FlexVPN-site-to-Site Configuration-voorbeeld

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor FlexVPN site-to-site Internet Protocol Security (IPsec)/Generic Routing Encapsulation (GRE)-tunnel.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor informatie over documentconventies.

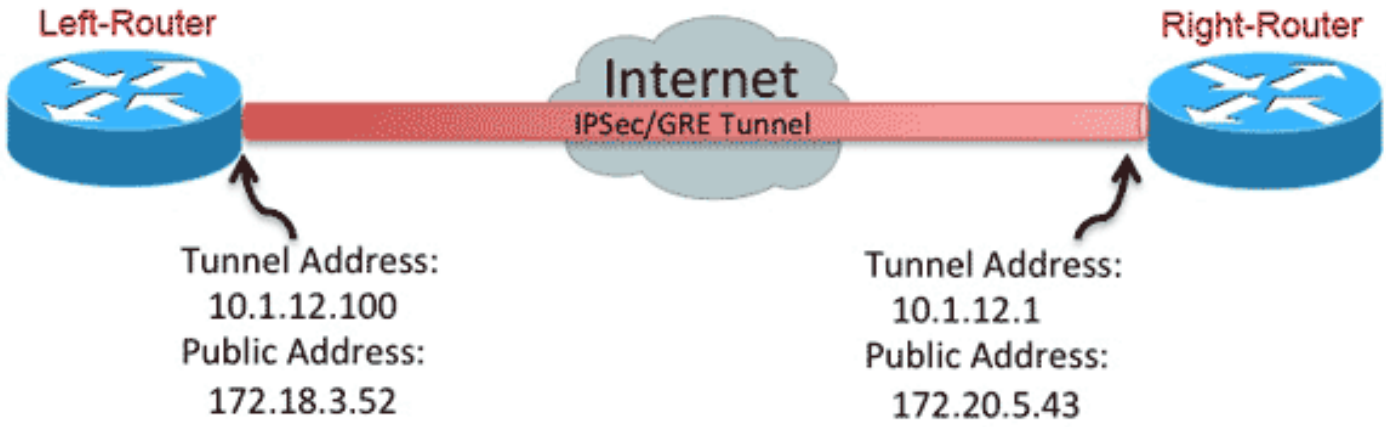
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



PSK-tunnelconfiguratie

De procedure in dit gedeelte beschrijft hoe u een vooraf gedeelde toets (PSK) kunt gebruiken om de tunnels in deze netwerkomgeving te configureren.

Links-router

1. Configureer de sleutelcode van Internet Key Exchange, versie 2 (IKEv2):

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

2. Herstelt het IKEv2-standaardprofiel om:
   overeenkomend met de IKE-idde authenticatiemethoden voor lokale en afstandsbediening instellenreferentie de in de vorige stap vermelde sleutelcode

```
 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. Herstel het standaard IPsec-profiel om naar het standaard IKEv2-profiel te verwijzen:

```
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. Configuratie van LAN en WAN interfaces:

```
 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
```

Rechts-router

Herhaal de stappen van de linker-routerconfiguratie, maar met deze noodzakelijke veranderingen:

```
 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
```

Configuratie PKI-tunnelbouw

Nadat de tunnel uit de voorgaande sectie is voltooid met PSK, kan deze gemakkelijk worden gewijzigd om PKI (Public Key Infrastructure) te gebruiken voor de authenticatie. In dit voorbeeld, authentiek de Linker-router zichzelf met een certificaat aan de Rechts-router. De rechterrouter blijft een PSK gebruiken om zichzelf aan de linkerrouter voor authentiek te verklaren. Dit is gedaan om asymmetrische authenticatie aan te tonen; het is echter triviaal om beide over te schakelen op het gebruik van certificatie .

Links-router

1. Configureer de Cisco IOS® certificaatautoriteit (CA) op router:

```
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. Verifieer en registreer het ID trustpoint:

```
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. Herstel het IKEv2-profiel:

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

Rechts-router

1. Verifieer het CA trustpoint zodat de router het certificaat van de Linker-router kan verifiëren:

```
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. Herstel het IKEv2-profiel om de inkomende verbinding aan te passen:

```
 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
```

Verifiëren

Gebruik de **show crypto ikev2 als gedetailleerde** opdracht om de configuratie te verifiëren.

De rechtse router toont dit:

- Auth Sign = Hoe deze router zichzelf voor authentiek verklaart aan links-router = Pre-gedeeld-Key
- Auth verify = Hoe links-router zichzelf authentiek maakt aan deze router = RSA (certificaatnummer)
- Lokale/afstandsbediening = De uitgewisselde ISAKMP-identiteiten

```
 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
```

Routing-configuratie

Het vorige configuratievoorbeeld maakt het mogelijk om de tunnel tot stand te brengen, maar geeft geen informatie over het routeren (dat wil zeggen welke bestemmingen beschikbaar zijn via de tunnel). Met IKEv2 kunnen we deze informatie op twee manieren uitwisselen: Dynamische routingprotocollen en IKEv2-routers.

Dynamische routingprotocollen

Aangezien de tunnel een punt-tot-punt GRE-tunnel is, gedraagt het zich zoals elke andere point-to-point interface (bijvoorbeeld: seriële, dialer) en het is mogelijk om elk protocol van de Gateway van het Binnenlandse Zaken (IGP)/Buitenkant (EGP) over de verbinding te gebruiken om routinginformatie uit te wisselen. Hier is een voorbeeld van het Enhanced Interior Gateway Routing Protocol (DHCP):

1. Configureer de linker router om DHCP in te schakelen en aan te geven op de LAN- en tunnelinterfaces:

   ```
   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. Configureer de juiste router om Ecu in de LAN- en tunnelinterfaces mogelijk te maken en aan te geven:

```
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. Bevestig dat de route naar 192.168.200.0/24 over de tunnel door middel van DHCP wordt geleerd:

```
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-routers

In plaats van dynamische routingprotocolroutes te gebruiken om bestemmingen in de tunnel te leren, kunnen routes worden uitgewisseld tijdens de oprichting van een IKEv2 Security Association (SA).

1. Op de linker-router, moet u een lijst vormen van de subnetten die de Linker-router aan de rechterkant-router adverteert:

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

2. Op de linker router, moet u een autorisatiebeleid configureren om de subnetten te specificeren die u moet adverteren:
/32 ingesteld op de tunnelinterface/24 route waarnaar in de ACL wordt verwezen

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

3. Op de linker-router dient u het IKEv2-profiel opnieuw in te stellen om het autorisatiebeleid aan te passen wanneer er vooraf gedeelde toetsen worden gebruikt:

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

4. Herhaal stap 1 en 2 op de rechterrouter en pas het IKEv2-profiel aan om het toelatingsbeleid

te bepalen wanneer certificaten worden gebruikt:

```
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. Gebruik de opdrachten **dicht** en **niet dicht** op de tunnelinterface om een nieuwe IKEv2 SA te forceren om te worden gebouwd.

6. Controleer dat de IKEv2-routes worden uitgewisseld. Zie "Afstandssubnetten" in deze voorbeelduitvoer:

```
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
```

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems]