FlexVPN のサイト間の設定例

内容

概要

本書では、FlexVPN のサイト間の IPSec（Internet Protocol Security）/Generic Routing Encapsulation（GRE）トンネルのサンプル設定について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

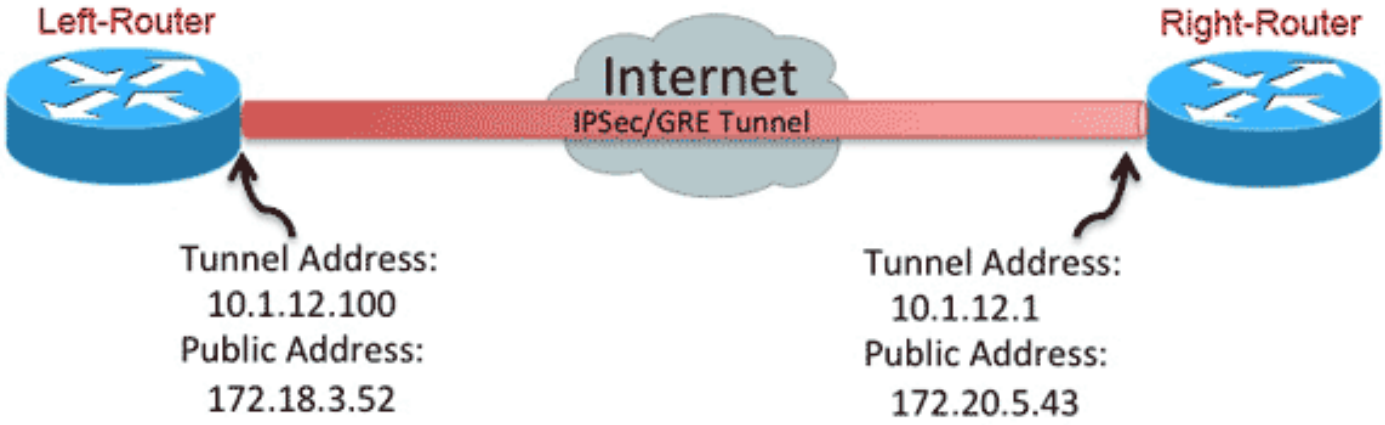
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



PSK トンネル構成

このセクションのプロシージャでは、このネットワーク環境でトンネルを設定するために事前共有キー（PSK）を使用する方法について説明します。

左側のルータ

1. インターネットキーエクスチェンジ バージョン 2 のキーリングの設定：

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

```
!
```

2. 次を行うために、IKEv2 デフォルト プロファイルを再設定します。
   IKE ID の一致ローカルおよびリモートの認証方式のセット前の手順で説明されているキーリングの参照

```
 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. デフォルトの IKEv2 プロファイルを参照するために次のデフォルトの IPsec プロファイルを再設定します。

```
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. 次の LAN インターフェイスと WAN インターフェイスを設定します。

```
 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
```

右側のルータ

左側のルータの設定手順を繰り返します。ただし、次の必要な変更を行います。

```
 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 トンネル構成

PSK を使用して前のセクションのトンネルの設定を完了させた後は、Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）を認証に使用するために簡単に変更できます。この例では、左側のルータは証明書を使用して右側のルータに対して自身を認証します。右側のルータは、左側のルータに対して自身を認証するために、PSK を使用し続けます。これは、非対称認証を表示するために行われていました。ただし、証明書認証を使用するために両方を切り替えることは大したことではありません。

左側のルータ

1. ルータ上で Cisco IOS® 認証局（CA）を設定します。

```
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. 次の ID トラストポイントを認証して登録します。

```
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. 次の IKEv2 プロファイルを再設定します。

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

右側のルータ

1. 次の CA トラストポイントを認証し、左側のルータの証明書を検証できるようにします。

```
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. 着信接続と一致させるために、次の IKEv2 プロファイルを再設定します。

```
 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
```

確認

構成を検証するために、**show crypto ikev2 sa detailed** コマンドを使用します。

右側のルータは次を示します。

- Auth Sign = このルータが左側のルータに対して自身を認証する方法 = 事前共有キー
- Auth Verify = 左側のルータがこのルータに対して自身を認証する方法 = RSA（証明書）
- Local/Remote id = ISAKMP ID の交換

```
 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
```

ルーティング設定

前回の構成例ではトンネルの確立を許可しましたが、ルーティングに関する情報（すなわち、どの接続先がトンネル上で利用可能であるかについて）は一切提供していません。 IKEv2 を使用した場合、この情報を交換する方法としては次の 2 つがあります。ダイナミック ルーティング プロトコルと IKEv2 ルート。

ダイナミック ルーティング プロトコル

トンネルは、ポイントツーポイント GRE トンネルであるため、他のポイントツーポイント インターフェイスのように動作します（例：シリアル、ダイヤラ）。また、このトンネルは、ルーティング情報を交換するために、リンク上で内部ゲートウェイ プロトコル（IGP）/外部ゲートウェイ プロトコル（EGP ）を実行することができます。Enhanced Interior Gateway Routing Protocol（EIGRP）の例を次に示します。

1. LAN とトンネル インターフェイス上で EIGRP を有効にしてアドバタイズするには、左側のルータを設定します。

   ```
   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. LAN とトンネル インターフェイス上で EIGRP を有効にしてアドバタイズするには、右側のルータを設定します。

```
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. EIGRP 経由で 192.168.200.0/24 へのルートがトンネル上で学習されたことを確認します。

```
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 ルート

トンネル全域で接続先を学習するために、ダイナミック ルーティング プロトコル ルーティングを使用する代わりに、IKEv2 セキュリティ アソシエーション（SA）の確立中にルートが交換されることがあります。

1. 左側のルータ上で、左側のルータが右側のルータにアドバタイズする次のサブネット一覧を設定します。

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

2. 左側のルータ上で、アドバタイズするサブネットを指定するために、次の認証ポリシーを設定します。
   トンネル インターフェイス上で設定された /32ACL 内で参照される /24 ルート

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

3. 左側のルータ上で、事前共有キーを使用するときに認証ポリシーを参照するために、次の IKEv2 プロファイルを再設定します。

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

4. 右側のルータ上で、証明書を使用するときに認証ポリシーを参照するために、手順 1 と 2 を

繰り返し、次の IKEv2 プロファイルを調整します。

```
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. 新しい IKEv2 SA の構築を強制させるために、トンネル インターフェイス上で **shut and no shut commands コマンドを使用します。**

6. IKEv2 ルートが交換されることを確認します。このサンプル出力の「リモート サブネット」を参照してください。

```
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
```

関連情報

- テクニカル サポートとドキュメント – Cisco Systems