FlexVPN站点到站点配置示例

目录

简介

本文档提供FlexVPN站点到站点互联网协议安全(IPsec)/通用路由封装(GRE)隧道的示例配置。

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。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

关于文件规则的信息，请参见Cisco技术提示规则。

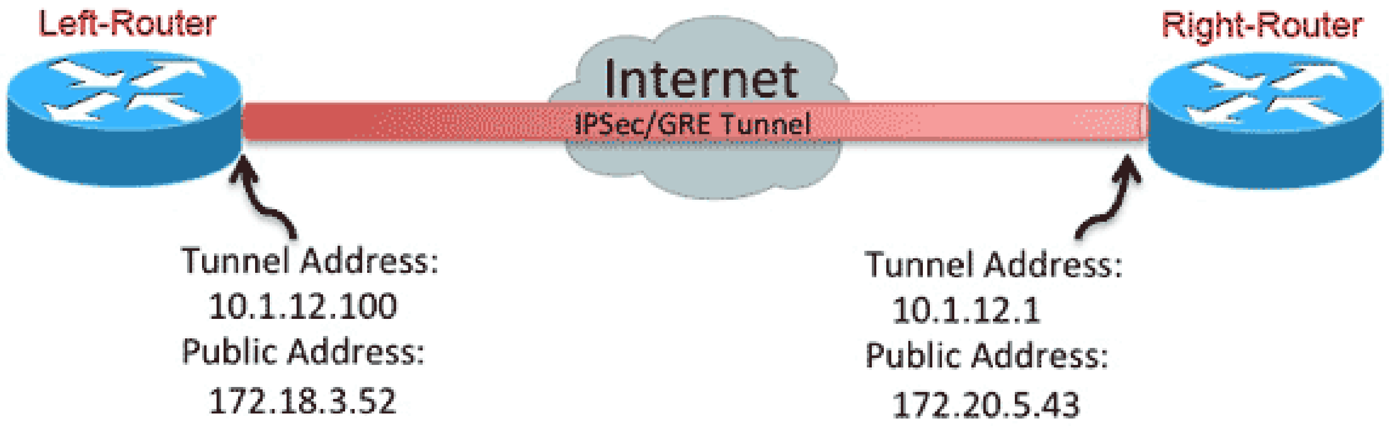
配置

本部分提供有关如何配置本文档所述功能的信息。

> **注意：**使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



PSK隧道配置

本节中的步骤介绍如何使用预共享密钥(PSK)来配置此网络环境中的隧道。

左路由器

1. 配置Internet密钥交换版本2(IKEv2)密钥环：

```
 crypto ikev2 keyring mykeys
peer Right-Router
address 172.20.5.43
pre-shared-key Cisco123
!
```

2. 重新配置IKEv2默认配置文件以：
   匹配IKE ID设置本地和远程的身份验证方法引用上一步中列出的键环

```
 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. 重新配置默认IPsec配置文件以引用默认IKEv2配置文件：

```
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. 配置LAN和WAN接口：

```
 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
```

右路由器

重复左侧路由器配置中的步骤，但需要进行以下必要更改：

```
 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
```

PKI隧道配置

使用PSK完成上一部分的隧道后，可以轻松更改隧道以使用公钥基础设施(PKI)进行身份验证。在本例中，左路由器使用证书向右路由器进行自身身份验证。右路由器继续使用PSK来向左路由器验证自身。这样做是为了显示非对称身份验证；但是，交换机和交换机都使用证书身份验证是微不足道的。

左路由器

1. 在路由器上配置Cisco IOS®证书颁发机构(CA):

```
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. 验证并注册ID信任点：

```
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. 重新配置IKEv2配置文件：

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

右路由器

1. 对CA信任点进行身份验证，以便路由器可以验证左路由器证书：

```
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. 重新配置IKEv2配置文件以匹配传入连接：

```
 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
```

验证

使用**show crypto ikev2 sa detailed命令**验证配置。

右路由器显示以下内容：

- Auth Sign =此路由器如何向左路由器进行自身身份验证=预共享密钥
- Auth Verify =左路由器如何向此路由器进行自身身份验证= RSA（证书）
- 本地/远程ID =交换的ISAKMP身份

```
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
```

路由配置

上一个配置示例允许建立隧道，但不提供有关路由的任何信息（即，哪些目标可通过隧道提供）。使用IKEv2时，有两种方式可以交换此信息：动态路由协议和IKEv2路由。

动态路由协议

由于隧道是点对点GRE隧道，因此它的行为与任何其他点对点接口类似(例如：串行、拨号)，并且可以通过链路运行任何内部网关协议(IGP)/外部网关协议(EGP)，以便交换路由信息。以下是增强型内部网关路由协议(EIGRP)的示例：

1. 配置左侧路由器，以在LAN和隧道接口上启用和通告EIGRP:

   ```
   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. 配置右路由器，以在LAN和隧道接口上启用和通告EIGRP:

   ```
   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. 确认通向192.168.200.0/24的路由是通过EIGRP通过隧道获知的：

   ```
   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
```

IKEv2路由

在建立IKEv2安全关联(SA)期间，可以交换路由，而不是使用动态路由协议路由来获取隧道中的目标。

1. 在左路由器上，配置左路由器通告给右路由器的子网列表：

   ```
   ip access-list standard Net-List
   permit 192.168.100.0 0.0.0.255
   ```
2. 在左侧路由器上，配置授权策略以指定要通告的子网：
   /32在隧道接口上配置/24 ACL中引用的路由
   ```
   crypto ikev2 authorization policy default
   route set interface
   route set access-list Net-List
   ```
3. 在左路由器上，重新配置IKEv2配置文件，以在使用预共享密钥时引用授权策略：

   ```
   crypto ikev2 profile default
   aaa authorization group psk list default default
   ```
4. 在右侧路由器上，重复步骤1和2并调整IKEv2配置文件，以在使用证书时引用授权策略：

   ```
   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. 在隧道接口上使用**shut**和**no shut**命令，以强制生成新的IKEv2 SA。

6. 检验IKEv2路由是否已交换。请参阅以下输出示例中的“远程子网”：

   ```
   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
```

相关信息

- 技术支持和文档 - Cisco Systems