Configurer le déploiement automatique (ZTD) des bureaux/rayons distants VPN

Contenu

Introduction

Ce document décrit comment une option de déploiement automatique (ZTD) est une solution économique et évolutive pour les déploiements.

Le déploiement sécurisé et efficace et la mise à disposition de routeurs de bureau distant (parfois appelés satellites) peuvent être une tâche difficile. Les bureaux distants peuvent se trouver dans des endroits où il est difficile de demander à un ingénieur de terrain de configurer le routeur sur site, et la plupart des ingénieurs choisissent de ne pas envoyer de routeurs satellite préconfigurés en raison du coût et du risque potentiel de sécurité.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Tout routeur Cisco IOS® disposant d'un port USB prenant en charge les lecteurs Flash USB. Pour plus d'informations, consultez Prise en charge des fonctionnalités USB eToken et USB

Flash.

- Il est confirmé que cette fonctionnalité fonctionne sur presque toutes les plates-formes Cisco 8xx. Pour plus de détails, consultez le livre blanc Fichiers de configuration par défaut (Prise en charge des fonctionnalités sur les routeurs ISR de la gamme Cisco 800).
- D'autres plates-formes dotées de ports USB tels que les routeurs à services intégrés (ISR) des gammes G2 et 43xx/44xx.

Components Used

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

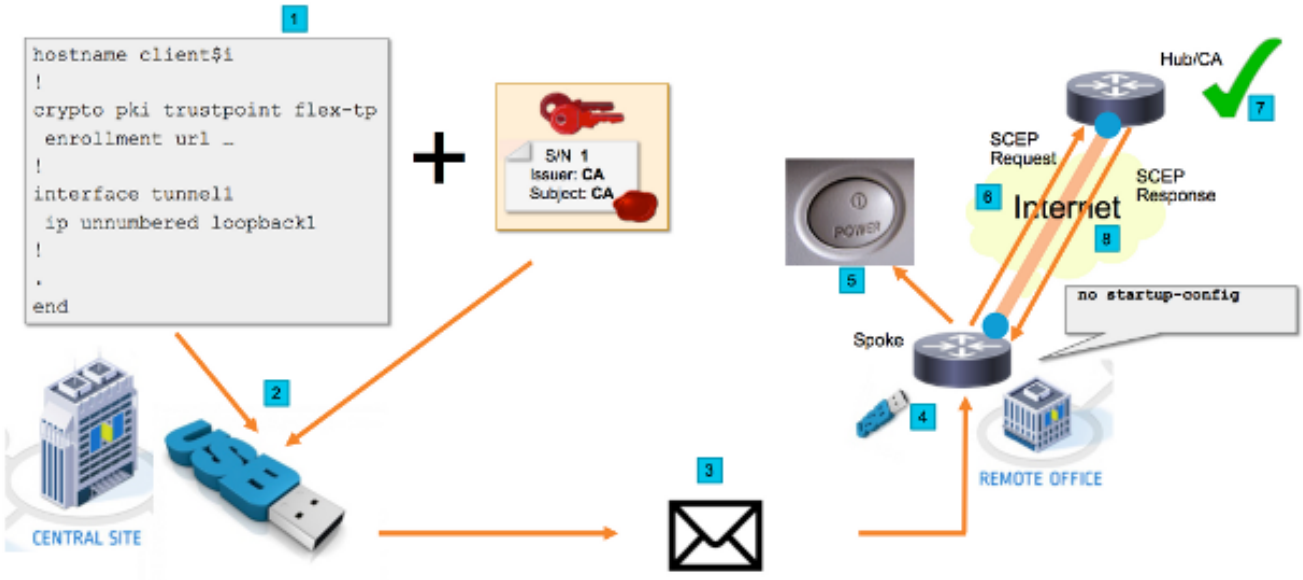
- SCEP (Simple Certificate Enrollment Protocol)
- Déploiement automatique via USB
- DMVPN/FlexVPN/VPN site à site

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.

