FlexVPN Site-to-Site 컨피그레이션 예

목차

소개

이 문서에서는 FlexVPN IPsec(Site-to-Site Internet Protocol Security)/GRE(Generic Routing Encapsulation) 터널의 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

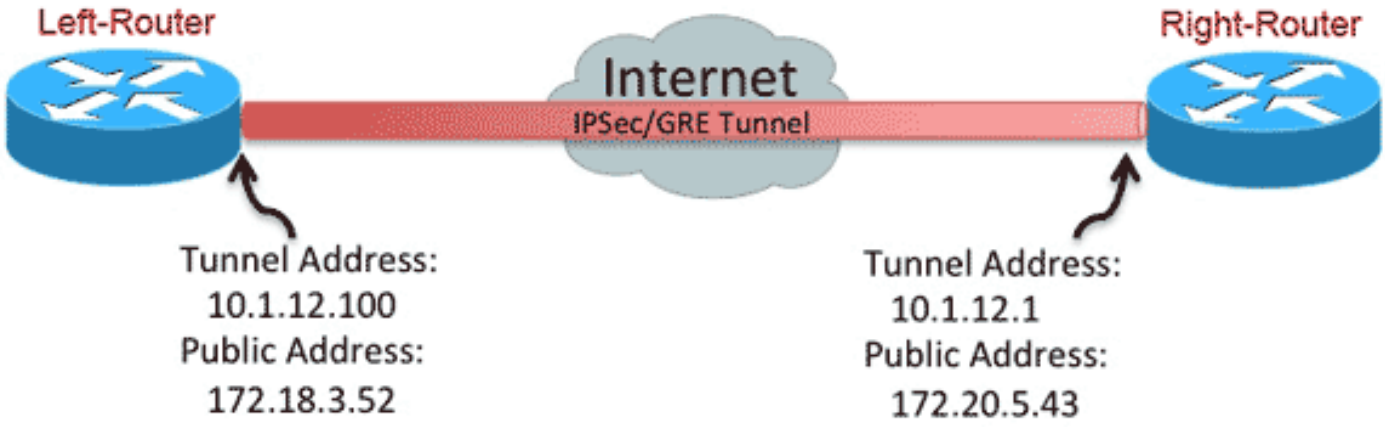
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



PSK 터널 컨피그레이션

이 섹션의 절차에서는 이 네트워크 환경에서 터널을 구성하기 위해 PSK(pre-shared key)를 사용하는 방법에 대해 설명합니다.

왼쪽 라우터

1. IKEv2(Internet Key Exchange version 2) 키링을 구성합니다.

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

2. 다음을 위해 IKEv2 기본 프로필을 재구성합니다.
   IKE ID에서 일치로컬 및 원격 인증 방법 설정이전 단계에 나열된 키보드 참조

```
 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. 기본 IKEv2 프로필을 참조하도록 기본 IPsec 프로필을 재구성합니다.

```
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. LAN 및 WAN 인터페이스를 구성합니다.

```
 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
```

오른쪽 라우터

Left-Router 컨피그레이션에서 단계를 반복하지만 다음과 같은 변경 사항이 적용됩니다.

```
 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 터널 컨피그레이션

이전 섹션의 터널이 PSK와 함께 완료되면 인증에 PKI(Public Key Infrastructure)를 사용하기 위해 쉽게 변경할 수 있습니다.이 예에서 왼쪽 라우터는 오른쪽 라우터에 대한 인증서를 사용하여 자신을 인증합니다.오른쪽 라우터는 왼쪽 라우터에 자신을 인증하기 위해 PSK를 계속 사용합니다.이는 비대칭 인증을 표시하기 위해 수행되었습니다.그러나 인증서 인증을 사용하기 위해 둘 다 전환하는 것은 간단합니다.

왼쪽 라우터

1. 라우터에서 Cisco IOS® CA(Certificate Authority)를 구성합니다.

```
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. ID 신뢰 지점 인증 및 등록:

```
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. IKEv2 프로파일을 재구성합니다.

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

오른쪽 라우터

1. 라우터가 Left-Router 인증서를 확인할 수 있도록 CA 신뢰 지점을 인증합니다.

```
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. 수신 연결과 일치하도록 IKEv2 프로필을 재구성합니다.

```
 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
```

다음을 확인합니다.

show crypto ikev2 sa detailed 명령을 사용하여 컨피그레이션을 확인합니다.

오른쪽 라우터에 다음이 표시됩니다.

- Auth Sign = 이 라우터가 Left-Router = Pre-shared-Key에 대해 자체적으로 인증하는 방법
- Auth Verify = Left-Router가 이 라우터에 자신을 인증하는 방법 = RSA(인증서)
- 로컬/원격 ID = 교환된 ISAKMP ID

```
 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
```

라우팅 컨피그레이션

이전 컨피그레이션 예에서는 터널을 설정할 수 있지만 라우팅에 대한 정보(즉, 터널을 통해 사용할 수 있는 대상)는 제공하지 않습니다. IKEv2에서는 다음 두 가지 방법으로 이 정보를 교환할 수 있습니다.동적 라우팅 프로토콜 및 IKEv2 경로.

동적 라우팅 프로토콜

터널은 포인트-투-포인트 GRE 터널이므로 다른 포인트-투-포인트 인터페이스와 동일하게 작동합니다(예:라우팅 정보를 교환하기 위해 링크를 통해 IGP(Interior Gateway Protocol)/EGP(External Gateway Protocol)를 실행할 수 있습니다.다음은 EIGRP(Enhanced Interior Gateway Routing Protocol)의 예입니다.

1. LAN 및 터널 인터페이스에서 EIGRP를 활성화하고 광고하려면 왼쪽 라우터를 구성합니다.

   ```
   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. LAN 및 터널 인터페이스에서 EIGRP를 활성화하고 광고하려면 오른쪽 라우터를 구성합니다.

   ```
   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. 192.168.200.0/24에 대한 경로가 EIGRP를 통해 터널을 통해 학습되는지 확인합니다.

```
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 경로

터널을 통해 목적지를 학습하기 위해 동적 라우팅 프로토콜 경로를 사용하는 대신 IKEv2 SA(Security Association)를 설정하는 동안 경로가 교환될 수 있습니다.

1. 왼쪽 라우터에서 왼쪽 라우터가 오른쪽 라우터에 광고하는 서브넷 목록을 구성합니다.

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

2. Left-Router에서 알릴 서브넷을 지정하기 위해 권한 부여 정책을 구성합니다.
   /32 터널 인터페이스에 구성됨ACL에서 참조되는 /24 경로

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

3. Left-Router에서 사전 공유 키를 사용할 때 권한 부여 정책을 참조하도록 IKEv2 프로필을 재구성합니다.

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

4. Right-Router에서 1단계와 2단계를 반복하고 인증서가 사용될 때 권한 부여 정책을 참조하도록 IKEv2 프로파일을 조정합니다.

```
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. 새 IKEv2 SA를 강제로 구축하려면 터널 인터페이스에서 **shut** 및 no shut 명령을 사용합니다.

6. IKEv2 경로가 교환되었는지 확인합니다.다음 샘플 출력의 "원격 서브넷"을 참조하십시오.

```
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
```

관련 정보

- 기술 지원 및 문서 – Cisco Systems