Instellen van Nul Touch-implementaties (ZTD) van VPN-afgelegen vestigingen/SPRAKEN configureren

Inhoud

Inleiding

Dit document beschrijft hoe een ZTD-optie (Zero Touch Deployment) een kostenefficiënte en schaalbare oplossing voor implementaties is.

Beveiligde en efficiënte implementatie en de levering van Remote Office-routers (soms Spokes genoemd) kunnen een moeilijke taak zijn. Afstandskantoren kunnen op locaties zijn waar het een uitdaging is om een Veldingenieur te hebben de router onsite configureren en de meeste ingenieurs kiezen er voor om vooraf ingestelde Spoke-routers niet te verzenden vanwege de kosten en mogelijke beveiligingsrisico's.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Elke Cisco IOS® router die een USB-poort heeft die USB-Flash-schijven ondersteunt. Zie Ondersteuning van USB-functies en USB-Flash.
- Deze optie is bevestigd dat u aan vrijwel elk Cisco 8xx-platform werkt. Zie Whitepaper over standaardconfiguratie van bestanden (ondersteuning voor functies op Cisco 800 Series ISR).
- Andere platforms die USB-poorten hebben, zoals Integrated Service Router (ISR) reeks G2 en 43xx/44xx.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

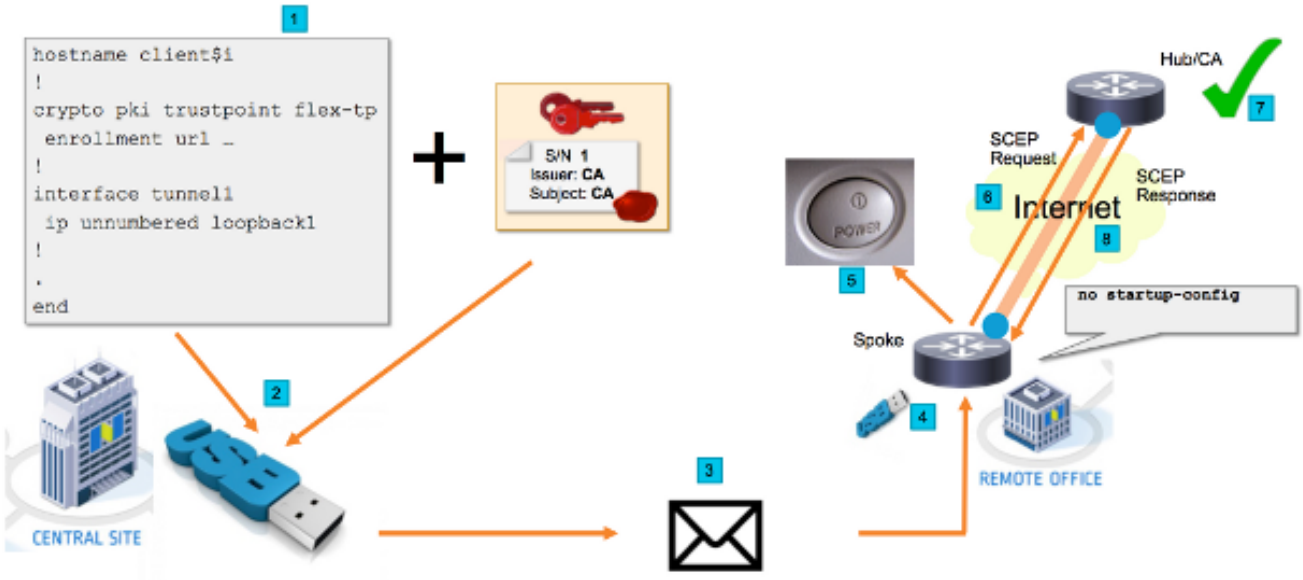
- Eenvoudig certificeringsprotocol (SCEP)
- plaatsing zonder aanraking via USB
- DMVPN/FlexVPN/Site-to-site VPN's

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



Netwerkstroom

1. Op de Central Site (Hoofdkwartier van het bedrijf) verschijnt een sjabloon met de Spoke-configuratie. De sjabloon bevat het certificaat van de certificeringsinstantie (CA) dat het certificaat van de VPN-hubrouter heeft ondertekend.

2. De configuratiesjabloon wordt op een USB-toets geconcretiseerd in een bestand dat **ciscortr.cfg** wordt genoemd. Dit configuratiebestand bevat de Spoke-specifieke configuratie voor de router die moet worden ingezet. Opmerking: De configuratie op het USB-apparaat bevat geen andere gevoelige informatie dan IP-adressen en het CA-certificaat. Er is geen privé-sleutel van de Spoke of CA Server.
3. De USB Flash-schijf wordt naar het Remote Office verzonden via de post of een verpakkingsbedrijf.
4. De router Spoke wordt ook rechtstreeks naar het Remote Office verzonden vanuit Cisco Fabric.
5. In het Remote Office is de router aangesloten op de stroom en op het netwerk aangesloten zoals wordt uitgelegd in de instructies die met de USB-flitser worden meegeleverd. Daarna wordt de USB-flitser in de router ingevoegd. Opmerking: Bij deze stap zijn weinig tot geen technische vaardigheden betrokken, zodat het gemakkelijk door elk kantoorpersoneel kan worden uitgevoerd.
6. Zodra de router opstart, leest het de configuratie van **usbflash0:/ciscortr.cfg**. Zodra de router is ingeschakeld, wordt een verzoek om een Eenvoudig certificaat in te voeren Protocol (SCEP) naar de CA Server verzonden.
7. Op de CA Server kan Handmatig of Automatische Toewijzing worden ingesteld op basis van het bedrijfsbeveiligingsbeleid. Indien geconfigureerd voor het handmatige verlenen van certificaten, moet de buiten-band verificatie van het SCEP-verzoek worden uitgevoerd (controle van IP-adresvalidatie, geloofsvalidatie voor het personeel dat de plaatsing uitvoert, enz.). Deze stap kan op basis van de CA Server verschillen die wordt gebruikt.
8. Zodra de SCEP Response wordt ontvangen door de Spoke router, die nu een geldig certificaat heeft, authenticeert de Internet Key Exchange (IKE)-sessie met de VPN-hub en de Tunnel vastlegt.

Op SUDI gebaseerde vergunning

Stap 7 behelst de handmatige verificatie van het ondertekeningsverzoek van het certificaat dat via het SCEP-protocol wordt verzonden. Dit kan omslachtig en moeilijk te verrichten zijn voor niet-technisch personeel. Om de beveiliging te verhogen en het proces te automatiseren, kunnen de Secure Unity Devices Identification (SUDI)-certificaten worden gebruikt. SUDI-certificaten zijn ingebouwd in ISR 4K-apparaten. Deze certificaten worden ondertekend door Cisco CA. Elk gefabriceerd hulpmiddel is voorzien van een ander certificaat en het serienummer van het hulpmiddel is opgenomen in de gemeenschappelijke naam van het certificaat. Het SUDI-certificaat, het bijbehorende sleutelpaar en de hele certificeringsketen worden opgeslagen in de tamper-resistente Trust Anchor-chip. Bovendien is het sleutelpaar cryptografisch gebonden aan een specifieke Betrouwankerchip en wordt de privé-sleutel nooit geëxporteerd. Op deze manier is het klonen of het afluisteren van identiteitsgegevens vrijwel onmogelijk.

De privé-sleutel van SUDI kan worden gebruikt om het SCEP verzoek te ondertekenen dat door de router gegenereerd is. De CA-server kan de handtekening controleren en de inhoud van het SUDI-certificaat van het apparaat lezen. Een CA-server kan de informatie uit het SUDI-certificaat halen (net als een serienummer) en op basis van die informatie een vergunning uitvoeren. De RADIUS-server kan worden gebruikt om op een dergelijk verzoek te reageren.

De beheerder maakt een lijst van de woordrouters en hun bijbehorende serienummers. De serienummers kunnen door het niet-technische personeel uit het geval van de router worden gelezen. Deze serienummers worden opgeslagen in de RADIUS-serverdatabase en de server geeft toestemming voor de SCEP-verzoeken op basis van die informatie, waardoor het certificaat

automatisch kan worden toegekend. Let op dat het serienummer cryptografisch aan een specifiek apparaat is gekoppeld via het door Cisco ondertekende SUDI-certificaat, zodat het niet kan worden vervalst.

Samengevat is de CA server ingesteld om automatisch verzoeken te verlenen die aan beide criteria voldoen:

- Ontworpen met particuliere sleutel gekoppeld aan een certificaat dat is ondertekend door Cisco SUDI CA
- Er wordt een vergunning verleend door de Radius-server op basis van de serienummer-informatie van het SUDI-certificaat

Plaatsingsscenario's

De CA-server kan rechtstreeks aan internet worden blootgesteld, zodat de klanten de inschrijving kunnen uitvoeren voordat de tunnel kan worden gebouwd. Een CA-server kan zelfs worden geconfigureerd op dezelfde router als VPN-hub. Het voordeel van deze topologie is eenvoud. Het nadeel is minder veiligheid aangezien de CA server direct wordt blootgesteld aan verschillende vormen van aanval via het internet.

In plaats hiervan kan de topologie ook worden uitgebreid door de server van de Registratie Autoriteit te configureren. De serverrol van de Registratie Autoriteit is het beoordelen en doorsturen van geldige certificaatsignaleringsaanvragen aan de CA-server. De RA-server zelf bevat niet de privé-sleutel van de CA en kan op zichzelf geen certificaten genereren. Bij een dergelijke installatie hoeft de CA server niet te worden blootgesteld aan het internet, hetgeen de algemene veiligheid verhoogt. "

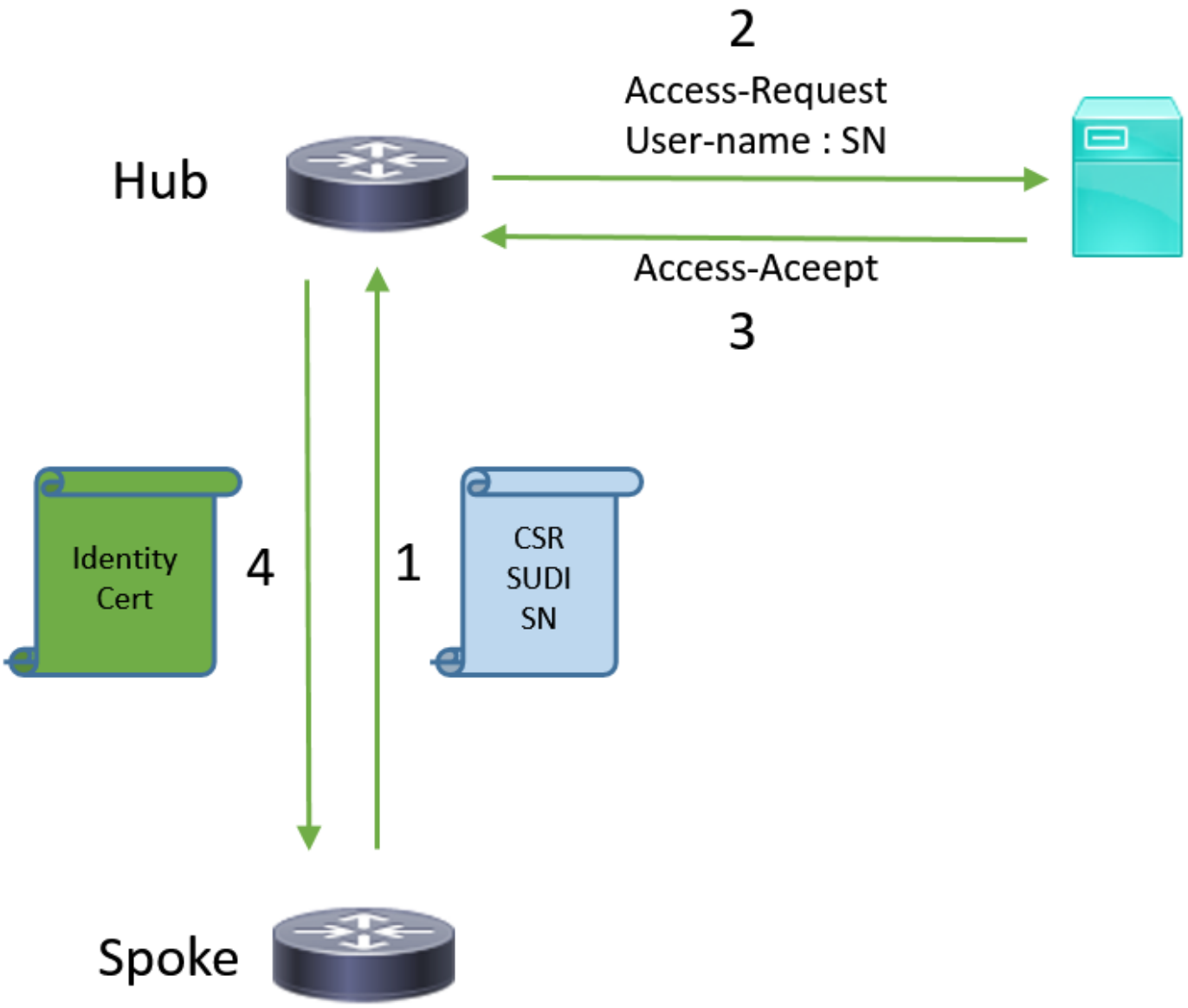
Netwerkstroom

1. De Spoke router maakt een SCEP-verzoek aan, tekent het met de privésleutel van het SUDI-certificaat en stuurt het naar de CA-server.

2. Als het verzoek naar behoren is ondertekend, wordt een RADIUS-verzoek gegenereerd. Het serienummer wordt gebruikt als een gebruikersnaam.

3. De RADIUS-server accepteert of wijst het verzoek af.

4. Als het verzoek wordt ingewilligd, wordt het verzoek op de CA-server ingewilligd. Als het wordt verworpen, antwoordt de CA server met "Hangende" status en probeert de client het verzoek opnieuw in nadat een backtimer verloopt.



Configuratie met alleen CA

```
!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
```

Configuratie met CA en RA

!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

Configuraties/sjabloon

Deze voorbeelduitvoer toont een voorbeeldige configuratie van FlexVPN Remote Office die op de flash-drive in het **subflash0:/ciscortr.cfg-**bestand wordt gezet.

```
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"
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

U kunt op de Spoke controleren of de tunnels zijn opgeblazen:

```
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
```

U kunt ook op de Spoke controleren of het certificaat correct is ingevoerd:

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Bekende zorgen en kwesties

Cisco bug-ID CSCu93989 - Wizard Config stopt de PnP-stroom op G2-platforms waardoor het systeem de configuratie niet vanaf de subflitser hoeft te laden:/ciscortr.cfg. In plaats daarvan kan het systeem stoppen bij de Wizard Config:

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

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

Opmerking: Zorg ervoor dat u een versie gebruikt die een oplossing voor dit defect bevat.

ZTD via USB vs Default Configuration Files

Merk op dat de optie **Default Configuration Files** die in dit document wordt gebruikt een andere functie is dan **Zero Touch Deployment via USB** wordt beschreven in Overzicht van Cisco 800 Series ISR-implementaties.

-	**plaatsing zonder aanraking via USB**	**Standaard configuratiebestanden**
Ondersteunde platforms	Beperkt tot slechts enkele 8x routers. Zie Overzicht van Cisco 800 Series ISR-implementaties voor meer informatie	Alle ISR's G2, 43xx en
Bestandsnaam	*.cfg	ciscortr.cfg
Hiermee slaat u de configuratie op een lokale flitser op	Ja, automatisch	Nee, Embedded Event Manager (EEM) vereis

Omdat meer platforms worden ondersteund door de functie **Default Configuration**, is deze technologie gekozen voor de oplossing die in dit artikel wordt voorgesteld.

Samenvatting

USB Default Configuration (met bestandsnaam **cisco.cfg** van een USB-flashdrive) biedt de netwerkbeheerders de mogelijkheid om Remote Office Spoke-router VPN's te implementeren (maar niet beperkt tot alleen VPN) zonder dat u zich op de externe locatie in het apparaat hoeft te loggen.

Gerelateerde informatie

- Eenvoudig certificeringsprotocol (SCEP)
- plaatsing zonder aanraking via USB
- DMVPN/FlexVPN/Site-to-site VPN's

- Technische ondersteuning en documentatie – Cisco Systems
- Cisco Anchor-technologie