FlexVPN站點到站點配置示例

目錄

簡介

本檔案將提供FlexVPN站點到站點網際網路通訊協定安全(IPsec)/通用路由封裝(GRE)通道的組態範例。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解有關檔案慣例的資訊。

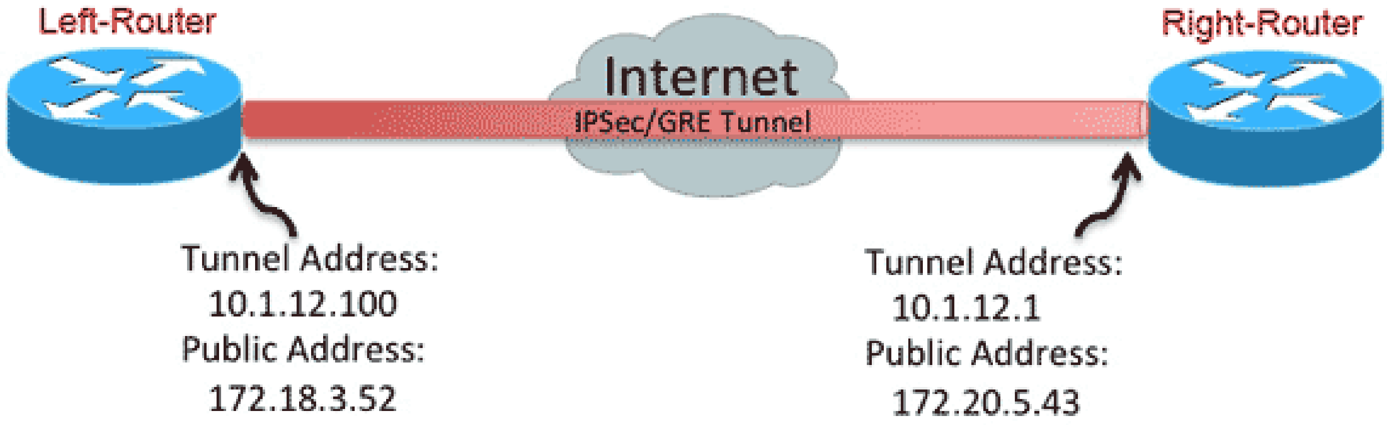
設定

本節提供用於設定本文件中所述功能的資訊。

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



PSK隧道配置

本節中的步驟說明如何使用預共用金鑰(PSK)在此網路環境中設定通道。

左路由器

1. 配置網際網路金鑰交換版本2(IKEv2)金鑰環：

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

2. 重新配置IKEv2預設配置檔案以便：
   匹配IKE ID設定本地和遠端身份驗證方法參考上一步中列出的金鑰環

```
 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. 重新配置預設IPsec配置檔案以引用預設IKEv2配置檔案：

```
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介面：

```
 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

重複左路由器配置中的步驟，但進行以下必要更改：

```
 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後，可以輕鬆地對其進行更改，以便使用公共金鑰基礎設施(PKI)進行身份驗證。在本範例中，左路由器使用到右路由器的憑證驗證自身。右路由器繼續使用PSK向左路由器驗證自己的身份。這樣做是為了顯示非對稱身份驗證；但是，將兩者都切換為使用證書身份驗證非常簡單。

左路由器

1. 在路由器上配置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. 驗證並註冊ID信任點：

   ```
   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配置檔案：

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

右路由器

1. 對CA信任點進行身份驗證，以便路由器驗證左路由器證書：

```
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配置檔案以匹配傳入連線：

```
 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
```

驗證

使用**show crypto ikev2 sa detailed**命令驗證配置。

右路由器顯示以下內容：

- 身份驗證簽名=此路由器如何向左路由器驗證自身=預共用金鑰
- Auth Verify =左路由器如何向此路由器驗證自身= RSA（證書）
- 本地/遠端ID =交換的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

上一個組態範例允許建立通道，但並未提供路由的任何資訊（即通道上有哪些目的地可用）。 使用IKEv2，有兩種方法可以交換此資訊：動態路由協定和IKEv2路由。

動態路由通訊協定

由於通道是點對點GRE通道，因此其行為與任何其他點對點介面相同(例如：串列和撥號程式)，並且可以通過鏈路運行任何內部網關協定(IGP)/外部網關協定(EGP)以交換路由資訊。以下是增強型內部閘道路由通訊協定(EIGRP)的範例：

1. 配置左路由器，以便在LAN和隧道介面上啟用和通告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和隧道介面上啟用和通告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. 確認通過EIGRP通過隧道獲知到192.168.200.0/24的路由：

   ```
   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

建立IKEv2安全關聯(SA)期間，可能會交換路由，而不是使用動態路由協定路由來通過隧道瞭解目的地。

1. 在左路由器上，配置左路由器向右路由器通告的子網清單：

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

2. 在左路由器上，配置授權策略以指定要通告的子網：
隧道介面上配置的/32/24 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配置檔案，以便在使用預共用金鑰時參考授權策略：

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

4. 在右路由器上，重複步驟1和2並調整IKEv2配置檔案，以便在使用證書時參考授權策略：

```
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. 在通道介面上使用**shut**和**no shut**指令，強制建立新的IKEv2 SA。

6. 檢驗IKEv2路由是否已交換。請參閱此輸出示例中的「遠端子網」：

```
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
```

相關資訊

- 技術支援與文件 - Cisco Systems