Migración de FlexVPN: Herencia EzVPN-NEM+ y FlexVPN en el mismo servidor

Contenido

Introducción

Este documento describe el proceso de migración del EzVPN a FlexVPN. FlexVPN es la nueva solución de VPN unificada ofrecida por Cisco. FlexVPN se aprovecha del protocolo IKEv2 y combina el Acceso Remoto, el sitio a localizar, el hub and spoke, y los despliegues de VPN de la Interconexión parcial. Con las Tecnologías de la herencia como el EzVPN, Cisco le anima fuertemente a emigrar a FlexVPN para aprovecharse de sus capacidades de los ricos de la característica.

Este documento examina un despliegue existente del EzVPN que consista en los hardwares cliente del EzVPN de la herencia que terminan los túneles en un dispositivo de cabecera basado correspondencia de criptografía del EzVPN de la herencia. La meta es emigrar de esta configuración para soportar FlexVPN con estos requisitos:

- Los clientes existentes de la herencia continuarán trabajando el seamlessly sin ningunos

cambios de configuración. Esto permite una migración organizada de estos clientes a FlexVPN en un cierto plazo.
- El dispositivo de cabecera debe soportar simultáneamente la terminación de los nuevos clientes de FlexVPN.

Dos componentes dominantes de la configuración IPSec se utilizan para ayudar a lograr estas metas de la migración: a saber, IKEv2 y interfaces del túnel virtuales (VTI). Estas metas se discuten abreviadamente en este documento.

Otros documentos en esta serie

- Guía de despliegue de FlexVPN: AnyConnect al headend IOS sobre el IPSec con IKEv2 y los Certificados

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

IKEv1 contra IKEv2

FlexVPN se basa en el protocolo IKEv2, que es el Key Management Protocol de la última generación basado en el RFC 4306, y una mejora del protocolo IKEv1. FlexVPN no es compatible con versiones anteriores con las Tecnologías que soportan solamente IKEv1 (por ejemplo, EzVPN). Éste es una de las consideraciones dominantes cuando usted emigra del EzVPN a FlexVPN. Para una introducción del protocolo en IKEv2 y la comparación con IKEv1, refiera a la versión 2 IKE de un vistazo.

Correspondencia de criptografía contra las interfaces del túnel virtuales

La interfaz del túnel virtual (VTI) es un nuevo método de configuración usado para el servidor VPN y las configuraciones del cliente. VTI:

- Reemplazo a las correspondencias cifradas dinámicas, que ahora se considera configuración heredada.
- Apoya al natural tunelización de IPSec.

- No requiere una correlación estática del sesión IPSec a una interfaz física; por lo tanto, proporciona la flexibilidad para enviar y para recibir el tráfico encriptado en cualquier interfaz física (por ejemplo, los trayectos múltiples).
- La configuración mínima como acceso virtual a pedido se reproduce de la interfaz de plantilla virtual.
- El tráfico es cifrado/desencriptado cuando es delantero a/desde la interfaz del túnel y es manejado por la tabla de IP Routing (de tal modo, desempeñando un papel importante en el proceso del cifrado).
- Las características se pueden cualquiera aplicar a los paquetes del texto claro en la interfaz VTI, o los paquetes encriptados en la interfaz física.

Los dos tipos de VTIs disponibles son:

- Estático (sVTI) — Una interfaz del túnel virtual estática tiene un origen y destino del túnel fijo y se utiliza típicamente en un escenario de instrumentación del sitio a localizar. Aquí está un ejemplo de una configuración del 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
```
- Dinámico (dVTI) — Una interfaz del túnel virtual dinámica se puede utilizar para terminar los túneles IPsec dinámicos que no tienen un destino del túnel fijo. Sobre la negociación de túnel acertada, las interfaces de acceso virtual serán reproducidas de una Virtual-plantilla y heredarán todas las características L3 en esa Virtual-plantilla. Aquí está un ejemplo de una configuración del dVTI:
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Refiera a estos documentos para más información sobre el dVTI:

- Configurando el Cisco Easy VPN con la interfaz del túnel virtual dinámica del IPSec (DVTI)
- Restricciones de IPsec Virtual Tunnel Interface
- Configurar el soporte Multi-SA para las interfaces del túnel virtuales dinámicas usando IKEv1

Para que los clientes del EzVPN y de FlexVPN coexistan, usted debe primero emigrar al servidor EzVPN de la configuración de la correspondencia de criptografía de la herencia a una configuración del dVTI. Las secciones siguientes explican detalladamente los pasos necesarios.

Topología de red

Configuración actual con el cliente EzVPN del modo de la herencia NEM+

Configuración del cliente

Abajo está una configuración del router típica del cliente EzVPN. En esta configuración, la extensión de la red más el modo (NEM+) se utiliza, que crea los pares múltiples SA para las interfaces interiores LAN así como el IP Address asignado de la configuración de modo para el cliente.

```
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
```

Configuración del servidor

En el servidor EzVPN, una configuración de la correspondencia de criptografía de la herencia se utiliza como la configuración baja antes de la migración.

```
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
```

Migración del servidor a FlexVPN

Según lo descrito en las secciones anteriores, FlexVPN utiliza IKEv2 como el protocolo del avión del control y no es compatible con versiones anteriores con una solución del EzVPN IKEv1-based. Como consecuencia, la idea general de esta migración es configurar al servidor EzVPN existente de una manera tal que permita que coexistan el EzVPN de la herencia (IKEv1) y FlexVPN (IKEv2). Para alcanzar esta meta, usted puede utilizar este acercamiento de dos etapas de la migración:

1. Mueva la configuración del EzVPN de la herencia en el headend desde una configuración basada correspondencia de criptografía al dVTI.
2. Agregue la configuración de FlexVPN, que también se basa en el dVTI.

Mueva la correspondencia de criptografía de la herencia al dVTI

Cambios de Configuración del servidor

Un servidor EzVPN configurado con la correspondencia de criptografía en la interfaz física incluye varias limitaciones cuando se trata del soporte de característica y de la flexibilidad. Si usted tiene EzVPN, Cisco le anima fuertemente a utilizar el dVTI en lugar de otro. En primer lugar para emigrar a una configuración coexistente del EzVPN y de FlexVPN, usted debe cambiarla a una configuración del dVTI. Esto proporcionará la separación IKEv1 e IKEv2 entre las diversas interfaces de plantilla virtual para acomodar ambos tipos de clientes.

Nota: Para soportar la extensión de la red más el modo de operación del EzVPN en los clientes EzVPN, el router de cabecera debe tener soporte para el SA multi en la característica del dVTI. Esto permite que IP múltiple los flujos sean protegidos por el túnel, que se requiere para que el headend cifre el tráfico a la red interna del cliente EzVPN, así como el dirección IP asignada al cliente con la configuración de modo IKEv1. Para más información sobre el soporte multi SA en el dVTI con IKEv1, refiera al soporte Multi-SA para las interfaces del túnel virtuales dinámicas para IKEv1.

Complete estos pasos para implementar el cambio de configuración en el servidor:

Paso 1 — Quite la correspondencia de criptografía de la interfaz de egreso física que termina los túneles del cliente EzVPN:

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

Paso 2 — Cree una interfaz de plantilla virtual de la cual se establezcan las interfaces de acceso virtual sean reproducidas una vez los túneles:

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

Paso 3 — Asocie esta interfaz de plantilla virtual creada recientemente al perfil del isakmp para el grupo configurado del EzVPN:

```
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
```

Los cambios de configuración antedichos se realizan, verifican una vez que los clientes EzVPN existentes continúan trabajando. Sin embargo, ahora sus túneles se terminan en una interfaz de acceso virtual dinámicamente creada. Esto se puede verificar con el comando de **sesión de criptografía de la demostración** como en este ejemplo:

```
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
```

Agregue la configuración de FlexVPN al servidor

Este ejemplo utiliza RSA-SIG (es decir, Certificate Authority) en ambos el cliente y servidor de FlexVPN. La configuración en esta sección asume que el servidor ha autenticado y ha alistado ya con éxito con el servidor de CA.

Paso 1 — Verifique la configuración predeterminada IKEv2 Smart.

Con IKEv2, usted puede ahora aprovecharse de la función predeterminada elegante introducida en 15.2(1)T. Se utiliza para simplificar una configuración de FlexVPN. Aquí están algunas configuraciones predeterminadas:

Directiva predeterminada de la autorización IKEv2:

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

Oferta predeterminada IKEv2:

```
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
```

Directiva predeterminada IKEv2:

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

IPSec predeterminada perfil:

```
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 } , }
```

IPSec predeterminada transforme el conjunto:

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

Para más información sobre la función predeterminada elegante IKEv2, refiera a los valores por defecto elegantes IKEv2 (clientes registrados solamente).

Paso 2 — Modifique la directiva de la autorización del valor por defecto IKEv2 y agregue un perfil del valor por defecto IKEv2 para los clientes de FlexVPN.

El perfil IKEv2 creado aquí hará juego en un Id de peer basado en el Domain Name cisco.com y las interfaces de acceso virtual creadas para los clientes serán spawn/generadas apagado de la plantilla virtual 2. También observe la directiva de la autorización define el pool de la dirección IP usado para asignar los IP Address de Peer así como las rutas que se intercambiarán vía el modo de configuración 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
```

Paso 3 — Cree la interfaz de plantilla virtual usada para los clientes de FlexVPN:

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

Configuración del cliente de 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
```

Configuración completada

Configuración del servidor híbrida completa

```
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
```

Configuración de cliente EzVPN completa 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
```

Configuración del cliente completa IKEv2 FlexVPN

```
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
```

Verificación de la configuración

Aquí están algunos de los comandos usados para verificar las operaciones del EzVPN/de FlexVPN en 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
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems