECDSA-AES256-CCM:!DHE-RSA-AES256- SHA	
	Other TLS Client Services: ?		
Other TLS Client Services:	<div style="border: 1px solid red; padding: 5px;"> <p>Other TLS Client Services</p> <p>TLS method is applicable for the following services:</p> <p>LDAP Updater Client SMTP Call-Ahead Remote Syslog Server</p> </div>		
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled	
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled	

选择“Edit Settings”（编辑设置）以显示配置选项。

- TLS v1.1和TLS v1.2已选中，且活动框用于选择其他协议。
- 每个TLS v1.3旁边的？是静态密码选项的重复。
- “其他TLS客户端服务：”(Other TLS Client Services：)现在提供仅使用TLS v1.0的选项（如果选择此项）。


SSL Configuration		
GUI HTTPS:	Methods:	<input type="checkbox"/> TLS v1.3 ? <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!e
	TLS Renegotiation:	<input checked="" type="checkbox"/> Enable
Inbound SMTP:	Methods:	<input type="checkbox"/> TLS v1.3 ? <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!e
	TLS Renegotiation:	<input checked="" type="checkbox"/> Enable
Outbound SMTP:	Methods:	<input type="checkbox"/> TLS v1.3 ? <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0
	SSL Cipher(s) to use:	ECDH+aRSA:ECDH+ECDSA:DHE+DSS+
Other TLS Client Services: ?	Methods:	<input type="checkbox"/> TLS v1.0
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	<input type="checkbox"/> Enable
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	<input type="checkbox"/> Enable

Informational ? for TLS Default Ciphers

Note:
 TLS protocols can be enabled only in sequence.
 The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

TLS协议选择选项包括TLS v1.0、TLS v1.1、TLS v1.2、TLS v1.3。

- 升级到AsyncOS 15.5后，默认情况下仅选择TLS v1.1和TLS v1.2协议。

 注意：TLS1.0已弃用，因此默认为禁用。如果所有者选择启用TLS v1.0，则它仍然可用。


- 复选框选项亮起，显示可用协议的粗体框和显示不兼容选项的灰色框。
- 图像中的示例选项说明了复选框选项。

<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3
<input checked="" type="checkbox"/> TLS v1.2	<input checked="" type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2
<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1	<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1
<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0

<input checked="" type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input checked="" type="checkbox"/> TLS v1.3
<input checked="" type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2
<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1
<input type="checkbox"/> TLS v1.0	<input checked="" type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0

提交后所选TLS协议的示例视图。

SSL Configuration		
GUI HTTPS:	Methods:	TLS v1.3 [?] TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:!aNULL:- EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Inbound SMTP:	Methods:	TLS v1.3 [?] TLS v1.2 TLS v1.1 TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:!aNULL:- EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Outbound SMTP:	Methods:	TLS v1.3 [?] TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!D ES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA! ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:!aNULL:- EXPORT:!IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA- AES128-CCM:!DHE-RSA-AES256-CCM:!ECDHE-ECDSA- CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128- SHA256:!ECDHE-ECDSA-CAMELLIA256- SHA384:!ECDHE-RSA-CAMELLIA256-SHA384:!ECDHE- ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM
Other TLS Client Services: [?]	Methods:	TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled

 注意：对GUI HTTPS TLS协议的修改会由于https服务重置而导致WebUI短时间断开连接。

CLI 配置：

SEG允许3个服务使用TLS v1.3：

- GUI HTTPS
- 入站SMTP
- 出站SMTP

执行命令> sslconfig时，会输出当前为GUI HTTPS、入站SMTP、出站SMTP配置的协议和密码

- GUI HTTPS方法：t1sv1_0t1sv1_1t1sv1_2t1sv1_3
- 入站SMTP方法：t1sv1_0t1sv1_1t1sv1_2t1sv1_3
- 出站SMTP方法：t1sv1_1t1sv1_2t1sv1_3

选择要执行的操作：

- GUI -编辑GUI HTTPS ssl设置。
- 入站-编辑入站SMTP ssl设置。


- 出站-编辑出站SMTP ssl设置。

[]>入站

输入要使用的入站SMTP SSL方法。

1. TLS v1.3
2. TLS v1.2
3. TLS v1.1
4. TLS v1.0

[2-4]> 1-3

 注意：SEG选择流程可以包括单个菜单编号（例如2）、一系列菜单编号（例如1-4）或用逗号1、2、3分隔的菜单编号。

CLI sslconfig后续提示通过按enter键或修改设置接受现有值。

使用命令> commit >>输入可选注释>>按Enter键完成更改。

验证

本节包括一些基本测试方案和由于TLS协议版本不匹配或语法错误而可能出现的错误。

由于目标不支持的TLS v1.3而生成拒绝的SEG传出SMTP协商的日志条目示例：

```
Wed Jan 17 20:41:18 2024 Info: DCID 485171 TLS deferring: (336151598, 'error:1409442E:SSL routines:ssl3
```

接收成功协商的TLS v1.3的发送SEG的日志条目示例：

```
Wed Jan 17 21:09:12 2024 Info: DCID 485206 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```


未启用TLS v1.3的接收SEG的日志条目示例。

```
Wed Jan 17 20:11:06 2024 Info: ICID 1020004 TLS failed: (337678594, 'error:14209102:SSL routines:tls_ea
```

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
```

要验证您的浏览器功能，只需打开一个到配置了TLSv1.3的SEG WebUI或NGUI的Web浏览器会话。

 注意：我们测试的所有网络浏览器均已配置为接受TLS v1.3。

- 测试：在Firefox上配置浏览器设置禁用TLS v1.3支持会在设备的ClassicUI和NGUI上生成错误。
- 将Firefox配置为排除TLS v1.3的传统UI用作测试。
- NGUI将收到相同的错误，唯一的例外是URL中的端口号4431（默认）。

Secure Connection Failed

An error occurred during a connection to dh6062-esa1.iphmx.com. Peer reports incompatible or unsupported protocol version.

Error code: SSL_ERROR_PROTOCOL_VERSION_ALERT

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox.

[Learn more...](#)

It looks like your network security settings might be causing this. Do you want the default settings to be restored?

- 为确保通信，请验证浏览器设置，以确保包含TLSv1.3。(此示例来自Firefox，使用数字1-4)

security.tls.version.fallback-limit	4
security.tls.version.max	4
security.tls.version.min	3

相关信息

- [思科安全邮件网关-设置指南](#)
- [支持指南的思科安全电邮网关发布页面](#)
- [思科安全邮件网关-版本说明](#)

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）。