Configuración de la implementación sin intervención (ZTD) de oficinas remotas/radios VPN

Contenido

Introducción

Este documento describe cómo una opción de implementación sin intervención (ZTD) es una solución rentable y escalable para implementaciones.

La implementación segura y eficiente y el suministro de routers de oficina remota (a veces llamados Spokes) pueden ser una tarea difícil. Las oficinas remotas pueden encontrarse en ubicaciones en las que es difícil que un ingeniero de campo configure el router in situ, y la mayoría de los ingenieros eligen no enviar routers radiales preconfigurados debido al coste y al riesgo potencial de seguridad.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cualquier router Cisco IOS® que tenga un puerto USB compatible con unidades flash USB. Para obtener más información, vea Soporte de Funciones USB eToken y USB Flash.
- Se ha confirmado que esta función funciona en casi cualquier plataforma 8xx de Cisco. Para obtener más información, vea el informe técnico Archivos de configuración predeterminados (Soporte de funciones en Cisco 800 Series ISR).
- Otras plataformas que disponen de puertos USB, como los routers de servicios integrados (ISR) series G2 y 43xx/44xx.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

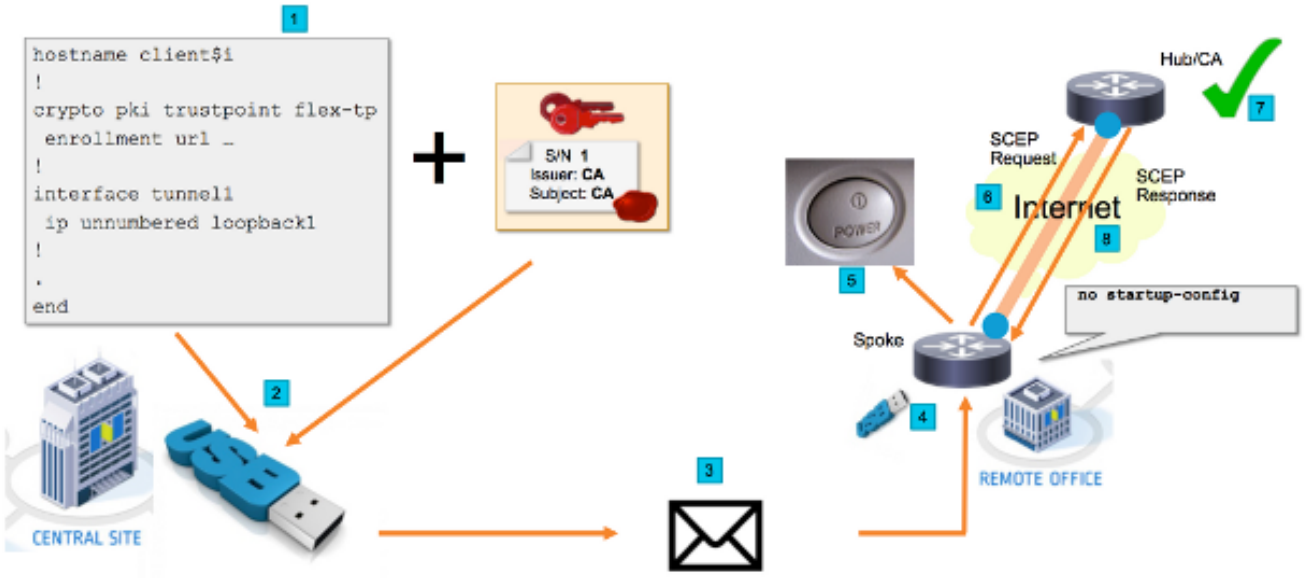
- Protocolo simple de inscripción de certificados (SCEP)
- Implementación sin intervención mediante USB
- VPN DMVPN/FlexVPN/VPN de sitio a sitio

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

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Flujo de red

1. En el sitio central (sede de la empresa), se crea una plantilla de la configuración Spoke. La plantilla contiene el certificado de autoridad certificadora (CA) que firmó el

certificado del router hub VPN.

2. La plantilla de configuración se crea una instancia en una llave USB en un archivo llamado **ciscortr.cfg**. Este archivo de configuración contiene la configuración específica de Spoke para el router que se va a implementar. **Nota:** La configuración en el USB no contiene información confidencial que no sea direcciones IP y el certificado CA. No hay clave privada del servidor Spoke o CA.
3. La unidad flash USB se envía a la oficina remota por correo o a una empresa de entrega de paquetes.
4. El router Spoke también se envía a la oficina remota directamente desde Cisco Manufacturing.
5. En la oficina remota, el router está conectado a la alimentación y conectado a la red como se explica en las instrucciones que se incluyen con la unidad flash USB. A continuación, se inserta la unidad flash USB en el router. **Nota:** En esta etapa hay poca o ninguna capacidad técnica, por lo que cualquier personal de oficina puede llevarla a cabo fácilmente.
6. Una vez que el router se inicia, lee la configuración de **usbflash0:/ciscortr.cfg**. Tan pronto como el router se ha encendido, se envía una solicitud de protocolo simple de inscripción de certificados (SCEP) al servidor de la CA.
7. En el servidor de la CA, la concesión manual o automática se puede configurar según la política de seguridad de la empresa. Cuando se configura para la concesión manual de certificados, se debe realizar una verificación fuera de banda de la solicitud SCEP (verificación de validación de dirección IP, validación de credenciales para el personal que realiza la implementación, etc.). Este paso puede ser diferente en función del servidor de la CA que se utiliza.
8. Una vez que el router Spoke recibe la respuesta SCEP, que ahora tiene un certificado válido, la sesión de Intercambio de claves de Internet (IKE) se autentica con el hub VPN y el túnel se establece correctamente.

Autorización basada en SUDI

El paso 7 implica la verificación manual de la solicitud de firma de certificado enviada a través del protocolo SCEP, que puede ser engorrosa y difícil de realizar para el personal no técnico. Para aumentar la seguridad y automatizar el proceso, se pueden utilizar los certificados de dispositivo de identificación única de dispositivos (SUDI) segura. Los certificados SUDI son certificados integrados en los dispositivos ISR 4K. Estos certificados están firmados por Cisco CA. Cada dispositivo fabricado se ha expedido con un certificado diferente y el número de serie del dispositivo está incluido en el nombre común del certificado. El certificado SUDI, el par de claves asociado y toda su cadena de certificados se almacenan en el chip Trust Anchor resistente a la manipulación. Además, el par de claves se enlaza criptográficamente a un chip Trust Anchor específico y la clave privada nunca se exporta. Esta función hace que la clonación o suplantación de la información de identidad sea prácticamente imposible.

La clave privada SUDI se puede utilizar para firmar la solicitud SCEP generada por el router. El servidor de la CA puede verificar la firma y leer el contenido del certificado SUDI del dispositivo. El servidor de la CA puede extraer la información del certificado SUDI (como un número de serie) y realizar una autorización basada en esa información. El servidor RADIUS se puede utilizar para responder a tal solicitud de autorización.

El administrador crea una lista de los routers radiales y sus números de serie asociados. El personal no técnico puede leer los números de serie del caso del router. Estos números de serie

se almacenan en la base de datos del servidor RADIUS y el servidor autoriza las solicitudes SCEP basándose en esa información que permite que el certificado se conceda automáticamente. Tenga en cuenta que el número de serie está vinculado criptográficamente a un dispositivo específico a través del certificado SUDI firmado por Cisco, por lo que es imposible falsificarlo.

En resumen, el servidor de la CA se configura para conceder automáticamente solicitudes que cumplan ambos criterios:

- Están firmados con una clave privada asociada a un certificado firmado por Cisco SUDI CA
- Están autorizados por el servidor Radius según la información del número de serie tomada del certificado SUDI

Escenarios de implementación

El servidor de la CA podría estar expuesto directamente a Internet, lo que permitiría a los clientes realizar la inscripción antes de que se pueda construir el túnel. El servidor de la CA puede incluso configurarse en el mismo router que el hub VPN. La ventaja de esta topología es la simplicidad. La desventaja es una menor seguridad, ya que el servidor de la CA está expuesto directamente a diversas formas de ataque a través de Internet.

Alternativamente, la topología se puede expandir configurando el servidor de la Autoridad de registro. La función de servidor de la Autoridad de registro es evaluar y reenviar solicitudes de firma de certificado válidas al servidor de la CA. El propio servidor RA no contiene la clave privada de la CA y no puede generar certificados por sí mismo. En dicha implementación, el servidor de la CA no necesita estar expuesto a Internet, lo que aumenta la seguridad general.'

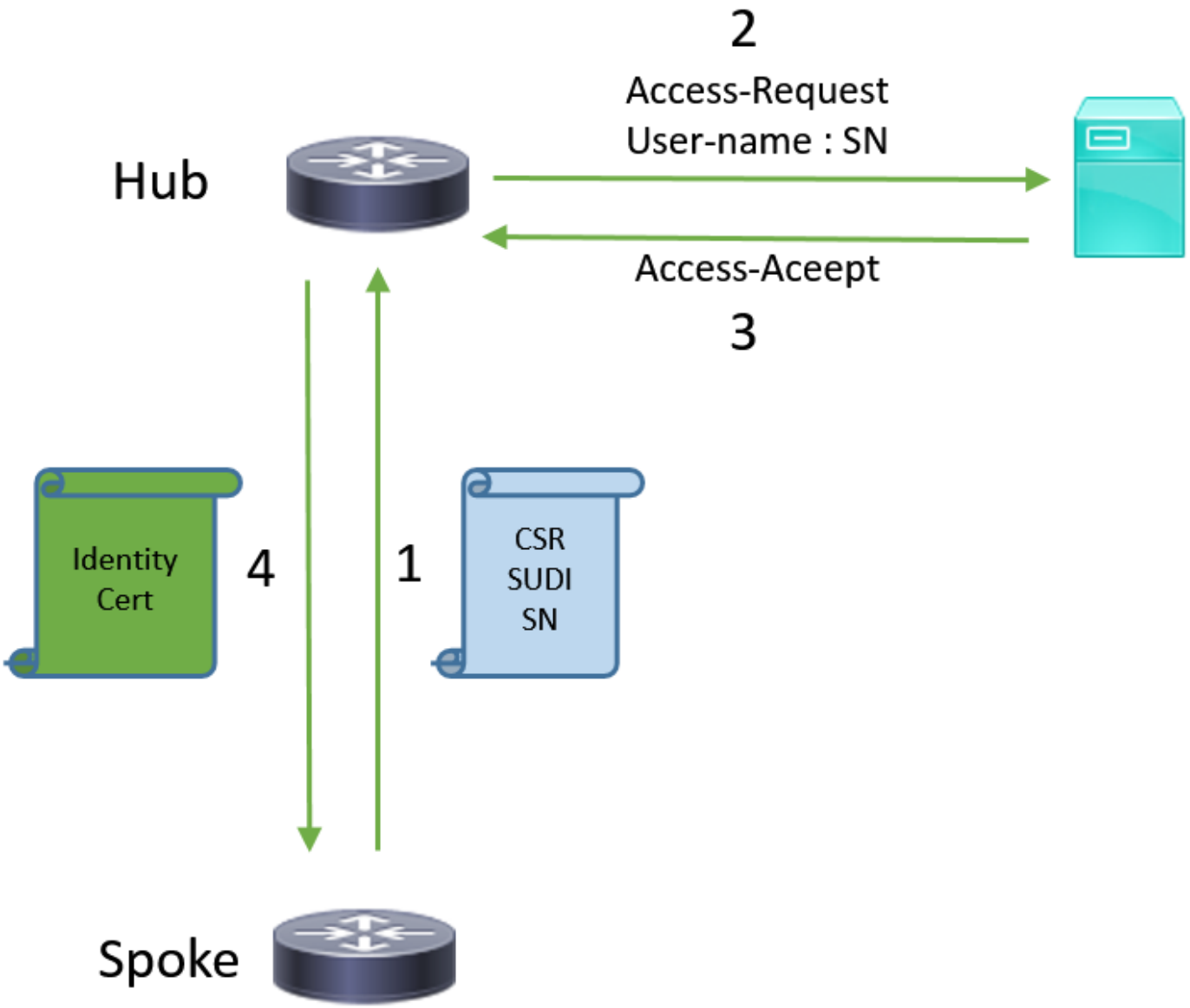
Flujo de red

1. El router Spoke crea una solicitud SCEP, la firma con la clave privada de su certificado SUDI y la envía al servidor CA.

2. Si la solicitud está firmada correctamente, se genera la solicitud RADIUS. El número de serie se utiliza como parámetro de nombre de usuario.

3. El servidor RADIUS acepta o rechaza la solicitud.

4. Si se acepta la solicitud, el servidor de la CA concede la solicitud. Si se rechaza, el servidor de la CA responde con el estado "Pendiente" y el cliente reintenta la solicitud después de que caduque un temporizador de reserva.



Configuración sólo con 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
```

Configuración con CA y 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

Configuraciones/Plantilla

Este ejemplo de resultado muestra una configuración de FlexVPN Remote Office ejemplar que se coloca en la unidad flash en el archivo **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"
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Puede verificar en Spoke si los túneles subieron:

```
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
```

También puede verificar en Spoke si el certificado se ha inscrito correctamente:

```
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

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Advertencias y problemas conocidos

Id. de bug Cisco CSCuu93989 - El asistente de configuración detiene el flujo de PnP en las plataformas G2 puede hacer que el sistema no cargue la configuración desde el usbflash:/ciscortr.cfg. En su lugar, el sistema podría detenerse en la función del asistente de configuración:

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

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

Nota: Asegúrese de utilizar una versión que contenga una corrección para este defecto.

ZTD mediante USB frente a archivos de configuración predeterminados

Tenga en cuenta que la función **Archivos de configuración predeterminados** que utiliza este documento es una función diferente a la **Implementación sin intervención mediante USB** que se describe en Descripción general de la implementación de ISR de Cisco serie 800.

-	**Implementación sin intervención mediante USB**	**Archivos de configura predeterminados**
Plataformas Soportadas	Limitado a sólo unos pocos routers 8xx. Para obtener más información, vea Descripción general de la implementación de ISR de Cisco serie 800	Todos los ISR G2, 4 44xx.
Nombre de Archivo	*.cfg	ciscortr.cfg
Guarda la configuración en la memoria flash local	Sí, automáticamente	No, se requiere Embedded Event Manager (EEM)

Debido a que la función **Archivos de configuración predeterminados** soporta más plataformas, esta tecnología se eligió para la solución presentada en este artículo.

Summary

La configuración predeterminada USB (con el nombre de archivo **ciscortr.cfg** de una unidad flash USB) ofrece a los administradores de red la posibilidad de implementar VPNs de router de radio de oficina remota (pero sin limitarse a VPN) sin la necesidad de iniciar sesión en el dispositivo en la ubicación remota.

Información Relacionada

- Protocolo simple de inscripción de certificados (SCEP)
- Implementación sin intervención mediante USB
- VPN DMVPN/FlexVPN/VPN de sitio a sitio
- Soporte Técnico y Documentación - Cisco Systems
- Tecnología de anclaje de Cisco