Verouderde EzVPN-NEM+ naar FlexVPN op dezelfde server

Inhoud

Inleiding

Dit document beschrijft het migratieproces van EzVPN naar FlexVPN. FlexVPN is de nieuwe Unified VPN-oplossing die door Cisco wordt aangeboden. FlexVPN maakt gebruik van het IKEv2-protocol en combineert externe toegang, site-to-site, hub en gedeelde mesh VPN-implementaties. Met oudere technologieën zoals EzVPN, moedigt Cisco u sterk aan om naar FlexVPN te migreren om voordeel te halen uit zijn mogelijkheden die veel eigenschappen hebben.

Dit document onderzoekt een bestaande EzVPN-implementatie die bestaat uit erfenis EzVPN hardware clients die tunnels op een erfenis crypto kaart gebaseerde EzVPN head-end apparaat beëindigen. Het doel is om van deze configuratie te migreren ter ondersteuning van FlexVPN met deze vereisten:

- Bestaande oudere klanten zullen naadloos blijven werken zonder dat de configuratie verandert. Dit maakt een gefaseerde migratie van deze klanten naar FlexVPN mogelijk in de

loop der tijd.
- Het head-end apparaat zou tegelijkertijd de beëindiging van nieuwe FlexVPN clients ondersteunen.

Er worden twee belangrijke configuratie-onderdelen van IPsec gebruikt om deze migratiedoelstellingen te helpen realiseren: met name IKEv2 en Virtual Tunnel Interfaces (VTI's). Deze doelstellingen worden in dit document kort besproken.

Overige documenten in deze serie

- FlexVPN-implementatiegids: AnyConnect met IOS Head-end over IPsec met IKEv2 en certificaten

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

IKEv1 vs IKEv2

FlexVPN is gebaseerd op het IKEv2-protocol, dat het volgende-generatie cruciale beheerprotocol is gebaseerd op RFC 4306 en een versterking van het IKEv1-protocol. FlexVPN is niet achterwaarts compatibel met technologieën die alleen IKEv1 ondersteunen (bijvoorbeeld EzVPN). Dit is een van de belangrijkste overwegingen bij de migratie van EzVPN naar FlexVPN. Voor een protocolinleiding op IKEv2 en vergelijking met IKEv1, zie IKE versie 2 in een oogopslag.

Crypto map vs. Virtual Tunnel Interfaces

Virtual Tunnel Interface (VTI) is een nieuwe configuratiemethode die in zowel VPN-server als client-configuraties wordt gebruikt. VTI:

- Vervanging naar dynamische crypto kaarten, die nu beschouwd wordt als bestaande configuratie.
- Ondersteunt native IPsec-tunneling.
- Vereist geen statische mapping van een IPsec-sessie naar een fysieke interface; biedt daarom flexibiliteit om versleuteld verkeer op elke fysieke interface te verzenden en ontvangen (bijvoorbeeld meerdere paden).
- Minimale configuratie als virtuele toegang op aanvraag is gekloond vanaf een virtuele

sjablooninterface.
- Het verkeer wordt versleuteld/gedecrypteerd wanneer het wordt verstuurd naar/van de tunnelinterface en wordt beheerd door de IP-routingtabel (waarbij een belangrijke rol wordt gespeeld in het encryptieproces).
- De functies kunnen worden toegepast op duidelijke tekstpakketten op de VTI-interface of versleutelde pakketten op de fysieke interface.

De twee beschikbare VTI's zijn:

- Static (sVTI) - Een statische virtuele tunnelinterface heeft een vaste tunnelbron en een bestemming en wordt gewoonlijk gebruikt in een site-to-site implementatiescenario. Hier is een voorbeeld van een sVTI configuratie:

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

- Dynamische (dVTI)—Een dynamische virtuele tunnelinterface kan worden gebruikt om dynamische IPsec-tunnels te sluiten die geen vaste tunnelbestemming hebben. Na succesvolle tunnelonderhandeling zullen de interfaces voor virtuele toegang van een virtueel sjabloon worden gekloond en alle L3 functies op dat Virtual-sjabloon erven. Hier is een voorbeeld van een dVTI configuratie:

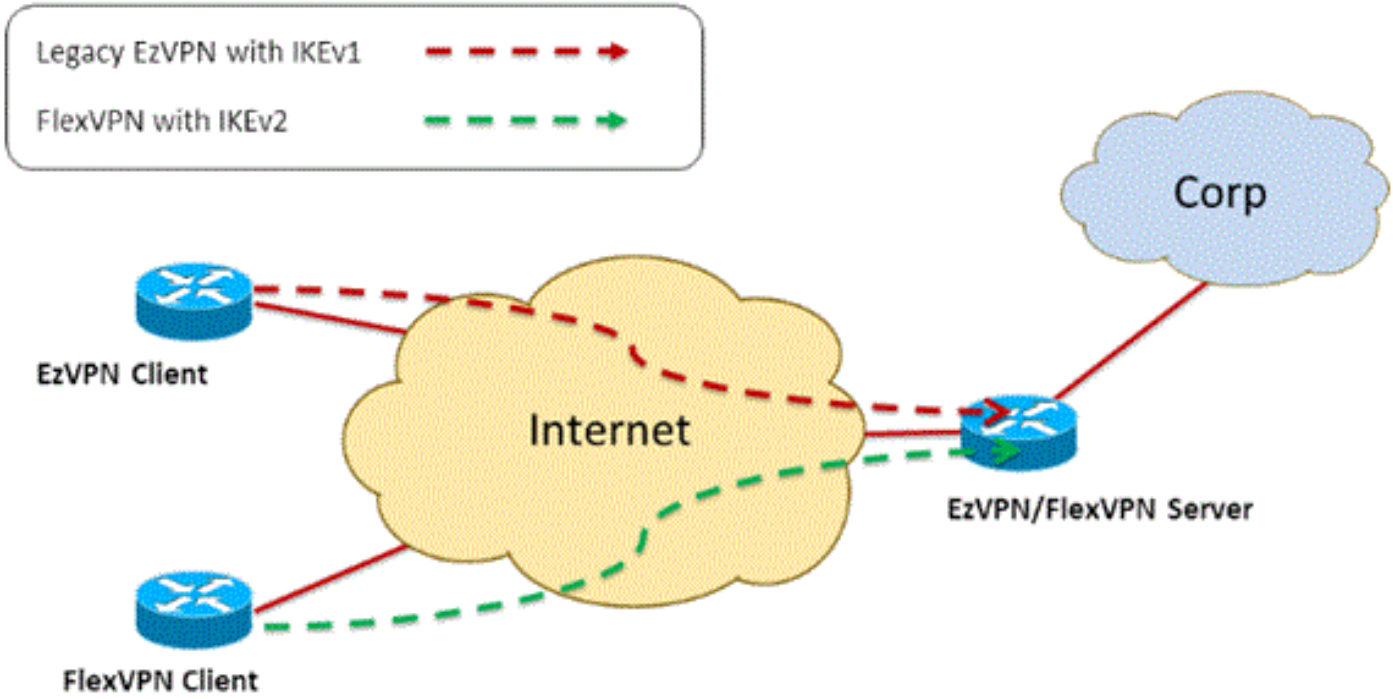
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Raadpleeg deze documenten voor meer informatie over dVTI:

- Cisco Easy VPN configureren met IPSec Dynamic Virtual Tunnel Interface (DVTI)
- Beperkingen voor IPsec virtuele tunnelinterface
- Ondersteuning van multi-SA configureren voor dynamische virtuele tunnelinterfaces met IKEv1

Om EzVPN- en FlexVPN-clients te kunnen coëxisteren, moet u eerst de EzVPN-server migreren van de bestaande crypto-kaartconfiguratie naar een dVTI-configuratie. In de volgende paragrafen worden de noodzakelijke stappen uitvoerig toegelicht.

Netwerktopologie



Huidige configuratie met Verouderde NEM+ mode EzVPN-client

Clientconfiguratie

Hieronder staat een standaard EzVPN-clientrouterconfiguratie. In deze configuratie wordt de modus Network Extension Plus (NEM+) gebruikt, die meerdere SA-paren maakt voor zowel de LAN-binneninterfaces als de mode-configuratie en het IP-adres voor de 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
```

Configuratie van servers

Op de EzVPN-server wordt de configuratie van de legacy-crypto-kaart gebruikt als basisconfiguratie voor de migratie.

```
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
```

Migratie van server naar FlexVPN

Zoals in de vorige secties is beschreven, gebruikt FlexVPN IKEv2 als het protocol op het besturingsplane en is deze niet achterwaarts compatibel met een op IKEv1 gebaseerde EzVPN-oplossing. Als resultaat hiervan is het algemene idee van deze migratie om de bestaande EzVPN server op dusdanige wijze te configureren dat zowel EzVPN (IKEv1) als FlexVPN (IKEv2) naast elkaar kunnen bestaan. Om dit doel te bereiken, kunt u deze tweestappenbenadering van migratie gebruiken:

1. Verplaats de EzVPN-configuratie op het hoofd van een crypto kaart gebaseerde configuratie naar dVTI.
2. Voeg de configuratie FlexVPN toe, die ook op dVTI is gebaseerd.

Verouderde versleuteling naar dVTI verplaatsen

Wijzigingen in serverconfiguratie

Een EzVPN-server die is geconfigureerd met crypto-map op de fysieke interface bevat

verschillende beperkingen als het gaat om ondersteuning en flexibiliteit. Als u EzVPN hebt, moedigt Cisco u sterk aan om dVTI in plaats daarvan te gebruiken. Als eerste stap naar een coëxistente EzVPN- en FlexVPN-configuratie moet u deze wijzigen in een dVTI-configuratie. Dit zal zorgen voor IKEv1- en IKEv2-scheiding tussen de verschillende virtuele-sjablooninterfaces om beide soorten klanten te kunnen ontvangen.

Opmerking: om de Network Extension Plus Mode van EzVPN-handeling op de EzVPN-clients te ondersteunen, moet de head-end router ondersteuning hebben voor de multi-SA-optie op dVTI-functie. Dit staat meerdere IP stromen toe om door de tunnel beschermd te worden, die voor het head-end om verkeer naar het binnen netwerk van de EzVPN client te versleutelen vereist is, evenals het IP-adres dat aan de client is toegewezen via IKEv1 mode-configuratie. Raadpleeg voor meer informatie over multi-SA ondersteuning op dVTI met IKEv1 de Ondersteuning van multi-SA voor Dynamic Virtual Tunnel Interfaces voor IKEv1.

Voltooi deze stappen om de configuratieverandering op de server uit te voeren:

Stap 1 - Verwijder de crypto kaart van de fysieke spanning interface die de EzVPN-clienttunnels beëindigt:

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

Stap 2 - Maak een virtuele-sjabloon-interface waarvan de virtuele toegangsinterfaces worden gekloond zodra de tunnels zijn geïnstalleerd:

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

Stap 3 - Associeer deze nieuwe virtuele sjablooninterface aan het isakmp-profiel voor de geconfigureerde EzVPN-groep:

```
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
```

Controleer, wanneer de bovenstaande configuratiewijzigingen zijn aangebracht, of de bestaande EzVPN-clients blijven werken. Maar nu worden hun tunnels afgesloten op een dynamisch gemaakte virtuele toegangsinterface. Dit kan worden geverifieerd met de opdracht **sessie crypto** als in dit voorbeeld:

```
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
```

Voeg de FlexVPN-configuratie aan de server toe

Dit voorbeeld gebruikt RSA-SIG (dat wil zeggen, certificaatautoriteit) op zowel de FlexVPN client als de server. De configuratie in deze sectie veronderstelt dat de server reeds met succes authentiek verklaard en met de server van CA heeft ingeschreven.

Stap 1 - Controleer de standaardconfiguratie van IKEv2.

Met IKEv2 kunt u nu gebruikmaken van de Smart Default optie die in 15.2(1)T is geïntroduceerd. Het wordt gebruikt om een FlexVPN-configuratie te vereenvoudigen. Hier zijn een aantal standaardinstellingen:

Standaard IKEv2-autorisatiebeleid:

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

Standaard IKEv2-voorstel:

```
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
```

Standaard IKEv2-beleid:

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

Standaard IPsec-profiel:

```
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 } ,
 }
```

Standaard IPsec-transformatie-set:

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

Raadpleeg voor meer informatie over de optie IKEv2 Smart Default IKEv2 Smart Default (alleen geregistreerde klanten).

Stap 2 - Wijzig het standaard IKEv2 autorisatiebeleid en voeg een standaard IKEv2 profiel toe voor de FlexVPN-clients.

Het hier gemaakte IKEv2-profiel komt overeen met een peer-ID op basis van de domeinnaam cisco.com en de virtuele toegangsinterfaces die voor de klanten zijn gemaakt, zullen worden verwijderd van virtueel sjabloon 2. Let ook op dat het vergunningsbeleid de IP-adrespool definieert die wordt gebruikt voor het toewijzen van IP-adressen en routes die via de IKEv2-configuratiemodus worden uitgewisseld:

```
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
```

Stap 3 - Maak de virtuele sjabloon-interface die voor de FlexVPN-clients wordt gebruikt:

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

FlexVPN-clientconfiguratie

```
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
```

Complete configuratie

Configuratie van volledige hybride server

```
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
```

Complete IKEv1 EZVPN-clientconfiguratie

```
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
```

Complete IKEv2 FlexVPN-clientconfiguratie

```
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
```

Configuratie-verificatie

Hier zijn enkele opdrachten die worden gebruikt om de EzVPN/FlexVPN-bewerkingen op een router te controleren:

```
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
```

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems