Migrazione da EzVPN-NEM+ legacy a FlexVPN sullo stesso server

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Confronto tra IKEv1 e IKEv2](#)
[Mappe crittografiche e interfacce tunnel virtuale](#)
[Topologia della rete](#)
[Configurazione corrente con client EzVPN modalità NEM+ legacy](#)
[Configurazione client](#)
[Configurazione server](#)
[Migrazione del server a FlexVPN](#)
[Sposta mappa crittografica legacy in dVTI](#)
[Aggiungi configurazione FlexVPN al server](#)
[Configurazione client FlexVPN](#)
[Configurazione completa](#)
[Completa configurazione server ibrido](#)
[Completamento configurazione client EzVPN IKEv1](#)
[Completamento configurazione client FlexVPN IKEv2](#)
[Verifica della configurazione](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive il processo di migrazione da EzVPN a FlexVPN. FlexVPN è la nuova soluzione VPN unificata offerta da Cisco. FlexVPN sfrutta il protocollo IKEv2 e combina l'accesso remoto, l'accesso da sito a sito, l'hub e lo spoke e le distribuzioni VPN mesh parziali. Con tecnologie legacy come EzVPN, Cisco ti incoraggia vivamente a migrare a FlexVPN per sfruttare le sue funzionalità complete.

Questo documento esamina una distribuzione EzVPN esistente costituita da client hardware EzVPN legacy che terminano i tunnel su un dispositivo headend EzVPN basato su una mappa crittografica legacy. L'obiettivo è migrare da questa configurazione per supportare FlexVPN con questi requisiti:

- I client legacy esistenti continueranno a funzionare senza problemi senza alcuna modifica alla configurazione. Ciò consente una migrazione graduale di questi client a FlexVPN nel tempo.

- Il dispositivo headend deve supportare contemporaneamente la terminazione di nuovi client FlexVPN.

Per raggiungere questi obiettivi di migrazione, vengono utilizzati due componenti chiave della configurazione IPsec: ovvero IKEv2 e VTI (Virtual Tunnel Interfaces). Questi obiettivi sono illustrati brevemente nel presente documento.

Altri documenti di questa serie

- Guida all'installazione di FlexVPN: AnyConnect a IOS Headend over IPsec con IKEv2 e certificati

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Confronto tra IKEv1 e IKEv2

FlexVPN si basa sul protocollo IKEv2, che è il protocollo di gestione delle chiavi di nuova generazione basato sulla RFC 4306, e su una versione migliorata del protocollo IKEv1. FlexVPN non è compatibile con le tecnologie precedenti che supportano solo IKEv1 (ad esempio, EzVPN). Questa è una delle considerazioni principali da tenere in considerazione quando si esegue la migrazione da EzVPN a FlexVPN. Per un'introduzione al protocollo IKEv2 e un confronto con IKEv1, consultare brevemente IKE versione 2.

Mappe crittografiche e interfacce tunnel virtuale

Virtual Tunnel Interface (VTI) è un nuovo metodo di configurazione utilizzato sia per le configurazioni dei client che dei server VPN. VTI

- Sostituzione con mappe crittografiche dinamiche, ora considerata configurazione legacy.
- Supporta il tunneling IPsec nativo.
- non richiede un mapping statico di una sessione IPsec a un'interfaccia fisica; pertanto, offre la flessibilità di inviare e ricevere traffico crittografato su qualsiasi interfaccia fisica (ad esempio, più percorsi).
- Configurazione minima in quanto l'accesso virtuale su richiesta viene clonato dall'interfaccia del modello virtuale.

- Il traffico viene criptato/decriptato quando viene inoltrato verso/dall'interfaccia del tunnel e gestito dalla tabella di routing IP (che svolge quindi un ruolo importante nel processo di crittografia).
- Le funzionalità possono essere applicate a pacchetti non crittografati sull'interfaccia VTI o a pacchetti crittografati sull'interfaccia fisica.

I due tipi di VTI disponibili sono:

- Statica (sVTI): un'interfaccia di tunnel virtuale statica ha un'origine e una destinazione tunnel fissa e viene in genere utilizzata in uno scenario di distribuzione da sito a sito. Di seguito è riportato l'esempio di una configurazione 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
```

- Dinamico (dVTI): è possibile utilizzare un'interfaccia tunnel virtuale dinamica per terminare i tunnel IPsec dinamici che non hanno una destinazione tunnel fissa. Una volta completata la negoziazione del tunnel, le interfacce di accesso virtuale verranno clonate da un modello virtuale e erediteranno tutte le funzionalità L3 in tale modello virtuale. Di seguito è riportato l'esempio di una configurazione dVTI:

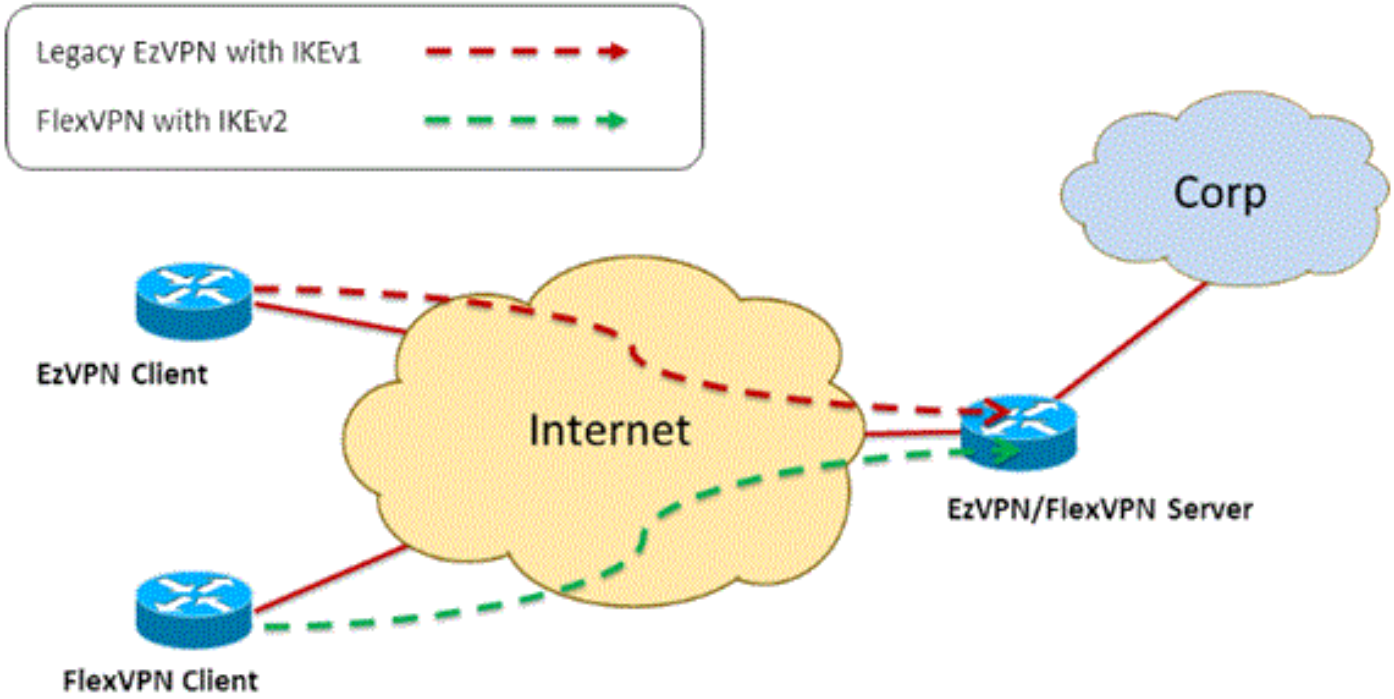
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Per ulteriori informazioni su dVTI, consultare i seguenti documenti:

- Configurazione di Cisco Easy VPN con IPSec Dynamic Virtual Tunnel Interface (DVTI)
- Restrizioni per IPsec Virtual Tunnel Interface
- Configurazione del supporto Multi-SA per le interfacce tunnel virtuali dinamiche con IKEv1

Affinché i client EzVPN e FlexVPN possano coesistere, è necessario innanzitutto eseguire la migrazione del server EzVPN dalla configurazione della mappa crittografica legacy a una configurazione dVTI. Nelle sezioni seguenti vengono illustrati in dettaglio i passaggi necessari.

Topologia della rete



Configurazione corrente con client EzVPN modalità NEM+ legacy

Configurazione client

Di seguito è riportata una configurazione tipica di router client EzVPN. In questa configurazione viene utilizzata la modalità Network Extension Plus (NEM+), che crea più coppie di SA per entrambe le interfacce LAN interne, nonché la configurazione della modalità con l'indirizzo IP assegnato al 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
```

Configurazione server

Sul server EzVPN, viene utilizzata una configurazione della mappa crittografica legacy come configurazione di base prima della migrazione.

```
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
```

Migrazione del server a FlexVPN

Come descritto nelle sezioni precedenti, FlexVPN usa IKEv2 come protocollo del control plane e non è compatibile con le versioni precedenti di una soluzione EzVPN basata su IKEv1. Di conseguenza, l'idea generale di questa migrazione è quella di configurare il server EzVPN esistente in modo che consenta la coesistenza di EzVPN (IKEv1) e FlexVPN (IKEv2) legacy. Per raggiungere questo obiettivo, è possibile utilizzare questo approccio di migrazione in due passaggi:

1. Spostare la configurazione EzVPN legacy sull'headend da una configurazione basata su mappa crittografica a dVTI.
2. Aggiungere la configurazione FlexVPN, anch'essa basata su dVTI.

Sposta mappa crittografica legacy in dVTI

Modifiche alla configurazione del server

Un server EzVPN configurato con mappa crittografica sull'interfaccia fisica presenta diverse limitazioni in termini di supporto e flessibilità delle funzionalità. Se si dispone di EzVPN, Cisco consiglia di utilizzare dVTI. Come primo passo per eseguire la migrazione a una configurazione EzVPN e FlexVPN coesistente, è necessario modificarla in una configurazione dVTI. In questo modo, IKEv1 e IKEv2 saranno separati tra le diverse interfacce del modello virtuale per supportare entrambi i tipi di client.

Nota: per supportare la modalità di estensione della rete Plus di EzVPN sui client EzVPN, il router headend deve essere in grado di supportare la funzionalità multi SA su dVTI. In questo modo, è possibile proteggere più flussi IP dal tunnel, necessario all'headend per crittografare il traffico sulla rete interna del client EzVPN, nonché l'indirizzo IP assegnato al client tramite la configurazione in modalità IKEv1. Per ulteriori informazioni sul supporto di più SA su dVTI con IKEv1, fare riferimento al supporto di più SA per le interfacce tunnel virtuali dinamiche per IKEv1.

Per implementare la modifica della configurazione sul server, completare i seguenti passaggi:

Passaggio 1 - Rimuovere la mappa crittografica dall'interfaccia fisica in uscita che termina i tunnel del client EzVPN:

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

Passaggio 2 - Creare un'interfaccia di modello virtuale da cui le interfacce di accesso virtuale verranno duplicate una volta stabiliti i tunnel:

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

Passaggio 3 - Associare l'interfaccia del modello virtuale appena creata al profilo isakmp per il gruppo EzVPN configurato:

```
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
```

Dopo aver apportato le modifiche alla configurazione di cui sopra, verificare che i client EzVPN esistenti continuino a funzionare. Tuttavia, ora i tunnel vengono terminati su un'interfaccia di accesso virtuale creata in modo dinamico. È possibile verificare questa condizione con il comando **show crypto session**, come mostrato nell'esempio:

```
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
```

Aggiungi configurazione FlexVPN al server

In questo esempio viene utilizzato RSA-SIG (ovvero Certificate Authority) sia sul client che sul server FlexVPN. La configurazione in questa sezione presuppone che il server sia già stato autenticato e registrato correttamente con il server CA.

Passaggio 1 - Verificare la configurazione predefinita di IKEv2 Smart.

Con IKEv2 è ora possibile sfruttare la funzionalità Smart Default introdotta nella versione 15.2(1)T. Viene utilizzata per semplificare una configurazione FlexVPN. Di seguito sono riportate alcune configurazioni predefinite:

Criterio di autorizzazione IKEv2 predefinito:

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

Proposta IKEv2 predefinita:

```
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
```

Criterio IKEv2 predefinito:

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

Profilo IPSec predefinito:

```
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 } ,
 }
```

Set di trasformazioni IPSec predefinito:

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

Per ulteriori informazioni sulla funzione Smart Default di IKEv2, fare riferimento a IKEv2 Smart Defaults (solo utenti registrati).

Passaggio 2 - Modificare il criterio di autorizzazione IKEv2 predefinito e aggiungere un profilo IKEv2 predefinito per i client FlexVPN.

Il profilo IKEv2 creato in questa pagina corrisponderà a un ID peer basato sul nome di dominio cisco.com e le interfacce di accesso virtuale create per i client verranno estratte dal modello virtuale 2. I criteri di autorizzazione definiscono inoltre il pool di indirizzi IP utilizzato per l'assegnazione degli indirizzi IP peer e delle route da scambiare tramite la modalità di configurazione 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
```

Passaggio 3 - Creare l'interfaccia del modello virtuale utilizzata per i client FlexVPN:

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

Configurazione 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
```

Configurazione completa

Completa configurazione server ibrido

```
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
```

Completamento configurazione 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
```

Completamento configurazione client FlexVPN IKEv2

```
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
```

Verifica della configurazione

Di seguito sono elencati alcuni comandi utilizzati per verificare le operazioni EzVPN/FlexVPN su un router:

```
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
```

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems