配置零的联系配置(ZTD) VPN远程办公室/Spoke

Contents

Introduction

本文描述零的联系配置(ZTD)选项如何是配置的一个有成本效益的和可扩展的解决方案。

安全和高效的配置和远端办公室路由器提供(有时告诉Spokes)可以是一项困难任务。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。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 有一个USB端口支持USB闪存驱动器的任何Cisco IOS路由器。关于详细资料，请参阅USB eToken和USB闪存功能支持。
- 此功能被确认在几乎所有Cisco 8xx平台运作。关于详细资料，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端口类似综合服务路由器的其他平台(ISR)系列G2和43xx/44xx。

Components Used

本文档中的信息基于以下软件和硬件版本：

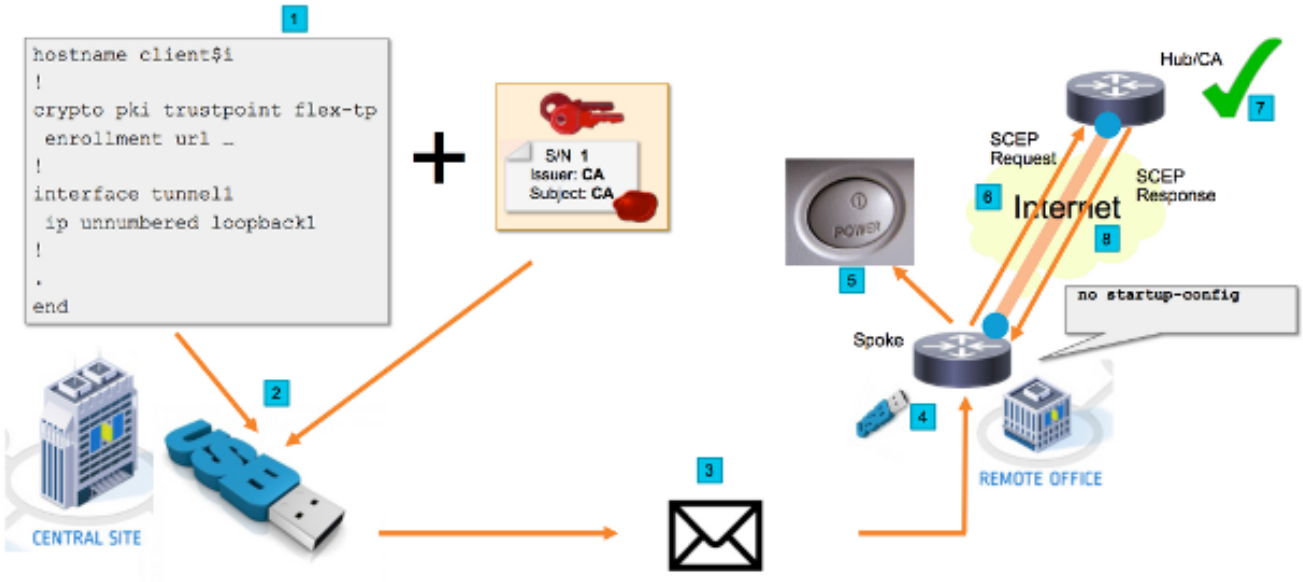
- 简单认证登记协议(SCEP)
- 零的联系配置通过USB
- DMVPN/FlexVPN/Site对站点VPN

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

Note: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。

Network Diagram



网络流

1. 在中心站点(公司的总部)，分支配置的模板被创建。模板包含签署VPN集线路由器的认证的Certificate Authority (CA)认证。
2. 配置模板是例示的在名为**ciscortr.cfg的**文件的一个USB密钥。**此**配置文件包含将配置的路由器的分支特定配置。 **Note**: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闪存驱动器被发送到远程办公室通过邮件或程序包运送公司。
4. 分支路由器也派遣到远程办公室直接地从Cisco制造。
5. 在远程办公室，路由器被连接供给动力并且被缚住对网络按照被包括在USB闪存驱动器中的指令说明。其次， USB闪存驱动器插入到路由器。 **Note**: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。当路由器启动了，简单认证登记协议(SCEP)请求被发送到CA服务器。
7. 在CA服务器手工或自动授予能根据公司安全策略被配置。当配置为授予手工的认证，必须进行SCEP请求的带外验证(IP地址验证检查、进行配置的证件验证人员的等等)。此步

骤也许有所不同基于使用的CA服务器。

8. 一旦SCEP答复由分支路由器收到，当前有一个有效证书， Internet Key Exchange (IKE)会话用VPN集线器验证，并且隧道成功设立。

基于苏堤的授权

第7步介入通过SCEP协议被发送的认证署名请求的手工的验证，也许是笨重和难为非技术性的人员实行。为了强化安全和自动化进程，可以使用安全的唯一设备标识(苏堤)设备证书。苏堤证书是证书被构件到ISR 4K设备。这些证书由Cisco CA签字。每个制作的设备发出了与不同的身份验证，并且设备的序列号在认证的普通的名字内包含。苏堤认证、相关的密匙对和其整个证书链在堵塞器抗性信任锚点芯片存储。此外，密匙对密码一定对一块特定信任锚点芯片，并且专用密钥从未被导出。此功能做克隆或伪装实际上不可能的身份信息。

苏堤专用密钥可以用于签署路由器生成的SCEP请求。CA服务器能验证签名和读设备的苏堤认证的内容。CA服务器可从苏堤认证提取信息(类似序列号)和执行根据该信息的授权。RADIUS服务器可以用于回答这样授权请求。

管理员建立辐射路由器和他们相关的序列号列表。序列号可以读从路由器的事例由非技术性的人员。这些序列号在RADIUS服务器数据库存储，并且服务器核准根据允许认证自动地授予的该信息的SCEP请求。注意序列号密码附加到一个特定设备通过Cisco签字的苏堤认证，因此被伪造无法的。

总之，配置CA服务器自动地同意满足这两个标准的请求：

- 用与认证产生关联的专用密钥签字签字由Cisco苏堤CA
- 由根据序列号信息的RADIUS服务器核准采取从苏堤认证

部署方案

在隧道可以被构建前， CA服务器也许显示直接地在互联网，因而允许客户端进行登记。CA服务器在同一路由器可能甚而被配置作为VPN集线器。此拓扑的优点是简单。因为CA服务器为各种各样攻击直接地显示通过互联网，缺点是被减少的安全。

或者，拓扑可以通过配置注册审批机构服务器扩展。注册审批机构服务器角色是估计和转发有效证书署名请求到CA服务器。RA服务器不包含CA的专用密钥，并且不能单独生成证书。在这样配置，CA服务器不需要显示在互联网，强化整体安全。‘

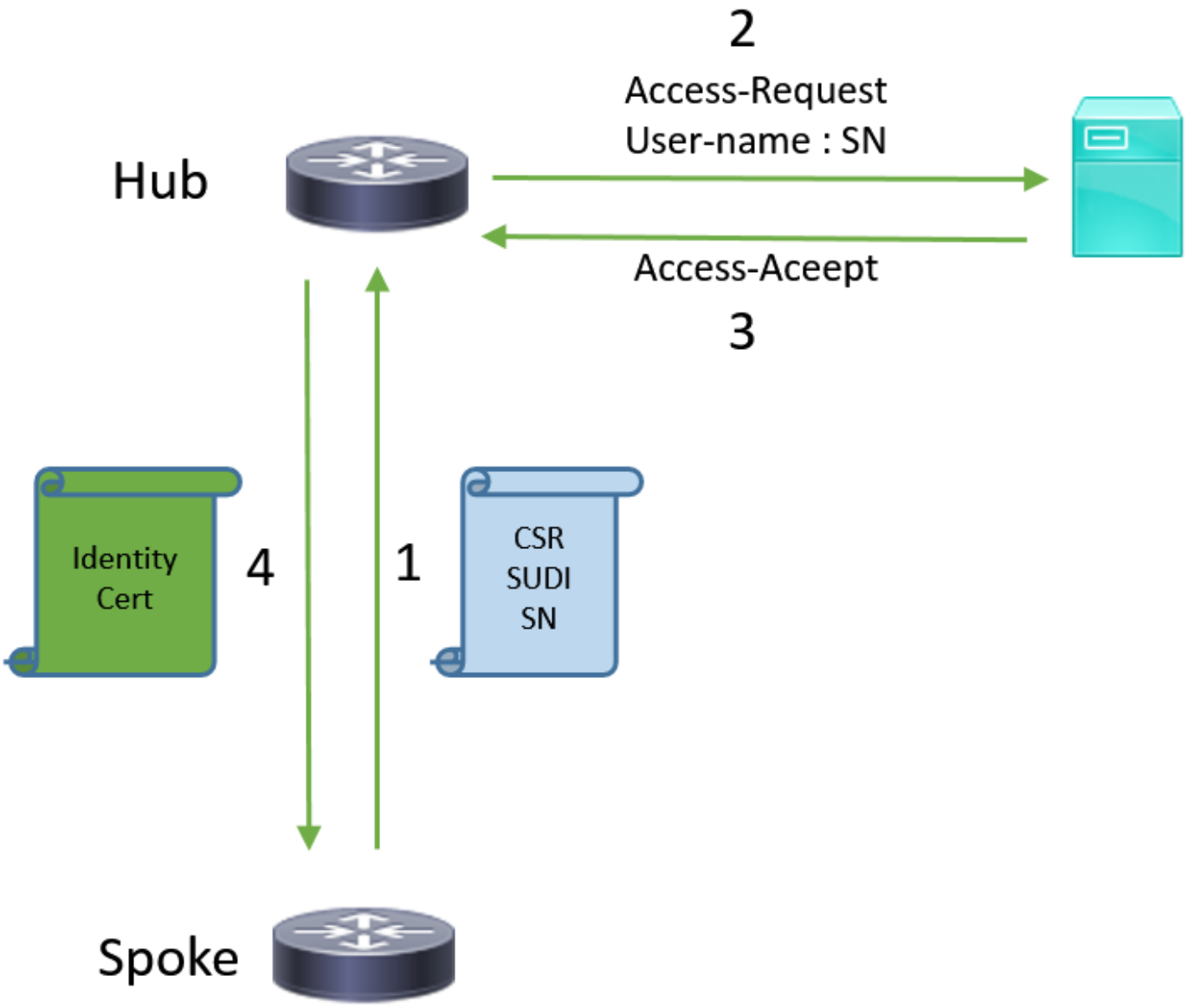
网络流

1. 分支路由器创建SCEP请求，用其苏堤认证专用密钥签署它并且发送它到CA服务器。

2. 如果请求适当地签字， RADIUS请求生成。序列号使用作为用户名参数。

3. RADIUS服务器接受或拒绝请求。

4. 如果请求被接受， CA服务器同意请求。如果它被拒绝， CA服务器回复以“等待”状态，并且客户端再试请求，在退路计时器到期后。



与仅CA的配置

```
!CA server

radius server RADSRV
address ipv4 10.10.20.30 auth-port 1812 acct-port 1813
key cisco123

aaa group server radius RADSRV
server name RADSRV

aaa authorization network SUDI group RADSRV

crypto pki server CA
! will grant certificate for requests signed by SUDI certificate automatically
grant auto trustpoint SUDI
issuer-name CN=ca.example.com
hash sha256
lifetime ca-certificate 7200
lifetime certificate 3600

crypto pki trustpoint CA
rsakeypair CA 2048
```

```
crypto pki trustpoint SUDI
! Need to import the SUDI CA certificate manually, for example with "crypto pki import" command
enrollment terminal
revocation-check none
! Authorize with Radius server
authorization list SUDI
! SN extracted from cert will be used as username in access-request
authorization username subjectname serialnumber
```

!CLIENT

```
crypto pki trustpoint FLEX
enrollment profile PROF
! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive prompt
will prevent the process from starting automatically
serial-number none
fqdn none
ip-address none
! Password needs to be specified to automate the process. However, it will not be used by CA
server
password 7 110A1016141D5A5E57
subject-name CN=spoke.example.com
revocation-check none
rsakeypair FLEX 2048
auto-enroll 85 crypto pki profile enrollment PROF ! CA server address enrollment url
http://192.0.2.1 enrollment credential CISCO_IDEVID_SUDI ! By pre-importing CA cert you will
avoid “crypto pki authenticate” step. If auto-enroll is configured, enrollment will also start
automatically crypto pki certificate chain FLEX certificate ca 01 30820354 3082023C A0030201
02020101 300D0609 2A864886 F70D0101 04050030 3B310E30 0C060355 040A1305 43697363 6F310C30
0A060355 040B1303 54414331 ----- output truncated ---- quit
```

RADIUS server:

The Radius needs to return Access-Accept with the following Cisco AV Pair to enable certificate enrollment:

```
pki:cert-application=all
```

与CA和RA的配置

!CA server

```
crypto pki server CATEST
   issuer-name CN=CATEST.example.com,OU=TAC,O=Cisco
   ! will grant the requests coming from RA automatically
   grant ra-auto
crypto pki trustpoint CATEST
   revocation-check crl
   rsakeypair CATEST 2048
```

!RA server

```
radius server RADSRV
   address ipv4 10.10.20.30 auth-port 1812 acct-port 1813
   key cisco123

aaa group server radius RADSRV
   server name RADSRV
```

```
aaa authorization network SUDI group RADSRV

crypto pki server RA
   no database archive
   ! will forward certificate requests signed by SUDI certificate automatically
   grant auto trustpoint SUDI
   mode ra

crypto pki trustpoint RA
   ! CA server address
   enrollment url http://10.10.10.10
   serial-number none
   ip-address none
   subject-name CN=ra1.example.com, OU=ioscs RA, OU=TAC, O=Cisco
   revocation-check crl
   rsakeypair RA 2048

crypto pki trustpoint SUDI
   ! Need to import the SUDI CA certificate manually, for example with "crypto pki import"
command
   enrollment terminal
   revocation-check none
   ! Authorize with Radius server
   authorization list SUDI
   ! SN extracted from cert will be used as username in access-request
   authorization username subjectname serialnumber
```

!CLIENT

```
crypto pki trustpoint FLEX
   enrollment profile PROF
   ! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive
prompt will prevent the process from starting automatically
   serial-number none
   fqdn none
   ip-address none
   ! Password needs to be specified to automate the process. However, it will not be used by CA
server
   password 7 110A1016141D5A5E57
   subject-name CN=spoke.example.com
   revocation-check none
   rsakeypair FLEX 2048
   auto-enroll 85

crypto pki profile enrollment PROF
   ! RA server address
   enrollment url  http://192.0.2.1
   enrollment credential CISCO_IDEVID_SUDI


! By pre-importing CA cert you will avoid “crypto pki authenticate” step. If auto-enroll is
configured, enrollment will also start automatically
crypto pki certificate chain FLEX
   certificate ca 01
  30820354 3082023C A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  3B310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
 ----- output truncated ----
  quit
```

```
!CLIENT

crypto pki trustpoint FLEX
   enrollment profile PROF
   ! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive
prompt will prevent the process from starting automatically
   serial-number none
   fqdn none
   ip-address none
   ! Password needs to be specified to automate the process. However, it will not be used by CA
server
   password 7 110A1016141D5A5E57
   subject-name CN=spoke.example.com
   revocation-check none
   rsakeypair FLEX 2048
   auto-enroll 85

crypto pki profile enrollment PROF
   ! RA server address
   enrollment url  http://192.0.2.1
   enrollment credential CISCO_IDEVID_SUDI


! By pre-importing CA cert you will avoid “crypto pki authenticate” step. If auto-enroll is
configured, enrollment will also start automatically
crypto pki certificate chain FLEX
   certificate ca 01
  30820354 3082023C A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  3B310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
 ----- output truncated ----
  quit
```

配置/模板

此输出示例:显示在闪存驱动器放置在usbflash0:/ciscortr.cfg文件的一种模范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
! This will differ if you use SUDI, please see above
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"
```

Verify

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。使用输出解释器工具来查看 show 命令输出的分析。

如果隧道上升，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
```

如果认证正确地，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
```

Troubleshoot

目前没有针对此配置的故障排除信息。

已知警告和问题

Cisco Bug ID CSCuu93989 -设置向导终止在G2平台的PnP流也许造成系统从usbflash不装载配置：/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
```

Note:保证您使用包含此缺陷的一个修正的一个版本。

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**零的联系配置**使用是一个不同的功能**通过**在Cisco 800系列ISR配置概述描述的**USB**。

--	**通过USB调零联系配置**	**默认配置文件**
支持的平台	对只有少量8xx路由器限制。 关于详细资料，请参阅Cisco 800系列ISR配置概述	所有ISR G2、43xx和44xx。
文件名	*.cfg	ciscortr.cfg
在本地闪存保存配置	是，自动地	不，嵌入式活动管理器(EEM)要求

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

摘要

USB默认配置(与从USB闪存驱动器的文件名**ciscortr.cfg**)在远端位置产生网络管理员能力配置远程办公室分支路由器VPN (但是没限制对VPN)，不用需要登录到设备。

Related Information

- 简单认证登记协议(SCEP)
- 零的联系配置通过USB
- DMVPN/FlexVPN/Site对站点VPN
- Technical Support & Documentation - Cisco Systems
- Cisco锚点技术