從舊版EzVPN-NEM+遷移至同一伺服器上的FlexVPN

目錄

簡介

本檔案介紹從EzVPN到FlexVPN的遷移過程。FlexVPN是思科提供的全新統一VPN解決方案。FlexVPN利用IKEv2協定，將遠端訪問、站點到站點、中心輻射和部分網狀VPN部署相結合。藉助EzVPN等傳統技術，思科強烈建議您遷移到FlexVPN，以利用其功能豐富的功能。

本文檔檢查現有EzVPN部署，該部署由在基於舊加密對映的EzVPN頭端裝置上終止隧道的舊EzVPN硬體客戶端組成。目標是從此配置遷移至支援具有以下要求的FlexVPN:

- 現有舊客戶端將繼續無縫工作，無需進行任何配置更改。這樣可隨著時間的推移將這些客戶端分階段遷移到FlexVPN。
- 頭端裝置應同時支援終止新的FlexVPN客戶端。

兩個關鍵的IPsec配置元件用於幫助實現這些遷移目標：即IKEv2和虛擬通道介面(VTI)。 本檔案將簡要討論這些目標。

此系列中的其他檔案

- FlexVPN部署指南：使用IKEv2和證書通過IPsec連線到IOS頭端

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

IKEv1與IKEv2

FlexVPN基於IKEv2協定（基於RFC 4306的下一代金鑰管理協定）和IKEv1協定的增強。FlexVPN與僅支援IKEv1的技術（例如EzVPN）不向後相容。 這是從EzVPN遷移到FlexVPN時需要考慮的關鍵問題之一。有關IKEv2的協定介紹以及與IKEv1的比較，請參閱IKE版本2一覽。

加密對映與虛擬通道介面

虛擬通道介面(VTI)是一種用於VPN伺服器和使用者端組態的新組態方法。VTI:

- 替代動態加密對映，現在被視為舊配置。
- 支援本地IPsec隧道。
- 不需要IPsec會話到物理介面的靜態對映；因此，可靈活地在任何實體介面（例如多個路徑）上傳送和接收加密流量。
- 從虛擬模板介面克隆按需虛擬訪問所需的最低配置。
- 當從通道介面轉送時，流量會進行加密/解密，並由IP路由表管理（因此，在加密過程中扮演重要角色）。
- 功能既可以應用於VTI介面上的明文資料包，也可以應用於物理介面上的加密資料包。

可用的兩種VTI包括：

- 靜態(sVTI) — 靜態虛擬隧道介面具有固定隧道源和目標，通常用於站點到站點部署方案。以下是sVTI配置的示例：

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

- 動態(dVTI) — 動態虛擬隧道介面可用於終止沒有固定隧道目標的動態IPsec隧道。成功進行通

道交涉後，虛擬訪問介面將從虛擬模板克隆，並將繼承該虛擬模板上的所有L3功能。以下是dVTI配置的示例：

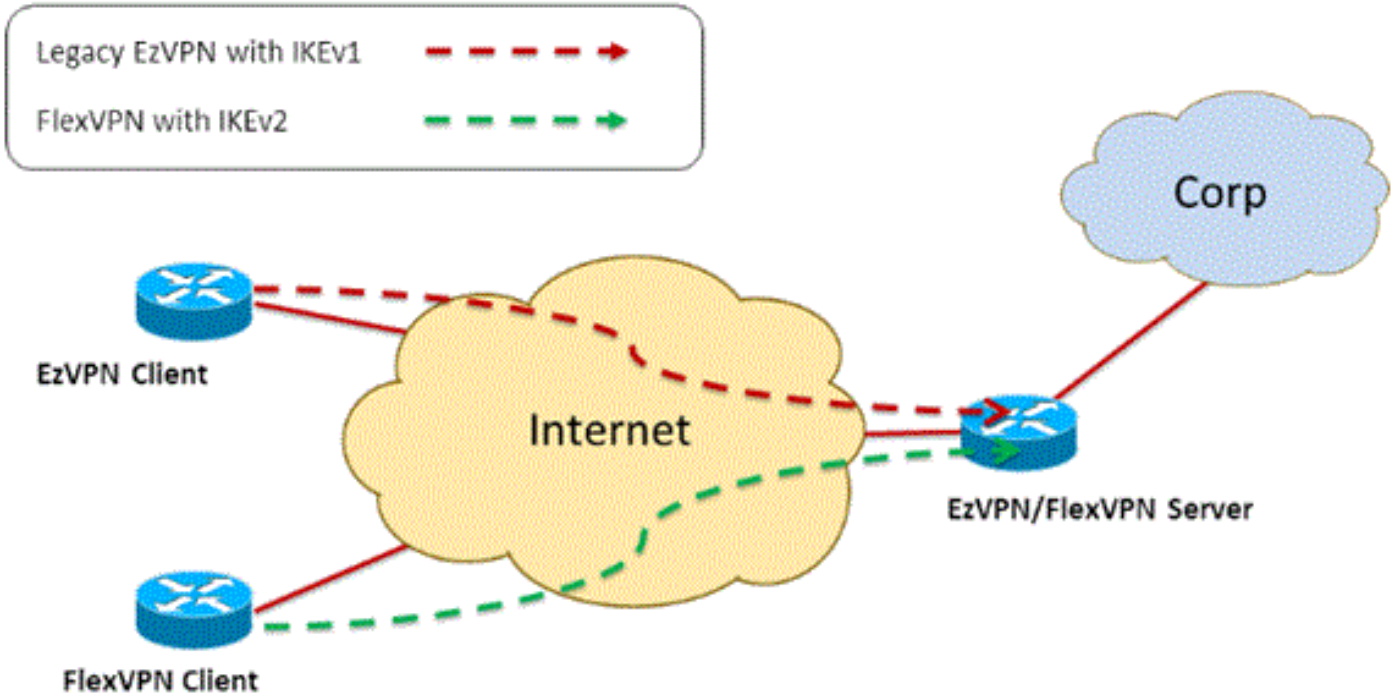
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

