与IP电话配置示例的SSLVPN

Contents

Introduction

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。两个Cisco Unified通信管理器(呼叫管理器)和证书的三种类型与此解决方案一起使用。呼叫管理器是：

- 思科统一通信管理器 (CUCM)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

证书类型是：

- 自署名的认证
- 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网关的配置和呼叫管理器完成，您必须加入IP电话本地。此enable (event)加入CUCM和使用正确的VPN信息和证书的电话。如果电话没有被加入本地，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自署名的认证和Cisco IOS自署名的认证的CUCM/Unified CME。结果，他们是最容易配置。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Cisco Unified通信管理器(CUCM)或Cisco Unified Communications Manager Express (Cisco Unified CME)
- SSL VPN (WebVPN)
- Cisco可适应的安全工具(ASA)
- 证书类型，例如自己签署的，第三方和认证权限

Components Used

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，许可证是Linksys电话的AnyConnect。
  - 对于ASA版本8.2.x或以上，许可证是Cisco 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 Software Release 12.4T或以上。
  - 不正式Cisco IOS Software Release 12.4T或以上支持如提供在SSL VPN配置指南上。
  - 在Cisco IOS Software Release 15.0(1)M， SSL VPN网关是在Cisco 880， Cisco 890， Cisco 1900， Cisco 2900和Cisco的一个位置计数的准许功能3900平台。有效许可证对于一次成功的SSL VPN会话是必需的。
- CallManager ：CUCM 8.0.1或以上或者统一的CME 8.5或以上。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Configure

> 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。

基本的ASA SSL VPN配置

基本的ASA SSL VPN配置在这些文件描述：

- 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，并且连接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。

Note:负载均衡的SSL VPN不为VPN电话支持。

CUCM ：与自署名的认证配置的ASA SSL VPN

使用AnyConnect详细信息，参考IP电话SSL VPN对ASA。

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

1. 请使用此命令为了从ASA导出自签证书：

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

此命令显示一个PEM编码的身份认证给终端。
2. 复制和插入认证对文本编辑，并且保存它作为.pem文件。请务必包括开始认证和END认证线路，否则认证不会正确地导入。请勿修改认证的格式，因为这将引起问题，当电话设法验证到ASA时。
3. 连接到**Cisco Unified操作系统的管理> Security > Certificate Management >加载认证/证书链**为了装载证书文件到CUCM的证书管理部分。
4. 从用于的同一个区域下载CallManager.pem、CAPF.pem和Cisco_Manufacturing_CA.pem证书从ASA装载自署名的认证(请参阅第1)步，并且救他们到您的桌面。
    1. 例如，为了导入CallManager.pem 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认证，请打开您从CUCM保存的文件，然后复制和插入Base64-encoded认证。请务必包括开始认证和END认证线路(与连字符)。
    3. 键入**末端**，然后按Return。
    4. 当提示**是**接受认证，类型，然后按Enter。
    5. 重复另外两证书(CAPF.pem， Cisco_Manufacturing_CA.pem)的第1步到第4步从CUCM。
5. 配置正确的VPN配置的CUCM，正如CUCM IPphone VPN config.pdf所描述。

Note:在VPN网关被配置在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：与自署名的认证配置部分的ASA SSLVPN，除了您使用第三方证书。用第三方证书配置在ASA的SSL VPN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。

> **Note**:您必须从ASA复制充分的证书链到CUCM和包括所有中间和根证明。如果CUCM不包括充分的一系列，电话没有必要的证书验证和失败SSL VPN握手。

基本的IOS SSL VPN配置

> **Note**:IP电话在IOS SSL VPN被选定作为不支持;配置在仅尽力。

基本的Cisco IOS SSL VPN配置在这些文件描述：

- 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，并且连接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 ：与自署名的认证配置的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 ：与自署名的认证配置部分的ASA SSLVPN。区别是：

1. 请使用此命令为了从路由器导出自签证书：

```
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：与自署名的认证配置部分的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：与自署名的认证配置部分的ASA SSLVPN。用一个第三方认证配置您的WebVPN。

> **Note**:您必须复制充分的WebVPN证书链到CUCM和包括所有中间和根证明。如果CUCM不包括充分的一系列，电话没有必要的证书验证和失败SSL VPN握手。

统一的CME ：与自署名的认证/第三方的ASA/Router SSL VPN证书配置

统一的CME的配置类似于CUCM的配置;例如， WebVPN终端配置是相同的。唯一的重大的区别是统一的CME呼叫代理程序的配置。配置VPN组和VPN策略统一的CME的正如配置SSL VPN客户端所描述SCCP IP电话的。

> **Note**:统一的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)。

> **Note**:没有需要从统一的CME导出证书对ASA或路由器。您只需要从ASA导出证书或路由器Webvpn gateway对统一的CME。

为了从Webvpn gateway导出证书，请参见ASA/router部分。如果使用一个第三方认证，您必须包括充分的证书链。为了导入证书统一的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电话是呼叫管理器和Webvpn gateway，没有需要配置在两个之间的证书。
- 配置在路由器的WebVPN，您通常会与自署名的认证或第三方证书。
- 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会连接到WebVPN。输入网关，然后用户名/密码组合。
- UC 520 IP电话是与Cisco小型企业IP电话SPA 525G电话兼容。

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。