Exemple de configuration de site à site de FlexVPN

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Configurez](#)
[Diagramme du réseau](#)
[Configuration de tunnel PSK](#)
[Quitter-routeur](#)
[Droit-routeur](#)
[Configuration de tunnel de PKI](#)
[Quitter-routeur](#)
[Droit-routeur](#)
[Vérifiez](#)
[Acheminement de la configuration](#)
[Protocoles de routage dynamique](#)
[Informations connexes](#)

Introduction

Ce document fournit une configuration d'échantillon pour le tunnel de l'encapsulation de routage d'IPSec de site à site de FlexVPN (IPsec) /Generic (GRE).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions de document.

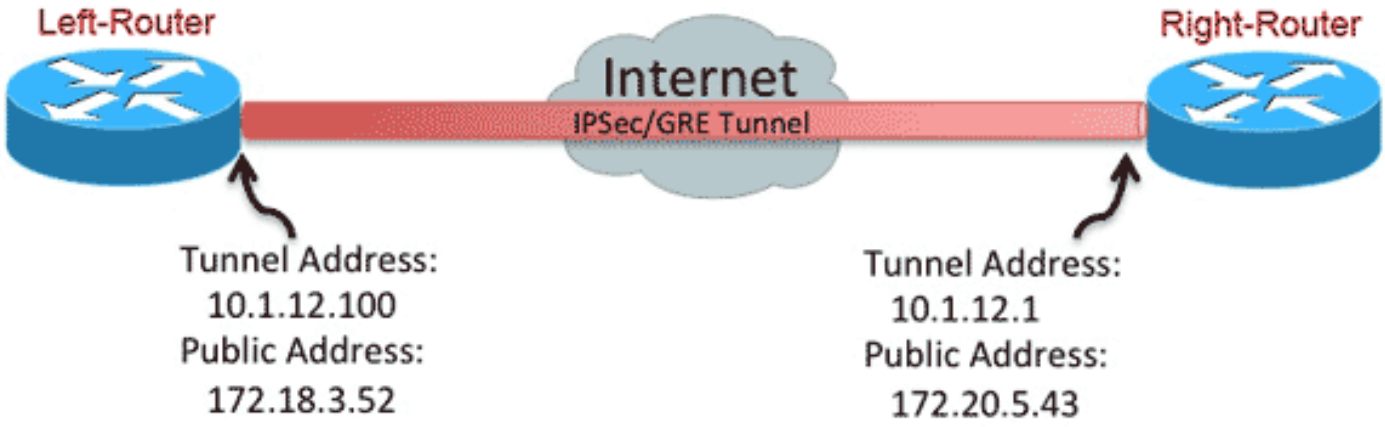
Configurez

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

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration de tunnel PSK

La procédure dans cette section décrit comment employer une clé pré-partagée (PSK) afin de configurer les tunnels dans cet environnement de réseau.

Quitter-routeur

1. Configurez le keyring de la version 2 d'échange de clés Internet (IKE) (IKEv2) :

```
 crypto ikev2 keyring mykeys
peer Right-Router
address 172.20.5.43
```

```
pre-shared-key Cisco123
!
```

2. Modifiez le profil IKEv2 par défaut :
   correspondance sur l'ID d'IKEplacez les méthodes d'authentification pour les gens du pays et le distantmettez en référence le keyring répertorié dans 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. Modifiez le profil IPSec par défaut afin de mettre en référence le profil du par défaut IKEv2 :

```
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 de 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
```

Droit-routeur

Répétez les étapes de la configuration de Quitter-routeur, mais avec ces 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 de tunnel de PKI

Après que le tunnel de la section précédente soit terminé avec PSK, il peut facilement être changé afin d'utiliser l'Infrastructure à clés publiques (PKI) pour l'authentification. Dans cet exemple, le Quitter-routeur s'authentifie avec un certificat au Droit-routeur. Le Droit-routeur continue à employer un PSK afin de s'authentifier au Quitter-routeur. Ceci a été fait pour afficher l'authentification asymétrique ; cependant, il est insignifiant pour commuter chacun des deux pour utiliser l'authentification de certificat.

Quitter-routeur

1. Configurez l'Autorité de certification (CA) de Cisco IOS® 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. Authentifiez et inscrivez-vous le point de confiance d'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. Modifiez le profil IKEv2 :

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

Droit-routeur

1. Authentifiez le point de confiance CA de sorte que le routeur puisse vérifier le certificat de Quitter-routeur :

```
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. Modifiez le profil IKEv2 afin d'apparier 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
```

Vérifiez

Employez la **crypto** commande **détaillée par SA d'ikev2 d'exposition** afin de vérifier la configuration.

Le Droit-routeur affiche ceci :

- Signe authentique = comment ce routeur s'authentifie au Quitter-routeur = au pre-shared-key
- Authentique vérifiez = comment le Quitter-routeur s'authentifie à ces routeur = RSA (le certificat)
- Id local/distant = les identités d'ISAKMP permutées

```
 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
```

Acheminement de la configuration

L'exemple de configuration précédente permet le tunnel à établir, mais ne fournit pas n'importe quelles informations au sujet du routage (c'est-à-dire, quelles destinations sont disponibles au-dessus du tunnel). Avec IKEv2, il y a deux manières de permuter ces informations : Protocoles de routage dynamique et artères IKEv2.

Protocoles de routage dynamique

Puisque le tunnel est un tunnel du Point à point GRE, il se comporte comme n'importe quelle autre interface point par point (par exemple : l'interface série, le numéroteur), et lui est possible pour exécuter tout Protocole IGP (Interior Gateway Protocol)/Protocole EGP (Exterior Gateway Protocol) au-dessus du lien afin de permuter les informations de routage. Voici un exemple de Protocole EIGPR (Enhanced Interior Gateway Routing Protocol) :

1. Configurez le Quitter-routeur afin d'activer et annoncer l'EIGRP sur le RÉSEAU LOCAL et les interfaces 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 Droit-routeur afin d'activer et annoncer l'EIGRP sur le RÉSEAU LOCAL et les interfaces 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. Confirmez que l'artère à 192.168.200.0/24 est apprise au-dessus du tunnel par l'intermédiaire de l'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
```

Artères IKEv2

Au lieu d'à l'aide des artères de protocole de routage dynamique afin d'apprendre des destinations à travers le tunnel, des artères pourraient être permutées pendant la création d'une association de sécurité IKEv2 (SA).

1. Sur le Quitter-routeur, configurez une liste des sous-réseaux que le Quitter-routeur annonce au Droit-routeur :

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

2. Sur le Quitter-routeur, configurez une stratégie d'autorisation afin de spécifier les sous-réseaux pour annoncer :
   /32 a configuré sur l'interface de tunnelartère de /24 référencée dans l'ACL`crypto ikev2`

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

3. Sur le Quitter-routeur, modifiez le profil IKEv2 afin de mettre en référence la stratégie d'autorisation quand des clés pré-partagées sont utilisées :

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

4. Sur le Droit-routeur, répétez les étapes 1 et 2 et ajustez le profil IKEv2 afin de mettre en référence la stratégie d'autorisation quand 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. N'utilisez la commande **fermée** et **aucune fermée** sur l'interface de tunnel afin de forcer nouvel IKEv2 SA à construire.

6. Vérifiez que les artères IKEv2 sont permutées. Voir « les sous-réseaux distants » dans cette sortie témoin :

```
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