Configurar o desenvolvimento zero do toque (ZTD) de escritórios remotos VPN/spokes

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar
Diagrama de Rede
Fluxo de rede
Autorização SUDI-baseada
Cenários de distribuição
Fluxo de rede
Configuração com CA somente
Configuração com CA e o RA
Configurações/molde
Verificar
Troubleshooting
Advertências conhecidas e edições
ZTD através do USB contra arquivos de configuração padrão
Summary
Informações Relacionadas

Introdução

Este original descreve como uma opção zero do desenvolvimento do toque (ZTD) é uma rentável e uma solução escalável para disposições.

O desenvolvimento seguro e eficiente e a disposição dos roteadores da sede remotos (chamados às vezes Spokes) podem ser umas tarefas difíciis. Os escritórios remotos puderam ser nos lugar onde é um desafio para mandar um engenheiro de campo configurar o no local do roteador, e a maioria de coordenadores escolhem não enviar o spoke PRE-configurado roteadores devido ao custo e ao risco de segurança potencial.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Todo o roteador de Cisco IOS® que tiver um porta usb que apoie o flash USB conduz. Para detalhes, veja o USB eToken e o apoio instantâneo das características USB.

- Esta característica é confirmada para trabalhar em quase toda a plataforma de Cisco 8xx. Para detalhes, veja o White Paper dos arquivos de configuração padrão (apoio das características no Cisco 800 Series ISR).
- Outras Plataformas que têm porta usb como as séries G2 e 43xx/44xx do roteador do serviço integrado (ISR).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

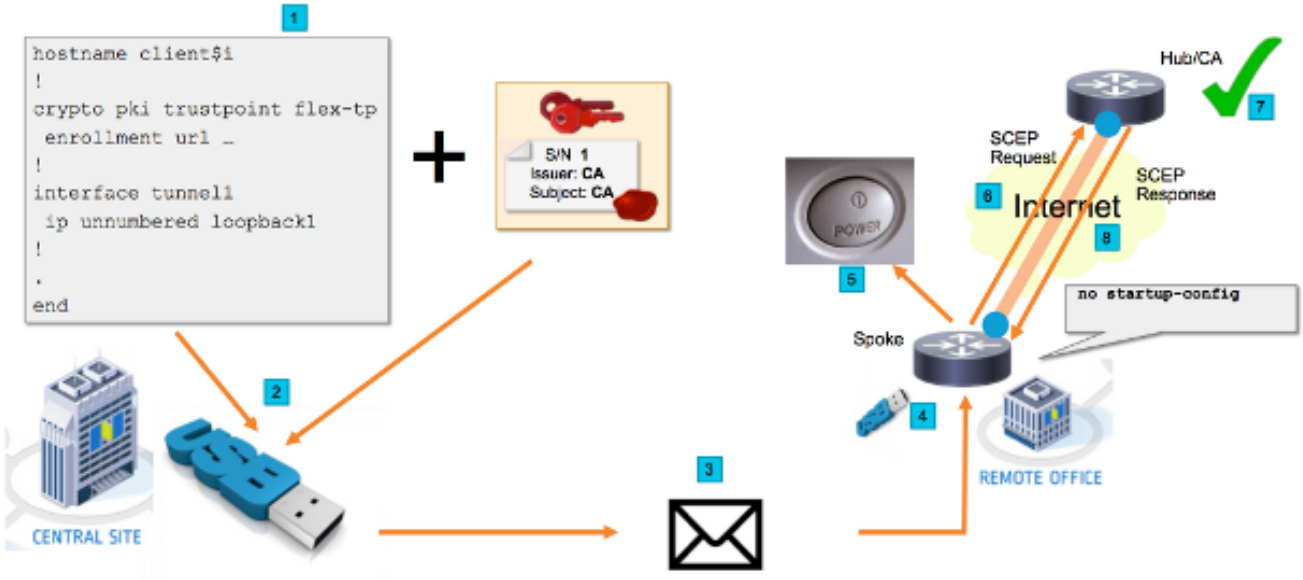
- Protocolo simple certificate enrollment (SCEP)
- Desenvolvimento zero do toque através do USB
- DMVPN/FlexVPN/Site-to-site VPN

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



Fluxo de rede

1. Na instalação central (a sede da empresa), um molde da configuração de raio é criado. O molde contém o certificado do Certificate Authority (CA) que assinou o certificado do roteador de hub VPN.
2. O gabarito de configuração instantiated em uma chave USB em um arquivo

chamado **ciscortr.cfg. Este** arquivo de configuração contém a configuração específica do spoke para que o roteador seja distribuído. **Note**: A configuração no USB não contém nenhuma informação sensível a não ser endereços IP de Um ou Mais Servidores Cisco ICM NT e o certificado de CA. Não há nenhuma chave privada do spoke ou do server de CA.

3. A movimentação do flash USB é enviada ao escritório remoto através do correio ou de uma empresa de entrega do pacote.
4. O roteador do spoke é enviado igualmente ao escritório remoto diretamente da fabricação de Cisco.
5. No escritório remoto, o roteador é conectado para pôr e cabografado à rede como explicado nas instruções que são incluídas com a movimentação do flash USB. Em seguida, a movimentação do flash USB é introduzida no roteador. **Note**: Há pouco a nenhumas habilidades técnicas envolvidas nesta etapa, assim que pode facilmente ser executada por todos os pessoais do escritório.
6. Uma vez as botas do roteador acima, lê a configuração de **usbflash0:/ciscortr.cfg**. Assim que o roteador puser acima, um pedido do protocolo simple certificate enrollment (SCEP) está enviado ao server de CA.
7. Ao conceder manual ou automática do server de CA pode ser configurado com base na política de segurança da empresa. Quando configurada para o certificado manual que concede, a verificação fora da banda do pedido SCEP deve ser executada (verificação da validação do endereço IP de Um ou Mais Servidores Cisco ICM NT, validação credencial para o pessoal que executa o desenvolvimento, etc.). Esta etapa pôde diferir baseado no server de CA que é usado.
8. Uma vez que a resposta SCEP é recebida pelo roteador do spoke, que tem agora um certificado válido, a sessão do Internet Key Exchange (IKE) autentica com o hub VPN e o túnel estabelece com sucesso.

Autorização SUDI-baseada

A etapa 7 envolve a verificação manual da solicitação de assinatura de certificado enviada através do protocolo scep, que pôde ser incômodo e difícil de executar para pessoais não técnicos. A fim aumentar a Segurança e automatizar o processo, os Certificados originais seguros do dispositivo da identificação de dispositivo (SUDI) podem ser usados. Os Certificados SUDI são Certificados construídos nos dispositivos ISR 4K. Estes Certificados são assinados por Cisco CA. Cada dispositivo manufaturado foi emitido com certificado diferente e o número de série do dispositivo é contido dentro do Common Name do certificado. O certificado SUDI, o par de chaves associado, e seu certificate chain inteiro são armazenados na microplaqueta resistente da âncora da confiança da calcadeira. Além disso, o par de chaves é limitado criptograficamente a uma microplaqueta específica da âncora da confiança e a chave privada é exportada nunca. Esta característica faz a clonagem ou a falsificação a informação de identidade virtualmente impossível.

A chave privada SUDI pode ser usada para assinar o pedido SCEP gerado pelo roteador. O server de CA pode verificar a assinatura e ler os índices do certificado SUDI do dispositivo. O server de CA pode extrair a informação do certificado SUDI (como um número de série) e executar a autorização baseada nessa informação. O servidor Radius pode ser usado para responder a tal pedido de autorização.

O administrador cria uma lista do Roteadores do spokes e de seus números de série associados. Os números de série podem ser lidos do exemplo do roteador pelos pessoais não técnicos. Estes números de série são armazenados na base de dados do servidor radius e o server autoriza os

pedidos SCEP baseados nessa informação que permite que o certificado seja concedido automaticamente. Note que o número de série está amarrado criptograficamente a um dispositivo específico através do certificado assinado Cisco SUDI, assim que é impossível ser forjado.

Em resumo, o server de CA é configurado para conceder automaticamente os pedidos que encontram ambos estes critérios:

- São assinados com a chave privada associada com um certificado assinado por Cisco SUDI CA
- São autorizados pelo servidor Radius baseado na informação do número de série tomada do certificado SUDI

Cenários de distribuição

O server de CA pôde ser exposto diretamente ao Internet, assim permitindo que os clientes executem o registro antes que o túnel possa ser construído. O server de CA pode mesmo ser configurado no mesmo roteador como o hub VPN. A vantagem desta topologia é simplicidade. A desvantagem é Segurança diminuída porque o server de CA é exposto diretamente para vários formulários do ataque através do Internet.

Alternativamente, a topologia pode ser expandida configurando o server da autoridade de registro. O papel do servidor da autoridade de registro é avaliar e enviar requisições de assinatura do certificado válido ao server de CA. O server próprio RA não contém a chave privada de CA e não pode gerar Certificados por si só. Em tal desenvolvimento, o server de CA não precisa de ser exposto ao Internet, que aumenta a segurança total. '

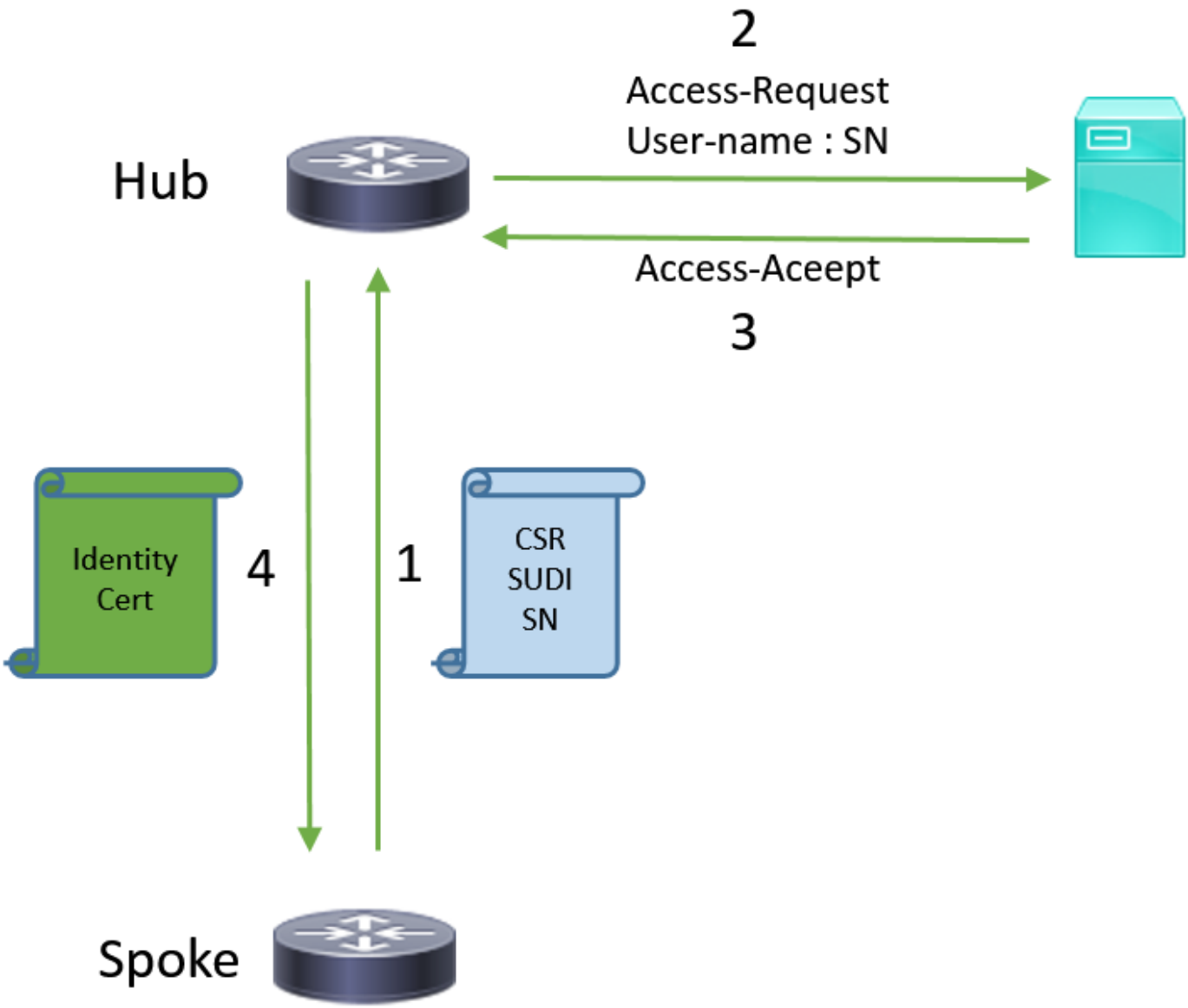
Fluxo de rede

1. O roteador do spoke cria o pedido SCEP, assina-o com a chave privada de seu certificado SUDI e envia-o ao server de CA.

2. Se o pedido é assinado corretamente, a requisição RADIUS está gerada. O número de série é usado como um parâmetro username.

3. O servidor Radius aceita ou rejeita o pedido.

4. Se o pedido é aceitado, o server de CA concede o pedido. Se é rejeitado, o server de CA responde com “durante” o estado e o cliente experimenta de novo o pedido depois que um temporizador da reserva expira.



Configuração com CA somente

```
!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
```

Configuração com CA e o 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
```

Configurações/molde

Este exemplo de saída mostra uma configuração exemplar do escritório remoto de FlexVPN que seja posta sobre a movimentação instantânea no arquivo **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"
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Você pode verificar no spoke se os túneis foram acima:

```
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
```

Você pode igualmente verificar no spoke se o certificado foi registrado corretamente:

```
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
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Advertências conhecidas e edições

Identificação de bug Cisco CSCuu93989 - O fluxo de PnP das paradas do assistente da configuração nas Plataformas G2 pôde fazer com que o sistema não carregue a configuração do usbflash: /ciscortr.cfg. Em lugar do sistema pôde parar na característica do assistente da configuração:

```
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: Assegure-se de que você use uma versão que contenha um reparo para este defeito.

ZTD através do USB contra arquivos de configuração padrão

Note que os **arquivos de configuração padrão** caracterizam que este original se usa é uma característica diferente do que o **desenvolvimento zero do toque através do USB** descrito na vista geral do desenvolvimento do Cisco 800 Series ISR.

-	**Zere o desenvolvimento do toque através do USB**	**Arquivos de configuração p**
Plataformas suportadas	Limitado somente a poucos 8xx Router. Para detalhes, veja a vista geral do desenvolvimento do Cisco 800 Series ISR	Todos os ISR G2, 43xx e 4
Nome de arquivo	*.cfg	ciscortr.cfg
Salvar a configuração no flash local	Sim, automaticamente	Não, o gerente encaixado d evento (EEM) exigiu

Porque mais Plataformas são apoiadas pela característica dos **arquivos de configuração padrão**, esta tecnologia foi escolhida para a solução apresentada neste artigo.

Resumo

A configuração padrão USB (com nome de arquivo **ciscortr.cfg de uma** movimentação do flash USB) dá a administradores de rede a capacidade para distribuir o roteador VPN do spoke do escritório remoto (mas não limitado apenas ao VPN) sem a necessidade de registrar no dispositivo na posição remota.

Informações Relacionadas

- Protocolo simple certificate enrollment (SCEP)
- Desenvolvimento zero do toque através do USB
- DMVPN/FlexVPN/Site-to-site VPN
- Suporte Técnico e Documentação - Cisco Systems
- Cisco ancora a tecnologia