Configurez le déploiement nul de toucher (ZTD) des bureaux distants/des rais VPN

Contenu

Introduction

Ce document décrit comment une option nulle du déploiement de toucher (ZTD) est une rentable et une solution évolutive pour des déploiements.

Le déploiement sécurisé et efficace et la fourniture des routeurs du bureau distant (parfois appelés Spokes) peuvent être une tâche difficile. Les bureaux distants pourraient être dans les emplacements où c'est un défi pour faire configurer à un ingénieur sur site le routeur sur le site, et la plupart des ingénieurs choisissent de ne pas envoyer les routeurs en étoile préconfigurés dus au coût et au risque de sécurité potentielle.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Tout routeur de Cisco IOS® qui a un port USB qui prend en charge des USB Flash Drive. Pour des détails, voir l'USB eToken et le support de caractéristiques de flash USB.

- Cette caractéristique est confirmée pour travailler à presque n'importe quelle plate-forme de Cisco 8xx. Pour des détails, voir le livre blanc de fichiers de configuration par défaut (support de caractéristiques sur gamme Cisco 800 ISR).
- D'autres Plateformes qui ont des ports USB comme la gamme G2 et 43xx/44xx du routeur de service intégré (ISR).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

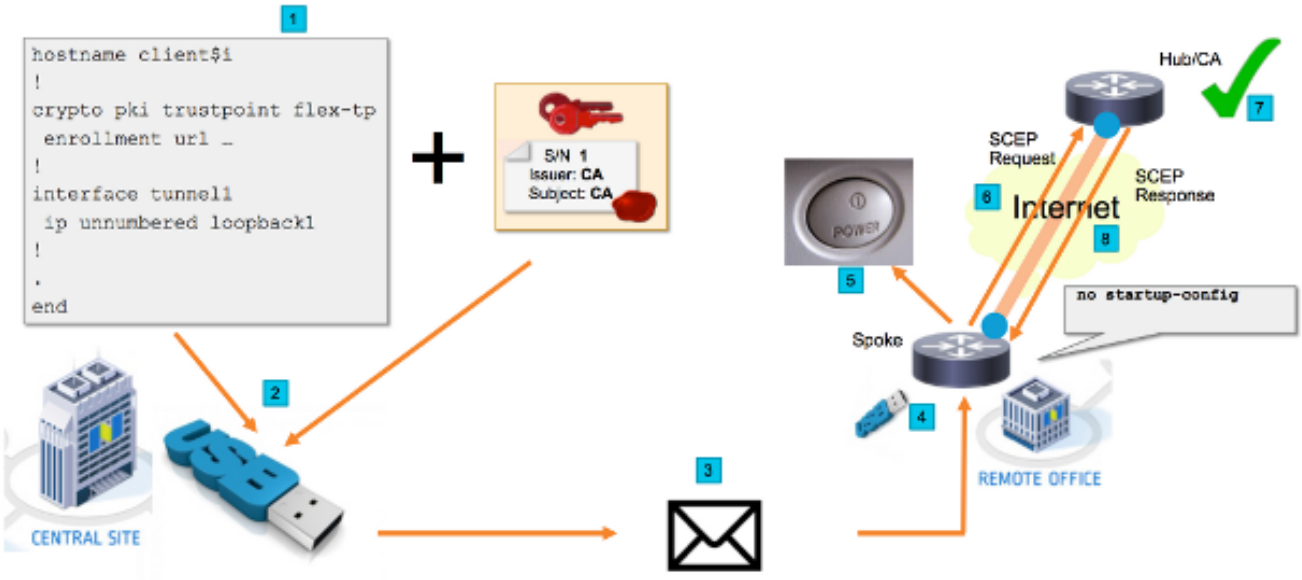
- Inscription de certificat simple Protocol (SCEP)
- Déploiement nul de toucher par l'intermédiaire d'USB
- DMVPN/FlexVPN/Site-to-site VPN

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurer

> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



Flux de réseau

1. Dans le lieu d'exploitation principal (le siège social de la société), un modèle de la configuration en étoile est créé. Le modèle contient le certificat d'Autorité de certification (CA) qui a signé le certificat du routeur concentrateur VPN.

2. Le modèle de configuration est instancié sur une clé USB dans un fichier appelé le **ciscortr.cfg. Ce** fichier de configuration contient la configuration spécifique de rai pour que le routeur soit déployé. **Note**: La configuration sur l'USB ne contient aucune informations confidentielles autre que des adresses IP et le certificat de CA. Il n'y a aucune clé privée du rai ou de serveur CA.
3. L'USB Flash Drive est envoyé au bureau distant par l'intermédiaire de la messagerie ou d'une société de livraison de module.
4. Le routeur en étoile est également envoyé au bureau distant directement de la fabrication de Cisco.
5. Dans le bureau distant, le routeur est connecté pour actionner et câblé au réseau comme expliqué dans les instructions qui sont incluses avec l'USB Flash Drive. Ensuite, l'USB Flash Drive est inséré dans le routeur. **Note**: Il y a peu à aucune compétences techniques impliquées dans cette étape, ainsi elle peut facilement être exécutée par n'importe quel personnel de bureau.
6. Une fois les amorçages d'un routeur, il lit la configuration d'**usbflash0:/ciscortr.cfg**. Dès que le routeur mettra sous tension, une demande simple de Protocol d'inscription de certificat (SCEP) est envoyée au serveur CA.
7. Sur l'octroi manuel ou automatique de serveur CA peut être configuré a basé sur la stratégie de sécurité d'entreprise. Une fois configurée pour le certificat manuel accordant, la vérification hors bande de la demande SCEP doit être exécutée (contrôle de validation d'adresse IP, validation de créance pour le personnel qui exécute le déploiement, etc.). Cette étape pourrait différer basé sur le serveur CA qui est utilisé.
8. Une fois que la réponse SCEP est reçue par le routeur en étoile, qui a maintenant un certificat valide, la session d'Échange de clés Internet (IKE) authentifie avec le hub VPN et le tunnel établit avec succès.

Autorisation basée sur SUDI

Étape 7 comporte la vérification manuelle de la requête envoyée de signature de certificat par l'intermédiaire du protocole SCEP, qui pourrait être encombrant et difficile à exécuter pour le personnel non technicien. Afin d'augmenter la Sécurité et automatiser le processus, les seuls Certificats sécurisés de périphérique de l'identification de périphérique (SUDI) peuvent être utilisés. Les Certificats SUDI sont des Certificats construits dans les périphériques ISR 4K. Ces Certificats sont signés par Cisco CA. Chaque périphérique manufacturé a été émis avec le certificat différent et le numéro de série du périphérique est contenu dans le nom commun du certificat. Le certificat SUDI, la paire de clés associée, et sa chaîne de certificat entière sont enregistrés dans la puce résistante d'ancre de confiance de bourreur. En outre, la paire de clés est cryptographiquement liée à une puce spécifique d'ancre de confiance et la clé privée n'est jamais exportée. Cette caractéristique fait le clonage ou la mystification les informations d'identité pratiquement impossibles.

La clé privée SUDI peut être utilisée pour signer la demande SCEP générée par le routeur. Le serveur CA peut vérifier la signature et indiquer le contenu du certificat SUDI du périphérique. Le serveur CA peut extraire les informations du certificat SUDI (comme un numéro de série) et exécuter l'autorisation basée sur ces informations. Le serveur de RADIUS peut être utilisé pour répondre à une telle demande d'autorisation.

L'administrateur crée une liste des Routeurs de rais et de leurs numéros de série associés. Les numéros de série peuvent être indiqués du cas du routeur par le personnel non technicien. Ces numéros de série sont enregistrés dans la base de données du serveur de RADIUS et le serveur autorise les demandes SCEP basées sur ces informations qui permettent le certificat à accorder

automatiquement. Notez que le numéro de série est cryptographiquement attaché à un appareil spécifique par l'intermédiaire du certificat SUDI signé par Cisco, ainsi il est impossible à être modifié.

En résumé, le serveur CA est configuré pour accorder automatiquement les demandes qui répondent à ces deux critères :

- Sont signés avec la clé privée associée avec un certificat signé par Cisco SUDI CA
- Sont autorisés par le serveur de Radius basé sur les informations de numéro de série prises du certificat SUDI

Scénarios de déploiement

Le serveur CA pourrait être exposé directement à l'Internet, de ce fait permettant aux clients pour exécuter l'inscription avant que le tunnel puisse être construit. Le serveur CA peut même être configuré sur le même routeur que le hub VPN. L'avantage de cette topologie est simplicité. L'inconvénient est Sécurité diminuée car le serveur CA est directement exposé pour différentes formes d'attaque par l'intermédiaire de l'Internet.

Alternativement, la topologie peut être développée en configurant le serveur d'autorité d'enregistrement. Le rôle de serveur d'autorité d'enregistrement est d'évaluer et expédier des demandes de signature de certificat valide au serveur CA. Le serveur de RA lui-même ne contient pas la clé privée du CA et ne peut pas générer des Certificats par lui-même. Dans un tel déploiement, le serveur CA n'a pas besoin d'être exposé à l'Internet, qui augmente la Sécurité globale. '

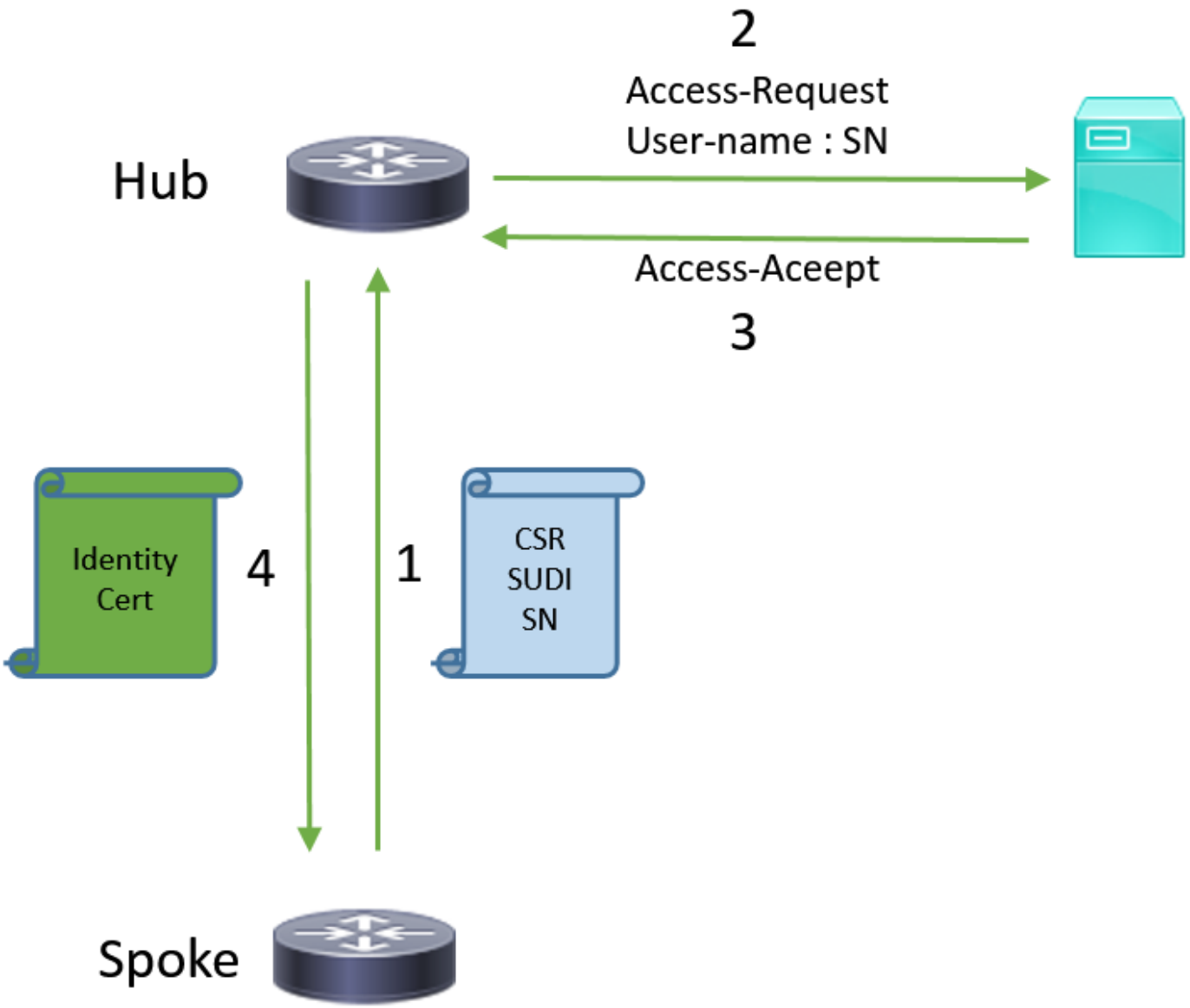
Flux de réseau

1. Le routeur en étoile crée la demande SCEP, la signe avec la clé privée de son certificat SUDI et l'envoie au serveur CA.

2. Si la demande est correctement signée, la demande RADIUS est générée. Le numéro de série est utilisé comme paramètre de nom d'utilisateur.

3. Le serveur de RADIUS reçoit ou rejette la demande.

4. Si la demande est reçue, le serveur CA accorde la demande. S'il est rejeté, le serveur CA répond avec « en attendant » l'état et le client relance la demande après qu'un temporisateur de retour expire.



Configuration avec le CA seulement

```
!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
```

Configuration avec le CA et le 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
```

```
!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
```

Configurations/modèle

Cette sortie témoin affiche à un FlexVPN exemplaire la configuration distante de bureau qui est mise sur le lecteur flash dans le fichier **usbflash0:/ciscortr.cfg**.

```
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"
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines **commandes d'affichage**. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Vous pouvez vérifier sur le rai si les tunnels montaient :

```
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
```

Vous pouvez également vérifier sur le rai si le certificat était inscrit correctement :

```
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
```

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Mises en garde et questions connues

ID de bogue Cisco CSCuu93989 - L'écoulement de PnP d'arrêts d'assistant de config sur les Plateformes G2 pourrait faire ne pas charger le système la configuration de l'usbflash : /ciscortr.cfg. Au lieu de cela le système pourrait arrêter à la caractéristique d'assistant de config :

```
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: Assurez-vous que vous utilisez une version qui contient une difficulté pour ce défaut.

ZTD par l'intermédiaire d'USB contre des fichiers de configuration par défaut

Notez que les **fichiers de configuration par défaut** comportent que ce document l'utilise est une caractéristique différente que le **déploiement nul de toucher par l'intermédiaire de l'USB** décrit dans l'aperçu du déploiement de la gamme Cisco 800 ISR.

-	**Déploiement nul de toucher par l'intermédiaire d'USB**	**Fichiers de configuration par d**
Plates-formes prises en charge	Limité seulement à peu de Routeurs 8xx. Pour des détails, voir l'aperçu du déploiement de la gamme Cisco 800 ISR	Tous les ISR G2, 43xx et 44xx
Nom du fichier	*.cfg	ciscortr.cfg
Enregistre la configuration sur l'éclair local	Oui, automatiquement	Non, le gestionnaire encastré d'événement (EEM) a exigé

Puisque plus de Plateformes sont prises en charge par la caractéristique de **fichiers de configuration par défaut**, cette technologie a été choisie pour la solution présentée en cet article.

Résumé

La configuration par défaut USB (avec nom du fichier **ciscortr.cfg d'un** USB Flash Drive) donne à des administrateurs réseau la capacité de déployer le routeur en étoile distant VPN de bureau (mais non limité juste au VPN) sans nécessité de se connecter dans le périphérique dans le site distant.

Informations connexes

- Inscription de certificat simple Protocol (SCEP)
- Déploiement nul de toucher par l'intermédiaire d'USB
- DMVPN/FlexVPN/Site-to-site VPN
- Support et documentation techniques - Cisco Systems
- Cisco ancrent la technologie