Esempio di configurazione da sito a sito di FlexVPN

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per il tunnel FlexVPN IPsec (Internet Protocol Security) da sito a sito/GRE (Generic Routing Encapsulation).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per informazioni sulle convenzioni dei documenti.

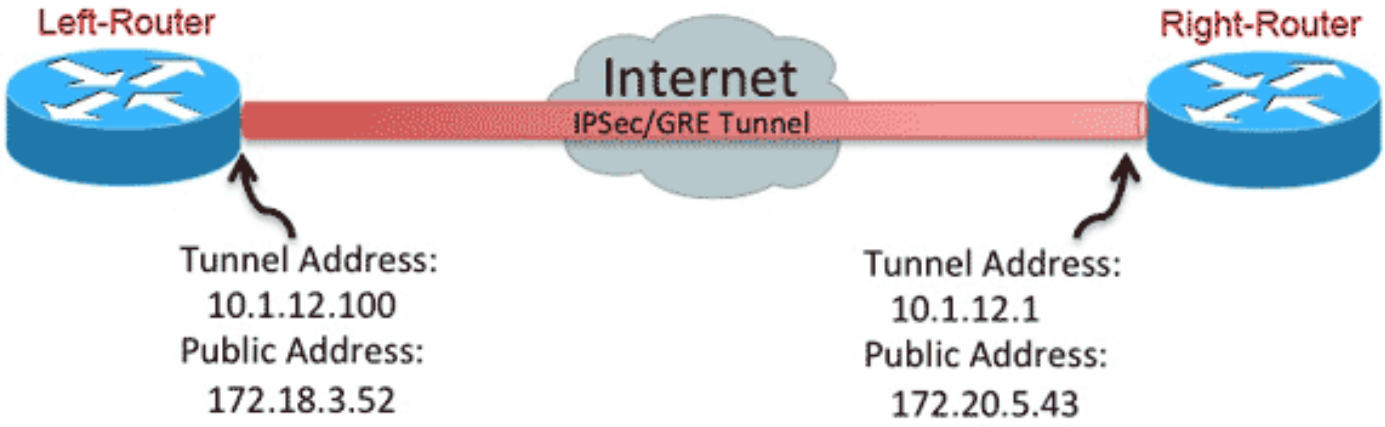
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione tunnel PSK

La procedura illustrata in questa sezione illustra come utilizzare una chiave già condivisa (PSK) per configurare i tunnel in questo ambiente di rete.

Router sinistro

1. Configurare il keyring di Internet Key Exchange versione 2 (IKEv2):

```
crypto ikev2 keyring mykeys
```

```
peer Right-Router
address 172.20.5.43
pre-shared-key Cisco123
!
```

2. Riconfigurare il profilo predefinito IKEv2 per:
   corrisponde all'ID IKEimpostare i metodi di autenticazione per locale e remotofare riferimento al keyring elencato nel passaggio precedente

```
 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. Riconfigurare il profilo IPsec predefinito in modo che faccia riferimento al profilo IKEv2 predefinito:

```
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. Configurare le interfacce LAN e WAN:

```
 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
```

Router destro

Ripetere i passaggi dalla configurazione del router sinistro, ma con le modifiche necessarie:

```
 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
```

Configurazione tunnel PKI

Dopo aver completato il tunnel della sezione precedente con PSK, è possibile modificarlo facilmente per utilizzare l'infrastruttura a chiave pubblica (PKI) per l'autenticazione. Nell'esempio, il router sinistro esegue l'autenticazione con un certificato per il router destro. Il router destro continua a utilizzare una chiave PSK per autenticarsi sul router sinistro. Questa operazione è stata effettuata per mostrare l'autenticazione asimmetrica; tuttavia, è banale passare a entrambi i tipi per utilizzare l'autenticazione dei certificati.

Router sinistro

1. Configurare Cisco IOS® Certificate Authority (CA) sul 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. Autenticare e registrare il trust point ID:

```
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. Riconfigurare il profilo IKEv2:

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

Router destro

1. Autenticare il trust point CA in modo che il router possa verificare il certificato del router sinistro:

```
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. Riconfigurare il profilo IKEv2 in modo che corrisponda alla connessione in ingresso:

```
 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
```

Verifica

Per verificare la configurazione, usare il comando **show crypto ikev2 sa detailed**.

Sul router destro viene visualizzato quanto segue:

- Auth Sign = Modalità di autenticazione del router verso il router sinistro = Pre-shared-Key
- Verifica autenticazione = modalità di autenticazione del router sinistro su questo router = RSA (certificato)
- ID locale/remoto = identità ISAKMP scambiate

```
 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
```

Configurazione routing

L'esempio di configurazione precedente consente di stabilire il tunnel, ma non fornisce informazioni sul routing (ossia le destinazioni disponibili sul tunnel). Con IKEv2, è possibile scambiare queste informazioni in due modi: Protocolli di routing dinamico e route IKEv2.

Protocolli di routing dinamico

Poiché il tunnel è un tunnel GRE point-to-point, si comporta come qualsiasi altra interfaccia point-to-point (ad esempio: seriale, dialer) ed è possibile eseguire qualsiasi IGP (Interior Gateway Protocol)/EGP (Exterior Gateway Protocol) sul collegamento per scambiare informazioni di routing. Di seguito è riportato un esempio di Enhanced Interior Gateway Routing Protocol (EIGRP):

1. Configurare il router sinistro per abilitare e annunciare l'EIGRP sulle interfacce LAN e tunnel:

```
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. Configurare il router destro per abilitare e annunciare l'EIGRP sulle interfacce LAN e tunnel:

```
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. Confermare che il percorso verso 192.168.200.0/24 sia appreso attraverso il tunnel tramite 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
```

Route IKEv2

Anziché utilizzare i percorsi del protocollo di routing dinamico per conoscere le destinazioni attraverso il tunnel, è possibile scambiare i percorsi durante la creazione di un'associazione di sicurezza (SA) IKEv2.

1. Sul router sinistro, configurare un elenco delle subnet che il router sinistro annuncia al router destro:

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

2. Sul router sinistro, configurare un criterio di autorizzazione per specificare le subnet da annunciare:
   /32 configurato sull'interfaccia del tunnel/24 route a cui si fa riferimento nell'ACL

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

3. Sul router sinistro, riconfigurare il profilo IKEv2 in modo che faccia riferimento ai criteri di autorizzazione quando vengono utilizzate chiavi già condivise:

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

4. Sul router destro ripetere i passaggi 1 e 2 e regolare il profilo IKEv2 in modo da fare riferimento ai criteri di autorizzazione quando vengono utilizzati i certificati:

```
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. Per forzare la compilazione di una nuova associazione di sicurezza IKEv2, usare i comandi **shut** e **no shut** sull'interfaccia del tunnel.

6. Verificare che le route IKEv2 siano state scambiate. Vedere "Subnet remote" in questo output di esempio:

```
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
```

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems