Configurar ZTD (Zero Touch Deployment, implantação zero-touch) de VPN Remote Offices/Spokes

Contents

Introduction

Este documento descreve como a opção ZTD (Zero Touch Deployment, implantação zero-touch) é uma solução econômica e escalável para implantações.

A implantação segura e eficiente e o fornecimento de roteadores de escritórios remotos (às vezes chamados de Spokes) podem ser uma tarefa difícil. Os escritórios remotos podem estar em locais onde é um desafio ter um engenheiro de campo configurando o roteador no local, e a maioria dos engenheiros opta por não enviar roteadores spoke pré-configurados devido ao custo e ao risco potencial à segurança.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Qualquer roteador Cisco IOS® que tenha uma porta USB que suporte unidades flash USB. Para obter detalhes, consulte Suporte a recursos USB eToken e USB Flash.
- Confirmou-se que esse recurso funciona em quase qualquer plataforma Cisco 8xx. Para obter detalhes, consulte o White Paper Default Configuration Files (Recursos de suporte no Cisco 800 Series ISR).
- Outras plataformas que têm portas USB, como Integrated Service Router (ISR) Series G2 e 43xx/44xx.

Componentes Utilizados

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

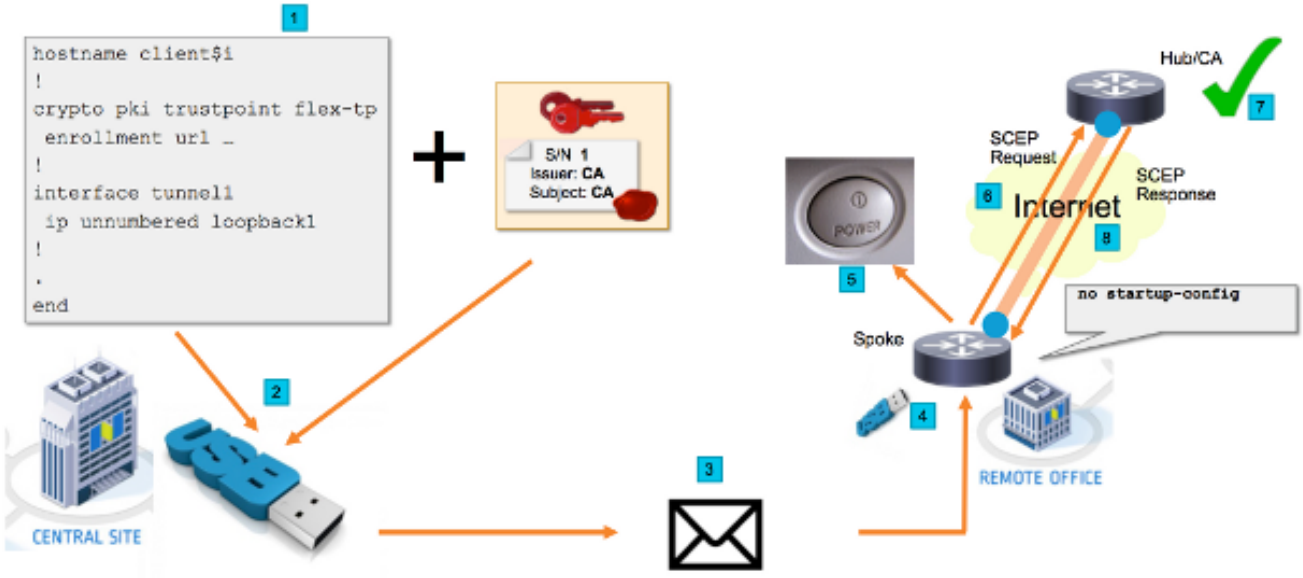
- Simple Certificate Enrollment Protocol (SCEP)
- Implantação automatizada via USB
- DMVPN/FlexVPN/VPNs site a site

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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. No site central (sede da empresa), um modelo da configuração do Spoke é criado. O modelo contém o certificado da autoridade de certificação (CA) que assinou o

certificado do roteador do VPN Hub.

2. O modelo de configuração é instanciado em uma chave USB em um arquivo chamado **ciscortr.cfg**. Esse arquivo de configuração contém a configuração específica de Spoke para o roteador a ser implantado. **Note**: A configuração no USB não contém nenhuma informação confidencial além dos endereços IP e do certificado CA. Não há chave privada do Spoke ou do CA Server.
3. A unidade flash USB é enviada para o escritório remoto por correio ou por uma empresa de entrega de pacotes.
4. O roteador Spoke também é enviado para o escritório remoto diretamente do Cisco Manufacturing.
5. No escritório remoto, o roteador está conectado à alimentação e cabeado à rede, conforme explicado nas instruções que estão incluídas com a unidade flash USB. Em seguida, a unidade flash USB é inserida no roteador. **Note**: Há pouca ou nenhuma habilidade técnica envolvida nesta etapa, portanto, ela pode ser facilmente executada por qualquer pessoal de escritório.
6. Quando o roteador é inicializado, ele lê a configuração de **usbflash0:/ciscortr.cfg**. Assim que o roteador é ligado, uma solicitação do Simple Certificate Enrollment Protocol (SCEP) é enviada ao Servidor CA.
7. No CA Server, pode ser configurado Manual ou Automatic Grant com base na política de segurança da empresa. Quando configurado para a concessão manual de certificado, a verificação fora da banda da solicitação SCEP deve ser executada (verificação de validação de endereço IP, validação de credencial para o pessoal que executa a implantação, etc.). Esta etapa pode ser diferente com base no servidor CA usado.
8. Quando a Resposta SCEP é recebida pelo roteador Spoke, que agora tem um certificado válido, a sessão Internet Key Exchange (IKE) é autenticada com o VPN Hub e o túnel é estabelecido com êxito.

Autorização com base em SUDI

A etapa 7 envolve a verificação manual da solicitação de assinatura de certificado enviada por meio do protocolo SCEP, o que pode ser complicado e difícil de executar para pessoal não técnico. Para aumentar a segurança e automatizar o processo, os certificados do dispositivo Secure Unique Device Identification (SUDI) podem ser usados. Os certificados SUDI são certificados incorporados nos dispositivos ISR 4K. Esses certificados são assinados pela CA da Cisco. Cada dispositivo fabricado recebeu um certificado diferente e o número de série do dispositivo está contido no nome comum do certificado. O certificado SUDI, o par de chaves associado e toda a cadeia de certificados são armazenados no chip Trust Anchor resistente a adulteração. Além disso, o par de chaves está vinculado criptograficamente a um chip Trust Anchor específico e a chave privada nunca é exportada. Esse recurso torna a clonagem ou falsificação das informações de identidade praticamente impossível.

A chave privada SUDI pode ser usada para assinar a solicitação SCEP gerada pelo roteador. O servidor de CA pode verificar a assinatura e ler o conteúdo do certificado SUDI do dispositivo. O servidor de CA pode extrair as informações do certificado SUDI (como um número de série) e executar a autorização com base nessas informações. O servidor RADIUS pode ser usado para responder a tal solicitação de autorização.

O administrador cria uma lista dos roteadores spokes e seus números de série associados. Os números de série podem ser lidos do caso do roteador pelo pessoal não técnico. Esses números

de série são armazenados no banco de dados do servidor RADIUS e o servidor autoriza as solicitações SCEP com base nessas informações que permitem que o certificado seja concedido automaticamente. Observe que o número de série está vinculado criptograficamente a um dispositivo específico por meio do certificado SUDI assinado pela Cisco, portanto, é impossível forjar.

Em resumo, o servidor de CA é configurado para conceder solicitações automaticamente que atendam a ambos os critérios:

- São assinados com uma chave privada associada a um certificado assinado pela AC SUDI da Cisco
- São autorizados pelo servidor Radius com base nas informações do número de série obtidas do certificado SUDI

Cenários de implantação

O servidor CA pode ser exposto diretamente à Internet, permitindo assim que os clientes executem a inscrição antes que o túnel possa ser criado. O servidor CA pode ser configurado no mesmo roteador que o hub VPN. A vantagem dessa topologia é a simplicidade. A desvantagem é a redução da segurança, pois o servidor CA é exposto diretamente para várias formas de ataque via Internet.

Como alternativa, a topologia pode ser expandida configurando o servidor de Autoridade de Registro. A função de servidor Autoridade de Registro é avaliar e encaminhar solicitações de assinatura de certificado válidas para o servidor de CA. O servidor RA em si não contém a chave privada da CA e não pode gerar certificados por si só. Nessa implantação, o servidor CA não precisa ser exposto à Internet, o que aumenta a segurança geral."

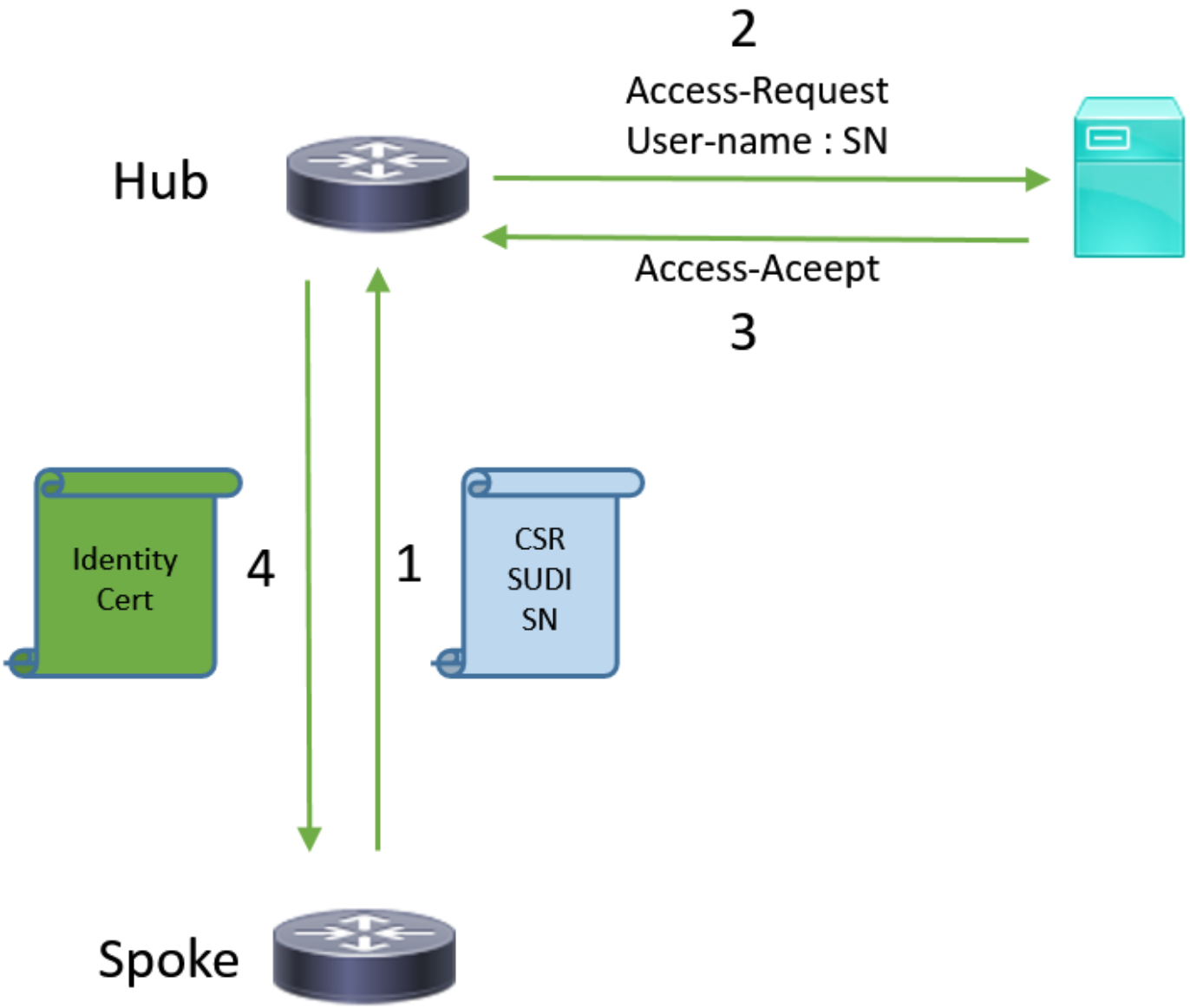
Fluxo de rede

1. O roteador Spoke cria a solicitação SCEP, o assina com a chave privada de seu certificado SUDI e o envia ao servidor CA.

2. Se a solicitação estiver assinada corretamente, a solicitação RADIUS será gerada. O número de série é usado como parâmetro de nome de usuário.

3. O servidor RADIUS aceita ou rejeita a solicitação.

4. Se a solicitação for aceita, o servidor CA concede a solicitação. Se for rejeitado, o servidor da AC responde com o status "Pendente" e o cliente repete a solicitação após a expiração de um temporizador de fallback.



Configuração somente com 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
```

Configuração com CA e 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

Configurações/modelo

Este exemplo de saída mostra uma configuração de Escritório Remoto FlexVPN exemplar que é colocada na unidade flash 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 subiram:

```
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 também pode 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
```

Troubleshoot

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

Advertências e problemas conhecidos

ID de bug da Cisco CSCuu93989 - O Assistente de configuração interrompe o fluxo de PnP em plataformas G2 pode fazer com que o sistema não carregue a configuração do usbflash:/ciscortr.cfg. Em vez disso, o sistema pode parar no recurso Assistente de configuração:

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

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

Note: Certifique-se de usar uma versão que contenha uma correção para esse defeito.

ZTD via USB versus arquivos de configuração padrão

Observe que o recurso **Default Configuration Files** usado neste documento é um recurso diferente do **Zero Touch Deployment via USB** descrito em Overview of Cisco 800 Series ISR Deployment.

-	**Implantação automatizada via USB**	**Arquivos de configuração pa**
Plataformas suportadas	Limitado a apenas alguns roteadores 8xx. Para obter detalhes, consulte Visão geral da implantação do Cisco 800 Series ISR	Todos os ISRs G2, 43xx e 4
Nome de arquivo	*.cfg	ciscortr.cfg
Salva a configuração na flash local	Sim, automaticamente	Não, é necessário o Embedd Event Manager (EEM)

Como mais plataformas são suportadas pelo recurso **Default Configuration Files**, esta tecnologia foi escolhida para a solução apresentada neste artigo.

Summary

A configuração padrão USB (com o nome de arquivo **ciscortr.cfg** de uma unidade flash USB) dá aos administradores de rede a capacidade de implantar VPNs de roteador Remote Office Spoke (mas não limitado a apenas VPN) sem a necessidade de fazer login no dispositivo no local remoto.

Informações Relacionadas

- Simple Certificate Enrollment Protocol (SCEP)
- Implantação automatizada via USB
- DMVPN/FlexVPN/VPNs site a site
- Suporte Técnico e Documentação - Cisco Systems

- Tecnologia Anchor da Cisco