带IP电话的SSLVPN配置示例

目录

简介

本文档介绍如何通过安全套接字层VPN(SSL VPN)（也称为WebVPN）配置IP电话。此解决方案使用两个Cisco Unified Communications Manager(CallManager)和三种类型的证书。CallManager包括：

- 思科统一通信管理器 (CUCM)
- 思科统一通信管理器快捷版(Cisco Unified CME)

证书类型为：

- 自签名证书
- 第三方证书，如Entrust、Thawte和GoDaddy
- Cisco IOS®/自适应安全设备(ASA)证书颁发机构(CA)

要了解的关键概念是，一旦SSL VPN网关和CallManager上的配置完成，您必须在本地加入IP电话。这使电话能够加入CUCM并使用正确的VPN信息和证书。如果电话未在本地加入，则无法找到SSL VPN网关，并且没有正确的证书来完成SSL VPN握手。

最常见的配置是CUCM/Unified CME，带ASA自签名证书和Cisco IOS自签名证书。因此，它们最容易配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科统一通信管理器(CUCM)或思科统一通信管理器快捷版(Cisco Unified CME)
- SSL VPN(WebVPN)
- 思科自适应安全设备(ASA)
- 证书类型，例如自签名、第三方和证书颁发机构

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA高级版许可证。
- AnyConnect VPN电话许可证。
  - 对于ASA版本8.0.x，许可证为Linksys电话的AnyConnect。
  - 对于ASA 8.2.x版或更高版本，许可证为AnyConnect for Cisco VPN Phone。
- SSL VPN 网关:ASA 8.0或更高版本（带AnyConnect for Cisco VPN电话许可证）或Cisco IOS软件版本12.4T或更高版本。
  - Cisco IOS软件版本12.4T或更高版本不受正式支持，如《SSL VPN配置指南》中所述。
  - 在Cisco IOS软件版本15.0(1)M中，SSL VPN网关是Cisco 880、Cisco 890、Cisco 1900、Cisco 2900和Cisco 3900平台上的计席许可功能。成功的SSL VPN会话需要有效的许可证。
- CallManager ：CUCM 8.0.1或更高版本，或Unified CME 8.5或更高版本。

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。

配置

> **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。
>
> 命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。

基本ASA SSL VPN配置

以下文档中介绍了基本ASA SSL VPN配置：

- ASA 8.x：VPN访问与使用自签名证书的AnyConnect VPN客户端配置示例
- 配置AnyConnect VPN客户端连接

完成此配置后，远程测试PC应能连接到SSL VPN网关、通过AnyConnect连接并ping CUCM。确保ASA具有AnyConnect for Cisco IP电话许可证。(使用**show ver**命令。) TCP和UDP端口443必须在网关和客户端之间打开。

注意：VPN电话不支持负载均衡SSL VPN。

CUCM:具有自签名证书配置的ASA SSL VPN

有关详细信息，请参阅使用AnyConnect将IP电话SSL VPN连接到ASA。

ASA必须具有适用于思科VPN电话的AnyConnect的许可证。在配置SSL VPN后，为VPN配置CUCM。

1. 使用以下命令可从ASA导出自签名证书：

```
ciscoasa(config)# crypto ca export trustpoint name identity-certificate
```

此命令向终端显示pem编码的身份证书。
2. 将证书复制并粘贴到文本编辑器，并将其另存为.pem文件。请务必包括BEGIN CERTIFICATE和END CERTIFICATE行，否则证书将无法正确导入。请勿修改证书的格式，因为当电话尝试向ASA进行身份验证时，这会导致问题。
3. 导航至**Cisco Unified Operating System Administration > Security > Certificate Management > Upload Certificate/Certificate Chain**，以便将证书文件加载到CUCM的CERTIFICATE MANAGEMENT部分。
4. 从用于从ASA加载自签名证书的同一区域下载CallManager.pem、CAPF.pem和Cisco_Manufacturing_CA.pem证书（请参阅步骤1），并将其保存到桌面。
   1. 例如，要将CallManager.pem导入ASA，请使用以下命令：

```
ciscoasa(config)# crypto ca trustpoint certificate-name
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate certificate-name
```

   2. 当系统提示您复制并粘贴信任点的相应证书时，请打开从CUCM保存的文件，然后复制并粘贴Base64编码的证书。请务必包括BEGIN CERTIFICATE和END CERTIFICATE行（带连字符）。
   3. 键入**end**，然后按**Return**。
   4. 当系统提示接受证书时，键入**yes**，然后按**Enter键**。
   5. 对来自CUCM的其他两个证书(CAPF.pem、Cisco_Manufacturing_CA.pem)重复步骤1至4。
5. 按照CUCM IPphone VPN config.pdf中的说明，为CUCM配置正确的VPN配置。

注意：在CUCM上配置的VPN网关必须与在VPN网关上配置的URL匹配。如果网关和URL不匹配，电话无法解析该地址，并且您将看不到VPN网关上的任何调试。

- 在CUCM上：VPN网关URL为https://192.168.1.1/VPNPhone
- 在ASA上，使用以下命令：

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- 您可以在自适应安全设备管理器(ASDM)或连接配置文件下使用这些命令。

CUCM:具有第三方证书配置的ASA SSL VPN

此配置与CUCM中描述的配置非常相似：ASA SSLVPN with Self-Signed Certificates Configuration部分，但您使用的是第三方证书。在ASA上使用第三方证书配置SSL VPN，如ASA 8.x手动安装第三方供应商证书以与WebVPN配置示例中所述。

> **注意**：您必须将完整的证书链从ASA复制到CUCM，并包括所有中间证书和根证书。如果CUCM不包含完整链，电话将没有进行身份验证所需的证书，SSL VPN握手将失败。

基本IOS SSL VPN配置

> **注意**：IP电话被指定为IOS SSL VPN不支持；配置只是尽力而为。

以下文档中介绍了基本Cisco IOS SSL VPN配置：

- 在 IOS 上使用 SDM 配置 SSL VPN 客户端 (SVC) 的示例
- 具有基于 IOS 区域的策略防火墙配置的 IOS 路由器上的 AnyConnect VPN 客户端示例

完成此配置后，远程测试PC应能连接到SSL VPN网关、通过AnyConnect连接并ping CUCM。在Cisco IOS 15.0及更高版本中，您必须拥有有效的SSL VPN许可证才能完成此任务。TCP和UDP端口443必须在网关和客户端之间打开。

CUCM:具有自签名证书配置的IOS SSL VPN

此配置与CUCM中描述的配置类似：具有第三方证书配置和CUCM的ASA SSLVPN:ASA SSLVPN with Self-Signed Certificates Configuration部分。区别是：

1. 使用以下命令可从路由器导出自签名证书：

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. 使用以下命令导入CUCM证书：

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

WebVPN情景配置应显示以下文本：

```
gateway webvpn_gateway domain VPNPhone
```

按照CUCM中所述配置CUCM:ASA SSLVPN with Self-Signed Certificates Configuration部分。

CUCM:具有第三方证书配置的IOS SSL VPN

此配置与CUCM中描述的配置类似：ASA SSLVPN with Self-Signed Certificates Configuration部分。使用第三方证书配置WebVPN。

> **注意**：您必须将完整的WebVPN证书链复制到CUCM，并包括所有中间证书和根证书。如果CUCM不包含完整链，电话将没有进行身份验证所需的证书，SSL VPN握手将失败。

Unified CME:具有自签名证书/第三方证书配置的ASA/路由器SSL VPN

Unified CME的配置与CUCM的配置类似；例如，WebVPN终端配置相同。唯一显着区别是Unified CME呼叫代理的配置。按照为SCCP IP电话配置SSL VPN客户端中所述，为Unified CME配置VPN组和VPN策略。

> **注意**：Unified CME仅支持瘦呼叫控制协议(SCCP)，不支持VPN电话会话发起协议(SIP)。

> **注意**：无需将证书从Unified CME导出到ASA或路由器。您只需将证书从ASA或路由器WebVPN网关导出到Unified CME。

要从WebVPN网关导出证书，请参阅ASA/路由器部分。如果使用第三方证书，则必须包括完整的证书链。要将证书导入Unified CME，请使用与将证书导入路由器相同的方法：

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

UC 520 IP电话，带SSL VPN配置

思科统一通信500系列型号UC 520 IP电话与CUCM和CME配置截然不同。

- 由于UC 520 IP电话既是CallManager又是WebVPN网关，因此无需在两者之间配置证书。
- 在路由器上配置WebVPN，与通常使用自签名证书或第三方证书时一样。
- UC 520 IP电话有内置的WebVPN客户端，您可以像配置普通PC连接WebVPN一样配置它。输入网关，然后输入用户名/密码组合。
- UC 520 IP电话与思科S系列IP电话SPA 525G电话兼容。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。