Ejemplo de Configuración de Sitio a Sitio de FlexVPN

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para el túnel de seguridad de protocolo de Internet (IPsec)/encapsulación de routing genérico (GRE) de sitio a sitio FlexVPN.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Convenciones

Consulte las Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones de los documentos.

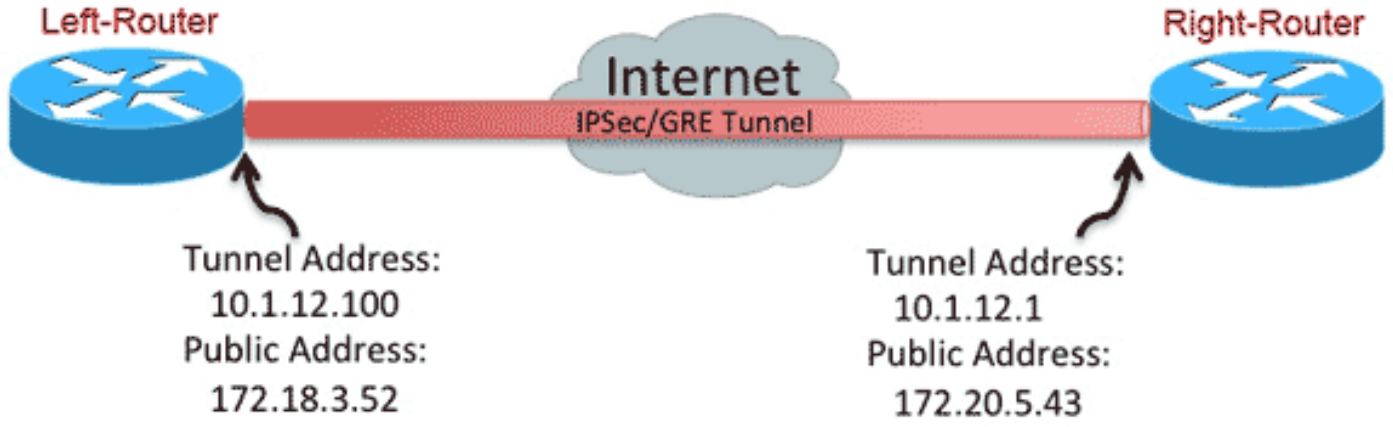
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración del Túnel PSK

El procedimiento de esta sección describe cómo utilizar una clave previamente compartida (PSK) para configurar los túneles en este entorno de red.

Router izquierdo

1. Configuración del llavero de Internet Key Exchange versión 2 (IKEv2):

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

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

2. Reconfigure el perfil predeterminado de IKEv2 para:
   coincidencia en la ID IKEestablezca los métodos de autenticación para local y remotohacer referencia al anillo de claves enumerado en el paso anterior

```
 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. Reconfigure el perfil IPSec predeterminado para hacer referencia al perfil IKEv2 predeterminado:

```
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. Configure las interfaces LAN y 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 derecho

Repita los pasos de la configuración del router izquierdo, pero con estos cambios necesarios:

```
 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
```

Configuración del Túnel PKI

Después de que el túnel de la sección anterior se complete con PSK, se puede cambiar fácilmente para utilizar la infraestructura de clave pública (PKI) para la autenticación. En este ejemplo, el router izquierdo se autentica con un certificado al router derecho. El router derecho continúa utilizando un PSK para autenticarse en el router izquierdo. Esto se ha hecho para mostrar la autenticación asimétrica; sin embargo, es trivial conmutar ambos para utilizar la autenticación de certificados.

Router izquierdo

1. Configure Cisco IOS® Certificate Authority (CA) en el 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. Autentique e inscriba el punto de confianza de 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. Reconfigure el perfil IKEv2:

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

Router derecho

1. Autentique el trustpoint de CA para que el router pueda verificar el certificado del router izquierdo:

```
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. Vuelva a configurar el perfil IKEv2 para que coincida con la conexión 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
```

Verificación

Utilice el comando **show crypto ikev2 como** detallado para verificar la configuración.

El router derecho muestra lo siguiente:

- Signo de autenticación = Cómo se autentica este router a sí mismo en el router izquierdo = clave precompartida
- Verificación de autenticación = Cómo se autentica el router izquierdo en este router = RSA (Certificado)
- ID local/remota = Las identidades ISAKMP intercambiadas

```
 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
```

Configuración de Ruteo

El ejemplo de configuración anterior permite establecer el túnel, pero no proporciona ninguna información sobre el ruteo (es decir, qué destinos están disponibles a través del túnel). Con IKEv2, hay dos maneras de intercambiar esta información: Protocolos de ruteo dinámicos y rutas IKEv2.

Protocolos de enrutamiento dinámico

Dado que el túnel es un túnel GRE punto a punto, se comporta como cualquier otra interfaz punto a punto (por ejemplo: serial, dialer) y es posible ejecutar cualquier protocolo de gateway interior (IGP)/protocolo de gateway exterior (EGP) a través del enlace para intercambiar información de routing. A continuación se muestra un ejemplo del protocolo de routing de gateway interior mejorado (EIGRP):

1. Configure el router izquierdo para habilitar y anunciar EIGRP en las interfaces LAN y de túnel:

```
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. Configure el router derecho para habilitar y anunciar EIGRP en las interfaces LAN y de túnel:

```
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. Confirme que la ruta a 192.168.200.0/24 se aprende a través del túnel a través de 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
```

Rutas IKEv2

En lugar de utilizar rutas de protocolo de routing dinámico para aprender destinos a través del túnel, las rutas podrían intercambiarse durante el establecimiento de una asociación de seguridad (SA) IKEv2.

1. En el router izquierdo, configure una lista de las subredes que el router izquierdo anuncia al router derecho:

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

2. En el router izquierdo, configure una política de autorización para especificar las subredes para anunciar:
   /32 configurado en la interfaz de túnel/24 ruta a la que se hace referencia en la ACL

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

3. En el router izquierdo, reconfigure el perfil IKEv2 para hacer referencia a la política de autorización cuando se utilizan claves previamente compartidas:

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

4. En el router derecho, repita los pasos 1 y 2 y ajuste el perfil IKEv2 para hacer referencia a la política de autorización cuando se utilizan certificados:

```
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. Utilice los comandos **shut** y **no shut** en la interfaz de túnel para forzar la construcción de una nueva SA IKEv2.

6. Verifique que se intercambien las rutas IKEv2. Consulte "Subredes remotas" en este ejemplo de salida:

```
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
```

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems