Transfert de FlexVPN : Legs EzVPN-NEM+ et FlexVPN sur le même serveur

Contenu

Introduction

Ce document décrit le procédé de transfert de l'EzVPN à FlexVPN. FlexVPN est la nouvelle solution VPN unifiée offerte par Cisco. FlexVPN tire profit du protocole IKEv2 et combine l'Accès à distance, le site à site, le hub and spoke, et les déploiements VPN partiels de maille. Avec des Technologies existantes comme l'EzVPN, Cisco vous encourage fortement à migrer vers FlexVPN afin de tirer profit de ses capacités de riche en fonctionnalités.

Ce document examine un déploiement existant d'EzVPN qui se compose des clients matériels existants d'EzVPN qui terminent des tunnels sur un crypto périphérique à base de cartes existant de headend d'EzVPN. Le but est de migrer de cette configuration pour prendre en charge FlexVPN avec ces conditions requises :

- Les clients existants existants continueront à ne travailler sans faille sans aucune modification de configuration. Ceci permet un transfert échelonné de ces clients à FlexVPN au fil du

temps.
- Le périphérique de headend devrait simultanément prendre en charge l'arrêt de nouveaux clients de FlexVPN.

Deux composants principaux de configuration d'IPsec sont utilisés afin d'aider à accomplir ces buts de transfert : à savoir, IKEv2 et interfaces de tunnel virtuelles (VTI). Ces buts sont brièvement discutés dans ce document.

D'autres documents dans cette gamme

- Guide de déploiement de FlexVPN : AnyConnect au Headend IOS au-dessus d'IPsec avec IKEv2 et Certificats

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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.

IKEv1 contre IKEv2

FlexVPN est basé sur le protocole IKEv2, qui est le protocole de gestion de clés de la deuxième génération basé sur RFC 4306, et une amélioration du protocole IKEv1. FlexVPN n'est pas rétrocompatible avec les Technologies qui prennent en charge seulement IKEv1 (par exemple, EzVPN). C'est l'une des considérations principales quand vous migrez de l'EzVPN vers FlexVPN. Pour une introduction de protocole sur IKEv2 et la comparaison avec IKEv1, référez-vous à la version 2 d'IKE d'un coup d'oeil.

Crypto map contre les interfaces de tunnel virtuelles

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

- Remplacement aux crypto-cartes dynamiques, qui est maintenant considéré configuration existante.
- Prend en charge le Tunnellisation indigène d'IPsec.
- N'exige pas un mappage statique d'une session d'IPsec à une interface physique ; , fournit donc la flexibilité d'envoyer et recevoir le trafic chiffré sur n'importe quelle interface physique (par exemple, des plusieurs chemins).

- La configuration minimale en tant qu'accès virtuel sur demande est copiée de l'interface de modèle virtuel.
- Le trafic est chiffré/déchiffré si en avant à/de l'interface de tunnel et est géré par la table de Routage IP (de ce fait, jouant un important rôle dans le procédé de cryptage).
- Des caractéristiques peuvent être appliquées aux paquets de libellé sur l'interface VTI, ou aux paquets chiffrés sur l'interface physique.

Les deux types de VTIs disponibles sont :

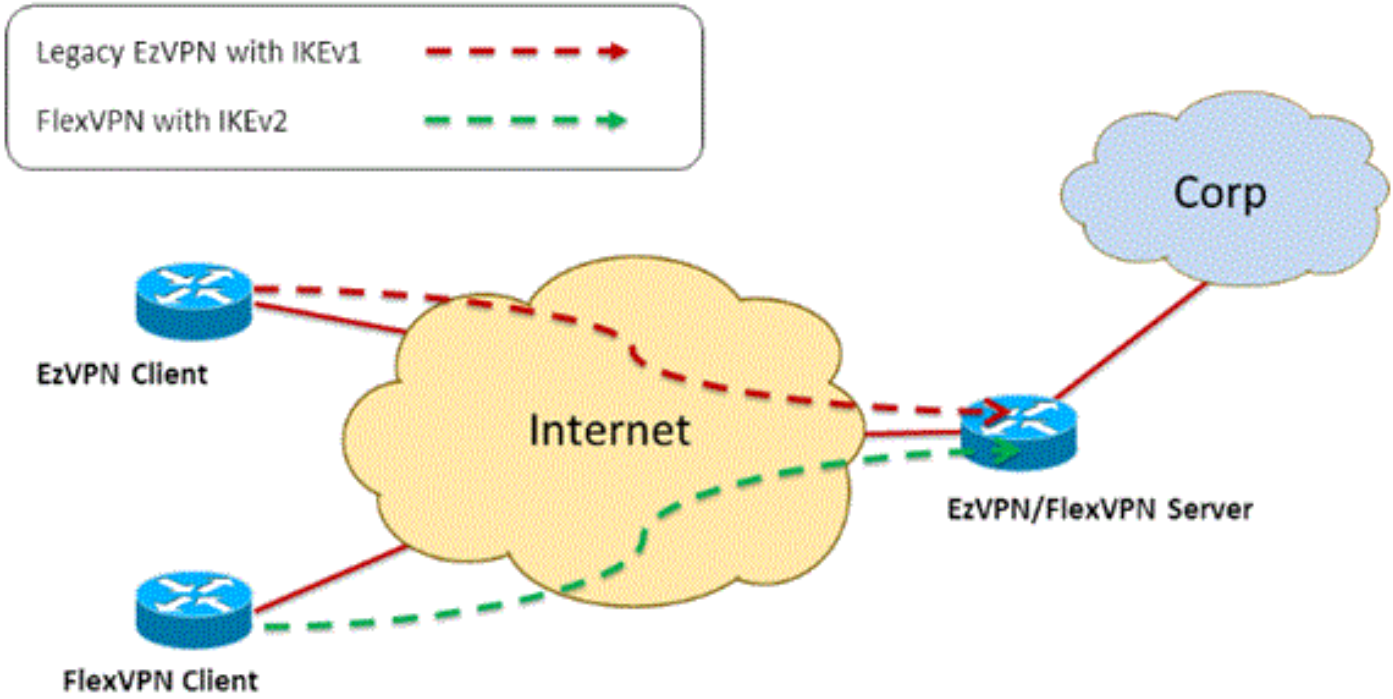
- Statique (sVTI) — Une interface de tunnel virtuelle statique a une source du tunnel et une destination fixes et est typiquement utilisée dans un scénario de déploiement de site à site. Voici un exemple d'une configuration de sVTI :
```
interface Tunnel2
 ip address negotiated
 tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile testflex
```
- Dynamique (dVTI) — Une interface de tunnel virtuelle dynamique peut être utilisée pour terminer les tunnels dynamiques d'IPsec qui n'ont pas une destination fixe de tunnel. Sur la négociation réussie de tunnel, des interfaces d'accès virtuel seront copiées d'un virtual-template et hériteront de toutes les caractéristiques L3 sur ce virtual-template. Voici un exemple d'une configuration de dVTI :
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Référez-vous à ces documents pour plus d'informations sur le dVTI :

- Configurant la Solution Cisco Easy VPN avec l'interface de tunnel virtuelle dynamique d'IPSec (DVTI)
- Restrictions pour l'interface de tunnel virtuelle d'IPsec
- Configurer le soutien Multi-SA des interfaces de tunnel virtuelles dynamiques utilisant IKEv1

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

Topologie du réseau



Configuration en cours avec le client existant d'EzVPN de mode NEM+

Configuration de client

Est ci-dessous une configuration typique de routeur client d'EzVPN. Dans cette configuration, l'extension de réseau plus le mode (NEM+) est utilisée, qui crée de plusieurs paires SA pour les interfaces internes de RÉSEAU LOCAL aussi bien que l'adresse IP assignée par configuration de 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 d'EzVPN, une configuration existante de crypto map est utilisée comme configuration de base avant le transfert.

```
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
```

Transfert de serveur à FlexVPN

Comme décrit dans les sections précédentes, FlexVPN utilise IKEv2 comme protocole d'avion de contrôle et n'est pas arrière - compatible avec une solution d'EzVPN IKEv1-based. En conséquence, l'idée générale de ce transfert est de configurer le serveur existant d'EzVPN de telle manière qu'il permette à l'EzVPN existant (IKEv1) et au FlexVPN (IKEv2) de coexister. Afin d'atteindre ce but, vous pouvez utiliser cette approche en deux étapes de transfert :

1. Déplacez la configuration existante d'EzVPN sur le headend d'une crypto configuration à base de cartes au dVTI.
2. Ajoutez la configuration de FlexVPN, qui est également basée sur le dVTI.

Déplacez le crypto map existant au dVTI

Modifications de configuration du serveur

Un serveur d'EzVPN configuré avec le crypto map sur l'interface physique inclut plusieurs limites quand il s'agit de prise en charge de fonctionnalité et flexibilité. Si vous avez l'EzVPN, Cisco vous encourage fortement à utiliser le dVTI à la place. Dans un premier temps pour migrer vers une

configuration de coexistence d'EzVPN et de FlexVPN, vous devez la changer à une configuration de dVTI. Ceci fournira la séparation IKEv1 et IKEv2 entre les différentes interfaces de modèle virtuel afin de faciliter les deux types de clients.

Remarque: Afin de prendre en charge l'extension de réseau plus le mode de l'exécution d'EzVPN sur les clients d'EzVPN, le routeur de headend doit avoir le soutien de SA multi sur la caractéristique de dVTI. Ceci permet des écoulements de plusieurs IP à protéger par le tunnel, qui est exigé pour que le headend chiffre le trafic au réseau intérieur du client d'EzVPN, aussi bien que l'adresse IP assignée au client par le config du mode IKEv1. Pour plus d'informations sur le support multi SA sur le dVTI avec IKEv1, référez-vous au soutien Multi-SA des interfaces de tunnel virtuelles dynamiques pour IKEv1.

Terminez-vous ces étapes afin d'implémenter la modification de configuration sur le serveur :

Étape 1 — Retirez le crypto map de l'interface de sortie physique qui termine les tunnels de client d'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 dont des interfaces d'accès virtuelles seront copiées une fois les tunnels sont établies :

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

Étape 3 — Associez cette interface de modèle virtuel de création récente au profil d'ISAKMP pour le groupe configuré d'EzVPN :

```
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 ci-dessus de configuration sont apportées, vérifient que les clients existants d'EzVPN continuent à travailler. Cependant, maintenant leurs tunnels sont terminés sur une interface d'accès virtuelle dynamiquement créée. Ceci peut être vérifié avec le comme indiqué dans cet exemple d'ordre de **show crypto session** :

```
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
```

Ajoutez la configuration de FlexVPN au serveur

Cet exemple utilise RSA-SIG (c'est-à-dire, autorité de certification) sur chacun des deux le client et serveur de FlexVPN. La configuration dans cette section suppose que le serveur a déjà avec succès authentifié et s'est inscrit avec le serveur CA.

Étape 1 — Vérifiez la configuration par défaut IKEv2 intelligente.

Avec IKEv2, vous pouvez maintenant tirer profit de la fonctionnalité introduite par défaut intelligente dans 15.2(1)T. Il est utilisé pour simplifier une configuration de FlexVPN. Voici quelques configurations par défaut :

Stratégie par défaut de l'autorisation IKEv2 :

```
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 transformations par défaut d'IPsec :

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

Pour plus d'informations sur la caractéristique IKEv2 par défaut intelligente, référez-vous aux par défaut IKEv2 intelligents (clients enregistrés seulement).

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

Le profil IKEv2 créé ici s'assortira sur un ID de pair basé sur le nom de domaine cisco.com et les interfaces d'accès virtuelles créées pour les clients seront engendrées hors fonction du modèle virtuel 2. Notez également la stratégie d'autorisation définit le groupe d'adresse IP utilisé pour assigner des adresses IP aussi bien que des artères de pair à permuter par l'intermédiaire du 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 de FlexVPN :

```
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
```

```
 tunnel protection ipsec profile default
```

Configuration de client de 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 du serveur hybride complète

```
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 de client complète de l'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 de client complète 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 configuration

Voici certaines des commandes utilisées pour vérifier les exécutions d'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