FlexVPN Site-to-Site-Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für einen FlexVPN Site-to-Site Internet Protocol Security (IPsec)/Generic Routing Encapsulation (GRE)-Tunnel.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

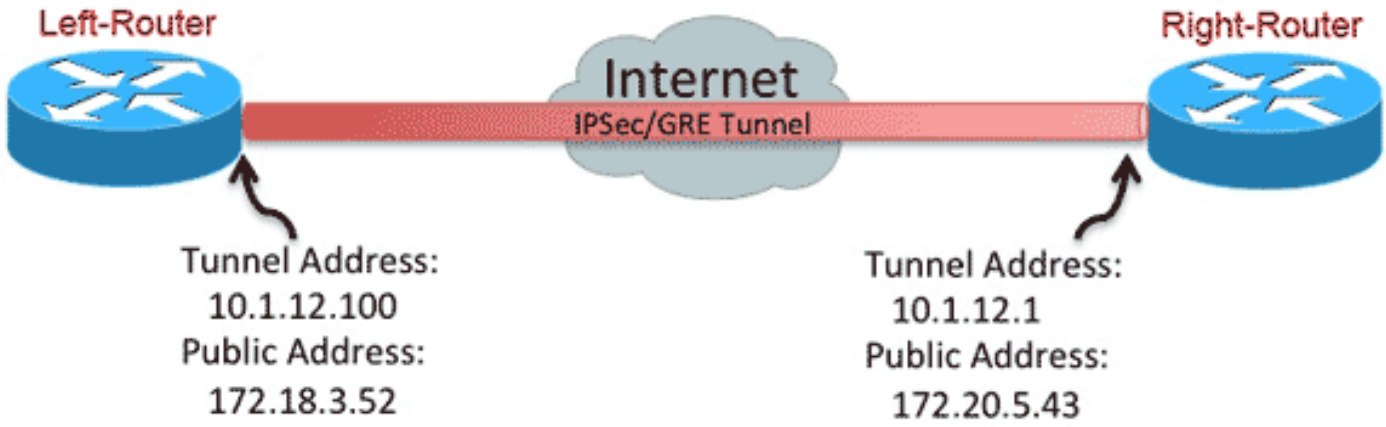
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration des PSK-Tunnels

Das Verfahren in diesem Abschnitt beschreibt die Verwendung eines Pre-Shared Key (PSK) zur Konfiguration der Tunnel in dieser Netzwerkumgebung.

Links-Router

1. Konfigurieren Sie den Internet Key Exchange Version 2 (IKEv2)-Keyring:

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

2. Konfigurieren Sie das IKEv2-Standardprofil neu, um Folgendes zu erreichen: Übereinstimmung auf der IKE-IDLegen Sie die Authentifizierungsmethoden für lokal und remote fest.Verweis auf den im vorherigen Schritt aufgeführten Keyring

```
 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. Konfigurieren Sie das Standard-IPsec-Profil neu, um auf das Standard-IKEv2-Profil zu verweisen:

```
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. Konfigurieren Sie die LAN- und WAN-Schnittstellen:

```
 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
```

Rechter Router

Wiederholen Sie die Schritte aus der Konfiguration für den linken Router, jedoch mit den folgenden erforderlichen Änderungen:

```
 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-Tunnel-Konfiguration

Nachdem der Tunnel aus dem vorherigen Abschnitt mit PSK abgeschlossen wurde, kann er problemlos geändert werden, um die Public Key Infrastructure (PKI) für die Authentifizierung zu verwenden. In diesem Beispiel authentifiziert sich der Left-Router selbst mit einem Zertifikat für den Right-Router. Der rechte Router verwendet weiterhin ein PSK, um sich beim linken Router zu authentifizieren. Auf diese Weise wird die asymmetrische Authentifizierung angezeigt. Es ist jedoch trivial, beide Geräte für die Verwendung der Zertifikatsauthentifizierung zu verwenden.

Links-Router

1. Konfigurieren der Cisco IOS® Certificate Authority (CA) auf dem 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. Authentifizierung und Registrierung des ID Trustpoints:

```
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. Konfigurieren Sie das IKEv2-Profil neu:

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

Rechter Router

1. Authentifizierung des CA-Trustpoints, sodass der Router das Zertifikat für den linken Router überprüfen kann:

```
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. Konfigurieren Sie das IKEv2-Profil neu, um die eingehende Verbindung zu übernehmen:

```
 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
```

Überprüfen

Verwenden Sie den Befehl **show crypto ikev2 als detaillierten** Befehl, um die Konfiguration zu überprüfen.

Der rechte Router zeigt Folgendes:

- Auth-Signatur = Wie sich dieser Router bei Left-Router authentifiziert = Pre-shared-Key
- Auth Verify = Wie sich der Linker-Router an diesen Router authentifiziert = RSA (Zertifikat)
- Local/Remote ID (Lokale/Remote-ID) = die ausgetauschten ISAKMP-Identitäten

```
 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-Konfiguration

Im vorherigen Konfigurationsbeispiel kann der Tunnel eingerichtet werden, es werden jedoch keine Informationen zum Routing bereitgestellt (d. h., welche Ziele über den Tunnel verfügbar sind). Bei IKEv2 gibt es zwei Möglichkeiten, diese Informationen auszutauschen: Dynamische Routing-Protokolle und IKEv2-Routen.

Dynamische Routing-Protokolle

Da der Tunnel ein Punkt-zu-Punkt-GRE-Tunnel ist, verhält er sich wie jede andere Point-to-Point-Schnittstelle (z. B.: seriell, dialer) und es ist möglich, über die Verbindung ein Interior Gateway Protocol (IGP)/Exterior Gateway Protocol (EGP) auszuführen, um Routing-Informationen auszutauschen. Hier ein Beispiel für das Enhanced Interior Gateway Routing Protocol (EIGRP):

1. Konfigurieren Sie den Left-Router so, dass EIGRP auf den LAN- und Tunnelschnittstellen aktiviert und angekündigt wird:

   ```
   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. Konfigurieren Sie den Right-Router, um EIGRP auf den LAN- und Tunnelschnittstellen zu aktivieren und anzukündigen:

```
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. Bestätigen Sie, dass die Route zu 192.168.200.0/24 über den Tunnel über EIGRP erlernt wird:

```
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-Routen

Anstatt dynamische Routing-Protokoll-Routen zu verwenden, um Ziele im Tunnel zu ermitteln, können Routen während der Einrichtung einer IKEv2 Security Association (SA) ausgetauscht werden.

1. Konfigurieren Sie auf dem linken Router eine Liste der Subnetze, die der linke Router dem rechten Router ankündigt:

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

2. Konfigurieren Sie auf dem linken Router eine Autorisierungsrichtlinie, um die anzuzeigenden Subnetze anzugeben:
   /32 auf der Tunnelschnittstelle konfiguriertAuf die in der ACL referenzierte /24-Route
```
crypto ikev2 authorization policy default
route set interface
route set access-list Net-List
```

3. Konfigurieren Sie auf dem linken Router das IKEv2-Profil neu, um auf die Autorisierungsrichtlinie zu verweisen, wenn vorinstallierte Schlüssel verwendet werden:

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

4. Wiederholen Sie auf dem rechten Router die Schritte 1 und 2, und passen Sie das IKEv2-Profil an, um auf die Autorisierungsrichtlinie bei Verwendung von Zertifikaten zu verweisen:

```
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. Erzwingen Sie die Erstellung einer neuen IKEv2 SA mithilfe der Befehle **shut** und **no shutdown** an der Tunnelschnittstelle.

6. Überprüfen Sie, ob die IKEv2-Routen ausgetauscht werden. Siehe "Remote Subnets" in dieser Beispielausgabe:

```
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
```

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems