Migração de FlexVPN: Legado EzVPN-NEM+ e FlexVPN no mesmo server

Índice

Introdução

Este documento descreve o processo de migração do EzVPN a FlexVPN. FlexVPN é a solução de VPN unificada nova oferecida por Cisco. FlexVPN aproveita-se do protocolo IKEv2 e combina-se o Acesso remoto, a site para site, o hub and spoke, e as distribuições VPN da malha parcial. Com Tecnologias do legado como o EzVPN, Cisco incentiva-o fortemente migrar a FlexVPN a fim aproveitar-se de suas capacidades ricos em características.

Este documento examina um desenvolvimento existente do EzVPN que consista nos clientes da ferragem do EzVPN do legado que terminam túneis em um dispositivo de fim de cabeçalho baseado em mapas cripto do EzVPN do legado. O objetivo é migrar desta configuração para apoiar FlexVPN com estas exigências:

- Os clientes existentes do legado continuarão a trabalhar continuamente sem nenhumas alterações de configuração. Isto permite uma migração posta em fase destes clientes a

FlexVPN ao longo do tempo.
- O dispositivo de fim de cabeçalho deve simultaneamente apoiar a terminação de clientes novos de FlexVPN.

Dois componentes chaves da configuração IPSec são usados a fim ajudar a realizar estes objetivos da migração: a saber, IKEv2 e interfaces de túnel virtuais (VTI). Estes objetivos são discutidos momentaneamente neste documento.

Outros documentos nesta série

- Guia de distribuição de FlexVPN: AnyConnect ao final do cabeçalho IO sobre o IPsec com IKEv2 e Certificados

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

IKEv1 contra IKEv2

FlexVPN é baseado no protocolo IKEv2, que é o protocolo do gerenciamento de chave da próxima geração baseado no RFC 4306, e em um realce do protocolo IKEv1. FlexVPN não é para trás-compatível com Tecnologias que apoiam somente IKEv1 (por exemplo, EzVPN). Esta é uma das considerações chaves quando você migra do EzVPN a FlexVPN. Para uma introdução do protocolo em IKEv2 e a comparação com IKEv1, refira a versão 2 IKE duma olhada.

Crypto map contra interfaces de túnel virtuais

A interface de túnel virtual (VTI) é um método de configuração novo usado para o servidor de VPN e as configurações de cliente. VTI:

- Substituição aos mapas cripto dinâmico, que é considerada agora configuração legada.
- Apoia o tunelamento de IPSec nativo.
- Não exige um mapeamento estático de uma sessão IPSec a uma interface física; , fornece consequentemente a flexibilidade enviar e receber o tráfego criptografado em toda a interface física (por exemplo, caminhos múltiplos).
- A configuração mínima como o acesso virtual por encomenda é clonada da interface de molde virtual.

- O tráfego é cifrado/decifrado quando dianteiro para/desde a interface de túnel e é controlado pela tabela de IP Routing (desse modo, jogando um papel importante no processo da criptografia).
- As características podem ser aplicadas aos pacotes da minuta na relação VTI, ou em pacotes criptografado na interface física.

Os dois tipos de VTIs disponíveis são:

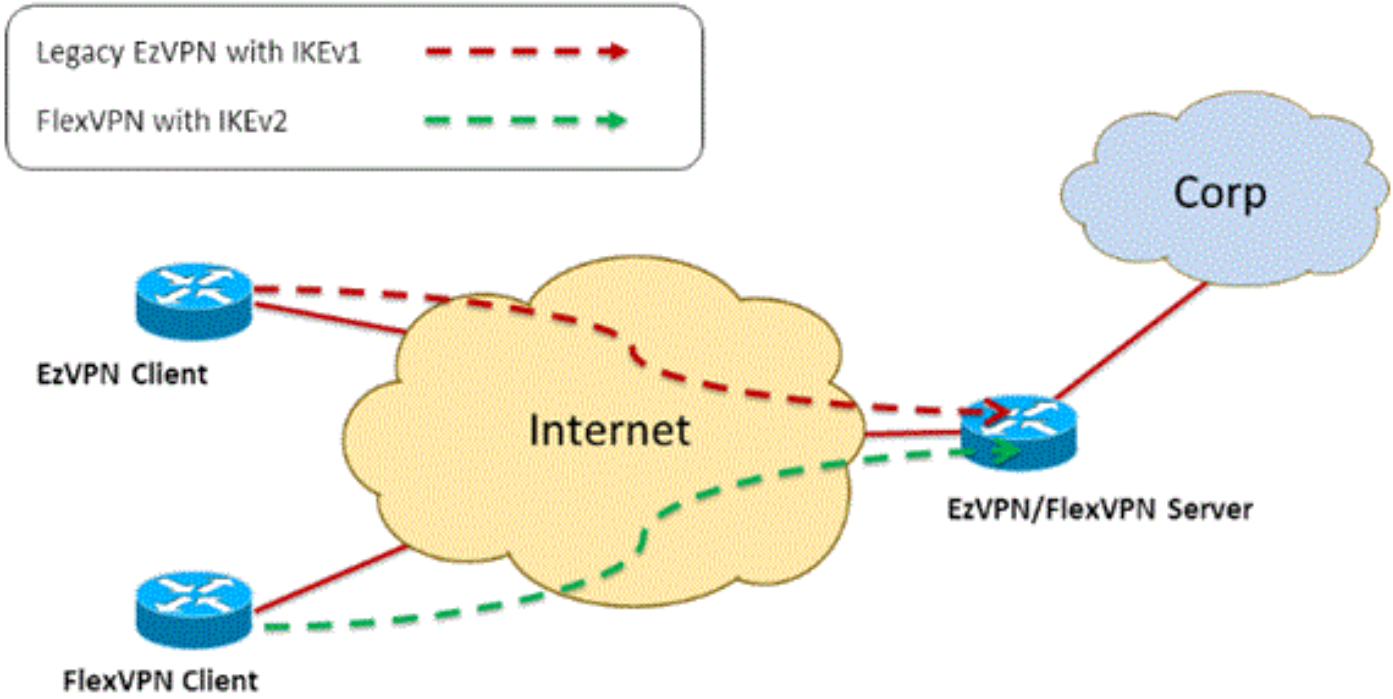
- Estático (sVTI) — Uma interface de túnel virtual estática tem um origem e destino do túnel fixo e é usada tipicamente em um cenário de distribuição de site para site. Está aqui um exemplo de uma configuração do sVTI:
```
interface Tunnel2
 ip address negotiated
 tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile testflex
```
- Dinâmico (dVTI) — Uma interface de túnel virtual dinâmica pode ser usada para terminar os túneis de IPsec dinâmicos que não têm um destino de túnel fixo. Em cima da negociação do túnel bem sucedida, as interfaces de acesso virtual serão clonadas de um Virtual-molde e herdarão todas as características L3 nesse Virtual-molde. Está aqui um exemplo de uma configuração do dVTI:
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Refira estes documentos para obter mais informações sobre do dVTI:

- Configurando o Cisco Easy VPN com interface de túnel virtual dinâmica do IPsec (DVTI)
- Limitações para a interface de túnel virtual do IPsec
- Configurando o apoio Multi-SA para interfaces de túnel virtuais dinâmicas usando IKEv1

Para que os clientes do EzVPN e do FlexVPN coexistam, você deve primeiramente migrar o servidor de EzVPN da configuração do crypto map do legado a uma configuração do dVTI. As seguintes seções explicam em detalhe as etapas necessárias.

Topologia de rede



Configuração atual com o cliente ezvpn do modo do legado NEM+

Configuração de cliente

Está abaixo uma configuração de roteador típica do cliente ezvpn. Nesta configuração, a extensão de rede mais o modo (NEM+) é usada, que cria pares múltiplos SA para as interfaces internas LAN assim como o endereço IP atribuído da configuração de modo para o 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
```

Configuração do servidor

No servidor de EzVPN, uma configuração do crypto map do legado é usada como a configuração baixa antes da migração.

