零的联系部署(ZTD) VPN远程办公室/Spoke配置示例

目录

简介

安全和高效部署和远端办公室路由器提供(有时呼叫Spokes)可以是困难任务。 远程办公室也许是在它是让的挑战现场工程师配置现场的路由器的位置，并且多数工程师选择不发送预先配置的分支路由器由于费用和可能性安全风险。本文描述零的联系部署(ZTD)选项如何是这样部署的一个有成本效益的和可扩展的解决方案。

先决条件

要求

- 所有Cisco IOS路由器有该的一个的USB端口支持USB闪存驱动器。关于详细信息，请参阅USB eToken和USB闪烁功能支持。
- 此功能在几乎所有思科8xx平台被确认运作。关于详细信息请参阅默认配置文件白皮书(在Cisco 800系列ISR的功能支持)。
- 有USB端口类似集成服务路由器的其他平台(ISR)系列G2和43xx/44xx。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 简单证书注册协议 (SCEP)
- 零的联系部署通过USB

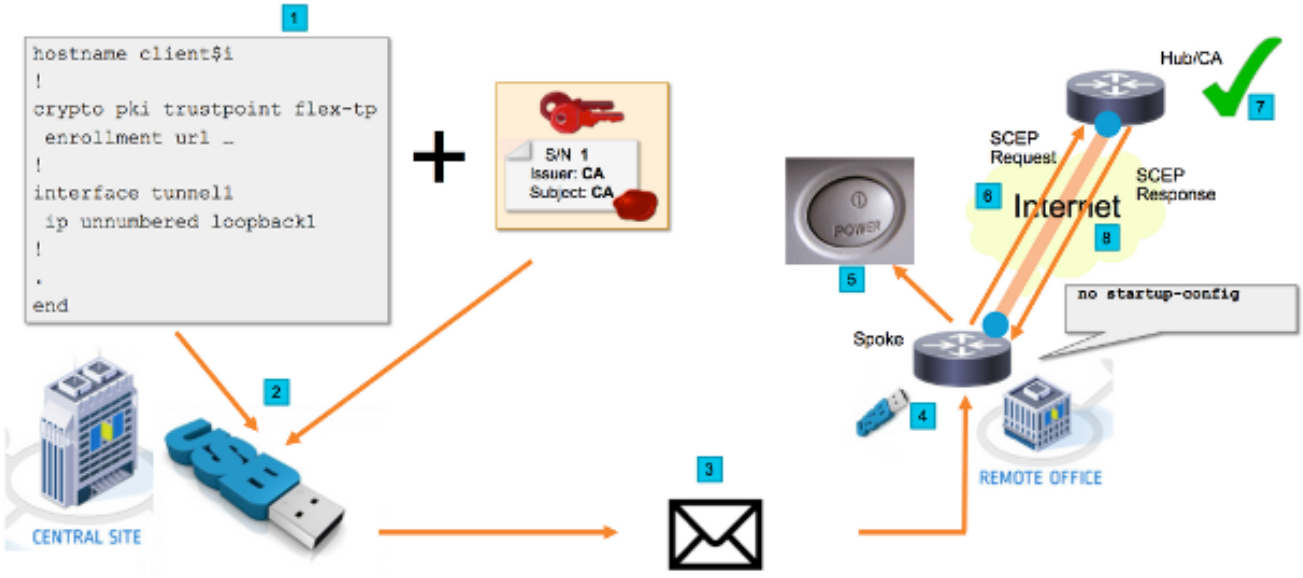
- DMVPN/FlexVPN/Site对站点VPN

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。

网络图



网络流

1. 在中心站点(公司的总部)辐条配置的模板创建。模板包含签署VPN中心路由器的证书的Certificate Authority (CA)证书。
2. 配置模板是例示的在呼叫**ciscortr.cfg的**文件的一个USB密钥。**此**配置文件包含能将部署的路由器的分支特定配置。 **注意**：除IP地址和CA证书之外，在USB的配置不包含任何敏感信息。没有分支或CA服务器的专用密钥。
3. USB闪存驱动器发送到远程办公室通过邮件或包运送公司。
4. 分支路由器也派遣到远程办公室直接地从思科制造。
5. 在远程办公室路由器连接供给动力并且被缚住对网络按照用USB闪存驱动器包括的说明说明。其次USB闪存驱动器插入到路由器。 **注意**：有一点对在此步骤涉及的没有技术技能，因此可能由所有办公室人员容易地执行。
6. 一旦路由器启动读从**usbflash0:/ciscortr.cfg的配置。**当路由器供给动力了简单认证登记协议(SCEP)请求发送到CA服务器。
7. 在CA服务器手工或自动授权能根据公司安全策略配置。当配置为授权手工的证书，应该进行SCEP请求的带外验证(IP地址验证检查、进行部署的证件验证人员的等等)。此步骤也许有所不同基于CA服务器t帽子使用。
8. 一旦SCEP答复由分支路由器接收，当前有一个有效证书， IKE会话用VPN集线器验证，并且通道成功设立。

配置/模板

此输出示例:显示在闪存驱动器放置在**usbflash0:/ciscortr.cfg**文件的一模范FlexVPN远程办公室配置。

```
hostname client1
!
interface GigabitEthernet0
 ip address dhcp
!
crypto pki trustpoint client1
! CA Server's URL
 enrollment url http://10.122.162.242:80
! These fields needs to be filled, to avoid prompt while doing enroll
serial-number none
 ip-address none
 password
 subject-name cn=client1.cisco.com ou=cisco ou
!
crypto pki certificate chain client1
 certificate ca 01
 ! CA Certificate here
       quit
!
crypto ikev2 profile default
 match identity remote any
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint client1
 aaa authorization group cert list default default
!
interface Tunnel1
 ip unnumbered GigabitEthernet0
 tunnel source GigabitEthernet0
 tunnel mode ipsec ipv4
! Destination is Internet IP Address of VPN Hub
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
event manager applet import-cert
! Start importing certificates only after 60s after bootup
! Just to give DHCP time to boot up
 event timer watchdog time 60
 action 1.0 cli command "enable"
 action 2.0 cli command "config terminal"
! Enroll spoke's certificate
 action 3.0 cli command "crypto pki enroll client1"
! After enrollement request is sent, remove that EEM script
 action 4.0 cli command "no event manager applet import-cert"
 action 5.0 cli command "exit"
event manager applet write-mem
 event syslog pattern "PKI-6-CERTRET"
 action 1.0 cli command "enable"
 action 2.0 cli command "write memory"
 action 3.0 syslog msg "Automatically saved configuration"
```

验证

使用本部分可确认配置能否正常运行。

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。

如果通道上升，您在分支能验证：

```
client1#show crypto session
Crypto session current status

Interface: Tunnel1
Profile: default
Session status: UP-ACTIVE
Peer: 172.16.0.2 port 500
 Session ID: 1
 IKEv2 SA: local 172.16.0.1/500 remote 172.16.0.2/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map
```

如果证书正确地，被登记了您在分支能也验证：

```
client1#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: client1
    hostname=client1
    cn=client1.cisco.com ou=cisco ou
  Validity Date:
    start date: 01:34:34 PST Apr 26 2015
    end   date: 01:34:34 PST Apr 25 2016
  Associated Trustpoints: client1
  Storage: nvram:CA#6.cer

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=CA
 Subject:
   cn=CA
 Validity Date:
   start date: 01:04:46 PST Apr 26 2015
   end   date: 01:04:46 PST Apr 25 2018
 Associated Trustpoints: client1
 Storage: nvram:CA#1CA.cer
```

故障排除

目前没有针对此配置的故障排除信息。

已知问题说明和问题

Cisco Bug ID CSCuu93989 -设置向导终止在G2平台的PnP流也许造成系统不装载从usbflash的配置：/ciscortr.cfg.反而系统也许终止在设置向导功能：

```
client1#show crypto pki certificates
Certificate
```

```
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: client1
    hostname=client1
    cn=client1.cisco.com ou=cisco ou
  Validity Date:
    start date: 01:34:34 PST Apr 26 2015
    end   date: 01:34:34 PST Apr 25 2016
  Associated Trustpoints: client1
  Storage: nvram:CA#6.cer

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=CA
 Subject:
   cn=CA
 Validity Date:
   start date: 01:04:46 PST Apr 26 2015
   end   date: 01:04:46 PST Apr 25 2018
 Associated Trustpoints: client1
 Storage: nvram:CA#1CA.cer
```

保证您使用包含此缺陷的一个修正的版本。

ZTD通过USB与默认配置文件

注意**默认配置文件**以为特色本文比**零的联系Deployement**使用是一个不同的功能**通过**在Cisco 800系列ISR部署概述desribed的**USB**。

--	**通过USB调零联系Deployement**	**默认配置文件**
支持的平台	对只有少量8xx路由器限制。 关于详细信息，请参阅Cisco 800系列ISR部署概述	所有ISR G2、43xx和44xx。
文件名	*.cfg	ciscortr.cfg
保存在本地闪存的配置	是，自动地	不， Embeded活动管理器(EEM

由于**默认配置文件**功能支持更多平台，此技术为在此条款提交的解决方案选择。

摘要

USB默认配置(与从USB闪存驱动器的文件名**ciscortr.cfg**)在远程位置给网络管理员能力部署远程办公室分支路由器VPN (但是没限制对VPN)，不用需要登录设备。

相关信息

- 简单证书注册协议 (SCEP)
- 零的联系部署通过USB
- DMVPN/FlexVPN/Site对站点VPN
- 技术支持和文档 - Cisco Systems