Exemple de configuration de site à site FlexVPN

Contenu

Introduction

Ce document fournit un exemple de configuration pour le tunnel GRE (Internet Protocol Security) site à site FlexVPN.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Conventions

Reportez-vous aux Conventions des conseils techniques de Cisco pour plus d'informations sur les conventions du document.

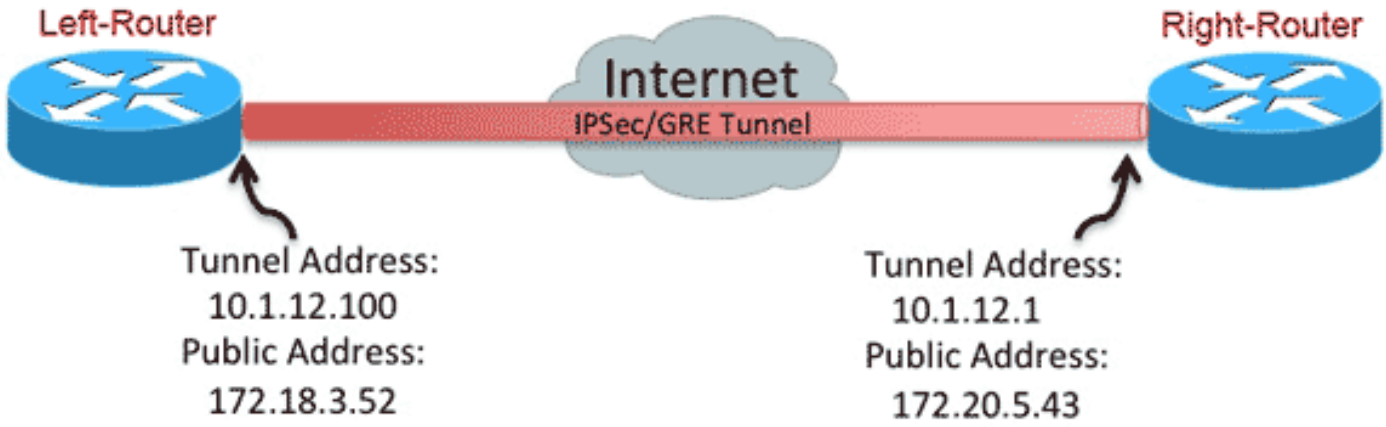
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration du tunnel PSK

La procédure décrite dans cette section décrit comment utiliser une clé prépartagée (PSK) afin de configurer les tunnels dans cet environnement réseau.

Routeur gauche

1. Configurez la clé Internet Key Exchange version 2 (IKEv2) :

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

2. Reconfigurer le profil par défaut IKEv2 afin de :
   correspondance sur l'ID IKEdéfinir les méthodes d'authentification pour les réseaux locaux et distantsréférencez la sonnerie indiquée à l'étape précédente.

```
 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. Reconfigurer le profil IPsec par défaut afin de référencer le profil IKEv2 par défaut :

```
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. Configurez les interfaces LAN et 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
```

Routeur droit

Répétez les étapes de la configuration du routeur gauche, mais avec les modifications nécessaires :

```
 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
```

Configuration du tunnel PKI

Une fois le tunnel de la section précédente terminé avec PSK, il peut être facilement modifié afin d'utiliser l'infrastructure à clé publique (PKI) pour l'authentification. Dans cet exemple, le routeur de gauche s'authentifie avec un certificat au routeur de droite. Le routeur de droite continue à utiliser une clé PSK afin de s'authentifier auprès du routeur de gauche. Cela a été fait pour montrer l'authentification asymétrique ; cependant, il est trivial de basculer entre les deux pour utiliser l'authentification par certificat.

Routeur gauche

1. Configurez Cisco IOS® Certificate Authority (CA) sur le routeur :

```
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. Authentifier et inscrire le point de confiance de l'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. Reconfigurer le profil IKEv2 :

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

Routeur droit

1. Authentifiez le point de confiance de l'autorité de certification de sorte que le routeur puisse vérifier le certificat du routeur de gauche :

```
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. Reconfigurer le profil IKEv2 afin de correspondre à la connexion entrante :

```
 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
```

Vérification

Utilisez la commande **show crypto ikev2 sa detail** afin de vérifier la configuration.

Le routeur de droite affiche ceci :

- Authentification = Comment ce routeur s'authentifie sur le routeur de gauche = Clé pré-partagée
- Vérification de l'authentification = Comment le routeur gauche s'authentifie sur ce routeur = RSA (certificat)
- ID local/distant = Les identités ISAKMP échangées

```
 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
```

Configuration du routage

L'exemple de configuration précédent permet d'établir le tunnel, mais ne fournit aucune information sur le routage (c'est-à-dire les destinations disponibles sur le tunnel). Avec IKEv2, il existe deux façons d'échanger ces informations : Protocoles de routage dynamique et routes IKEv2.

Protocoles de routage dynamique

Comme le tunnel est un tunnel GRE point à point, il se comporte comme toute autre interface point à point (par exemple : Serial, Dialer) et il est possible d'exécuter n'importe quel protocole IGP (Interior Gateway Protocol)/EGP (Exterior Gateway Protocol) sur la liaison afin d'échanger des informations de routage. Voici un exemple du protocole EIGRP (Enhanced Interior Gateway Routing Protocol) :

1. Configurez le routeur gauche afin d'activer et d'annoncer le protocole EIGRP sur les interfaces LAN et de 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. Configurez le routeur de droite afin d'activer et d'annoncer le protocole EIGRP sur les interfaces LAN et de 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. Vérifiez que la route vers 192.168.200.0/24 est apprise via le tunnel via 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
```

Routes IKEv2

Au lieu d'utiliser des routes de protocole de routage dynamique afin d'apprendre des destinations à travers le tunnel, les routes peuvent être échangées lors de l'établissement d'une association de sécurité (SA) IKEv2.

1. Sur le routeur de gauche, configurez une liste des sous-réseaux que le routeur de gauche annonce au routeur de droite :

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

2. Sur le routeur de gauche, configurez une stratégie d'autorisation afin de spécifier les sous-réseaux à annoncer :
   /32 configuré sur l'interface de tunnelroute /24 référencée dans la liste de contrôle d’accès

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

3. Sur le routeur de gauche, reconfigurez le profil IKEv2 afin de référencer la stratégie d'autorisation lorsque des clés pré-partagées sont utilisées :

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

4. Sur le routeur de droite, répétez les étapes 1 et 2 et ajustez le profil IKEv2 afin de référencer la stratégie d'autorisation lorsque des certificats sont utilisés :

```
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. Utilisez les commandes **shutdown** et **no shut** sur l'interface du tunnel afin de forcer la création d'une nouvelle SA IKEv2.

6. Vérifiez que les routes IKEv2 sont échangées. Reportez-vous à « Sous-réseaux distants » dans cet exemple de résultat :

```
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
```

Informations connexes

- Support et documentation techniques - Cisco Systems