```
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
```

Migração do server a FlexVPN

Como descrito nas seções anterior, FlexVPN usa IKEv2 como o protocolo do plano do controle e não é inverso - compatível com uma solução do EzVPN IKEv1-based. Em consequência, a ideia geral desta migração é configurar o servidor de EzVPN existente de tal maneira que permite que o EzVPN do legado (IKEv1) e FlexVPN (IKEv2) coexistam. A fim conseguir este objetivo, você pode usar esta aproximação da migração do pas-de-deux:

1. Mova a configuração do EzVPN do legado no final do cabeçalho de uma configuração baseada em mapas cripto para o dVTI.
2. Adicionar a configuração de FlexVPN, que é baseada igualmente no dVTI.

Mova o crypto map do legado para o dVTI

Mudanças de configuração do servidor

Um servidor de EzVPN configurado com o crypto map na interface física inclui diversas limitações quando se trata do suporte de recurso e da flexibilidade. Se você tem o EzVPN, Cisco incentiva-o fortemente usar pelo contrário o dVTI. Em primeiro para migrar a uma configuração de coexistência do EzVPN e do FlexVPN, você deve mudá-la a uma configuração do dVTI. Isto

fornecerá a separação IKEv1 e IKEv2 entre as interfaces de molde virtual diferentes a fim acomodar ambos os tipos de clientes.

Nota: A fim apoiar a extensão de rede mais o modo de operação do EzVPN nos clientes ezvpn, o roteador do fim do cabeçalho deve ter o apoio para o multi SA na característica do dVTI. Isto permite que os fluxos múltiplos IP sejam protegidos pelo túnel, que é exigido para que o final do cabeçalho cifre o tráfego à rede interna do cliente ezvpn, assim como o pelo endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído ao cliente com o config de modo IKEv1. Para obter mais informações sobre do multi apoio SA no dVTI com IKEv1, refira o apoio Multi-SA para interfaces de túnel virtuais dinâmicas para IKEv1.

Termine estas etapas a fim executar a alteração de configuração no server:

Etapa 1 — Remova o crypto map da interface de saída física que termina os túneis do cliente ezvpn:

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

Etapa 2 — Crie uma interface de molde virtual de que as interfaces de acesso virtual serão clonadas uma vez os túneis são estabelecidas:

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

Etapa 3 — Associe esta relação virtual do molde recém-criado ao perfil do isakmp para o grupo configurado do 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
```

Uma vez as alterações de configuração acima são feitas, verificam que os clientes ezvpn existentes continuam a trabalhar. Contudo, seus túneis são terminados agora em uma interface de acesso virtual dinamicamente criada. Isto pode ser verificado com o comando de **sessão de criptografia da mostra** como neste exemplo:

```
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
```

Adicionar a configuração de FlexVPN ao server

Este exemplo usa RSA-SIG (isto é, Certificate Authority) em ambos o cliente e servidor de FlexVPN. A configuração nesta seção supõe que o server já com sucesso autenticou e se registrou com o server de CA.

Etapa 1 — Verifique a configuração padrão IKEv2 Smart.

Com IKEv2, você pode agora aproveitar-se da característica padrão esperta introduzida em 15.2(1)T. É usado para simplificar uma configuração de FlexVPN. Estão aqui algumas configurações padrão:

Política da autorização do padrão IKEv2:

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

Proposta do padrão 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
```

Política do padrão IKEv2:

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

Perfil do IPSec padrão:

```
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 } , }
```

O IPSec padrão transforma o grupo:

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

Para obter mais informações sobre da característica padrão IKEv2 esperta, refira os padrões IKEv2 espertos (clientes registrados somente).

Etapa 2 — Altere a política da autorização do padrão IKEv2 e adicionar um perfil do padrão IKEv2 para os clientes de FlexVPN.

O perfil IKEv2 criado aqui combinará em um ID de peer baseado no Domain Name cisco.com e as interfaces de acesso virtual criadas para os clientes serão desovadas fora do molde virtual 2. Igualmente note a política da autorização define o pool do endereço IP de Um ou Mais Servidores Cisco ICM NT usado atribuindo os endereços IP do peer assim como as rotas a ser trocados através do modo de configuração 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
```

Etapa 3 — Crie a relação virtual do molde usada para os clientes de FlexVPN:

```
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
```

```
 tunnel protection ipsec profile default
```

Configuração de 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
```

Configuração completa

Termine a configuração do servidor híbrida

```
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
```

Termine a configuração de cliente ezvpn 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
```

Termine a configuração de cliente 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
```

Verificação da configuração

Estão aqui alguns dos comandos usados para verificar as operações do EzVPN/FlexVPN em um roteador:

```
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
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems