配置VPN远程办公室/分支的零接触部署(ZTD)

目录

简介

本文档介绍零接触部署(ZTD)选项如何成本高效且可扩展的部署解决方案。

安全、高效的部署和远程办公室路由器（有时称为分支）的调配可能是一项艰巨的任务。远程办公室可能位于现场工程师在现场配置路由器是一项挑战的位置，由于成本和潜在安全风险，大多数工程师选择不发送预配置的分支路由器。

先决条件

要求

Cisco 建议您了解以下主题：

- 任何具有支持USB闪存驱动器的USB端口的Cisco IOS®路由器。有关详细信息，请参阅USB eToken和USB闪存功能支持。
- 此功能已确认几乎适用于任何思科8xx平台。有关详细信息，请参阅默认配置文件白皮书(Features Support on Cisco 800 Series ISR)。
- 其他具有USB端口的平台，如集成多业务路由器(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：

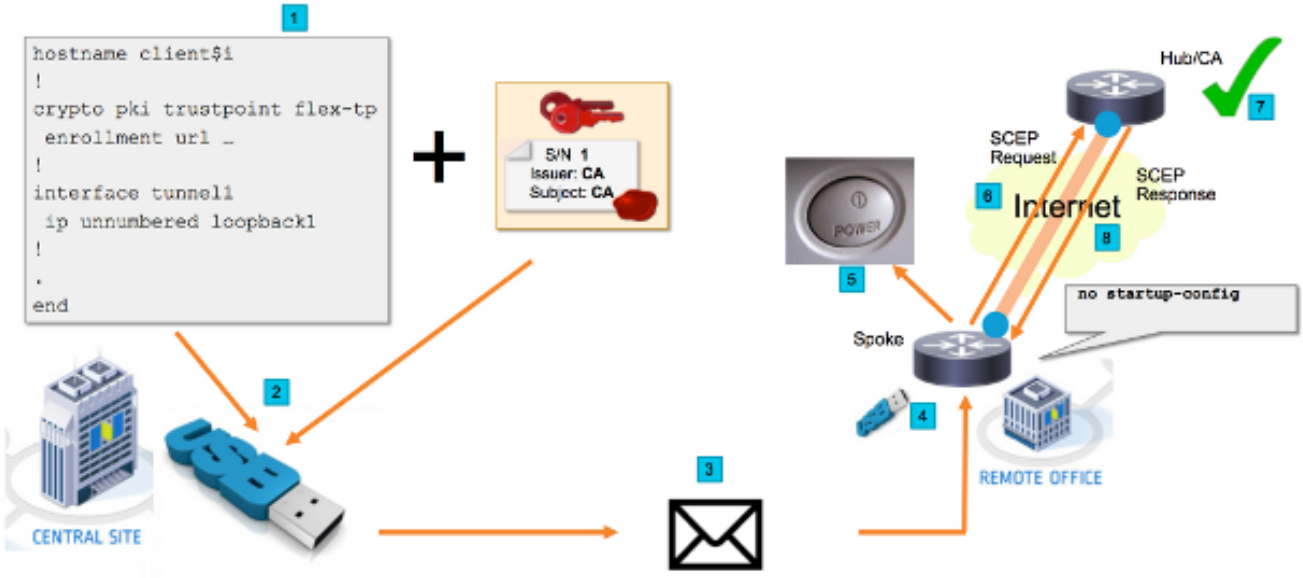
- 简单证书注册协议 (SCEP)
- 通过USB实现零接触部署
- DMVPN/FlexVPN/站点到站点VPN

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（公司总部）中，创建分支配置的模板。模板包含签署VPN中心路由器证书的证书颁发机构(CA)证书。
2. 配置模板在名为ciscortr.cfg的文件中的USB密钥上实**例化**。此配置文件包含要部署的路由器的分支特定配置。 **注意：**USB上的配置不包含除IP地址和CA证书以外的任何敏感信息。分支或CA服务器没有私钥。
3. USB闪存驱动器通过邮件或包寄送公司发送到远程办公室。
4. 分支路由器也直接从Cisco Manufacturing发送到远程办公室。
5. 在远程办公室中，路由器连接到电源并连接到网络，如USB闪存驱动器随附的说明中所述。然后，USB闪存驱动器插入路由器。 **注意：**此步骤中几乎不涉及任何技术技能，因此任何办公人员都可以轻松执行。
6. 路由器启动后，会从usbflash0:**/ciscortr.cfg读取配置**。一旦路由器通电，就会向CA服务器发送简单证书注册协议(SCEP)请求。
7. 在CA服务器上，可以根据公司安全策略配置手动或自动授予。为手动证书授予配置时，必须执行SCEP请求的带外验证（IP地址验证检查、执行部署的人员的凭证验证等）。

此步骤可能因所使用的CA服务器而异。

8. 分支路由器收到SCEP响应后，Internet密钥交换(IKE)会话将与VPN中心进行身份验证，隧道成功建立。

基于SUDI的授权

第7步包括手动验证通过SCEP协议发送的证书签名请求，这可能会非技术人员操作繁琐且难以执行。为了提高安全性并自动化流程，可以使用安全唯一设备标识(SUDI)设备证书。SUDI证书是内置于ISR 4K设备中的证书。这些证书由思科CA签名。每个制造的设备都使用不同的证书颁发，并且设备的序列号包含在证书的公用名中。SUDI证书、关联密钥对及其整个证书链存储在防篡改信任锚芯片中。此外，密钥对被密码绑定到特定的信任锚芯片，并且私钥从不导出。此功能使克隆或欺骗身份信息几乎不可能。

SUDI私钥可用于对路由器生成的SCEP请求进行签名。CA服务器能够验证签名并读取设备的SUDI证书的内容。CA服务器可以从SUDI证书（如序列号）中提取信息，并基于该信息执行授权。RADIUS服务器可用于响应此类授权请求。

管理员创建分支路由器及其关联序列号的列表。非技术人员可以从路由器的机箱中读取序列号。这些序列号存储在RADIUS服务器数据库中，服务器根据允许自动授予证书的信息授权SCEP请求。请注意，序列号通过思科签名的SUDI证书以加密方式绑定到特定设备，因此不可能伪造。

总之，CA服务器配置为自动授予满足以下两个条件的请求：

- 使用与思科SUDI CA签名的证书关联的私钥签名
- 由Radius服务器根据从SUDI证书获取的序列号信息进行授权

部署方案

CA服务器可能直接暴露在互联网上，因此允许客户端在建立隧道之前执行注册。CA服务器甚至可以配置在与VPN集线器相同的路由器上。此拓扑的优点是简单。缺点是CA服务器直接暴露在通过Internet进行的各种攻击中，从而降低了安全性。

或者，可以通过配置注册机构服务器来扩展拓扑。注册机构服务器角色是评估有效证书签名请求并将其转发到CA服务器。RA服务器本身不包含CA的私钥，无法自行生成证书。在这种部署中，CA服务器不需要暴露在互联网上，这提高了整体安全性。'

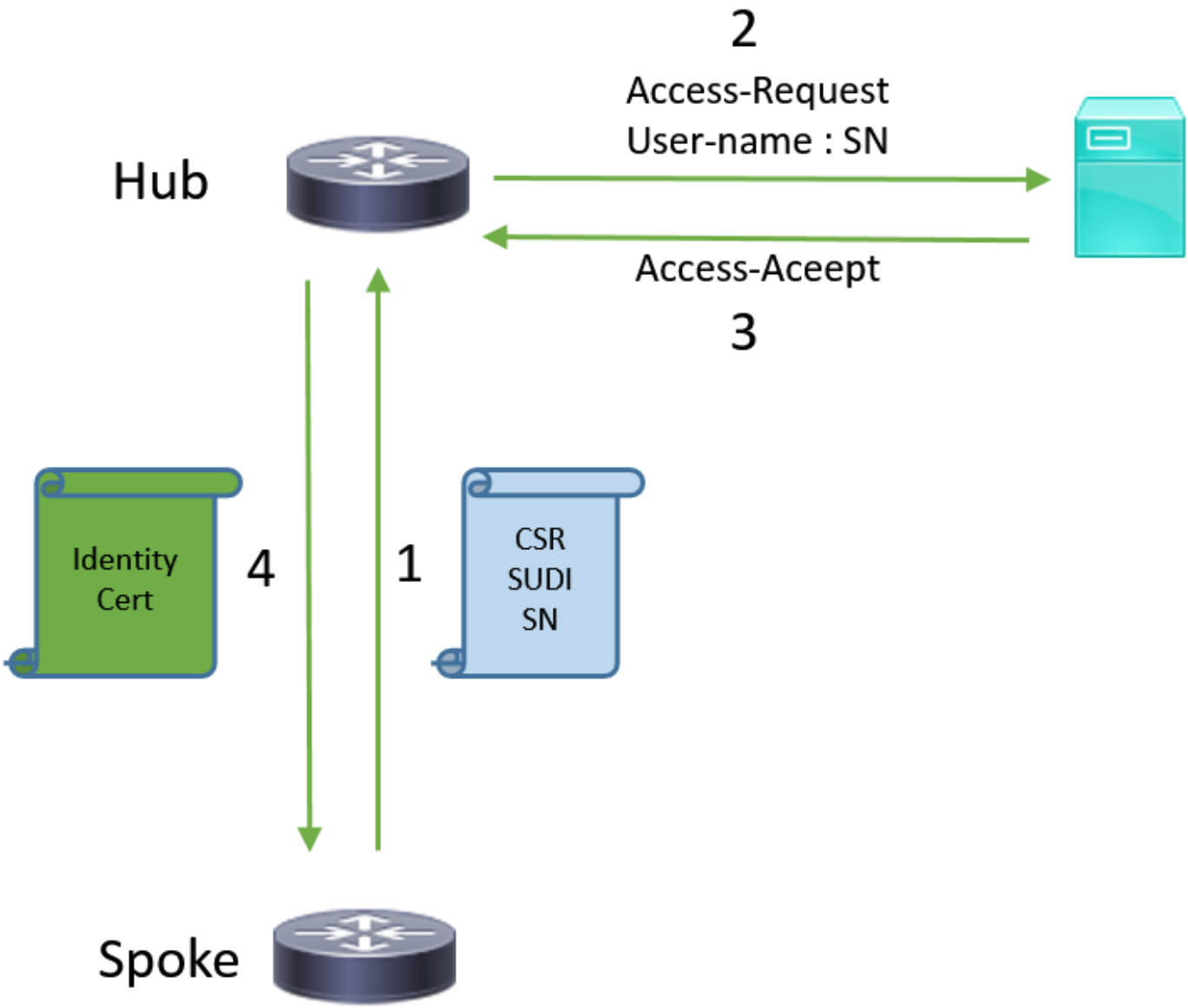
网络流

1.分支路由器创建SCEP请求，用其SUDI证书的私钥签名并将其发送到CA服务器。

2.如果请求已正确签名，则生成RADIUS请求。序列号用作用户名参数。

3. RADIUS服务器接受或拒绝请求。

4.如果请求被接受，CA服务器将授予该请求。如果拒绝，CA服务器将回复“待处理”状态，客户端在回退计时器到期后重试请求。



仅CA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
```

使用CA和RA进行配置

!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
```

RADIUS server:

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

pki:cert-application=all

配置/模板

此示例输出显示了示例性的FlexVPN远程办公室配置，该配置放在usbflash0:/ciscortr.cfg文件的闪存驱动器上。

```
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"
```

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。使用输出解释器工具来查看 show 命令输出的分析。

如果隧道启动，您可以在Spoke上验证：

```
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
```

您还可以在辐条上验证证书是否注册正确：

```
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。

已知警告和问题

Cisco Bug ID CSCuu93989 — 配置向导在G2平台上停止PnP流可能导致系统不从usbflash:/ciscortr.cfg加载配置。系统可能停止在配置向导功能：

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

注意：确保使用包含此缺陷修复的版本。

ZTD（通过USB）与默认配置文件

请注意，本文**档使用的**默认配置文件功能与Cisco 800系列ISR部署概述中描述的通过**USB实现零接触部**署的功能不同。

-	**通过USB实现零接触部署**	**默认配置文件**
支持的平台	仅限少量8xx路由器。 有关详细信息，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
在本地闪存上保存配置	是，自动	否，需要嵌入式事件管理器(EE

由于默认配置文件功**能支持更**多平台，因此本文中介绍的解决方案选择了此技术。

摘要

USB默认配置(从USB闪存驱动器中使用文件名**ciscortr.cfg**)使网络管理员能够部署远程办公室分支路由器VPN（但不限于VPN），而无需登录远程位置的设备。

相关信息

- **简单证书注册协议 (SCEP)**
- **通过USB实现零接触部署**
- **DMVPN/FlexVPN/站点到站点VPN**
- **技术支持和文档 - Cisco Systems**
- **思科锚技术**