FlexVPN站点到站点配置示例

目录

简介

本文为FlexVPN站点到站点Internet协议安全性(IPsec) /Generic路由封装(GRE)通道提供一配置示例。

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。

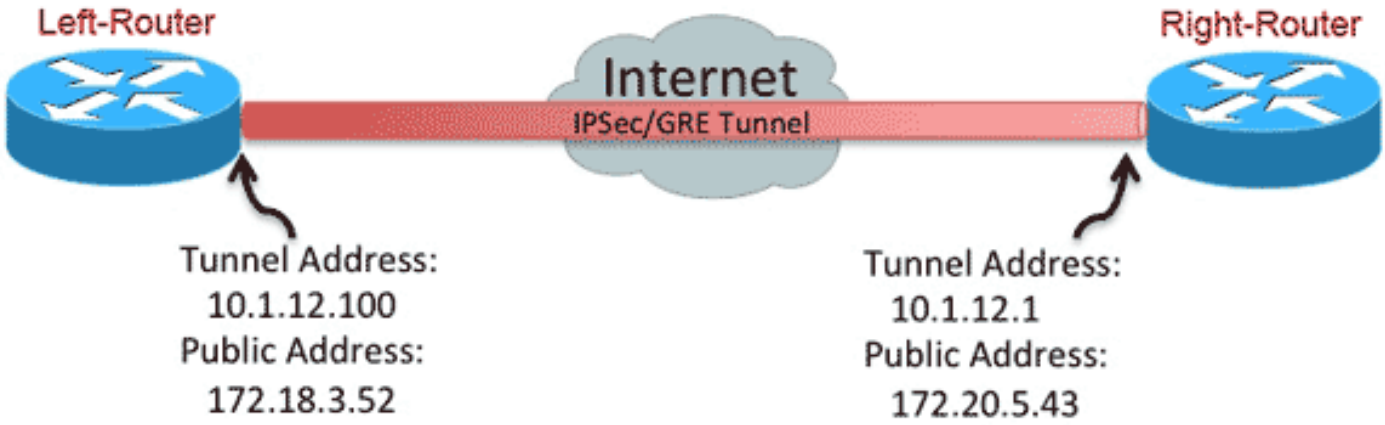
配置

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

在此部分的步骤描述如何使用预先共享密钥(PSK)为了配置在此网络环境的通道。

离开路由器

1. 配置互联网密钥交换版本2 (IKEv2)钥匙圈：
```
 crypto ikev2 keyring mykeys
peer Right-Router
address 172.20.5.43
pre-shared-key Cisco123
!
```
2. 重新配置IKEv2默认配置文件为了：
在IKE ID的匹配设置本地和远程的认证方法参考列出的钥匙圈上一步
```
 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配置文件为了参考默认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和广域网接口：

```
 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
```

右岸堤防路由器

重复步骤从离开路由器配置，但是与这些必要的更改：

```
 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

在从前面部分的通道完成与PSK后，可能容易地更改为了使用公共密钥基础设施(PKI)验证。在本例

中，离开路由器验证与证书到右岸堤防路由器。右岸堤防路由器继续使用PSK为了验证到离开路由器。这是完成显示不对称验证;然而，它是琐细换成两个使用身份验证验证。

离开路由器

1. 配置在路由器的Cisco IOS Certificate Authority (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. 验证并且登记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
```

右岸堤防路由器

1. 验证CA信任点，以便路由器能验证离开路由器证书：

```
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配置文件为了匹配流入连接：

```
 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

请使用**detailed命令显示crypto的ikev2 sa**为了验证配置。

右岸堤防路由器显示此：

- 验证符号=此路由器如何验证对离开路由器=预共享密钥
- 验证验证=离开路由器如何验证对此路由器= RSA (证书)
- 本地/Remote id=交换的ISAKMP标识

```
 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

先前配置示例允许将设立的通道，但是不提供关于路由的任何信息(即什么目的地在通道是可用的)。使用IKEv2，有两种方式交换此信息：动态路由协议和IKEv2路由。

动态路由协议

因为通道是一点到点GRE隧道，正常运行类似其他点对点接口(例如：序列，拨号程序)和是可能运行所有内部网关路由协议(IGP)/在链路的外部网关协议(EGP)为了交换路由信息。这是增强的内部网关路由选择协议(EIGRP)示例：

1. 配置离开路由器为了启用和通告在LAN和隧道接口的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. 配置右岸堤防路由器为了启用和通告在LAN和隧道接口的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. 确认路由到192.168.200.0/24在通道了解通过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
   ```

IKEv2路由

在IKEv2安全关联(SA)的建立期间，而不是使用动态路由协议路由为了学习在通道间的目的地，路由也许被交换。

1. 在离开路由器上，请配置离开路由器通告到右岸堤防路由器子网的列表：
   ```
   ip access-list standard Net-List
   permit 192.168.100.0 0.0.0.255
   ```
2. 在离开路由器上，请配置授权策略为了指定子网通告：
   /32在隧道接口配置ACL参考的/24路由`crypto ikev2 authorization policy default`
   ```
   route set interface
   route set access-list Net-List
   ```
3. 在离开路由器上，当使用时，请重新配置IKEv2配置文件为了参考授权策略预先共享密钥：
   ```
   crypto ikev2 profile default
   aaa authorization group psk list default default
   ```
4. 在右岸堤防路由器上，当使用时，请重复步骤1和2并且调节IKEv2配置文件为了参考授权策略证书：
   ```
   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. 请使用on命令隧道接口为了强制一新的IKEv2的**关闭的**和**no shut** SA被构件。

6. 验证IKEv2路由被交换。请参阅“远程子网”在此输出示例:中：
   ```
   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