Migrar do EzVPN-NEM+ legado para FlexVPN no mesmo servidor

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[IKEv1 vs IKEv2](#)
[Mapa de criptografia versus interfaces de túnel virtual](#)
[Topologia de rede](#)
[Configuração atual com cliente EzVPN do modo NEM+ legado](#)
[Configuração do Cliente](#)
[Configuração do servidor](#)
[Migração do servidor para FlexVPN](#)
[Mover o mapa de criptografia legado para dVTI](#)
[Adicione a configuração FlexVPN ao servidor](#)
[Configuração do cliente FlexVPN](#)
[Configuração completa](#)
[Configuração completa do servidor híbrido](#)
[Configuração completa do cliente EzVPN IKEv1](#)
[Configuração completa do cliente FlexVPN IKEv2](#)
[Verificação de configuração](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve o processo de migração de EzVPN para FlexVPN. FlexVPN é a nova solução de VPN unificada oferecida pela Cisco. O FlexVPN aproveita o protocolo IKEv2 e combina acesso remoto, site a site, hub e spoke e implantações VPN de malha parcial. Com tecnologias antigas, como EzVPN, a Cisco o incentiva a migrar para o FlexVPN para aproveitar seus recursos avançados.

Este documento examina uma implantação EzVPN existente que consiste em clientes de hardware EzVPN legados que terminam túneis em um dispositivo headend EzVPN baseado em mapa de criptografia legado. O objetivo é migrar dessa configuração para suportar FlexVPN com estes requisitos:

- Os clientes antigos existentes continuarão a funcionar perfeitamente sem nenhuma alteração de configuração. Isso permite uma migração em fases desses clientes para o FlexVPN ao

longo do tempo.
- O dispositivo headend deve suportar simultaneamente a terminação de novos clientes FlexVPN.

Dois componentes chave de configuração do IPsec são usados para ajudar a atingir essas metas de migração: ou seja, IKEv2 e Virtual Tunnel Interfaces (VTI). Esses objetivos são brevemente discutidos neste documento.

Outros documentos nesta série

- Guia de implantação da FlexVPN: AnyConnect para IOS Headend sobre IPsec com IKEv2 e certificados

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

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

IKEv1 vs IKEv2

O FlexVPN é baseado no protocolo IKEv2, que é o protocolo de gerenciamento de chaves de próxima geração baseado em RFC 4306, e uma melhoria do protocolo IKEv1. O FlexVPN não é compatível com versões anteriores de tecnologias que suportam somente IKEv1 (por exemplo, EzVPN). Essa é uma das principais considerações ao migrar de EzVPN para FlexVPN. Para uma introdução de protocolo no IKEv2 e comparação com IKEv1, consulte IKE versão 2 rapidamente.

Mapa de criptografia versus interfaces de túnel virtual

Virtual Tunnel Interface (VTI) é um novo método de configuração usado para configurações de servidor VPN e cliente. VTI:

- Substituição em mapas de criptografia dinâmicos, que agora é considerada uma configuração antiga.
- Suporta encapsulamento IPsec nativo.
- Não exige um mapeamento estático de uma sessão IPsec para uma interface física; portanto, oferece flexibilidade para enviar e receber tráfego criptografado em qualquer interface física (por exemplo, vários caminhos).
- Configuração mínima, pois o acesso virtual sob demanda é clonado a partir da interface de

modelo virtual.
- O tráfego é criptografado/descriptografado quando encaminhado para/da interface do túnel e gerenciado pela tabela de roteamento IP (portanto, desempenhando um papel importante no processo de criptografia).
- Os recursos podem ser aplicados a pacotes de texto claro na interface VTI ou a pacotes criptografados na interface física.

Os dois tipos de VTIs disponíveis são:

- Estático (sVTI)—Uma interface de túnel virtual estático tem uma origem e um destino de túnel fixos e é tipicamente usada em um cenário de implantação site a site. Aqui está um exemplo de uma configuração 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
```

- Dynamic (dVTI)—Uma interface de túnel virtual dinâmico pode ser usada para terminar túneis IPsec dinâmicos que não tenham um destino de túnel fixo. Após a negociação de túnel bem-sucedida, as interfaces de acesso virtual serão clonadas de um modelo virtual e herdarão todos os recursos L3 desse modelo virtual. Aqui está um exemplo de uma configuração dVTI:

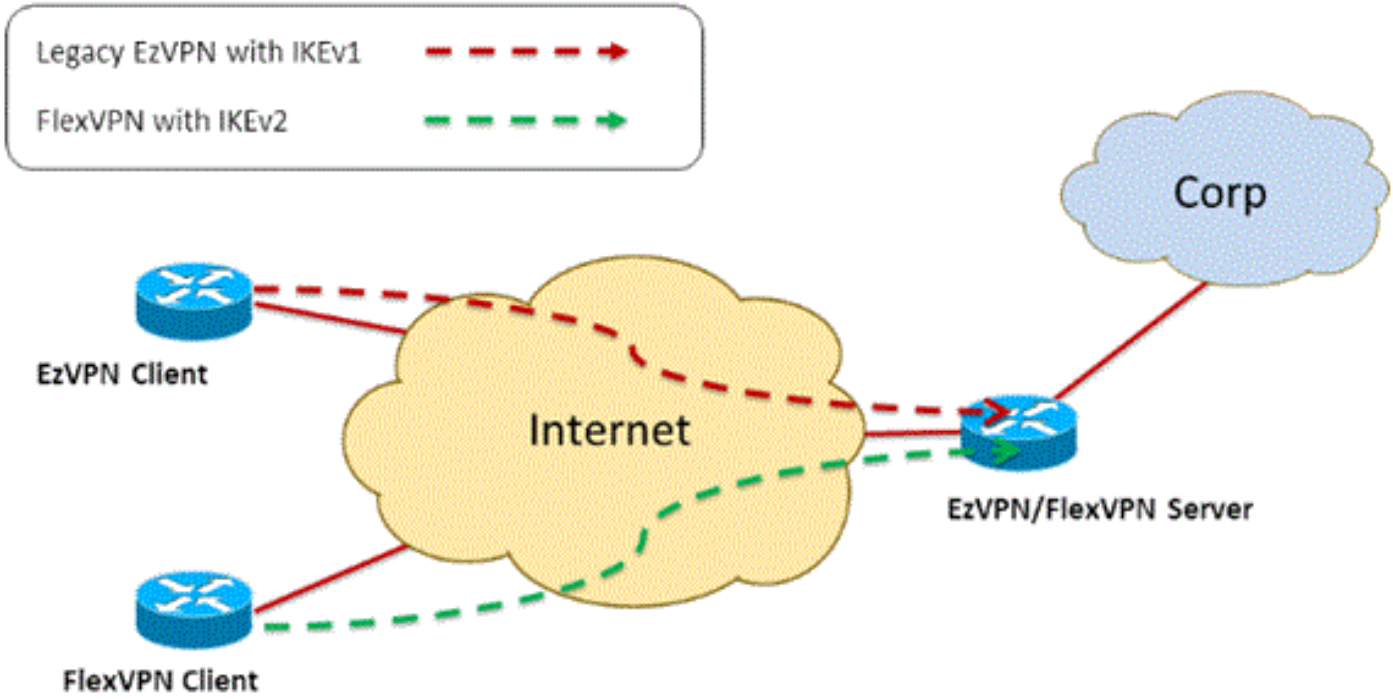
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Consulte estes documentos para obter mais informações sobre o dVTI:

- Configurando o Cisco Easy VPN com a Interface de Túnel Virtual Dinâmico (DVTI - Dynamic Virtual Tunnel Interface) IPSec
- Restrições para a Interface de Túnel Virtual IPsec
- Configuração do suporte multi-SA para interfaces dinâmicas de túnel virtual usando IKEv1

Para que os clientes EzVPN e FlexVPN coexistam, você deve primeiro migrar o servidor EzVPN da configuração do mapa de criptografia legado para uma configuração dVTI. As seções a seguir explicam detalhadamente as etapas necessárias.

Topologia de rede



Configuração atual com cliente EzVPN do modo NEM+ legado

Configuração do Cliente

Abaixo está uma configuração típica de roteador cliente EzVPN. Nesta configuração, o modo Network Extension Plus (NEM+) é usado, o que cria vários pares de SA para as interfaces internas da LAN, assim como a configuração de modo atribuída ao endereço IP do 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 EzVPN, uma configuração de mapa de criptografia legado é usada como a configuração básica 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 servidor para FlexVPN

Conforme descrito nas seções anteriores, o FlexVPN usa IKEv2 como o protocolo do plano de controle e não é compatível com versões anteriores de uma solução EzVPN baseada em IKEv1. Como resultado, a ideia geral dessa migração é configurar o servidor EzVPN existente de forma que ele permita a coexistência entre EzVPN (IKEv1) e FlexVPN (IKEv2) legados. Para atingir esse objetivo, você pode usar essa abordagem de migração em duas etapas:

1. Mova a configuração de EzVPN legada no headend de uma configuração baseada em mapa de criptografia para dVTI.
2. Adicione a configuração FlexVPN, que também é baseada em dVTI.

Mover o mapa de criptografia legado para dVTI

Alterações na configuração do servidor

Um servidor EzVPN configurado com mapa de criptografia na interface física inclui várias limitações quando se trata de suporte a recursos e flexibilidade. Se você tem EzVPN, a Cisco

recomenda que você use o dVTI. Como primeira etapa para migrar para uma configuração EzVPN e FlexVPN coexistentes, você deve alterá-la para uma configuração dVTI. Isso fornecerá separação IKEv1 e IKEv2 entre as diferentes interfaces de modelo virtual para acomodar ambos os tipos de clientes.

Observação: para suportar o modo Network Extension Plus da operação EzVPN nos clientes EzVPN, o roteador headend deve ter suporte para o recurso multi SA no dVTI. Isso permite que vários fluxos IP sejam protegidos pelo túnel, que é necessário para o headend criptografar o tráfego para a rede interna do cliente EzVPN, bem como o endereço IP atribuído ao cliente através da configuração do modo IKEv1. Para obter mais informações sobre o suporte multi SA no dVTI com IKEv1, consulte Suporte Multi-SA para interfaces de túnel virtual dinâmico para IKEv1.

Conclua estes passos para implementar a alteração de configuração no servidor:

Etapa 1—Remover o mapa de criptografia da interface física de saída 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 — Criar uma interface de modelo virtual a partir da qual as interfaces de acesso virtual serão clonadas depois que os túneis forem estabelecidos:

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

Etapa 3 — Associar esta recém-criada interface de modelo virtual ao perfil isakmp para o grupo EzVPN configurado:

```
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
```

Depois que as alterações de configuração acima forem feitas, verifique se os clientes EzVPN existentes continuam funcionando. No entanto, agora seus túneis são terminados em uma interface de acesso virtual criada dinamicamente. Isso pode ser verificado com o comando **show crypto session** 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
```

Adicione a configuração FlexVPN ao servidor

Este exemplo usa RSA-SIG (ou seja, Certificate Authority) no cliente e no servidor FlexVPN. A configuração nesta seção pressupõe que o servidor já foi autenticado e inscrito com êxito no servidor CA.

Etapa 1 — Verificar a configuração padrão inteligente do IKEv2.

Com o IKEv2, agora você pode aproveitar o recurso Smart Default introduzido no 15.2(1)T. É usado para simplificar a configuração do FlexVPN. Aqui estão algumas configurações padrão:

Política de autorização padrão do IKEv2:

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

Proposta padrão de 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 padrão do IKEv2:

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

Perfil 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 } ,
 }
```

Conjunto de transformação IPsec padrão:

```
VPN-Server#show crypto ipsec transform default
```

```
{ esp-aes esp-sha-hmac }
 will negotiate = { Transport, },
```

Para obter mais informações sobre o recurso padrão inteligente IKEv2, consulte Padrões inteligentes IKEv2 (somente clientes registrados).

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

O perfil IKEv2 criado aqui corresponderá a uma ID de peer com base no nome de domínio cisco.com e as interfaces de acesso virtual criadas para os clientes serão desgeradas do modelo virtual 2. Observe também que a política de autorização define o pool de endereços IP usado para atribuir endereços IP de peer, bem como as rotas a serem trocadas via 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 — Criar a interface de modelo virtual usada para os clientes FlexVPN:

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

Configuração do cliente 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

Configuração completa do servidor híbrido

```
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
```

Configuração completa do 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
```

Configuração completa do cliente FlexVPN IKEv2

```
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 de configuração

Aqui estão alguns dos comandos usados para verificar as operações de 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