有關dVTI的詳細資訊，請參閱以下文檔：

- 使用IPSec動態虛擬通道介面(DVTI)配置Cisco Easy VPN
- IPsec虛擬通道介面的限制
- 為使用IKEv1的動態虛擬通道介面配置多SA支援

要使EzVPN和FlexVPN客戶端共存，您必須首先將EzVPN伺服器從舊版加密對映配置遷移到dVTI配置。以下各節詳細說明了必要步驟。

網路拓撲



使用傳統NEM+模式EzVPN客戶端的當前配置

客戶端配置

以下是典型的EzVPN客戶端路由器配置。在此配置中，使用Network Extension Plus(NEM+)模式，該模式為LAN內部介面以及模式配置為客戶端分配的IP地址建立多個SA對。

```
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
```

伺服器配置

在EzVPN伺服器上，在遷移之前使用舊版加密對映配置作為基本配置。

```
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
```

將伺服器遷移到FlexVPN

如前幾節所述，FlexVPN使用IKEv2作為控制平面協定，並且不向後相容基於IKEv1的EzVPN解決方

案。因此，此遷移的一般想法是配置現有EzVPN伺服器，使其允許舊式EzVPN(IKEv1)和FlexVPN(IKEv2)共存。為了實現這一目標，您可以使用以下兩步遷移方法：

1. 將頭端上的傳統EzVPN配置從基於加密對映的配置移動到dVTI。
2. 新增FlexVPN配置，該配置也基於dVTI。

將舊版加密對映移動到dVTI

伺服器配置更改

在物理介面上配置了加密對映的EzVPN伺服器在功能支援和靈活性方面包含幾個限制。如果您有EzVPN，思科強烈建議您改用dVTI。作為遷移到共存的EzVPN和FlexVPN配置的第一步，您必須將其更改為dVTI配置。這將在不同虛擬模板介面之間提供IKEv1和IKEv2分離，以便同時容納這兩種型別的客戶端。

注意：要在EzVPN客戶端上支援EzVPN的網路擴展增強模式，頭端路由器必須支援dVTI上的多SA功能。這允許通道保護多個IP流，這是頭端加密通往EzVPN客戶端內部網路的流量，以及通過IKEv1模式配置分配給客戶端的IP地址所必需的。有關使用IKEv1的dVTI上的多SA支援的詳細資訊，請參閱IKEv1的動態虛擬通道介面的多SA支援。

完成以下步驟，以在伺服器上實施配置更改：

第1步 — 從終止EzVPN客戶端隧道的物理出口介面刪除加密對映：

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

第2步 — 建立虛擬模板介面，在建立隧道後，將從該介面克隆虛擬訪問介面：

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

第3步 — 將新建立的虛擬模板介面與配置的EzVPN組的isakmp配置檔案相關聯：

```
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
```

進行上述配置更改後，驗證現有EzVPN客戶端是否繼續工作。但是，現在它們的隧道在動態建立的虛擬訪問介面上終止。這可透過**show crypto session**命令驗證，如下例所示：

```
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
```

將FlexVPN配置新增到伺服器

此示例在FlexVPN客戶端和伺服器上都使用RSA-SIG（即證書頒發機構）。本節中的配置假定伺服器已成功通過CA伺服器身份驗證並註冊。

步驟1 — 驗證IKEv2智慧預設配置。

藉助IKEv2，您現在可以利用在15.2(1)T中引入的智慧預設功能。它用於簡化FlexVPN配置。以下是一些預設設定：

預設IKEv2授權策略：

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

預設IKEv2提議：

```
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
```

預設IKEv2策略：

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

預設IPsec配置檔案：

```
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 } ,
 }
```

預設IPsec轉換集：

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

有關IKEv2智慧預設功能的詳細資訊，請參閱IKEv2智慧預設值(僅限註冊客戶)。

第2步 — 修改FlexVPN客戶端的預設IKEv2授權策略並新增預設IKEv2配置檔案。

此處建立的IKEv2配置檔案將在基於域名cisco.com的對等ID上匹配，並且為客戶端建立的虛擬訪問介面將衍生自虛擬模板2。另請注意，授權策略定義了用於分配對等IP地址的IP地址池，以及要通過IKEv2配置模式交換的路由：

```
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
```

步驟3 — 建立用於FlexVPN客戶端的虛擬模板介面：

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

FlexVPN客戶端配置

```
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
```

完成配置

完成混合伺服器配置

```
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
```

完成IKEv1 EzVPN客戶端配置

```
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
```

完成IKEv2 FlexVPN客戶端配置

```
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
```

組態驗證

以下是用於驗證路由器上EzVPN/FlexVPN操作的一些命令：

```
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
```

相關資訊

- 技術支援與文件 - Cisco Systems