统一边界网元SIP TLS配置示例

目录

简介

Cisco Unified Border Element (多维数据集)支持会话初始化协议(SIP)对与传输层安全(TLS)的SIP呼叫。TLS提供SIP信令消息保密性和数据完整性在通信的两应用程序之间的。TLS被分层堆积在一个可靠传输协议顶部例如TCP。

在多维数据集的TLS可以配置根据每段基本类型为了允许TLS对非TLS SIP呼叫。同样地，而SIP段使用TLS，多维数据集使用IPSec为了绑信令和支持呼叫从H.323到SIP上用H.323段。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 基础知识如何配置和使用Cisco IOS语音(例如dial-peer)
- 基础知识如何配置和使用多维数据集
- 与基本安全概念的熟悉例如加密、证明、证书权限、PKI (密钥)和验证

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 求使用Cisco IOS版本12.4T在ISR的版本的立方
- 作为Certificate Authority (CA)配置的Cisco IOS路由器

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

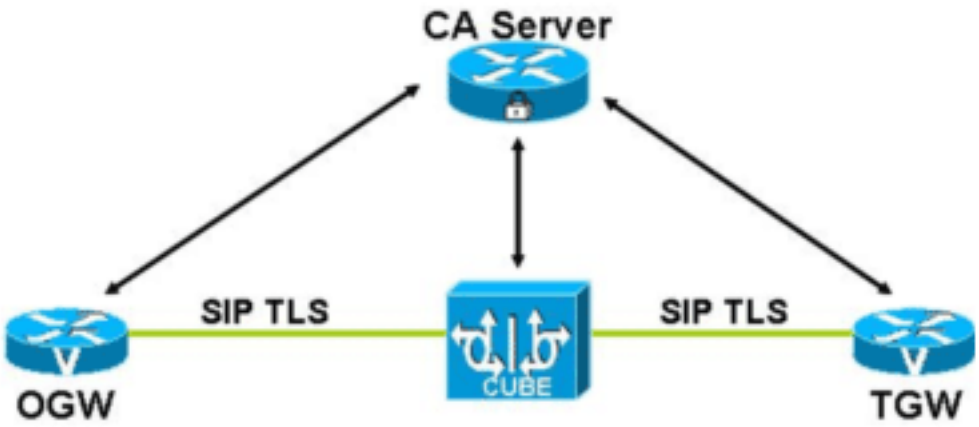
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

此图显示多维数据集示例与SIP TLS连接的。



- 始发网关(OGW)，终端网关(TGW)和多维数据集设备用CA服务器验证并且登记。证书由CA服务器签字。
- 当呼叫被做时，例如TLS握手启动在设备(OGW和多维数据集之间)，并且IOS PKI基础设施用于交换共同性委托CA签字的证书在握手期间。
- 在TLS握手期间，动态地生成的对称密钥和密码器算法协商在设备之间。
- 在TLS握手是成功的后，设备建立在他们之间的一个SIP会话。在TLS握手进程中被交换的密钥用于加密或解密所有SIP信令消息。URI方案“饮者：”使用SIP TLS消息。

TLS的RFC支持在多维数据集

为TLS要求的密码器套件根据SIP RFC 3261包括：

- TLS_RSA_WITH_AES_128_CBC_SHA强制性
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (可选) —要求为网络服务器(例如代理和重定向服务器后向兼容性的)

仅TLS_RSA_WITH_AES_128_CBC_SHA套件是可适用的求立方和支持。同样地，在多维数据集的

TLS实施支持RFC 2246仅必须密码器套件。

SIP协议使用一个对等型号。Therfore，多维数据集可以是TLS连接的服务器或客户端并且实现两边。当它是服务器端时，多维数据集总是进行相互验证。

配置步骤

配置CA服务器

您能使用此in命令全局配置模式为了配置Cisco IOS路由器装载与加密镜像：

```
router(config)#crypto pki server <ca-server-name> router(cs-server)#no shutdown
```

注意：

- 请使用**ip http server命令**在全局配置模式为了保证HTTP服务器在作为CA服务器配置的路由器运行。这要求，因为客户端信任点(CUBE/OGW/TGW)使用HTTP为了接收从CA服务器的证书。
- 必须同步在CA服务器和客户端信任点(CUBE/OGW/TGW)的时钟。否则，也许有与CA服务器发出的证书的正确性的问题。您能使用**show clock**和**clock set**命令为了同步在Cisco IOS路由器的时钟。或者，您能部署Ntp server为了同步时钟。

多维数据集的基本配置

请使用这些命令为了启用CUBE的IP到IP网关功能。这允许呼叫的VoIP呼叫和reoriginatiion的terminatation与出局的VoIP拨号对等体的。

```
voice service voip
  allow-connections h323 to sip
  allow-connections sip to h323
  allow-connections sip to sip
  allow-connections h323 to h323
```

TLS配置

完成这些步骤为了配置在多维数据集(和其它设备的TLS类似OGW和TGW)：

1. **生成RSA密钥对**请使用此in命令全局配置模式为了生成RSA密钥对：`router(config)#crypto key generate rsa general-keys label <label> modulus 1024`
2. **创建Pki trustpoint (多维数据集)**请使用此in命令全局配置模式为了创建Pki trustpoint (多维数据集)：`router(config)#crypto pki trustpoint <ca-server-name> router(ca-trustpoint)#enrollment url <http://ca-server-ip> router(ca-trustpoint)#rsakeypair <rsa keypair label>`
3. **验证一Pki trustpoint (多维数据集)用CA服务器**请使用此in命令全局配置模式为了验证一Pki trustpoint (多维数据集)用CA服务器：`router(config)#crypto pki authenticate <ca-server-name>` 此步骤触发CA服务器发送其证书到信任点(多维数据集)，应该接受。
4. **登记一Pki trustpoint (多维数据集)用CA服务器**请使用此in命令全局配置模式：`router(config)#crypto pki enroll <ca-server-name>` 对于此步骤，您必须输入私钥保护密码。CA服务器问题两证书对信任点(多维数据集)：一确认CA服务器的和其他确认信任点(多维数据集)。您能用**show run命令**检查证书。
5. **配置TLS作为Session transport**session transport可以配置到与**session transport tcp tls** at命令的TLS二者之一全局级别在“语音服务voip下”或在适当的VoIP拨号对等体。如果session transport为VoIP拨号对等体配置(流入或流出的或者两个)，则TLS传输仅使用已配置的段。传输段对段基本类型支持TLS。

6. **配置SIP UA的默认信任点**请使用此in命令“SIP UA”模式为了配置SIP UA的默认信任点：`router(config-sip-ua)#[no] crypto signaling [(remote-addr subnet mask) | default] trustpoint <label> [strict-cipher]` 信任点标签是指作为登记proces一部分，用Cisco IOS PKI命令生成的CUBE的证书。*严格密码器*意味着SIP TLS进程使用由SIP RFC要求仅的那些密码器套件。目前， RFC 3261指定TLS_RSA_WITH_AES_128_CBC_SHA和TLS_RSA_WITH_3DES_EDE_CBC_SHA套件。当您使用时严格*密码器*命令参数避免对配置的更改，如果SIP应该要求更新的密码器。在Cisco IOS的SSL层不支持TLS_RSA_WITH_3DES_EDE_CBC_SHA。所以，多维数据集在严格模式有效利用仅TLS_RSA_WITH_AES_128_CBC_SHA套件。当严格*密码器没有*指定时， SIP TLS进程根据支持使用更加大的套密码器在SSL层。*示例 1*当建立或接受TLS连接用在1.2.3.0子网内时的一远程设备下面的命令配置多维数据集使用其信任点标签**mylabel**。密码器套件在这种情况下是由在多维数据集的SSL层支持的整体集。

   `crypto signaling remote-addr 1.2.3.0 255.255.255.0 trustpoint mylabel` *示例 2*下面的命令配置多维数据集使用其信任点标签**主厨，**当建立或接受TLS连接用所有远程设备时，除非一单个子网标签配置匹配。

   `crypto signaling default trustpoint chef` *示例 3*当建立或接受TLS连接用在1.2.3.0子网内时的一远程设备下面的命令配置多维数据集使用其信任点标签**mylabel**。在TLS握手期间使用的密码器套件对TLS_RSA_WITH_AES_128_CBC_SHA套件被限制。

   `crypto signaling remote-addr 1.2.3.0 255.255.255.0 trustpoint mylabel strict-cipher`
7. **启用TLS监听程序波尔特**发出此in命令“SIP UA”模式为了使TCP的5061 TLS端口侦听：`transport tcp tls`
8. **配置SIP URL方案**“饮者：” URL方案可以配置在VoIP拨号对等体级别下或在全局级别。此命令使用配置“饮者：”在VoIP拨号对等体：

   `voice-class sip url sips` 为了配置“饮者：”在全局级别下的URL方案，使用此in命令“语音服务voip” “sip”模式：

   `voice service voip sip url sips` 使用SIP URL在信号路径要求所有跳使用TLS和SIP。这变得重要对SRTP，当密钥是在SDP和为安全连接在明文不应该发送信息。如果代理接收与SIP的一邀请(例如，请邀请sips:123@proxy SIP /2.0)代理必须使用SIP下一跳。当TLS与无格式SIP URL一起使用时，没有保证所有跳将使用TLS，潜在危及呼叫的端到端安全。如果“啜饮”URL配置，传输自动地将是TLS。

TLS实施注释

- 当前多维数据集操作要求使用TLS作为传输，当安全媒体配置时(SRTP)。将来增强可能增强此需求。
- 当SRTP配置巩固媒介连接，时*必须*也配置TLS或IPSec保护SIP信令消息。用于SRTP加密的密钥通过信令消息被交换–没保护信令信道导致在明文交换的SRTP密钥，并且这否定SRTP安全媒介连接的。
- 当前多维数据集操作要求使用“饮者：” TLS呼叫的URI方案。将来增强可能增强此需求。
- 当前多维数据集操作验证用仅单个CA服务器。

示例配置

多维数据集

ipipgw
ipipgw#**show run** Building configuration... Current configuration : 5096 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log

datetime msec no service password-encryption ! hostname ipipgw ! boot-start-marker boot system flash c3845-adventerprisek9_ivs-mz.124-3.9.PI3a boot-end-marker ! logging buffered 10000000 debugging no logging console ! no aaa new-model ! resource policy ! ip subnet-zero ip cef ! no ip domain lookup ! voice-card 0 no dspfarm ! voice service voip **allow-connections sip to sip sip url sips ! crypto pki trustpoint ca-server enrollment url http://9.13.46.14:80 serial-number revocation-check crl rsakeypair kkp ! crypto pki certificate chain ca-server certificate 04 3082020D 30820176 A0030201 02020104 300D0609 2A864886 F70D0101 04050030 14311230 10060355 04031309 63612D73 65727665 72301E17 0D303530 39323231 37333435 315A170D 30363039 32323137 33343531 5A303431 32300F06 03550405 13084337 33323231 3333301F 06092A86 4886F70D 01090216 1270696E 612D3338 34352D69 70697067 77312E30 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100 BBCC2977 637E8E42 17EB7C26 FB2BA0A3 6E1ECECB E01A64F8 8F18200F 9837E4FA 7D908B3C 1297A4DE A403D315 C7BB96C6 50D95291 0433FA7B CB8FFFFD 8FC1C211 CCC7BCA9 140FF942 C3ACF4BC 3EDCE2DC 28FCEA87 AA83629F D217F833 A727940A 0BBB8624 3EA9D1EC 1F69228F E1DFC113 243246B7 BF57696C 2278F5C3 674EE0E1 02030100 01A34F30 4D300B06 03551D0F 04040302 05A0301F 0603551D 23041830 16801486 7414D5D6 9B8299C1 787211AB 1B265B06 D2B62D30 1D060355 1D0E0416 0414FED1 97051946 D2F870D8 0DE819C3 AA1F3830 AD35300D 06092A86 4886F70D 01010405 00038181 00845AB8 F6589AED 17D0BB10 2AEA48AA 9299C130 4B358EA1 96632C84 0387D2DE 4774C776 6A14F25B 5D062E12 45EF730D 27D45795 62C17F55 A0428259 B13669BC 022201C7 EB6B7ACF 4C7143FA 8A038301 CEA17A0B D0662887 26BA8F0E C44410BB 4F982706 11F0D248 77D8A0E5 4417F0F4 3F993CE3 F62F6BDE BA2DD6BB B843391D 6D quit certificate ca 01 30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030 14311230 10060355 04031309 63612D73 65727665 72301E17 0D303530 39323031 37303335 375A170D 30383039 31393137 30333537 5A301431 12301006 03550403 13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100 BE7F0760 70D3B5C3 923D59FB C10AED17 71C6F477 7580851A 282FFAEB 43B918A1 2D867C1B 63963B36 F779FE18 D5DFFDB6 5E436276 459FC5EA A729C386 CDDD922B 2A0439AE 68A5F4C4 3B05F168 5BB93EF2 DF737F11 0BA3F5EB 3E62F423 CB5364D3 C39CCA09 8ADECBFF 4C0515A6 0750A283 ABA39ED2 F5866B98 D3361C1A B88AA62B 02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801486 7414D5D6 9B8299C1 787211AB 1B265B06 D2B62D30 1D060355 1D0E0416 04148674 14D5D69B 8299C178 7211AB1B 265B06D2 B62D300D 06092A86 4886F70D 01010405 00038181 00AC7DAF 0DF589CA C6175EC0 8F976C5F E08C3C91 85282FFA 94EE6F30 02EEE5B9 E60198ED 643151E0 CCE192FA A352BA3D 8BC5C006 EF89CFCF 59DA9B12 D729102C 3D6ADC3C 09931B96 3F1FB48C C0A85FDB 4F9A7C16 028673C3 91786D57 9D7C1016 62F9D4E9 78FED276 0C404815 B1FE3A11 4D215FCF 573536B4 477ECDB7 7060E221 31 quit** ! interface GigabitEthernet0/0 ip address 9.13.46.12 255.255.255.0 duplex auto speed auto media-type rj45 negotiation auto ! interface GigabitEthernet0/1 no ip address shutdown duplex auto speed auto media-type rj45 negotiation auto ! ip classless ip route 0.0.0.0 0.0.0.0 9.13.46.1 ! ip http server no ip http secure-server ! no cdp log mismatch duplex ! control-plane ! call treatment on ! dial-peer voice 1 voip session protocol sipv2 incoming called-number 9000 codec g711ulaw ! dial-peer voice 2 voip

```
destination-pattern 9000 session protocol sipv2 session
target ipv4:9.13.46.200 codec g711ulaw ! dial-peer voice
3 voip session protocol sipv2 incoming called-number
4000 codec g711ulaw ! dial-peer voice 4 voip
destination-pattern 4000 session protocol sipv2 session
target ipv4:9.13.32.75 codec g711ulaw ! dial-peer voice
5 voip destination-pattern 5000 session protocol sipv2
session target ipv4:9.13.0.10 codec g711alaw ! dial-peer
voice 7 voip destination-pattern 9999 session protocol
sipv2 session target ipv4:9.13.2.36 codec g711alaw !
dial-peer voice 12 pots destination-pattern 8400 ! dial-
peer voice 10 voip destination-pattern 50000 session
protocol sipv2 session target ipv4:9.13.2.150 codec
g711alaw ! dial-peer voice 11 voip session protocol
sipv2 session transport tcp tls incoming called-number
8004 codec g711ulaw ! dial-peer voice 13 voip
destination-pattern 8004 session protocol sipv2 session
target ipv4:9.13.2.70 codec g711ulaw ! dial-peer voice
20 voip destination-pattern 4444 session target
ipv4:9.13.46.111 codec g711ulaw ! dial-peer voice 21
voip incoming called-number 4444 codec g711ulaw ! sip-ua
retry invite 10 crypto signaling default trustpoint ca-
server ! gatekeeper shutdown ! line con 0 stopbits 1
line aux 0 stopbits 1 line vty 0 4 login ! scheduler
allocate 20000 1000 ! end
```

IOS CA服务器

CA服务器

```
ca-server#show run Building configuration... Current
configuration : 2688 bytes ! ! Last configuration change
at 17:11:41 UTC Tue Sep 20 2005 ! NVRAM config last
updated at 16:57:43 UTC Tue Sep 20 2005 ! version 12.4
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname ca-server ! boot-start-marker boot
system flash c2800nm-adventerprisek9_ivs-mz.124-3.9.PI3a
boot-end-marker ! no aaa new-model ! resource policy !
ip subnet-zero ! ip cef ! voice-card 0 no dspfarm !
crypto pki server ca-server grant auto ! crypto pki
trustpoint ca-server revocation-check crl rsakeypair ca-
server ! crypto pki certificate chain ca-server
certificate ca 01 30820201 3082016A A0030201 02020101
300D0609 2A864886 F70D0101 04050030 14311230 10060355
04031309 63612D73 65727665 72301E17 0D303530 39323031
37303335 375A170D 30383039 31393137 30333537 5A301431
12301006 03550403 13096361 2D736572 76657230 819F300D
06092A86 4886F70D 01010105 0003818D 00308189 02818100
BE7F0760 70D3B5C3 923D59FB C10AED17 71C6F477 7580851A
282FFAEB 43B918A1 2D867C1B 63963B36 F779FE18 D5DFFDB6
5E436276 459FC5EA A729C386 CDDD922B 2A0439AE 68A5F4C4
3B05F168 5BB93EF2 DF737F11 0BA3F5EB 3E62F423 CB5364D3
C39CCA09 8ADECBFF 4C0515A6 0750A283 ABA39ED2 F5866B98
D3361C1A B88AA62B 02030100 01A36330 61300F06 03551D13
0101FF04 05300301 01FF300E 0603551D 0F0101FF 04040302
0186301F 0603551D 23041830 16801486 7414D5D6 9B8299C1
787211AB 1B265B06 D2B62D30 1D060355 1D0E0416 04148674
14D5D69B 8299C178 7211AB1B 265B06D2 B62D300D 06092A86
4886F70D 01010405 00038181 00AC7DAF 0DF589CA C6175EC0
8F976C5F E08C3C91 85282FFA 94EE6F30 02EEE5B9 E60198ED
643151E0 CCE192FA A352BA3D 8BC5C006 EF89CFCF 59DA9B12
D729102C 3D6ADC3C 09931B96 3F1FB48C C0A85FDB 4F9A7C16
```

```
028673C3 91786D57 9D7C1016 62F9D4E9 78FED276 0C404815
B1FE3A11 4D215FCF 573536B4 477ECDB7 7060E221 31 quit !
interface FastEthernet0/0 ip address 9.13.46.14
255.255.255.0 duplex auto speed auto ! interface
FastEthernet0/1 no ip address shutdown duplex auto speed
auto ! ip classless ip route 0.0.0.0 0.0.0.0 9.13.46.1 !
ip http server no ip http secure-server ! no cdp log
mismatch duplex ! control-plane ! gatekeeper shutdown !
line con 0 line aux 0 line vty 0 4 login ! scheduler
allocate 20000 1000 ! end
```

验证

在呼叫被做后，此**show命令**可以用于为了验证用于呼叫的传输是否是TLS ：

```
router#show sip-ua connections tcp tls ? brief Show summary of connections detail Show detail
connection information
```

此命令的输出示例:在这些示例显示：

示例 1：详细信息输出

```
==========================================================================
router#show sip-ua connections tcp tls detail Total active connections : 1 No. of send failures
: 0 No. of remote closures : 3 No. of conn. failures : 0 No. of inactive conn. ageouts : 0 Max.
tls send msg queue size of 0, recorded for 0.0.0.0:0 TLS client handshake failures : 0 TLS
server handshake failures : 0 ---------Printing Detailed Connection Report--------- Note: **
Tuples with no matching socket entry - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition ++ Tuples with mismatched address/port entry - Do 'clear sip
<tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>' to overcome this error condition Remote-
Agent:9.13.46.12, Connections-Count:1 Remote-Port Conn-Id Conn-State WriteQ-Size ===========
======= =========== =========== 5061 1 Established 0
==========================================================================
```

示例 2：简要输出

```
==========================================================================
router#show sip-ua connections tcp tls brief Total active connections : 2 No. of send failures :
0 No. of remote closures : 0 No. of conn. failures : 0 No. of inactive conn. ageouts : 0 Max.
tls send msg queue size of 0, recorded for 0.0.0.0:0 TLS client handshake failures : 0 TLS
server handshake failures : 0
==========================================================================
```

或者， **debug ccsip messages命令**可以用于验证“通过：” TLS的报头包括。此输出是示例邀请使用SIP TLS和“饮者呼叫的请求：” URI方案：

```
INVITE sips:777@172.18.203.181 SIP/2.0
Via: SIP/2.0/TLS 172.18.201.173:5060;branch=z9hG4bK2C419
From: <sips:333@172.18.201.173>;tag=581BB98-1663
To: <sips:5555555@172.18.197.154>
Date: Wed, 28 Dec 2005 18:31:38 GMT
Call-ID: EB5B1948-770611DA-804F9736-BFA4AC35@172.18.201.173
Remote-Party-ID: "Bob" <sips:+14085559999@1.2.3.4>
Contact: <sips:123@host>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO
Max-Forwards: 70
Cseq: 104 INVITE
Expires: 60
Timestamp: 730947404
Content-Length: 298
Content-Type: application/sdp
```

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 8437 1929 IN IP4 172.18.201.173
s=SIP Call
c=IN IP4 1.1.1.1
t=0 0
m=audio 18378 RTP/AVP 0 19
c=IN IP4 1.1.1.1
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000
a=ptime:20
```

故障排除

TLS呼叫的一些故障排除提示包括：

- 为了允许CA服务器发行证书到信任点，请确保配置的IOS路由器，因为CA服务器有启用的HTTP (ip http server命令)。
- 必须同步在CA服务器的时钟和信任点。
- 如果TLS握手失效在两个设备之间(例如， OGW和多维数据集)，请检查证书的正确性在设备的。在TLS握手期间， **debug crypto pki**命令可以用于排除故障问题。
- 有时，当设备(例如， OGW和多维数据集)时在不同的子网，那里可以的TCP窗口尺寸协商问题导致这些错误：*I/O发送错误*和*I/O读取错误*。此问题可以用**ip tcp path-mtu-discovery命令**解决在两个设备。此问题也许在成功的TLS握手以后发生。
- “清楚SIP UA连接” in命令SIP UA模式可以用于清除TLS连接。`Router#`**`clear sip-ua tcp [tls] connections <id <`***`conn id`***`> | target <`***`ipv4:ip address:port`***`>`** 因为TLS乘坐在TCP顶部， **tls**选项在**tcp以后**出现。此命令运作类似TCP和UDP的现有清除命令。

相关信息

- 语音技术支持
- 语音和统一通信产品支持
- Cisco IP 电话故障排除
- 技术支持和文档 - Cisco Systems