Konfiguration der Zero-Touch-Bereitstellung (ZTD) von VPN-Außenstellen/Spokes

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie eine Zero Touch Deployment (ZTD)-Option eine kosteneffiziente und skalierbare Lösung für Bereitstellungen ist.

Eine sichere und effiziente Bereitstellung und die Bereitstellung von Routern für Außenstellen (manchmal auch Spokes genannt) können eine schwierige Aufgabe sein. Außenstellen können sich an Standorten befinden, an denen die Konfiguration des Routers durch einen Außendiensttechniker problematisch ist. Die meisten Techniker möchten aufgrund der Kosten und des potenziellen Sicherheitsrisikos keine vorkonfigurierten Spoke-Router senden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Jeder Cisco IOS®-Router mit einem USB-Port, der USB-Flash-Laufwerke unterstützt. Weitere Informationen finden Sie unter Unterstützung von USB-eToken- und USB-Flash-Funktionen.

- Diese Funktion ist für fast alle Cisco 8xx-Plattformen geeignet. Weitere Informationen finden Sie im White Paper zu Standardkonfigurationsdateien (Unterstützung von Funktionen auf Cisco ISR der Serie 800).
- Andere Plattformen mit USB-Ports wie Integrated Service Router (ISR) Serie G2 und 43xx/44xx.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

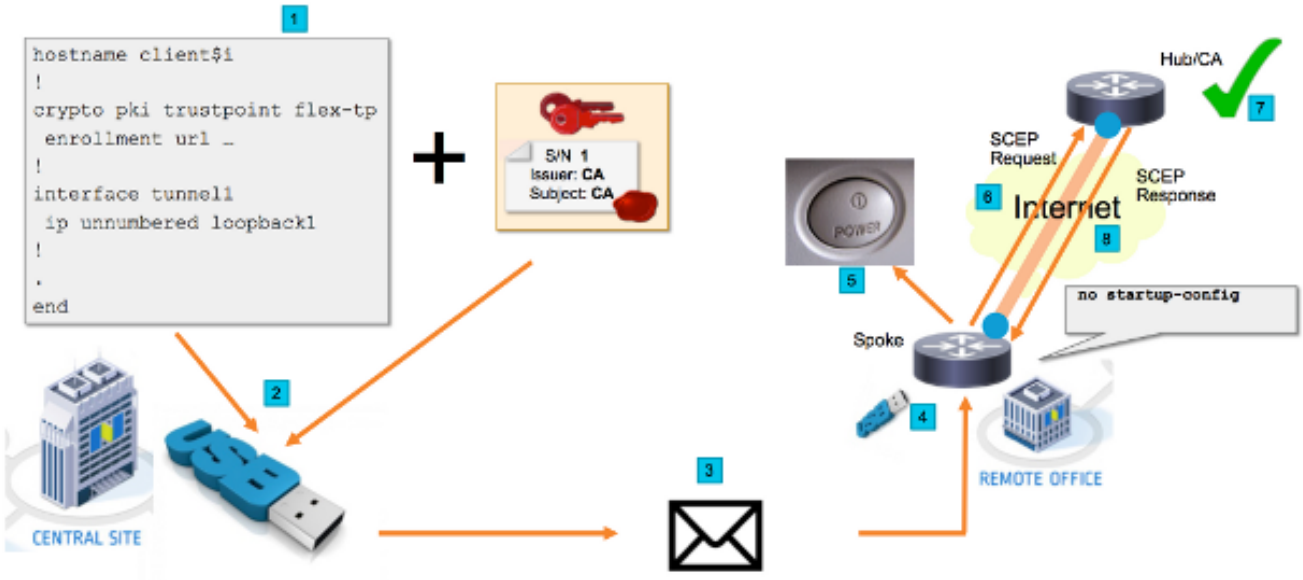
- Simple Certificate Enrollment Protocol (SCEP)
- Zero-Touch-Bereitstellung über USB
- DMVPN/FlexVPN/Site-to-Site-VPNs

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



Netzwerkfluss

1. In der Zentrale (Unternehmenshauptsitz) wird eine Vorlage für die Spoke-Konfiguration erstellt. Die Vorlage enthält das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA), das das Zertifikat des VPN-Hub-Routers signiert hat.

2. Die Konfigurationsvorlage wird auf einem USB-Stick in einer Datei mit dem Namen **ciscortr.cfg** instanziiert. Diese Konfigurationsdatei enthält die Spoke-spezifische Konfiguration für den bereitzustellenden Router. **Hinweis**: Die Konfiguration auf dem USB enthält keine vertraulichen Informationen außer IP-Adressen und dem CA-Zertifikat. Es gibt keinen privaten Schlüssel für den Spoke- oder CA-Server.
3. Das USB-Flash-Laufwerk wird über die Post oder eine Paketzustellungsfirma an die Außenstelle gesendet.
4. Der Spoke-Router wird auch direkt von Cisco Manufacturing an die Außenstelle gesendet.
5. In der Außenstelle wird der Router mit Strom versorgt und mit dem Netzwerk verkabelt, wie in den Anweisungen, die im Lieferumfang des USB-Flash-Laufwerks enthalten sind, beschrieben. Anschließend wird das USB-Flash-Laufwerk in den Router eingesetzt. **Hinweis**: Dieser Schritt beinhaltet kaum oder gar keine technischen Fähigkeiten, sodass er problemlos von jedem Büromitarbeiter durchgeführt werden kann.
6. Sobald der Router gestartet wurde, liest er die Konfiguration aus **usbflash0:/ciscortr.cfg**. Sobald der Router hochgefahren ist, wird eine SCEP-Anfrage (Simple Certificate Enrollment Protocol) an den CA-Server gesendet.
7. Auf dem CA-Server kann entweder Manual (Manuell) oder Automatic Granting (Automatische Zuweisung) basierend auf den Sicherheitsrichtlinien des Unternehmens konfiguriert werden. Bei der Konfiguration für die manuelle Zertifikatsgewährung muss eine Out-of-Band-Überprüfung der SCEP-Anforderung durchgeführt werden (Überprüfung der IP-Adresse, Überprüfung der Anmeldeinformationen für das Personal, das die Bereitstellung durchführt usw.). Dieser Schritt kann je nach dem verwendeten CA-Server abweichen.
8. Sobald die SCEP-Antwort beim Spoke-Router eingeht, der jetzt über ein gültiges Zertifikat verfügt, authentifiziert sich die Internet Key Exchange (IKE)-Sitzung beim VPN-Hub, und der Tunnel wird erfolgreich eingerichtet.

SUDI-basierte Autorisierung

Schritt 7 beinhaltet die manuelle Verifizierung der Zertifikatssignierungsanfrage, die über das SCEP-Protokoll gesendet wurde. Dies kann für nicht-technisches Personal umständlich und schwierig zu bewerkstelligen sein. Um die Sicherheit zu erhöhen und den Prozess zu automatisieren, können die Zertifikate für Secure Unique Device Identification (SUDI)-Geräte verwendet werden. SUDI-Zertifikate sind Zertifikate, die in die ISR 4K-Geräte integriert sind. Diese Zertifikate werden von der Cisco Zertifizierungsstelle signiert. Für jedes hergestellte Gerät wurde ein anderes Zertifikat ausgestellt, und die Seriennummer des Geräts ist im gemeinsamen Namen des Zertifikats enthalten. Das SUDI-Zertifikat, das zugehörige Schlüsselpaar und die gesamte Zertifikatskette werden im manipulationssicheren Trust Anchor-Chip gespeichert. Außerdem ist das Schlüsselpaar kryptografisch an einen bestimmten Trust Anchor-Chip gebunden, und der private Schlüssel wird nie exportiert. Diese Funktion macht das Klonen oder Spoofing von Identitätsinformationen praktisch unmöglich.

Der private SUDI-Schlüssel kann zum Signieren der vom Router generierten SCEP-Anforderung verwendet werden. Der CA-Server kann die Signatur überprüfen und den Inhalt des SUDI-Zertifikats des Geräts lesen. Der CA-Server kann die Informationen aus dem SUDI-Zertifikat extrahieren (wie eine Seriennummer) und die Autorisierung basierend auf diesen Informationen durchführen. Der RADIUS-Server kann verwendet werden, um auf eine solche Autorisierungsanfrage zu reagieren.

Der Administrator erstellt eine Liste der Spoke-Router und der zugehörigen Seriennummern. Die Seriennummern können vom nicht-technischen Personal im Fall des Routers gelesen werden. Diese Seriennummern werden in der RADIUS-Serverdatenbank gespeichert, und der Server autorisiert die SCEP-Anfragen anhand dieser Informationen, die die automatische Erteilung des Zertifikats ermöglichen. Beachten Sie, dass die Seriennummer über das von Cisco signierte SUDI-Zertifikat kryptografisch an ein bestimmtes Gerät gebunden ist, sodass es nicht möglich ist, gefälscht zu werden.

