Exemplo de configuração de site para site FlexVPN

Contents

Introduction

Este documento fornece uma configuração de exemplo para o túnel de VPN IPsec (Internet Protocol Security)/GRE (Generic Routing Encapsulation) de site a site FlexVPN.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

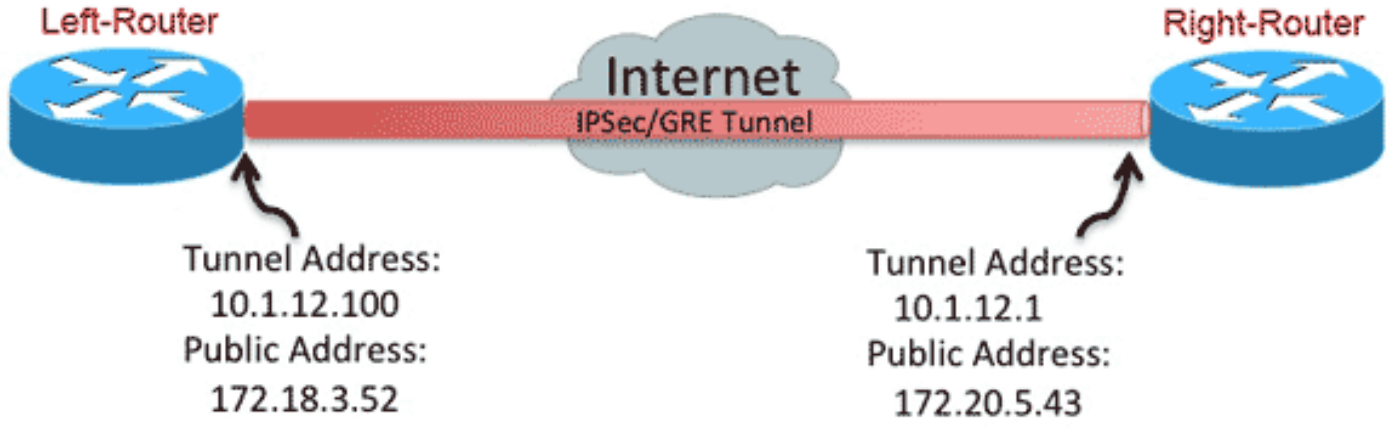
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração do túnel PSK

O procedimento nesta seção descreve como usar uma chave pré-compartilhada (PSK) para configurar os túneis neste ambiente de rede.

Roteador esquerdo

1. Configure o keyring IKEv2 (Internet Key Exchange versão 2):

```
 crypto ikev2 keyring mykeys
peer Right-Router
address 172.20.5.43
```

```
pre-shared-key Cisco123
!
```

2. Reconfigure o perfil padrão IKEv2 para:
   correspondência na ID IKEdefinir os métodos de autenticação para local e remotoconsulte o teclado listado na etapa anterior

```
 crypto ikev2 profile default
match identity remote address 172.20.5.43 255.255.255.255
authentication local pre-share
authentication remote pre-share
keyring local mykeys
dpd 60 2 on-demand
!
```

3. Reconfigure o perfil IPsec padrão para referenciar o perfil IKEv2 padrão:

```
crypto ipsec profile default
set ikev2-profile default
!
interface Tunnel0
ip address 10.1.12.100 255.255.255.0
tunnel source Ethernet0/0
tunnel destination 172.20.5.43
tunnel protection ipsec profile default
!
```

4. Configure as interfaces LAN e WAN:

```
 interface Ethernet0/0
description WAN
ip address 172.18.3.52 255.255.255.0
!
interface Ethernet0/1
description LAN
ip address 192.168.100.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.18.3.1 name route_to_internet
```

Roteador direito

Repita as etapas da configuração do roteador à esquerda, mas com estas alterações necessárias:

```
 crypto ikev2 keyring mykeys
peer Left-Router
address 172.18.3.52
pre-shared-key Cisco123
!
crypto ikev2 profile default
match identity remote address 172.18.3.52 255.255.255.255
authentication local pre-share
authentication remote pre-share
keyring local mykeys
dpd 60 2 on-demand
!
crypto ipsec profile default
set ikev2-profile default
!
interface Tunnel0
ip address 10.1.12.1 255.255.255.0
```

```
tunnel source Ethernet0/0
tunnel destination 172.18.3.52
tunnel protection ipsec profile default
!
interface Ethernet0/0
description WAN
ip address 172.20.5.43 255.255.255.0
!
interface Ethernet0/1
description LAN
ip address 192.168.200.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 172.20.5.1 name route_to_internet
```

Configuração do túnel PKI

Depois que o túnel da seção anterior é concluído com a PSK, ele pode ser facilmente alterado para usar a Public Key Infrastructure (PKI) para a autenticação. Neste exemplo, o roteador da esquerda autentica-se com um certificado para o roteador da direita. O Roteador Direito continua a usar uma PSK para se autenticar no Roteador Esquerdo. Isso foi feito para mostrar a autenticação assimétrica; no entanto, é trivial trocar ambos para usar a autenticação de certificado.

Roteador esquerdo

1. Configurar a Autoridade de Certificação (CA) do Cisco IOS® no roteador:

```
Left-Router#config t
Left-Router(config)#ip http server
Left-Router(config)#crypto pki server S2S-CA
Left-Router(cs-server)#issuer-name cn="S2S-CA"
Left-Router(cs-server)#grant auto
Left-Router(cs-server)#no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
% Exporting Certificate Server signing certificate and keys...
```

2. Autentique e inscreva o ponto confiável da ID:

```
Left-Router#config t
Left-Router(config)#ip domain name cisco.com
Left-Router(config)#crypto pki trustpoint S2S-ID
Left-Router(ca-trustpoint)#enrollment url http://172.18.3.52:80
Left-Router(ca-trustpoint)#subject-name cn=Left-Router.cisco.com
Left-Router(ca-trustpoint)#exit
Left-Router(config)#crypto pki authenticate S2S-ID
Certificate has the following attributes:
Fingerprint MD5: C11CD575 EC2DEACD 97E9AA3A 2DACFCAB
Fingerprint SHA1: A8A6E79B D1932175 F12652F1 4F967077 3AEFAF08

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Left-Router(config)#
```

```
Left-Router(config)#crypto pki enroll S2S-ID
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:
*Oct 29 15:15:50.287: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair

% The subject name in the certificate will include: cn=R1.cisco.com
% The subject name in the certificate will include: R1.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose S2S-ID' command will show the fingerprint.

*Oct 29 15:15:57.722: CRYPTO_PKI: Certificate Request Fingerprint MD5:
CA34FD51 A85007EF A785E058 60D8877D
*Oct 29 15:15:57.722: CRYPTO_PKI: Certificate Request Fingerprint SHA1:
E37AAE3C 851953C3 9FABE1FD 2F0EACD5 566F361E
Left-Router(config)#exit
Left-Router#
*Oct 29 15:16:57.829: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

3. Reconfigure o perfil IKEv2:

```
 crypto ikev2 profile default
authentication local rsa-sig
identity local dn
pki trustpoint S2S-ID
```

Roteador direito

1. Autentique o ponto confiável da CA para que o roteador possa verificar o certificado do roteador esquerdo:

```
Right-Router#config t
Right-Router(config)#ip domain name cisco.com
Right-Router(config)#crypto pki trustpoint S2S-ID
Right-Router(ca-trustpoint)#enrollment url http://172.18.3.52:80
Right-Router(ca-trustpoint)#revocation-check none
Right-Router(ca-trustpoint)#exit
Right-Router(config)#crypto pki authenticate S2S-IDCertificate has the following
attributes:
Fingerprint MD5: C11CD575 EC2DEACD 97E9AA3A 2DACFCAB
Fingerprint SHA1: A8A6E79B D1932175 F12652F1 4F967077 3AEFAF08

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Right-Router(config)#
```

2. Reconfigure o perfil IKEv2 para corresponder à conexão de entrada:

```
 crypto pki certificate map S2S-Cert-Map 10
issuer eq cn=S2S-CA
crypto ikev2 profile default
match certificate S2S-Cert-Map
authentication remote rsa-sig
```

Verificar

Use o comando **show crypto ikev2 como detailed** para verificar a configuração.

O roteador certo mostra o seguinte:

- Sinal de Autenticação = Como esse roteador se autentica para Roteador Esquerdo = Chave Pré-compartilhada
- Auth Verify = Como o roteador esquerdo se autentica neste roteador = RSA (certificado)
- id Local/Remota = As identidades ISAKMP trocadas

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local Remote fvrf/ivrf Status
1 172.20.5.43/500 172.18.3.52/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: RSA
Life/Active Time: 86400/3165 sec
CE id: 1043, Session-id: 22
Status Description: Negotiation done
Local spi: 3443E884EB151E8D Remote spi: 92779BC873F58132
Local id: 172.20.5.43
Remote id: hostname=Left-Router.cisco.com,cn=Left-Router.cisco.com
Local req msg id: 0 Remote req msg id: 4
Local next msg id: 0 Remote next msg id: 4
Local req queued: 0 Remote req queued: 4
Local window: 5 Remote window: 5
DPD configured for 60 seconds, retry 2
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

IPv6 Crypto IKEv2 SA
```

Configuração de roteamento

O exemplo de configuração anterior permite que o túnel seja estabelecido, mas não fornece nenhuma informação sobre o roteamento (ou seja, que destinos estão disponíveis no túnel). Com o IKEv2, há duas maneiras de trocar essas informações: Protocolos de roteamento dinâmico e rotas IKEv2.

Protocolos de roteamento dinâmico

Como o túnel é um túnel GRE ponto a ponto, ele se comporta como qualquer outra interface ponto a ponto (por exemplo: serial, discador) e é possível executar qualquer Interior Gateway Protocol (IGP)/Exterior Gateway Protocol (EGP) no link para trocar informações de roteamento. Aqui está um exemplo do Enhanced Interior Gateway Routing Protocol (EIGRP):

1. Configure o roteador da esquerda para ativar e anunciar o EIGRP nas interfaces de LAN e túnel:

```
router eigrp 100
no auto-summary
```

```
network 10.1.12.0 0.0.0.255
network 192.168.100.0 0.0.0.255
```

2. Configure o Roteador Direito para ativar e anunciar o EIGRP nas interfaces de LAN e túnel:

```
router eigrp 100
no auto-summary
network 10.1.12.0 0.0.0.255
network 192.168.200.0 0.0.0.255
```

3. Confirme se a rota para 192.168.200.0/24 é aprendida pelo túnel via EIGRP:

```
Left-Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 172.18.3.1 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.18.3.1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.12.0/24 is directly connected, Tunnel0
L 10.1.12.100/32 is directly connected, Tunnel0
172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.18.3.0/24 is directly connected, Ethernet0/0
L 172.18.3.52/32 is directly connected, Ethernet0/0
192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.100.0/24 is directly connected, Ethernet0/1
L 192.168.100.1/32 is directly connected, Ethernet0/1
D 192.168.200.0/24 [90/27008000] via 10.1.12.1, 00:00:22, Tunnel0
```

Rotas IKEv2

Em vez de usar rotas de protocolo de roteamento dinâmico para aprender destinos através do túnel, as rotas podem ser trocadas durante o estabelecimento de uma Associação de Segurança (SA - Security Association) IKEv2.

1. No Roteador da Esquerda, configure uma lista de sub-redes que o Roteador da Esquerda anuncia ao Roteador da Direita:

```
ip access-list standard Net-List
permit 192.168.100.0 0.0.0.255
```

2. No Roteador Esquerdo, configure uma política de autorização para especificar as sub-redes a anunciar:
   /32 configurado na interface de túnel/24 rota referenciada na ACL

```
crypto ikev2 authorization policy default
route set interface
route set access-list Net-List
```

3. No Roteador Esquerdo, reconfigure o perfil IKEv2 para referenciar a política de autorização quando chaves pré-compartilhadas forem usadas:

```
crypto ikev2 profile default
aaa authorization group psk list default default
```

4. No Roteador Direito, repita as etapas 1 e 2 e ajuste o perfil IKEv2 para referenciar a política de autorização quando os certificados forem usados:

```
ip access-list standard Net-List
permit 192.168.200.0 0.0.0.255

crypto ikev2 authorization policy default
route set interface
route set access-list Net-List

crypto ikev2 profile default
aaa authorization group cert list default default
```

5. Use os comandos **shut** e **no shut** na interface do túnel para forçar a criação de uma nova SA IKEv2.

6. Verifique se as rotas IKEv2 são trocadas. Consulte "Sub-redes remotas" nesta saída de exemplo:

```
Right-Router#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 172.20.5.43/500 172.18.3.52/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: RSA
Life/Active Time: 86400/3165 sec
CE id: 1043, Session-id: 22
Status Description: Negotiation done
Local spi: 3443E884EB151E8D Remote spi: 92779BC873F58132
Local id: 172.20.5.43
Remote id: hostname=R100.cisco.com,cn=R100.cisco.com
Local req msg id: 0 Remote req msg id: 4
Local next msg id: 0 Remote next msg id: 4
Local req queued: 0 Remote req queued: 4
Local window: 5 Remote window: 5
DPD configured for 60 seconds, retry 2
NAT-T is not detected
Cisco Trust Security SGT is disabled Initiator of SA : No

Remote subnets:
10.1.12.100 255.255.255.255
192.168.100.0 255.255.255.0

IPv6 Crypto IKEv2 SA
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems