与IP电话配置示例的SSLVPN

目录

简介

本文描述如何配置在安全套接字协议层VPN (SSL VPN)，亦称WebVPN的IP电话。两Cisco Unified Communications Manager (CallManager)和证书的三种类型与此解决方案一起使用。
CallManager是：

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

证书类型是：

- 自签名证书
- 第三方证书，例如Entrust、Thawte和GoDaddy
- Cisco IOS /Adaptive安全工具(ASA) Certificate Authority (CA)

要了解的关键概念是，一次在SSL VPN网关的配置和CallManager完成，您必须加入IP电话本地。这使电话加入CUCM和使用正确VPN信息和证书。如果电话没有加入本地，他们找不到SSL VPN网关，并且没有完成正确的证书SSL VPN握手。

多数常见配置是与ASA自签名证书和Cisco IOS自签名证书的CUCM/Unified CME。结果，他们是最容易配置。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager (CUCM)或Cisco Unified Communications Manager Express (Cisco Unified CME)
- SSL VPN (WebVPN)
- 思科可适应安全工具(ASA)
- 证书类型，例如自己签署的，第三方和证书权限

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA优质许可证。
- AnyConnect VPN电话许可证。
  - 对于ASA版本8.0.x，许可证是Linksys电话的AnyConnect。
  - 对于ASA版本8.2.x或以上，许可证是思科VPN电话的AnyConnect。
- SSL VPN网关：ASA 8.0或以上(与Cisco VPN电话许可证的AnyConnect)，或者Cisco IOS软件版本12.4T或以上。
  - Cisco IOS软件版本12.4T或以后不正式支持如提供在SSL VPN配置指南上。
  - 在Cisco IOS版本15.0(1)M， SSL VPN网关是在Cisco 880， Cisco 890， Cisco 1900， Cisco 2900和Cisco的一个位置计数的许可授权的功能3900平台。有效许可证为一成功的SSL VPN会话要求。
- CallManager ：CUCM 8.0.1或以上或者Unified CME 8.5或以上。

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。请使用Output Interpreter Tool为了查看show命令输出分析。

基本ASA SSL VPN配置

基本ASA SSL VPN配置在这些文档描述：

- 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

一旦此配置完成，远程测试PC应该能连接到SSL VPN网关，通过AnyConnect连接，并且ping CUCM。保证ASA有Cisco IP电话许可证的AnyConnect。(请使用**show ver命令**。)TCP和UDP端口

443一定是开放的在网关和客户端之间。

注意：负载均衡的SSL VPN不为VPN电话支持。

CUCM ：与自签名证书配置的ASA SSL VPN

对ASA的参考的IP电话SSL VPN使用AnyConnect欲知更多详细信息。

ASA必须有AnyConnect的一个许可证思科VPN电话的。在您配置SSL VPN后，您然后配置您的VPN的CUCM。

1. 请使用此命令为了导出从ASA的自签名证书：

   ```
   ciscoasa(config)# crypto ca export trustpoint name identity-certificate
   ```
   此命令显示一PEM编码的身份证书到终端。
2. 复制和插入证书对文本编辑，并且保存它作为.pem文件。请务必包括开始证书和END证书线路，否则证书不会正确地导入。请勿修改证书的格式，因为这将引起问题，当电话设法验证到ASA时。
3. 导航到**Cisco Unified操作系统的管理> Security > Certificate Management >加载证书/证书链**为了装载证书文件到CUCM的证书管理部分。
4. 下载从用于的同一个区域的CallManager.pem、CAPF.pem和Cisco_Manufacturing_CA.pem证书装载从ASA的自签名证书(请参阅步骤1)，并且救他们到您的桌面。
   1. 例如，为了导入CallManager.pem到ASA，请使用这些命令：

      ```
      ciscoasa(config)# crypto ca trustpoint certificate-name
      ciscoasa(config-ca-trustpoint)# enrollment terminal
      ciscoasa(config)# crypto ca authenticate certificate-name
      ```
   2. 当提示您复制和插入信任点的时对应的证书，请打开您从CUCM保存的文件，然后复制和插入Base64-encoded证书。请务必包括开始证书和END证书线路(与连字符)。
   3. 键入**末端**，然后按Return。
   4. 当提示接受证书，请键入**是**，然后按回车。
   5. 重复另外两证书的(CAPF.pem， Cisco_Manufacturing_CA.pem)步骤1到4从CUCM。
5. 配置正确VPN配置的CUCM，正如CUCM Ipphone VPN config.pdf所描述。

注意：在VPN网关配置在CUCM配置的VPN网关必须匹配URL。如果网关和URL不配比，电话不能解析地址，并且您将看不到在VPN网关的所有调试。

- 在CUCM ：VPN网关URL是https://192.168.1.1/VPNPhone
- 在ASA，请使用这些命令：

```
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
```

- 您能使用这些on命令可适应安全设备管理器(ASDM)或在连接配置文件下。

CUCM ：与第三方证书配置的ASA SSL VPN

此配置非常类似于在CUCM描述的配置：与自签名证书配置部分的ASA SSLVPN，除了您使用第三方证书。配置在ASA的SSL VPN与第三方证书正如ASA 8.x所描述手工安装第三方供应商证书为了用在WebVPN配置示例上。

> **注意**：您必须复制从ASA的全双工证书链到CUCM和包括所有中间和根证明。如果CUCM不包括全双工一系列，电话没有必要的证书验证和失败SSL VPN握手。

基本IOS SSL VPN配置

> **注意**：IP电话被选定作为不支持的在IOS SSL VPN;配置在仅尽力。

基本Cisco IOS SSL VPN配置在这些文档描述：

- 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

一旦此配置完成，远程测试PC应该能连接到SSL VPN网关，通过AnyConnect连接，并且ping CUCM。在Cisco IOS 15.0及以后，您必须有一个有效SSL VPN许可证完成此任务。TCP和UDP端口443一定是开放的在网关和客户端之间。

CUCM ：与自签名证书配置的IOS SSL VPN

此配置类似于在CUCM描述的配置：与第三方证书配置和CUCM的ASA SSLVPN ：与自签名证书配置部分的ASA SSLVPN。差异是：

1. 请使用此命令为了导出从路由器的自签名证书：

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

2. 请使用这些命令为了导入CUCM证书：

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

WebVPN上下文配置应该显示此文本：

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

配置CUCM正如CUCM所描述：与自签名证书配置部分的ASA SSLVPN。

CUCM ：与第三方证书配置的IOS SSL VPN

此配置类似于在CUCM描述的配置：与自签名证书配置部分的ASA SSLVPN。配置您的与一第三方证书的WebVPN。

> **注意**：您必须复制全双工WebVPN证书链到CUCM和包括所有中间和根证明。如果CUCM不包括全双工一系列，电话没有必要的证书验证和失败SSL VPN握手。

Unified CME ：与自签名证书/第三方的ASA/Router SSL VPN证书配置

Unified CME的配置类似于CUCM的配置;例如， WebVPN终端配置是相同的。唯一的重大的差异是Unified CME呼叫代理的配置。配置VPN组和VPN策略Unified CME的正如配置SSL VPN客户端所描述SCCP IP电话的。

> **注意**：Unified CME支持仅内部呼叫控制协议(SCCP)，并且不支持VPN电话的会话初始化协议(SIP)。

> **注意**：没有需要导出从Unified CME的证书到ASA或路由器。您只需要导出从ASA的证书或路由器Webvpn gateway到Unified CME。

为了导出从Webvpn gateway的证书，参考ASA/router部分。如果使用一第三方证书，您必须包括全双工证书链。为了导入证书到Unified CME，请使用方法和用于一样进口证明书到路由器：

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

与SSL VPN配置的UC 520 IP电话

Cisco Unified通信500系列型号UC 520 IP电话是相当与CUCM和CME配置不同。

- 因为UC 520 IP电话是CallManager和Webvpn gateway，没有需要配置在两个之间的证书。
- 配置在路由器的WebVPN，您通常会与自签名证书或第三方证书。
- 在WebVPN客户端有构件的UC 520 IP电话，并且您能配置它正您正常PC会连接对WebVPN。输入网关，然后用户名/密码组合。
- UC 520 IP电话是与思科小型企业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。