Configuration

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

Diagramme du réseau



Flux réseau

1. Dans le site central (siège social de la société), un modèle de configuration Spoke est créé. Le modèle contient le certificat d'autorité de certification qui a signé le certificat du routeur concentrateur VPN.

2. Le modèle de configuration est instancié sur une clé USB dans un fichier appelé **ciscortr.cfg**. Ce fichier de configuration contient la configuration spécifique de Spoke pour le routeur à déployer. **Note**: La configuration sur l'USB ne contient aucune information sensible autre que les adresses IP et le certificat de l'autorité de certification. Il n'existe aucune clé privée du serveur Spoke ou CA.
3. Le lecteur Flash USB est envoyé au Bureau à distance par courrier ou par une société de livraison de paquets.
4. Le routeur Spoke est également envoyé au bureau distant directement à partir de Cisco Manufacturing.
5. Dans le Bureau à distance, le routeur est connecté à l'alimentation et câblé au réseau comme expliqué dans les instructions fournies avec le lecteur flash USB. Ensuite, le lecteur flash USB est inséré dans le routeur. **Note**: Cette étape n'a que peu ou pas de compétences techniques et peut donc être réalisée par n'importe quel personnel de bureau.
6. Une fois le routeur démarré, il lit la configuration à partir de **usbflash0:/ciscortr.cfg**. Dès que le routeur est sous tension, une demande SCEP (Simple Certificate Enrollment Protocol) est envoyée au serveur AC.
7. Sur le serveur AC, l'octroi manuel ou automatique peut être configuré en fonction de la stratégie de sécurité de l'entreprise. Lorsqu'elle est configurée pour l'octroi manuel de certificats, la vérification hors bande de la demande SCEP doit être effectuée (contrôle de validation d'adresse IP, validation des informations d'identification du personnel qui effectue le déploiement, etc.). Cette étape peut différer selon le serveur AC utilisé.
8. Une fois la réponse SCEP reçue par le routeur Spoke, qui possède maintenant un certificat valide, la session Internet Key Exchange (IKE) s'authentifie avec le concentrateur VPN et le tunnel s'établit correctement.

Autorisation basée sur SUDI

L'étape 7 implique la vérification manuelle de la demande de signature de certificat envoyée via le protocole SCEP, qui peut être lourde et difficile à exécuter pour le personnel non technique. Afin d'améliorer la sécurité et d'automatiser le processus, les certificats de périphérique SUDI (Secure Unique Device Identification) peuvent être utilisés. Les certificats SUDI sont des certificats intégrés aux périphériques ISR 4K. Ces certificats sont signés par Cisco CA. Chaque appareil fabriqué a reçu un certificat différent et le numéro de série de l'appareil est indiqué dans le nom commun du certificat. Le certificat SUDI, la paire de clés associée et l'ensemble de sa chaîne de certificats sont stockés dans la puce Trust Anchor résistant aux altérations. En outre, la paire de clés est cryptographiquement liée à une puce d'ancrage de confiance spécifique et la clé privée n'est jamais exportée. Cette fonctionnalité rend le clonage ou l'usurpation d'identité pratiquement impossible.

La clé privée SUDI peut être utilisée pour signer la requête SCEP générée par le routeur. Le serveur AC peut vérifier la signature et lire le contenu du certificat SUDI du périphérique. Le serveur AC peut extraire les informations du certificat SUDI (comme un numéro de série) et effectuer l'autorisation en fonction de ces informations. Le serveur RADIUS peut être utilisé pour répondre à une telle demande d'autorisation.

L'administrateur crée une liste des routeurs de rayons et des numéros de série associés. Les numéros de série peuvent être lus à partir du cas du routeur par le personnel non technique. Ces numéros de série sont stockés dans la base de données du serveur RADIUS et le serveur autorise les requêtes SCEP en fonction de ces informations qui permettent l'octroi automatique du certificat. Notez que le numéro de série est cryptographiquement lié à un périphérique spécifique

via le certificat SUDI signé par Cisco. Il est donc impossible de le falsifier.

En résumé, le serveur AC est configuré pour accorder automatiquement des demandes qui répondent aux deux critères suivants :

- Sont signées avec une clé privée associée à un certificat signé par l'autorité de certification SUDI de Cisco
- Sont autorisés par le serveur Radius en fonction des informations de numéro de série extraites du certificat SUDI

Scénarios de déploiement

Le serveur AC peut être directement exposé à Internet, ce qui permet aux clients d'effectuer l'inscription avant que le tunnel ne puisse être construit. Le serveur AC peut même être configuré sur le même routeur que le concentrateur VPN. L’avantage de cette topologie est la simplicité. L'inconvénient est une diminution de la sécurité, car le serveur AC est directement exposé à diverses formes d'attaque via Internet.

Vous pouvez également développer la topologie en configurant le serveur d'Autorité d'enregistrement. Le rôle du serveur d'autorité d'enregistrement consiste à évaluer et à transmettre les demandes de signature de certificat valides au serveur d'autorité de certification. Le serveur RA lui-même ne contient pas la clé privée de l'autorité de certification et ne peut pas générer de certificats par lui-même. Dans un tel déploiement, le serveur AC n'a pas besoin d'être exposé à Internet, ce qui augmente la sécurité globale.'

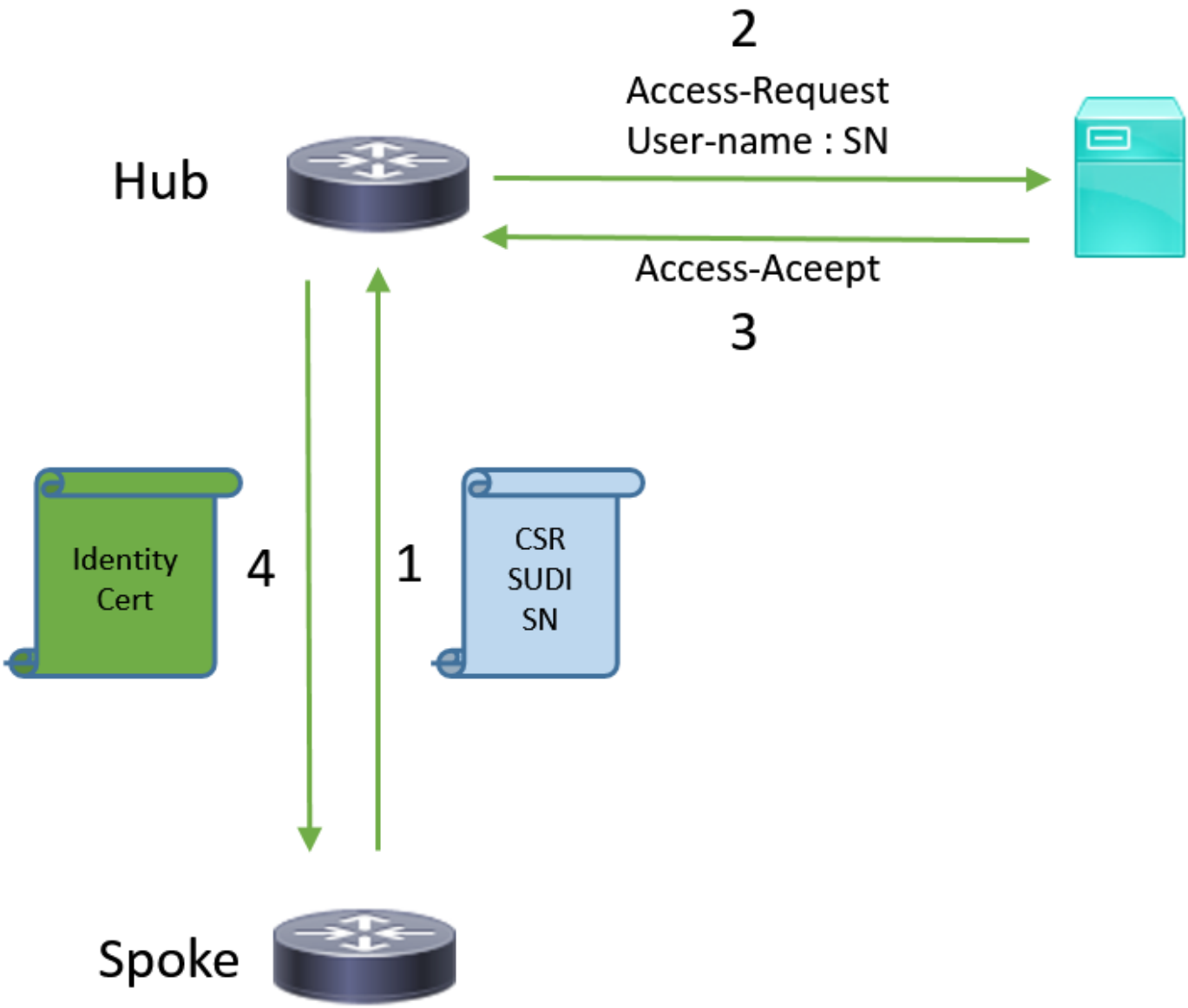
Flux réseau

1. Le routeur Spoke crée une requête SCEP, la signe avec la clé privée de son certificat SUDI et l'envoie au serveur AC.

2. Si la requête est signée correctement, la requête RADIUS est générée. Le numéro de série est utilisé comme paramètre de nom d'utilisateur.

3. Le serveur RADIUS accepte ou rejette la demande.

4. Si la demande est acceptée, le serveur AC accorde la demande. S'il est rejeté, le serveur AC répond avec l'état « En attente » et le client recommence la requête après l'expiration d'un compteur de secours.



Configuration avec CA uniquement

```
!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
```

Configuration avec CA et 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

Configurations/Modèle

Cet exemple de sortie montre une configuration exemplaire de FlexVPN Remote Office qui est placée 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
! 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"
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Vous pouvez vérifier sur le satellite si les tunnels ont augmenté :

```
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 Spoke si le certificat a été 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
```

Dépannage

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

Cavasses et problèmes connus

ID de bogue Cisco CSCuu93989 - L'Assistant de configuration arrête le flux PnP sur les plates-formes G2 peut empêcher le système de charger la configuration à partir de la mémoire flash:/ciscortr.cfg. Au lieu de cela, le système peut s'arrêter à la fonction Assistant de configuration :

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

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

Note: Assurez-vous d'utiliser une version contenant un correctif pour ce défaut.

ZTD via USB et fichiers de configuration par défaut

Notez que la fonctionnalité **Fichiers de configuration par défaut** utilisée par ce document est différente de la **fonctionnalité Déploiement automatique via USB** décrite dans Présentation du déploiement ISR de la gamme Cisco 800.

-	**Déploiement automatique via USB**	**Fichiers de configuratio défaut**
Plates-formes prises en charge	Limité à seulement quelques routeurs 8xx. Pour plus d'informations, consultez Présentation du déploiement des ISR de la gamme Cisco 800	Tous les ISR G2, 43xx 44xx.
Nom de fichier	*.cfg	ciscortr.cfg
Enregistre la configuration sur la mémoire flash locale	Oui, automatiquement	Non, Gestionnaire d'événements intégré (requis

Étant donné que davantage de plates-formes sont prises en charge par la fonctionnalité **Fichiers de configuration par défaut**, cette technologie a été choisie pour la solution présentée dans cet article.

Résumé

La configuration par défaut USB (avec le nom de fichier **ciscortr.cfg** à partir d'un lecteur flash USB) permet aux administrateurs réseau de déployer des VPN de routeur Remote Office Spoke (mais pas uniquement VPN) sans avoir à se connecter au périphérique à l'emplacement distant.

Informations connexes

- SCEP (Simple Certificate Enrollment Protocol)

- Déploiement automatique via USB
- DMVPN/FlexVPN/VPN site à site
- Support et documentation techniques - Cisco Systems
- Technologie d'ancrage Cisco