Contenu

Introduction

Le déploiement sécurisé et efficace et la fourniture des routeurs du bureau distant (parfois appelés Spokes) peuvent être une tâche difficile. Les bureaux distants pourraient être dans les emplacements où c'est un défi pour faire configurer à un ingénieur sur site le routeur sur le site, et la plupart des ingénieurs choisissent de ne pas envoyer les routeurs en étoile préconfigurés dus au coût et au risque de sécurité potentielle. Ce document décrit comment une option nulle du déploiement de toucher (ZTD) est une rentable et une solution évolutive pour de tels déploiements.

Conditions préalables

Conditions requises

- Tout routeur d'Â® de Cisco IOS qui a un port USB qui prend en charge des USB Flash Drive. Pour des détails, voir l'USB eToken et le support de caractéristiques de flash USB.
- Cette caractéristique est confirmée pour travailler à presque n'importe quelle plate-forme de Cisco 8xx. Pour des détails voir le livre blanc de fichiers de configuration par défaut (support de caractéristiques sur gamme Cisco 800 ISR).
- D'autres Plateformes qui ont des ports USB comme la gamme G2 et 43xx/44xx du routeur de service intégré (ISR).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

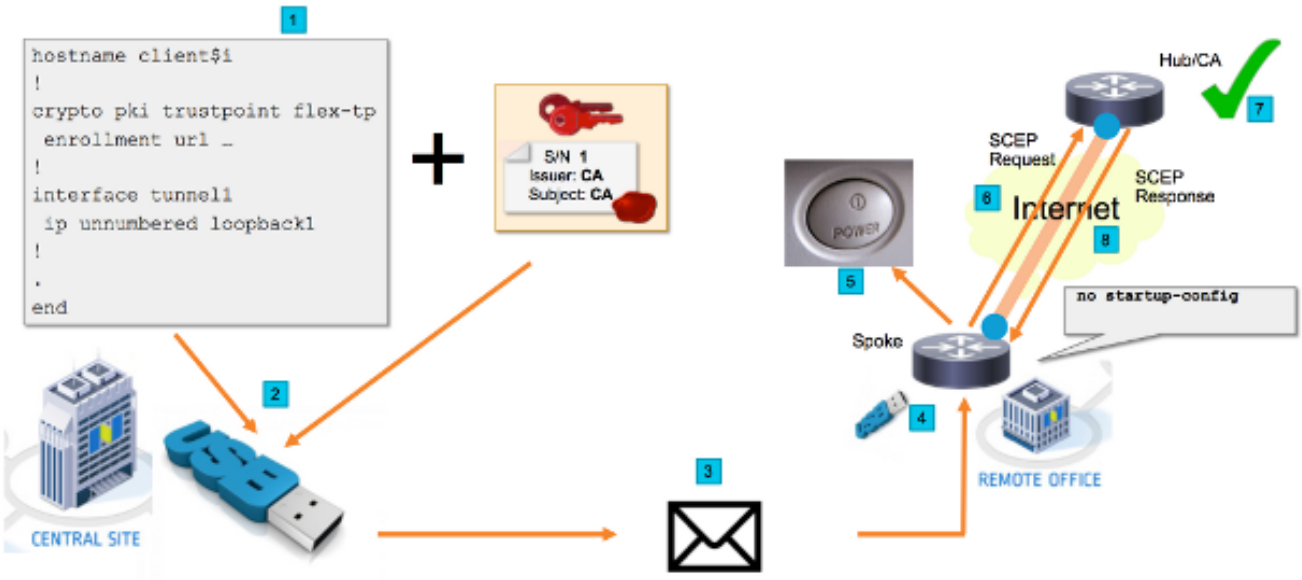
- Inscription de certificat simple Protocol (SCEP)
- Déploiement nul de toucher par l'intermédiaire d'USB
- DMVPN/FlexVPN/Site-to-site VPN

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



Flux de réseau

1. Dans le lieu d'exploitation principal (le siège social de la société) un modèle de la configuration en étoile est créé. Le modèle contient le certificat d'Autorité de certification (CA) qui a signé le certificat du routeur concentrateur VPN.
2. Le modèle de configuration est instancié sur une clé USB dans un fichier appelé le **ciscortr.cfg. Ce** fichier de configuration contient la configuration spécifique de rai pour que le routeur soit déployé. Remarque: La configuration sur l'USB ne contient aucune informations confidentielles autre que des adresses IP et le certificat de CA. Il n'y a aucune clé privée du rai ou de serveur CA.
3. L'USB Flash Drive est envoyé au bureau distant par l'intermédiaire de la messagerie ou d'une société de livraison de module.
4. Le routeur en étoile est également envoyé au bureau distant directement de la fabrication de Cisco.
5. Dans le bureau distant le routeur est connecté pour actionner et câblé au réseau comme expliqué dans les instructions qui sont incluses avec l'USB Flash Drive. Ensuite l'USB Flash

Drive est inséré dans le routeur. Remarque: Il y a peu à aucune compétences techniques impliquées dans cette étape, ainsi elle peut facilement être exécutée par n'importe quel personnel de bureau.

6. Une fois que les amorçages d'un routeur vers le haut de lui indique la configuration d'**usbflash0:/ciscortr.cfg.** Dès que le routeur actionnera vers le haut d'une inscription de certificat simple Protocol (SCEP) la demande est envoyée au serveur CA.
7. Sur l'octroi manuel ou automatique de serveur CA peut être configuré a basé sur la stratégie de sécurité d'entreprise. Une fois configurée pour le certificat manuel accordant, la vérification hors bande de la demande SCEP devrait être exécutée (contrôle de validation d'adresse IP, validation de créance pour le personnel qui exécute le déploiement, etc.). Cette étape pourrait différer basé sur le serveur CA que le chapeau t est utilisé.
8. Une fois que la réponse SCEP est reçue par le routeur en étoile, qui a maintenant un certificat valide, la session d'IKE authentifie avec le hub VPN et le tunnel établit avec succès.

Configurations/modèle

Cette sortie témoin affiche à un FlexVPN exemplaire la configuration distante de bureau qui est mise sur le lecteur flash dans le fichier **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"
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Vous pouvez vérifier sur le rai si les tunnels montaient :

```
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
```

Vous pouvez également vérifier sur le rai si le certificat était inscrit correctement :

```
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
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Mises en garde et questions connues

ID de bogue Cisco CSCuu93989 - L'écoulement de PnP d'arrêts d'assistant de config sur les Plateformes G2 pourrait faire ne pas charger le système la configuration de l'usbflash : /ciscortr.cfg. Au lieu de cela le système pourrait arrêter à la caractéristique d'assistant de 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
```

Assurez-vous l'utilisation une version qui contient une difficulté pour ce défaut.

ZTD par l'intermédiaire d'USB contre des fichiers de configuration par défaut

Notez que les **fichiers de configuration par défaut** comportent que ce document l'utilise est une caractéristique différente que le **toucher zéro Deployement par l'intermédiaire de l'USB** desribed dans l'aperçu du déploiement de la gamme Cisco 800 ISR.

-	**Toucher zéro Deployement par l'intermédiaire d'USB**	**Fichiers de configuration par dé**

Plates-formes prises en charge	Limité seulement à peu de Routeurs 8xx. Pour des détails, voir l'aperçu du déploiement de la gamme Cisco 800 ISR	Tous les ISR G2, 43xx et 44xx.
Nom du fichier	*.cfg	ciscortr.cfg
Enregistre la configuration sur l'éclair local	Oui, automatiquement	Non, le gestionnaire d'événeme d'Embeded (EEM) a exigé

Puisque plus de Plateformes sont prises en charge par la caractéristique de **fichiers de configuration par défaut**, cette technologie a été choisie pour la solution présentée en cet article.

Résumé

La configuration par défaut USB (avec nom du fichier **ciscortr.cfg d'un** USB Flash Drive) donne à des administrateurs réseau la capacité de déployer le routeur en étoile distant VPN de bureau (mais non limité juste au VPN) sans nécessité de se connecter dans le périphérique dans le site distant.

Informations connexes

- Inscription de certificat simple Protocol (SCEP)
- Déploiement nul de toucher par l'intermédiaire d'USB
- DMVPN/FlexVPN/Site-to-site VPN
- Support et documentation techniques - Cisco Systems