Zusammenfassend lässt sich sagen, dass der CA-Server so konfiguriert ist, dass er automatisch Anforderungen erteilt, die beide folgenden Kriterien erfüllen:

- Sie werden mit einem privaten Schlüssel signiert, der einem Zertifikat zugeordnet ist, das von der Cisco SUDI CA signiert wurde.
- Werden vom Radius-Server anhand der Seriennummern-Informationen aus dem SUDI-Zertifikat autorisiert

Bereitstellungsszenarien

Der CA-Server kann direkt dem Internet verfügbar gemacht werden, sodass die Clients die Registrierung durchführen können, bevor der Tunnel erstellt werden kann. CA-Server können sogar auf demselben Router wie der VPN-Hub konfiguriert werden. Der Vorteil dieser Topologie ist Einfachheit. Der Nachteil ist die verringerte Sicherheit, da der CA-Server direkt für verschiedene Arten von Angriffen über das Internet verfügbar ist.

Alternativ kann die Topologie durch die Konfiguration des Registrierungs-Authority-Servers erweitert werden. Die Serverrolle der Registrierungsstelle besteht darin, gültige Zertifikatssignierungsanforderungen zu bewerten und an den CA-Server weiterzuleiten. Der RA-Server selbst enthält nicht den privaten Schlüssel der CA und kann keine Zertifikate selbst generieren. Bei einer solchen Bereitstellung muss der CA-Server nicht dem Internet ausgesetzt werden, was die Sicherheit insgesamt erhöht."

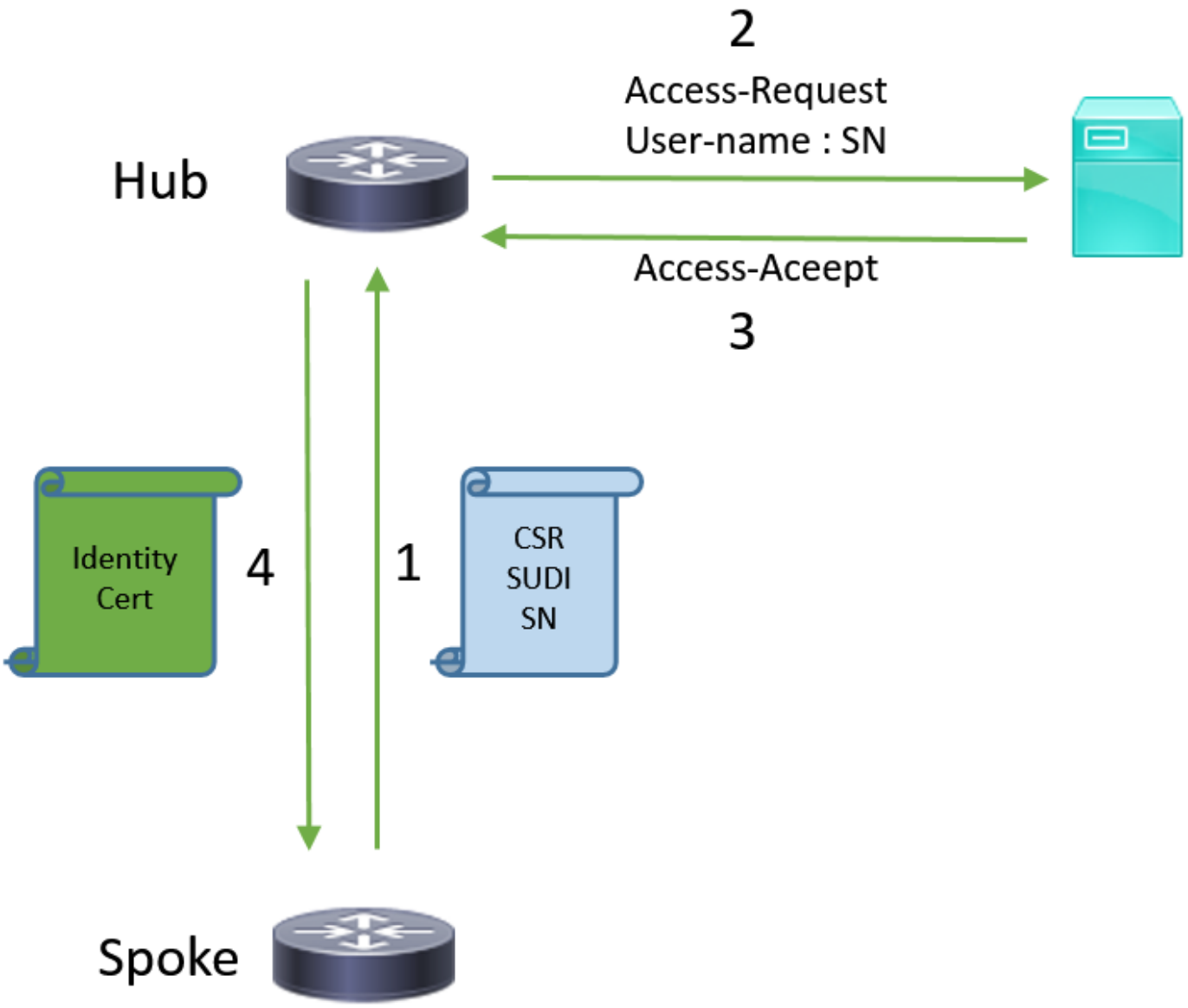
Netzwerkfluss

1. Der Spoke-Router erstellt eine SCEP-Anforderung, signiert diese mit dem privaten Schlüssel des SUDI-Zertifikats und sendet sie an den CA-Server.

2. Wenn die Anforderung ordnungsgemäß signiert ist, wird eine RADIUS-Anforderung generiert. Die Seriennummer wird als Parameter für den Benutzernamen verwendet.

3. Der RADIUS-Server akzeptiert oder lehnt die Anforderung ab.

4. Wenn die Anforderung angenommen wird, erteilt der CA-Server die Anforderung. Wird sie abgelehnt, antwortet der CA-Server mit dem Status "Ausstehend", und der Client versucht die Anforderung nach Ablauf eines Fallback-Timers erneut.



Konfiguration nur mit 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
```

Konfiguration mit CA und 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

Konfigurationen/Vorlage

Diese Beispielausgabe zeigt eine beispielhafte FlexVPN Remote Office-Konfiguration, die auf dem Flash-Laufwerk in der Datei **usbflash0:/ciscortr.cfg** gespeichert ist.

```
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"
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Sie können auf dem Spoke überprüfen, ob die Tunnel hochgefahren sind:

```
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
```

Sie können auch auf dem Spoke überprüfen, ob das Zertifikat korrekt registriert wurde:

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Bekannte Einwände und Probleme

Cisco Bug ID CSCuu93989 - Config Wizard Stoppt den PnP-Fluss auf G2-Plattformen kann dazu führen, dass das System die Konfiguration nicht aus dem usbflash lädt:/ciscortr.cfg. Stattdessen kann das System bei der Funktion des Konfigurationsassistenten anhalten:

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

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

> **Hinweis**: Stellen Sie sicher, dass Sie eine Version verwenden, die eine Behebung für diesen Fehler enthält.

ZTD über USB und Standard-Konfigurationsdateien

Beachten Sie, dass die in diesem Dokument verwendete Funktion für **Standardkonfigurationsdateien** eine andere Funktion ist als die **Bereitstellung ohne Benutzereingriff über USB, die** unter Übersicht über die Bereitstellung der Cisco ISR der Serie 800 beschrieben wird.

-	**Zero-Touch-Bereitstellung über USB**	**Standardkonfigurationsdateien**
Unterstützte Plattformen	Begrenzt auf nur wenige 8xx-Router. Weitere Informationen finden Sie unter Übersicht über die Bereitstellung der Cisco ISR der Serie 800.	Alle ISRs G2, 43xx und 44xx.
Dateiname	*.cfg	ciscortr.cfg
Speichert die Konfiguration im lokalen Flash-Speicher	Ja, automatisch	Nein, Embedded Event Manager (EEM) erforderlich

Da weitere Plattformen von der Funktion **Standardkonfigurationsdateien** unterstützt werden, wurde diese Technologie für die in diesem Artikel vorgestellte Lösung ausgewählt.

Zusammenfassung

Die USB-Standardkonfiguration (mit dem Dateinamen **ciscortr.cfg** von einem USB-Flash-Laufwerk aus) gibt Netzwerkadministratoren die Möglichkeit, VPNs für Spoke-Router in der Außenstelle bereitzustellen (jedoch nicht nur auf VPN beschränkt), ohne sich beim Gerät am Remote-Standort anzumelden.

Zugehörige Informationen

- Simple Certificate Enrollment Protocol (SCEP)
- Zero-Touch-Bereitstellung über USB
- DMVPN/FlexVPN/Site-to-Site-VPNs
- Technischer Support und Dokumentation - Cisco Systems
- Ankertechnologie von Cisco