

Desenvolvimento zero do toque (ZTD) do exemplo de configuração dos escritórios remotos/spokes VPN

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Fluxo de rede](#)

[Configurações/molde](#)

[Verificar](#)

[Troubleshooting](#)

[Advertências conhecidas e edições](#)

[ZTD através do USB contra arquivos de configuração padrão](#)

[Resumo](#)

[Informações Relacionadas](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

O desenvolvimento seguro e eficiente e a disposição dos roteadores da sede remotos (chamados às vezes Spokes) podem ser umas tarefas difíceis. 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. Este documento descreve como uma opção zero do desenvolvimento do toque (ZTD) é uma rentável e uma solução escalável para tais disposições.

Pré-requisitos

Requisitos

- Todo o roteador do [®] do 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:

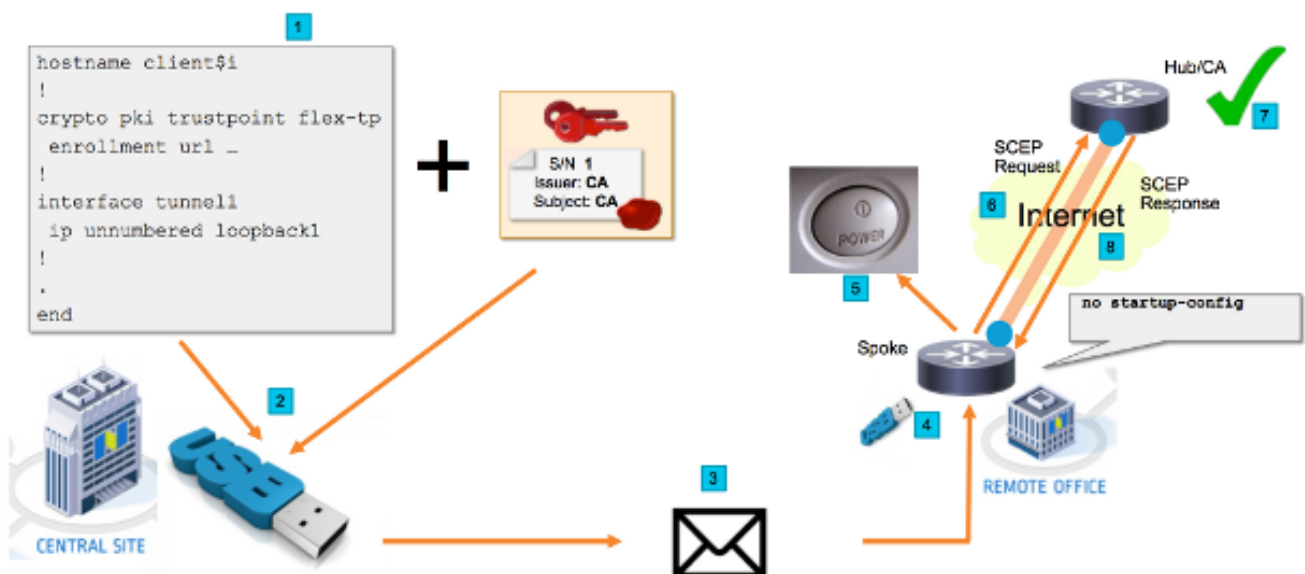
- [Protocolo simple certificate enrollment \(SCEP\)](#)
- [Desenvolvimento zero do toque através do USB](#)
- [DMVPN/FlexVPN/Site-to-site VPN](#)

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 é instantiado 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 pôt e cabografado à rede como explicado nas instruções que são incluídas com a movimentação do flash USB. A movimentação do flash USB é introduzida em seguida no roteador. **Note:** Há pouco a nenhuma habilidades técnicas envolvidas nesta etapa, assim que pode facilmente ser executada por todos os pessoais do escritório.
6. Uma vez que as botas do roteador acima dela leem a configuração de **usbflash0:/ciscotr.cfg**. Assim que o roteador puser acima de um protocolo simple certificate enrollment (SCEP) o pedido é 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 chapéu do server t de CA é usada.
8. Uma vez que a resposta SCEP é recebida pelo roteador do spoke, que tem agora um certificado válido, a sessão de IKE autentica com o hub VPN e o túnel estabelece com sucesso.

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:/ciscotr.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
 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 Tunnell
 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 \(clientes registrados somente\)](#) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

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: /ciscotr.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
```

Assegure-lhe o uso 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 documento se usa é uma característica diferente do que o **toque zero Deployment através do USB** desribed na [vista geral do desenvolvimento do Cisco 800 Series ISR](#).

-	Zere o toque Deployment através do USB	Arquivos de configuração padrão
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 44xx
Nome de arquivo	*.cfg	ciscortr.cfg
Salvar a configuração no flash local	Sim, automaticamente	Não, o gerente do evento de Embeded (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](#)