在同一服务器上从传统EzVPN-NEM+迁移到FlexVPN

目录

简介

本文档介绍从EzVPN到FlexVPN的迁移过程。FlexVPN是思科提供的新统一VPN解决方案。FlexVPN利用IKEv2协议，将远程访问、站点到站点、中心和分支以及部分网状VPN部署相结合。借助EzVPN等传统技术，思科强烈鼓励您迁移至FlexVPN，以利用其功能丰富的功能。

本文档将检查现有EzVPN部署，该部署由基于传统加密映射的EzVPN头端设备上终止隧道的传统EzVPN硬件客户端组成。目标是从此配置迁移，以支持满足以下要求的FlexVPN:

- 现有传统客户端将继续无缝工作，无需更改任何配置。这允许随着时间推移将这些客户端分阶段迁移到FlexVPN。
- 头端设备应同时支持终止新的FlexVPN客户端。

为帮助实现这些迁移目标，使用了两个关键IPsec配置组件：即IKEv2和虚拟隧道接口(VTI)。 本文档将简要讨论这些目标。

此系列中的其他文档

- FlexVPN部署指南：使用IKEv2和证书通过IPsec连接到IOS头端

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

IKEv1与IKEv2

FlexVPN基于IKEv2协议（IKEv2协议是基于RFC 4306的下一代密钥管理协议）和IKEv1协议的增强功能。FlexVPN不向后兼容仅支持IKEv1（例如EzVPN）的技术。 这是从EzVPN迁移到FlexVPN时的主要考虑事项之一。有关IKEv2协议简介和与IKEv1的比较，请一眼看IKE第2版。

加密映射与虚拟隧道接口

虚拟隧道接口(VTI)是一种新的配置方法，用于VPN服务器和客户端配置。VTI:

- 替换为动态加密映射，现在被视为旧配置。
- 支持本地IPsec隧道。
- 不需要IPsec会话到物理接口的静态映射；因此，可以灵活地在任何物理接口（例如，多条路径）上发送和接收加密流量。
- 从虚拟模板接口克隆按需虚拟访问时的最低配置。
- 当转发到/从隧道接口时，流量会被加密/解密，并由IP路由表管理（因此，在加密过程中起着重要作用）。
- 功能可以应用于VTI接口上的明文数据包，也可以应用于物理接口上的加密数据包。

可用的两种VTI类型是：

- 静态(sVTI) — 静态虚拟隧道接口具有固定的隧道源和目标，通常用于站点到站点部署场景。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
```

- 动态(dVTI) — 动态虚拟隧道接口可用于终止没有固定隧道目标的动态IPsec隧道。隧道协商成

功后，虚拟访问接口将从虚拟模板克隆，并继承该虚拟模板上的所有L3功能。以下是dVTI配置的示例：

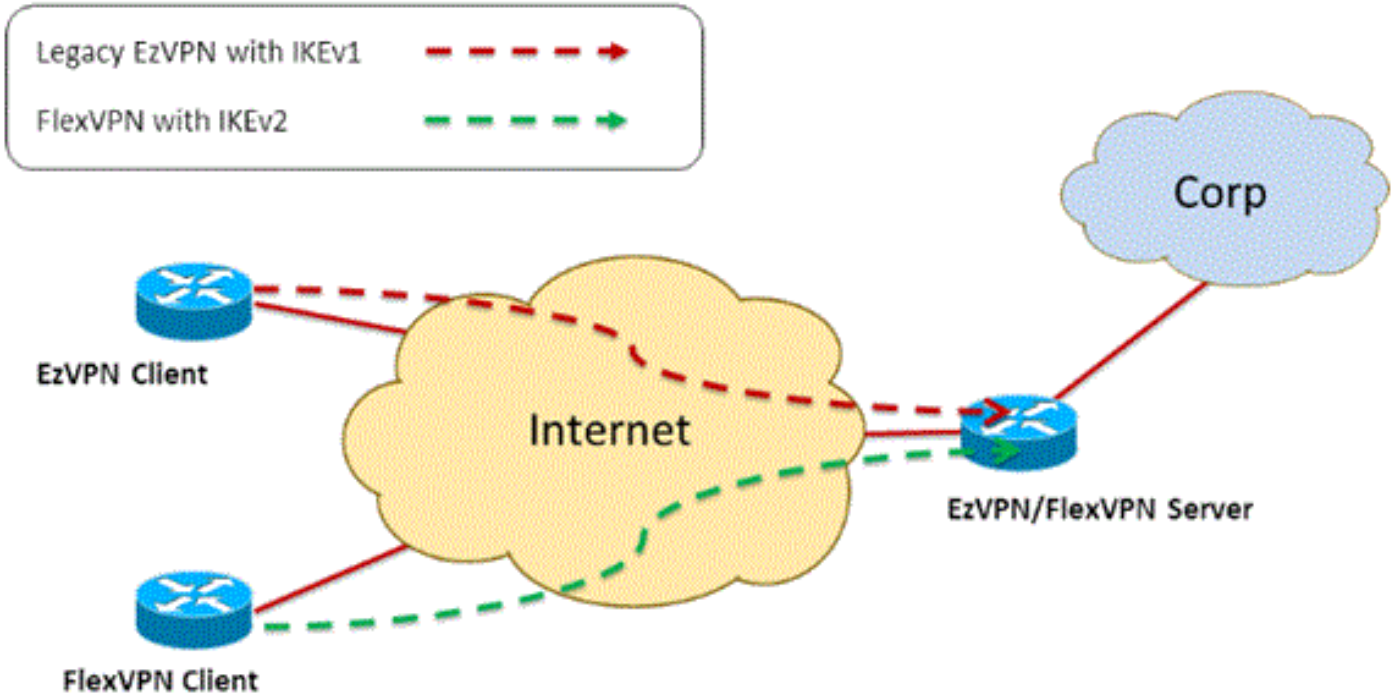
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

有关dVTI的详细信息，请参阅以下文档：

- 配置带IPSec动态虚拟隧道接口(DVTI)的Cisco Easy VPN
- IPsec虚拟隧道接口的限制
- 使用IKEv1配置动态虚拟隧道接口的多SA支持

要使EzVPN和FlexVPN客户端共存，必须先将EzVPN服务器从传统加密映射配置迁移到dVTI配置。以下各节详细说明了必要的步骤。

网络拓扑



使用传统NEM+模式EzVPN客户端的当前配置

客户端配置

以下是典型的EzVPN客户端路由器配置。在此配置中，使用Network Extension Plus(NEM+)模式，这为LAN内部接口和为客户端分配的IP地址的模式配置创建多个SA对。

```
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
```

服务器配置

在EzVPN服务器上，迁移前使用传统加密映射配置作为基本配置。

```
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
```

服务器迁移到FlexVPN

如前几节所述，FlexVPN使用IKEv2作为控制层协议，并且不向后兼容基于IKEv1的EzVPN解决方案

。因此，此迁移的一般思想是配置现有EzVPN服务器，使其允许旧版EzVPN(IKEv1)和FlexVPN(IKEv2)共存。为了实现此目标，您可以使用以下两步迁移方法：

1. 将头端上的传统EzVPN配置从基于加密映射的配置移至dVTI。
2. 添加FlexVPN配置，该配置也基于dVTI。

将传统加密映射移至dVTI

服务器配置更改

在物理接口上配置了加密映射的EzVPN服务器在功能支持和灵活性方面存在一些限制。如果您有EzVPN，思科强烈建议您改用dVTI。作为迁移到共存EzVPN和FlexVPN配置的第一步，您必须将其更改为dVTI配置。这将提供不同虚拟模板接口之间的IKEv1和IKEv2分离，以便支持这两种类型的客户端。

注意：要支持EzVPN客户端上EzVPN操作的网络扩展加模式，头端路由器必须支持dVTI上的多SA功能。这允许多个IP流受隧道保护，隧道是头端加密到EzVPN客户端内部网络的流量所必需的，也是通过IKEv1模式配置分配给客户端的IP地址。有关在带IKEv1的dVTI上支持多SA的详细信息，请参阅对IKEv1的动态虚拟隧道接口支持多SA。

要在服务器上实施配置更改，请完成以下步骤：

第1步 — 从终止EzVPN客户端隧道的物理出口接口删除加密映射：

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

第2步 — 创建虚拟模板接口，一旦建立隧道，将从其克隆虚拟访问接口：

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

第3步 — 将此新创建的虚拟模板接口关联到已配置EzVPN组的isakmp配置文件：

```
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
```

完成上述配置更改后，验证现有EzVPN客户端是否继续工作。但是，现在它们的隧道在动态创建的虚拟访问接口上终止。这可以通过show crypto session**命令**进行验证，如本例所示：

```
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
```

将FlexVPN配置添加到服务器

本示例在FlexVPN客户端和服务器上都使用RSA-SIG（即证书颁发机构）。本节中的配置假设服务器已成功通过身份验证并注册到CA服务器。

第1步 — 检验IKEv2智能默认配置。

使用IKEv2，您现在可以利用15.2(1)T中引入的智能默认功能。它用于简化FlexVPN配置。以下是一些默认配置：

默认IKEv2授权策略：

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

默认IKEv2建议：

```
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
```

默认IKEv2策略：

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

默认IPsec配置文件：

```
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 } ,
 }
```

默认IPsec转换集：

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

有关IKEv2智能默认功能的详细信息，请参阅IKEv2智能默认(仅注册客户)。

第2步 — 修改默认IKEv2授权策略并为FlexVPN客户端添加默认IKEv2配置文件。

此处创建的IKEv2配置文件将基于域名cisco.com在对等ID上匹配，为客户端创建的虚拟访问接口将从虚拟模板2衍生出来。另请注意，授权策略定义用于分配对等IP地址的IP地址池以及通过IKEv2配置模式交换的路由：

```
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
```

第3步 — 创建用于FlexVPN客户端的虚拟模板接口：

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

FlexVPN客户端配置

```
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

完整的混合服务器配置

```
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客户端配置

```
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客户端配置

```
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
```

配置验证

以下是用于验证路由器上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
```

相关信息

- 技术支持和文档 - Cisco Systems