Migrer de EzVPN-NEM+ hérité vers FlexVPN sur le même serveur

Contenu

Introduction

Ce document décrit le processus de migration d'EzVPN vers FlexVPN. FlexVPN est la nouvelle solution VPN unifiée proposée par Cisco. FlexVPN tire parti du protocole IKEv2 et combine l'accès à distance, site à site, concentrateur et satellite et les déploiements VPN à maillage partiel. Grâce à des technologies héritées telles que EzVPN, Cisco vous encourage vivement à migrer vers FlexVPN afin de tirer parti de ses nombreuses fonctionnalités.

Ce document examine un déploiement EzVPN existant qui se compose de clients matériels EzVPN hérités qui terminent des tunnels sur un périphérique de tête de réseau EzVPN basé sur une carte de chiffrement héritée. L'objectif est de migrer à partir de cette configuration pour prendre en charge FlexVPN avec ces exigences :

- Les clients existants continueront à fonctionner de manière transparente sans modification de configuration. Cela permet une migration progressive de ces clients vers FlexVPN au fil du

temps.
- Le périphérique de tête de réseau doit simultanément prendre en charge la terminaison de nouveaux clients FlexVPN.

Deux composants de configuration IPsec clés sont utilisés afin d'aider à atteindre ces objectifs de migration : à savoir, IKEv2 et les interfaces de tunnel virtuel (VTI). Ces objectifs sont brièvement abordés dans ce document.

Autres documents de cette série

- Guide de déploiement FlexVPN : AnyConnect à la tête de réseau IOS sur IPsec avec IKEv2 et certificats

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Comparaison entre IKEv1 et IKEv2

FlexVPN est basé sur le protocole IKEv2, qui est le protocole de gestion des clés de nouvelle génération basé sur RFC 4306, et une amélioration du protocole IKEv1. FlexVPN n'est pas rétrocompatible avec les technologies qui prennent en charge uniquement IKEv1 (par exemple, EzVPN). Il s'agit d'une des considérations clés lorsque vous migrez d'EzVPN vers FlexVPN. Pour une introduction de protocole sur IKEv2 et une comparaison avec IKEv1, référez-vous à IKE version 2 en un coup d'oeil.

Carte de chiffrement par rapport aux interfaces de tunnel virtuel

L'interface de tunnel virtuel (VTI) est une nouvelle méthode de configuration utilisée pour les configurations de serveur et de client VPN. VTI :

- Remplacement par des crypto-cartes dynamiques, qui est désormais considéré comme une configuration héritée.
- Prend en charge la tunnellisation IPsec native.
- Ne nécessite pas de mappage statique d'une session IPsec vers une interface physique ; par conséquent, offre la flexibilité nécessaire pour envoyer et recevoir du trafic chiffré sur n'importe quelle interface physique (par exemple, plusieurs chemins).

- La configuration minimale en tant qu'accès virtuel à la demande est clonée à partir de l'interface de modèle virtuel.
- Le trafic est chiffré/décrypté lorsqu'il est transféré vers/depuis l'interface du tunnel et est géré par la table de routage IP (jouant ainsi un rôle important dans le processus de cryptage).
- Les fonctionnalités peuvent être appliquées aux paquets en texte clair sur l'interface VTI ou aux paquets chiffrés sur l'interface physique.

Les deux types de VTI disponibles sont les suivants :

- Statique (sVTI) : une interface de tunnel virtuel statique a une source et une destination de tunnel fixes et est généralement utilisée dans un scénario de déploiement de site à site. Voici un exemple de configuration sVTI :

```
interface Tunnel2
 ip address negotiated
 tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile testflex
```

- Dynamic (dVTI) : une interface de tunnel virtuel dynamique peut être utilisée pour terminer les tunnels IPsec dynamiques qui n'ont pas de destination de tunnel fixe. Une fois la négociation de tunnel réussie, les interfaces d'accès virtuel sont clonées à partir d'un modèle virtuel et héritent de toutes les fonctionnalités de couche 3 sur ce modèle virtuel. Voici un exemple de configuration dVTI :

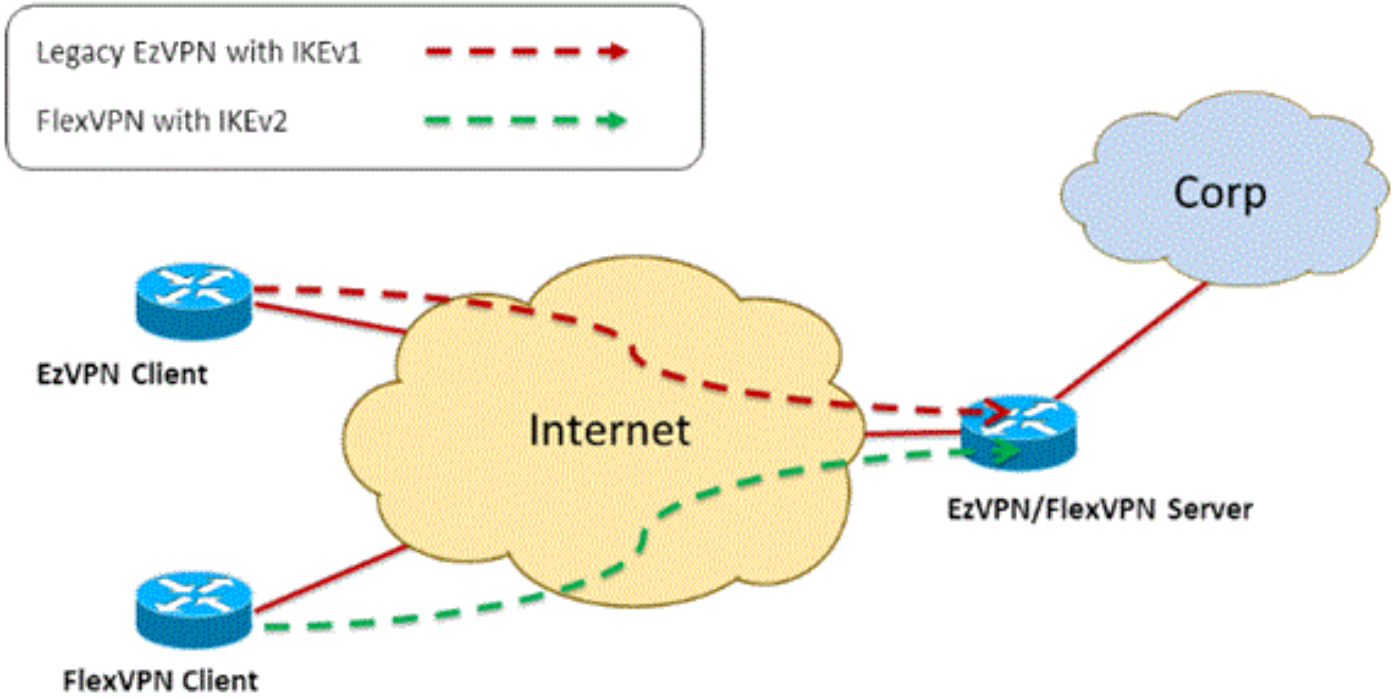
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Pour plus d'informations sur dVTI, reportez-vous aux documents suivants :

- Configuration de Cisco Easy VPN avec DVTI (Dynamic Virtual Tunnel Interface) IPSec
- Restrictions pour l'interface de tunnel virtuel IPsec
- Configuration de la prise en charge Multi-SA pour les interfaces de tunnel virtuel dynamiques à l'aide d'IKEv1

Pour que les clients EzVPN et FlexVPN coexistent, vous devez d'abord migrer le serveur EzVPN de la configuration de crypto-carte existante vers une configuration dVTI. Les sections suivantes décrivent en détail les étapes nécessaires.

Topologie du réseau



Configuration actuelle avec le client EzVPN en mode NEM+ hérité

Configuration du client

Voici une configuration type de routeur client EzVPN. Dans cette configuration, le mode Network Extension Plus (NEM+) est utilisé, ce qui crée plusieurs paires de SA pour les interfaces internes du LAN ainsi que l'adresse IP attribuée à la configuration du mode pour le client.

```
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-plus
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description EzVPN WAN interface
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description EzVPN LAN inside interface
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
```

Configuration du serveur

Sur le serveur EzVPN, une configuration de crypto-carte héritée est utilisée comme configuration de base avant la migration.

```
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network ezvpn-author local
!
username client1 password 0 client1
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address respond
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description EzVPN server WAN interface
 ip address 192.168.1.10 255.255.255.0
 crypto map client-map
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
!
ip access-list extended split-tunnel-acl
  remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
```

Migration du serveur vers FlexVPN

Comme décrit dans les sections précédentes, FlexVPN utilise IKEv2 comme protocole de plan de contrôle et n'est pas rétrocompatible avec une solution EzVPN basée sur IKEv1. Par conséquent, l'idée générale de cette migration est de configurer le serveur EzVPN existant de telle manière qu'il permette la coexistence d'EzVPN hérité (IKEv1) et de FlexVPN (IKEv2). Pour atteindre cet objectif, vous pouvez utiliser cette approche de migration en deux étapes :

1. Déplacez la configuration EzVPN héritée sur la tête de réseau dVTI à partir d'une configuration basée sur une carte de chiffrement.
2. Ajoutez la configuration FlexVPN, également basée sur dVTI.

Déplacer la carte de chiffrement existante vers dVTI

Modifications de la configuration du serveur

Un serveur EzVPN configuré avec une carte de chiffrement sur l'interface physique comporte

plusieurs limitations en matière de prise en charge et de flexibilité des fonctionnalités. Si vous disposez d'EzVPN, Cisco vous encourage vivement à utiliser dVTI à la place. Dans un premier temps, pour migrer vers une configuration EzVPN et FlexVPN coexistante, vous devez la remplacer par une configuration dVTI. Cela fournira une séparation IKEv1 et IKEv2 entre les différentes interfaces de modèles virtuels afin de prendre en charge les deux types de clients.

Remarque : afin de prendre en charge le mode Network Extension Plus du mode EzVPN sur les clients EzVPN, le routeur de tête de réseau doit prendre en charge la fonctionnalité multi SA sur dVTI. Cela permet de protéger plusieurs flux IP par le tunnel, qui est requis pour que la tête de réseau chiffre le trafic vers le réseau interne du client EzVPN, ainsi que l'adresse IP attribuée au client via la configuration du mode IKEv1. Pour plus d'informations sur la prise en charge de plusieurs SA sur dVTI avec IKEv1, référez-vous à Prise en charge de Multi-SA pour les interfaces de tunnel virtuel dynamique pour IKEv1.

Complétez ces étapes afin de mettre en oeuvre la modification de configuration sur le serveur :

Étape 1 - Supprimez la carte de chiffrement de l'interface de sortie physique qui termine les tunnels client EzVPN :

```
interface Ethernet0/0
 ip address 192.168.1.10 255.255.255.0
 no crypto map client-map
```

Étape 2 - Créez une interface de modèle virtuel à partir de laquelle les interfaces d'accès virtuel seront clonées une fois les tunnels établis :

```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
```

Étape 3 - Associez cette nouvelle interface de modèle virtuel au profil isakmp pour le groupe EzVPN configuré :

```
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address initiate
   client configuration address respond
   virtual-template 1
```

Une fois les modifications de configuration ci-dessus effectuées, vérifiez que les clients EzVPN existants continuent à fonctionner. Cependant, maintenant, leurs tunnels sont terminés sur une interface d'accès virtuelle créée dynamiquement. Ceci peut être vérifié avec la commande **show crypto session** comme dans cet exemple :

```
PE-EzVPN-Server#show crypto session
Crypto session current status
Interface: Virtual-Access1
Username: client1
Profile: Group-One-Profile
Group: Group-One
Assigned address: 10.1.1.101
```

```
Session status: UP-ACTIVE
Peer: 192.168.2.101 port 500
  IKEv1 SA: local 192.168.1.10/500 remote 192.168.2.101/500 Active
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 host 10.1.1.101
        Active SAs: 2, origin: crypto map
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 172.16.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

Ajouter la configuration FlexVPN au serveur

Cet exemple utilise RSA-SIG (c'est-à-dire, Certificate Authority) sur le client et le serveur FlexVPN. La configuration de cette section suppose que le serveur a déjà été authentifié et inscrit avec succès auprès du serveur AC.

Étape 1 - Vérifiez la configuration par défaut intelligente IKEv2.

Avec IKEv2, vous pouvez désormais profiter de la fonctionnalité Smart Default introduite dans 15.2(1)T. Il est utilisé pour simplifier la configuration FlexVPN. Voici quelques configurations par défaut :

Stratégie d'autorisation IKEv2 par défaut :

```
VPN-Server#show crypto ikev2 authorization policy default
 IKEv2 Authorization Policy : default
 route set interface
 route accept any tag : 1 distance : 1
```

Proposition IKEv2 par défaut :

```
VPN-Server#show crypto ikev2 proposal default
 IKEv2 proposal: default
 Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
 Integrity : SHA512 SHA384 SHA256 SHA96 MD596
 PRF : SHA512 SHA384 SHA256 SHA1 MD5
 DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

Stratégie IKEv2 par défaut :

```
VPN-Server#show crypto ikev2 policy default
 IKEv2 policy : default
 Match fvrf : any
 Match address local : any
 Proposal : default
```

Profil IPsec par défaut :

```
VPN-Server#show crypto ipsec profile default
IPSEC profile default
 Security association lifetime: 4608000 kilobytes/3600 seconds
 Responder-Only (Y/N): N
 PFS (Y/N): N
 Transform sets={
 default: { esp-aes esp-sha-hmac } ,
 }
```

Jeu de transformation IPsec par défaut :

```
VPN-Server#show crypto ipsec transform default
{ esp-aes esp-sha-hmac }
 will negotiate = { Transport, },
```

Pour plus d'informations sur la fonctionnalité par défaut intelligente IKEv2, référez-vous à Paramètres par défaut intelligents IKEv2 (clients enregistrés uniquement).

Étape 2 - Modifiez la stratégie d'autorisation IKEv2 par défaut et ajoutez un profil IKEv2 par défaut pour les clients FlexVPN.

Le profil IKEv2 créé ici correspond à un ID d'homologue basé sur le nom de domaine cisco.com et les interfaces d'accès virtuel créées pour les clients seront générées à partir du modèle virtuel 2. Notez également que la stratégie d'autorisation définit le pool d'adresses IP utilisé pour attribuer des adresses IP homologues ainsi que des routes à échanger via le mode de configuration IKEv2 :

```
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
```

Étape 3 - Créez l'interface de modèle virtuel utilisée pour les clients FlexVPN :

```
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
```

Configuration du client FlexVPN

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
```

```
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
```

Configuration complète

Configuration complète du serveur hybride

```
hostname VPN-Server
!
!
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network default local
aaa authorization network ezvpn-author local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=vpn-server.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 07
 certificate ca 01
username client1 password 0 client1
username cisco password 0 cisco
!
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
```

```
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
 save-password
crypto isakmp profile Group-One-Profile
 match identity group Group-One
 client authentication list client-xauth
 isakmp authorization list ezvpn-author
 client configuration address initiate
 client configuration address respond
 virtual-template 1
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto ipsec profile default
 set ikev2-profile default
!
crypto ipsec profile legacy-profile
 set transform-set aes-sha
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description WAN
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.0.1 255.255.255.0
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
ip local pool flexvpn-pool 10.1.1.201 10.1.1.250
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip access-list extended split-tunnel-acl
 remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
!
access-list 1 permit 172.16.0.0 0.0.0.255
```

Configuration complète du client EzVPN IKEv1

```
hostname Client1
!
crypto ipsec client ezvpn legacy-client
```

```
 connect manual
 group Group-One key cisco123
 mode network-extension
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description LAN
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

Configuration complète du client IKEv2 FlexVPN

```
hostname Client2
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 redundancy
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=Client2.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 06
 certificate ca 01
!
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
```

```
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.102 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
!
access-list 1 permit 172.16.2.0 0.0.0.255
```

Vérification de la configuration

Voici quelques-unes des commandes utilisées pour vérifier les opérations EzVPN/FlexVPN sur un routeur :

```
show crypto session

show crypto session detail

show crypto isakmp sa

show crypto ikev2 sa

show crypto ipsec sa detail

show crypto ipsec client ez (for legacy clients)

show crypto socket

show crypto map
```

Informations connexes

- Support et documentation techniques - Cisco Systems