FlexVPN迁移：传统EzVPNNEM+和FlexVPN在同一个服务器

目录

简介

本文描述从EzVPN的迁移进程到FlexVPN。FlexVPN是思科提供的新的统一的VPN解决方案。FlexVPN利用IKEv2协议并且结合远程访问，站点到站点，星型网和部分网状VPN部署。使用传统技术类似EzVPN，思科严格鼓励您移植到FlexVPN为了利用其丰富的特性功能。

本文检查包括传统EzVPN硬件客户端终止在传统加密映射基于EzVPN数据转发设备的通道的一现有EzVPN部署。目标是移植从此配置支持与这些需求的FlexVPN ：

- 现有传统客户端将继续工作无缝地，不用任何配置更改。这随着时间的推移允许这些客户端的被逐步采用的迁移对FlexVPN。
- 数据转发设备应该同时支持新的FlexVPN客户端的终端。

两个关键IPSec配置组件用于为了帮助实现这些迁移目标：即， IKEv2和虚拟隧道接口(VTI)。这些目标在本文简要地讨论。

其他文档此系列

- FlexVPN部署指南：对IOS头端的AnyConnect在与IKEv2和证书的IPsec

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根据IKEv2协议，是根据RFC 4306的下一代密钥管理协议和IKEv1协议的增强。FlexVPN与例如支持仅IKEv1的技术不是向后兼容的(EzVPN)。当您从EzVPN移植到FlexVPN时，这是其中一关键考虑事项。对于在IKEv2的一协议介绍和比较跟IKEv1，一览参考IKE版本2。

加密映射与虚拟隧道接口

虚拟隧道接口(VTI)是用于VPN服务器和客户端配置的一个新的配置方法。VTI ：

- 对动态加密映射的更换，当前认为传统配置。
- 支持本地IPSec建立隧道。
- 不要求IPSec会话的静态映射对物理接口;因此，提供灵活性发送和收到在任何物理接口的加密流量(例如，多条路径)。
- 最小配置作为根据要求虚拟访问从虚拟模板接口被克隆。
- 流量由IP路由表加密/解密，当到/从隧道接口的转发和管理(从而，播放在加密进程的一重要的角色)。
- 功能可能应用到在VTI接口或者加密的信息包的明文数据包在物理接口。

VTIs联机的两种类型是：

- 静态(sVTI) —一个静态虚拟隧道接口有一个已修复隧道源及目的地和典型地用于一个站点到站点部署方案。这是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) —一个动态虚拟隧道接口可以用于终止没有已修复隧道目的地的动态IPSec隧道。在成功的隧道协商，虚拟访问接口从虚拟模板将被克隆，并且请继承在该虚拟模板的所有L3功能。这是dVTI配置的示例：`interface Virtual-Template1 type tunnel`

```
     ip unnumbered Ethernet0/1
     tunnel mode ipsec ipv4
     tunnel protection ipsec profile testflex
```

参考这些文档关于dVTI的更多信息：

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

为了EzVPN和FlexVPN客户端能共存，您必须首先移植从传统加密映射配置的EzVPN服务器到dVTI配置。以下部分详细说明必要的步骤。

网络拓扑

与传统NEM+模式EzVPN客户端的当前配置

客户端配置

下面一个典型的EzVPN客户端路由器配置。在此配置中，加上(NEM+)模式使用网络范围，创建LAN内部接口以及模式配置指定的IP地址的多个SA对客户端的。

```
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，传统加密映射配置使用作为在迁移前的基本配置。

```
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
```

服务器的迁移对FlexVPN的

正如前面部分所描述， FlexVPN使用IKEv2作为控制层面协议并且与IKEv1-based EzVPN解决方案不是向后兼容的。结果，此迁移一般想法是配置现有EzVPN服务器，在这种情况下允许传统EzVPN (IKEv1)和FlexVPN (IKEv2)共存。为了达到此目标，您能使用此两步迁移方法：

1. 移动在头端的传统EzVPN配置从加密映射基于配置向dVTI。
2. 添加FlexVPN配置，根据dVTI也。

移动传统加密映射向dVTI

服务器配置配置更改

EzVPN服务器配置与在物理接口的加密映射包括几个限制当谈到功能支持和灵活性。如果有EzVPN，思科严格鼓励您使用dVTI。首先移植到一共存的EzVPN和FlexVPN配置，您必须更改它到dVTI配置。这将提供IKEv1和IKEv2区别虚拟模板接口之间的分离为了适应客户端两个类型。

注意： 为了支持网络范围加上EzVPN操作模式在EzVPN客户端的，数据转发路由器必须有多的SA支持在dVTI功能。这允许通道，要求为了头端能加密流量到EzVPN客户端的网络内部，以及IP地址将保护的多个IP流分配到客户端通过IKEv1模式配置。关于在dVTI的SA多支持的更多信息与IKEv1，动态虚拟隧道接口的参考的多SA支持IKEv1的。

完成这些步骤为了实现在服务器的配置更改：

Step1 —从终止EzVPN客户端通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
```

步骤2 —创建虚拟访问接口一次将被克隆通道设立的虚拟模板接口：

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

步骤3 —关联此新建立的虚拟模板接口对已配置的EzVPN组的ISAKMP简档：

```
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
```

一旦上述配置更改做，请验证现有EzVPN客户端继续工作。然而，他们的通道在一个动态地已创建虚拟访问接口当前终止。这可以用**显示crypto session命令**验证正如在此示例：

```
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
```

添加FlexVPN配置到服务器

此示例在两个使用RSA-SIG (即认证机关) FlexVPN客户端和服务器。在此部分的配置假设，服务器用CA服务器已经顺利地验证并且登记。

Step1 —验证IKEv2聪明的默认配置。

使用IKEv2，您能当前利用在15.2(1)T介绍的聪明的默认功能。它用于简单化FlexVPN配置。这是一些默认配置：

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 } , }
```

设置的默认IPSec转换：

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

关于IKEv2聪明的默认功能的更多信息，参考IKEv2聪明的默认(仅限注册用户)。

步骤2 —修改默认IKEv2授权策略并且添加FlexVPN客户端的默认IKEv2配置文件。

创建的IKEv2配置文件此处在根据域名的对等体ID配比cisco.com，并且为客户端创建的虚拟访问接口将产生虚拟模板2。并且请注释授权策略定义了分配对等体IP地址以及路由使用的IP地址池将交换通过IKEv2配置模式：

```
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
```

步骤3 —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
```

完整的配置

完整混合的服务器配置

```
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
```

完整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
```

完整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

这是用于的某些命令验证在路由器的EzVPN/FlexVPN操作：

```
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