配置VPN遠端辦公室/輻條的零接觸部署(ZTD)

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[設定](#)
[網路圖表](#)
[網路流量](#)
[基於SUDI的授權](#)
[部署方案](#)
[網路流量](#)
[僅使用CA的配置](#)
[使用CA和RA進行配置](#)
[配置/模板](#)
[驗證](#)
[疑難排解](#)
[已知警告和問題](#)
[通過USB的ZTD與預設配置檔案](#)
[摘要](#)
[相關資訊](#)

簡介

本文檔介紹零接觸部署(ZTD)選項如何成為經濟高效且可擴展的部署解決方案。

安全高效的部署和配置遠端辦公室路由器（有時稱為分支）是一項艱鉅的任務。遠端辦公室可能位於現場工程師很難在現場配置路由器的位置，而且由於成本和潛在的安全風險，大多數工程師選擇不傳送預配置的分支路由器。

必要條件

需求

思科建議您瞭解以下主題：

- 具有支援USB快閃記憶體驅動器的USB埠的任何Cisco IOS®路由器。有關詳細資訊，請參閱USB eToken和USB快閃記憶體功能支援。
- 幾乎所有的Cisco 8xx平台都確認可以使用此功能。有關詳細資訊，請參閱預設配置檔案白皮書（Cisco 800系列ISR上的功能支援）。
- 具有USB埠的其他平台，如整合服務路由器(ISR)系列G2和43xx/44xx。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

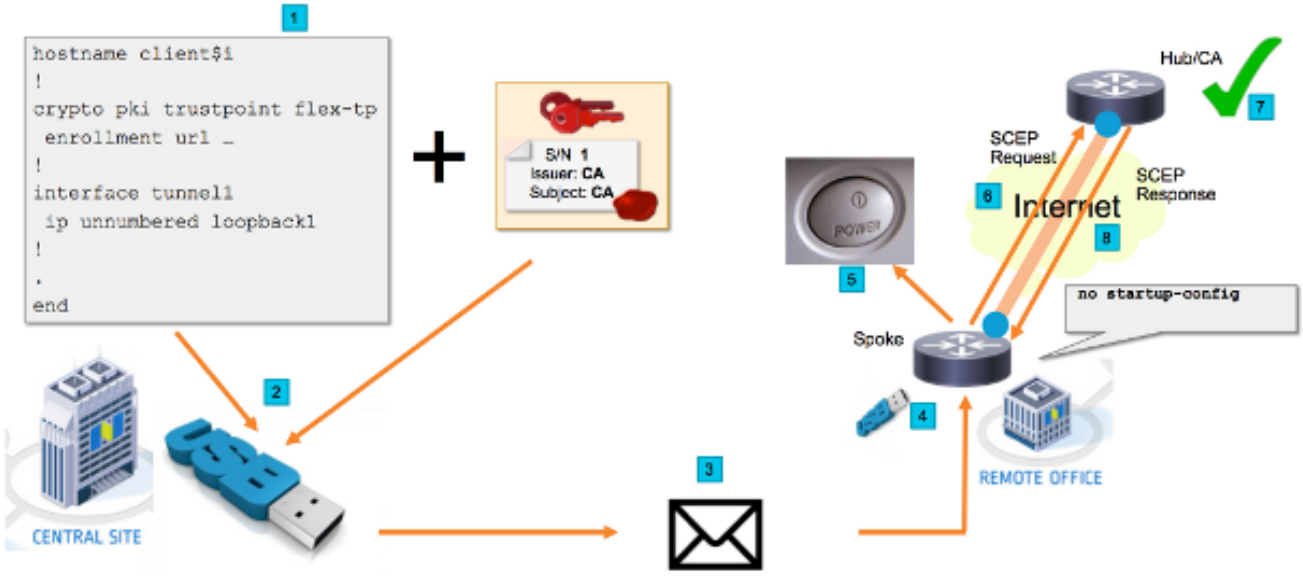
- 簡單憑證註冊通訊協定(SCEP)
- 通過USB實現零接觸部署
- DMVPN/FlexVPN/站點到站點VPN

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



網路流量

1. 在中心站點（公司總部）中建立分支配置的模板。該模板包含簽署VPN中心路由器證書的證書頒發機構(CA)證書。
2. 配置模板在名為**ciscortr.cfg**的檔案中的USB金鑰上例項化。此配置檔案包含要部署的路由器的分支特定配置。 **附註**：USB上的配置不包含除IP地址和CA證書以外的任何敏感資訊。分支或CA伺服器沒有私鑰。
3. USB快閃記憶體驅動器通過郵件或包遞送公司傳送到遠端辦公室。
4. 分支路由器也會直接從思科製造部門傳送到遠端辦公室。
5. 在遠端辦公室中，路由器已連線到電源，並已通過電纜連線到網路，如USB快閃記憶體驅動器隨附的說明中所述。然後，將USB快閃記憶體驅動器插入路由器。 **附註**：此步驟中幾乎不涉及任何技術技能，因此任何辦公室人員都可以輕鬆地執行該步驟。
6. 路由器啟動後，會從**usbflash0:/ciscortr.cfg**讀取配置。路由器通電後，系統會向CA伺服器傳送簡單憑證註冊通訊協定(SCEP)要求。
7. 在CA伺服器上，可以根據公司安全策略配置手動或自動授予。當配置為手動證書授予時，必須執行SCEP請求的帶外驗證（IP地址驗證檢查、執行部署的人員的憑據驗證等）。

此步驟可能因使用的CA伺服器而異。

8. 分支路由器收到SCEP響應後（現在擁有有效證書），網際網路金鑰交換(IKE)會話將通過VPN中心進行身份驗證，並且隧道成功建立。

基於SUDI的授權

第7步涉及手動驗證通過SCEP協定傳送的證書簽名請求，對於非技術人員來說，這可能非常麻煩且難以執行。為了提高安全性並使流程自動化，可以使用安全唯一裝置標識(SUDI)裝置證書。SUDI證書是ISR 4K裝置中內建的證書。這些憑證由Cisco CA簽署。每個生產的裝置都以不同的證書簽發，並且裝置的序列號包含在證書的公用名中。SUDI證書、關聯的金鑰對及其整個證書鏈儲存在防篡改信任錨晶片中。此外，金鑰對以密碼方式繫結到特定信任錨點晶片，並且從不匯出私鑰。此功能使克隆或欺騙身份資訊變得幾乎不可能。

SUDI私鑰可用於對路由器生成的SCEP請求進行簽名。CA伺服器可以驗證簽名並讀取裝置的SUDI證書的內容。CA伺服器可以從SUDI證書提取資訊（如序列號），並根據該資訊進行授權。RADIUS伺服器可用於回應此類授權要求。

管理員建立輻條路由器及其相關序列號清單。非技術人員可以從路由器的機箱中讀取序列號。這些序列號儲存在RADIUS伺服器資料庫中，伺服器根據允許自動授予證書的資訊授權SCEP請求。請注意，序列號通過思科簽名的SUDI證書以密碼方式繫結到特定裝置，因此無法偽造。

總之，CA伺服器配置為自動授予符合以下兩個條件的請求：

- 使用與Cisco SUDI CA簽名的證書關聯的私鑰進行簽名
- 由Radius伺服器根據從SUDI證書獲取的序列號資訊授權

部署方案

CA伺服器可能直接暴露於網際網路，因此允許使用者端在可以建立通道之前執行註冊。CA伺服器甚至可以配置在與VPN中心相同的路由器上。此拓撲的優點是簡單。缺點是安全性降低，因為CA伺服器會直接暴露在通過Internet進行的各種形式的攻擊中。

或者，可以通過配置註冊機構伺服器來擴展拓撲。註冊機構伺服器角色是評估有效的證書簽名請求並將其轉發到CA伺服器。RA伺服器本身不包含CA的私鑰，因此無法自行生成證書。在這種部署中，CA伺服器無需暴露於網際網路，這提高了整體安全性。」

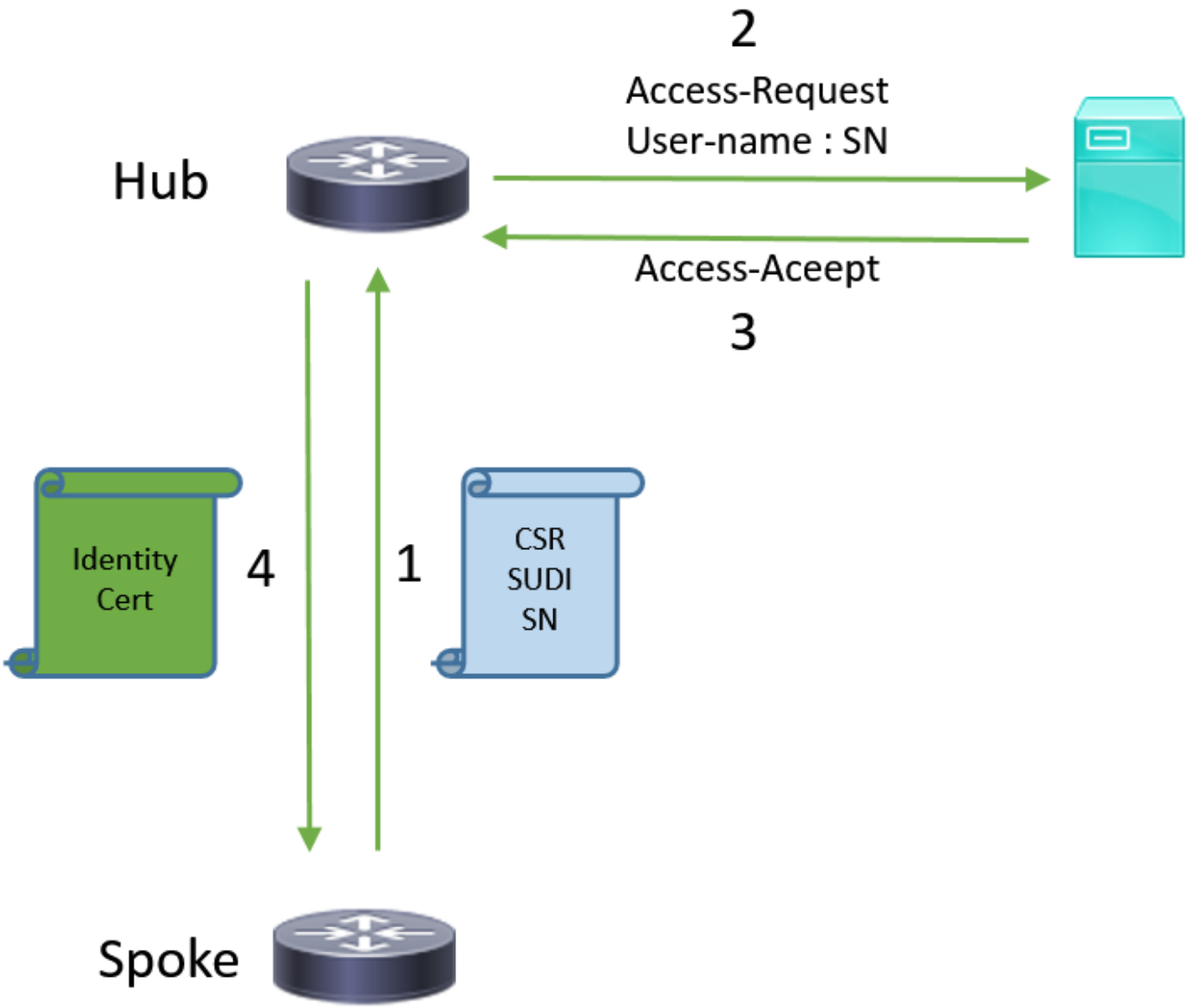
網路流量

1.分支路由器建立SCEP請求，使用其SUDI證書的私鑰對其進行簽名，並將其傳送到CA伺服器。

2.如果請求簽名正確，則生成RADIUS請求。序列號用作使用者名稱引數。

3. RADIUS伺服器接受或拒絕該要求。

4.如果請求被接受，則CA伺服器將授予該請求。如果被拒絕，CA伺服器會以「Pending」狀態回覆，客戶端會在回退計時器到期後重試請求。



僅使用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
```

使用CA和RA進行配置

!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

此輸出示例顯示了放在usbflash0:/ciscortr.cfg檔案中的快閃記憶體驅動器上的示例FlexVPN遠端辦公室配置。

```
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"
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

您可以在Spoke上驗證通道是否啟動：

```
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
```

您也可以在分支上驗證證書是否正確註冊：

```
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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

已知警告和問題

思科錯誤ID CSCuu93989 — 配置嚮導停止G2平台上的PnP流可能會導致系統無法從usbflash:/ciscortr.cfg載入配置。相反，系統可能會停止配置嚮導功能：

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

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

附註：請確保使用的版本包含此缺陷的修復程式。

通過USB的ZTD與預設配置檔案

請注意，本文檔使用的**預設配置檔案**功能與Overview of Cisco 800 Series ISR Deployment中所述的**通過USB進行零接觸部署的功能不同。**

-	**通過USB實現零接觸部署**	**預設組態檔**
支援的平台	僅限於幾台8xx路由器。 有關詳細資訊，請參閱Cisco 800系列ISR部署概述	所有ISR G2、43xx和44xx。
檔名	*.cfg	ciscortr.cfg
在本地快閃記憶體上儲存配置	是，自動	否，需要嵌入式事件管理器(

由於**預設配置檔案**功能支援更多平台，因此選擇此技術用於本文中介紹的解決方案。

摘要

USB預設配置(使用USB快閃記憶體驅動器中的檔名**ciscortr.cfg**)使網路管理員能夠部署遠端辦公室分支路由器VPN（但不限於VPN），而無需登入到遠端位置的裝置。

相關資訊

- **簡單憑證註冊通訊協定(SCEP)**
- **通過USB實現零接觸部署**
- **DMVPN/FlexVPN/站點到站點VPN**
- **技術支援與文件 - Cisco Systems**
- **思科錨點技術**