Despliegue cero del tacto (ZTD) del ejemplo de configuración de las oficinas remotas/del spokes VPN

Contenido

Introducción

El despliegue seguro y eficiente y la disposición de los routeres de oficina remota (a veces llamados Spokes) pueden ser una tarea difícil. Las oficinas remotas pudieron ser en las ubicaciones donde está un desafío para tener un ingeniero de campo configurar al router onsite, y la mayoría de los ingenieros eligen no enviar a los routeres radiales preconfigurados debido al coste y al riesgo de seguridad potencial. Este documento describe cómo una opción cero del despliegue del tacto (ZTD) es una rentable y una solución escalable para tales implementaciones.

Prerrequisitos

Requisitos

- Cualquier router del ® del Cisco IOS que tenga un puerto USB que soporte memorias USB USB. Para los detalles, vea el [USB eToken y el soporte de destello de las características USB](#).
- Esta característica se confirma para trabajar en casi cualquier plataforma de Cisco 8xx. Para los detalles vea el [White Paper de los archivos de configuración predeterminada (soporte de las características en las Cisco 800 Series ISR)](#).
- Otras Plataformas que tienen puertos USB como las series G2 y 43xx/44xx del router del servicio integrado (ISR).

Componentes Utilizados

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

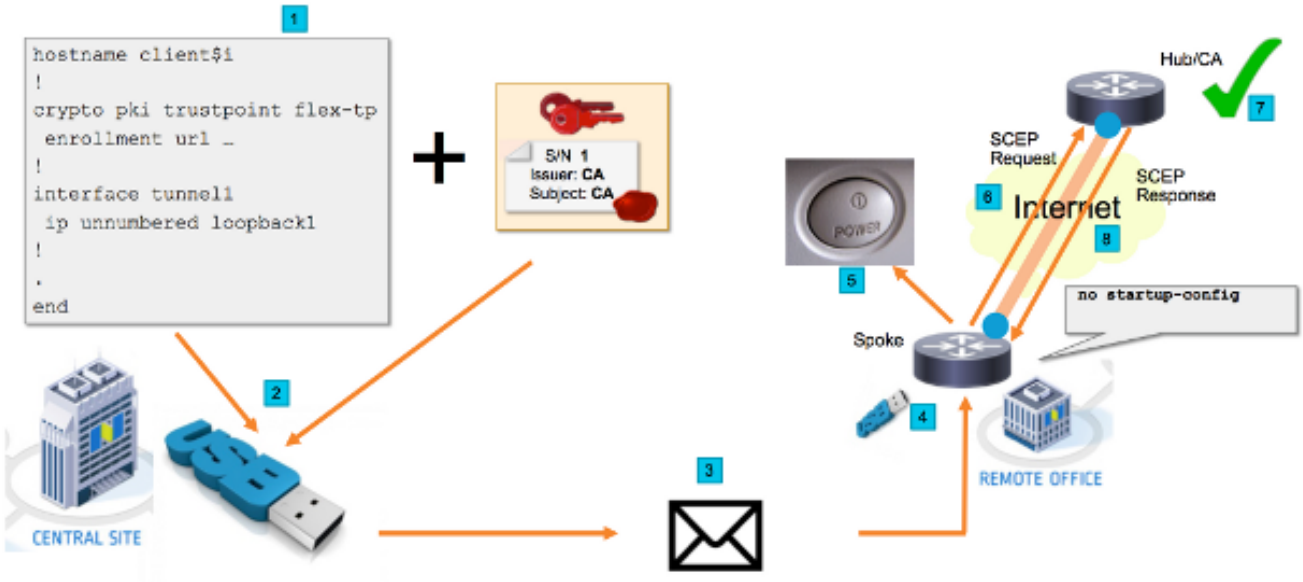
- Protocolo simple certificate enrollment (SCEP)
- Despliegue cero del tacto vía el USB
- DMVPN/FlexVPN/Site-to-site VPN

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

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 (la sede de la compañía) una plantilla de la configuración radial se crea. La plantilla contiene el certificado del Certificate Authority (CA) que firmó el certificado del router de eje de conexión VPN.
2. La plantilla de configuración se ejemplifica en llave USB en un archivo llamado **ciscortr.cfg. Este** archivo de configuración contiene la configuración específica del spoke para que el router sea desplegado. Nota: La configuración en el USB no contiene ninguna información vulnerable con excepción de los IP Addresses y del certificado de CA. No hay clave privada del spoke o del servidor de CA.
3. Memoria USB se envía a la oficina remota vía el correo o una empresa de distribución del

paquete.

4. Envían el router radial también a la oficina remota directamente de la fabricación de Cisco.
5. En la oficina remota el router está conectado para accionar y telegrafiado a la red como se explica en las instrucciones que se incluyen con memoria USB. Memoria USB se inserta después en el router. Nota: Hay poco a ningunas habilidades técnicas implicadas en este paso, así que puede ser realizado fácilmente por cualquier personal de la oficina.
6. Una vez que los inicios del router encima de él leen la configuración de **usbflash0:/ciscortr.cfg.** Tan pronto como el router haya accionado encima de un protocolo simple certificate enrollment (SCEP) la petición se envía al servidor de CA.
7. Al conceder manual o automática del servidor de CA puede ser configurado sobre la base de la política de seguridad de la compañía. Cuando está configurada para el certificado manual que concede, la verificación fuera de banda de la petición SCEP debe ser realizada (comprobación de validación de la dirección IP, validación credencial para el personal que realiza el despliegue, etc.). Se utiliza este paso pudo diferenciar basado en el sombrero del servidor t de CA.
8. Una vez que la respuesta SCEP es recibida por el router radial, que ahora tiene un certificado válido, la sesión IKE autentica con el concentrador VPN y el túnel establece con éxito.

Configuraciones/plantilla

Esta salida de muestra muestra una configuración ejemplar de la oficina remota de FlexVPN que se ponga en memoria USB 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
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

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Usted puede verificar en el spoke si subieron los túneles:

```
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
```

Usted puede también verificar en el spoke si el certificado fue alistado 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
```

Troubleshooting

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

Advertencias conocidas y problemas

Id. de bug Cisco CSCuu93989 - El flujo de PnP de las paradas del Asisitente de los Config en las Plataformas G2 pudo hacer el sistema no cargar la configuración del usbflash: /ciscortr.cfg. En lugar el sistema pudo parar en la característica del Asisitente de los 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
```

Asegúrele el uso una versión que contenga un arreglo para este defecto.

ZTD vía el USB contra los archivos de configuración predeterminada

Observe que los **archivos de configuración predeterminada** ofrecen que este documento utiliza es una diversa característica que el **tacto cero Deployement vía el USB** desribed en la descripción del despliegue de las Cisco 800 Series ISR.

-	**Ponga a cero el tacto Deployement vía el USB**	**Archivos de configuración predeterminada**
Plataformas Soportadas	Limitado solamente a pocos 8xx Router. Para los detalles, vea la descripción del despliegue de las Cisco 800 Series ISR	Todos los ISR G2, 43xx y 44xx
Nombre de archivo	*.cfg	ciscortr.cfg
Guarda la configuración en el flash local	Sí, automáticamente	No, el administrador del event Embeded (EEM) requirió

Porque más Plataformas son soportadas por la característica de los **archivos de configuración predeterminada**, esta tecnología fue elegida para la solución presentada en este artículo.

Resumen

La configuración predeterminada USB (con el nombre del archivo **ciscortr.cfg de** memoria USB) da a administradores de la red la capacidad de desplegar al router radial VPN de la oficina remota (pero no limitado apenas al VPN) sin la necesidad de registrar en el dispositivo en el lugar remoto.

Información Relacionada

- Protocolo simple certificate enrollment (SCEP)
- Despliegue cero del tacto vía el USB
- DMVPN/FlexVPN/Site-to-site VPN
- Soporte Técnico y Documentación - Cisco Systems