ダイナミックIPアドレスを持つピアとのサイト間FlexVPNトンネルの設定

内容

はじめに

このドキュメントでは、リモートピアにダイナミックIPアドレスがある場合に、2台のCiscoルータ間にFlexVPNサイト間VPNトンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FlexVPN
- IKEv2プロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CSR1000Vデバイス
- Cisco IOS® XEソフトウェアバージョン17.3.4

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、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ネットワーク図

ダイナミックピアのトポロジ

この例のトポロジは、Ciscoルータと、パブリック側インターフェイスにダイナミックIPアドレスを持つ別のCiscoルータを示しています。

コンフィギュレーション

このセクションでは、リモートピアがダイナミックIPアドレスを使用する場合に、Ciscoルータでサイト間FlexVPNトンネルを設定する方法について説明します。

この設定例では、使用される認証方式は事前共有キー(PSK)ですが、公開キーインフラストラクチャ(PKI)も使用できます。

本社ルータの設定

この例では、ルータからのIKEv2スマートデフォルトが使用されています。IKEv2 Smart Defaults機能は、ほとんどのユースケースをカバーすることで、FlexVPN設定を最小限に抑えます。IKEv2スマートデフォルトは、特定の使用例に合わせてカスタマイズできますが、お勧めできません。スマートデフォルトには、IKEv2許可ポリシー、IKEv2プロポーザル、IKEv2ポリシー、インターネットプロトコルセキュリティ(IPsec)プロファイル、およびIPsecトランスフォームセットが含まれます。

デバイスのデフォルト値を確認するには、次に示すコマンドを実行します。

- show crypto ikev2 authorization policy default
- show crypto ikev2 proposal default
- show crypto ikev2 policy default
- show crypto ipsec profile default

- show crypto ipsec transform-set default

手順1 IKEv2キーリングを設定します。

- この場合、本社のルータはダイナミックIDであるためピアIPを認識しないため、任意のIPアドレスと照合されます。
- リモートキーとローカルキーも設定されます。
- 脆弱性を回避するために、強力なキーを使用することをお勧めします。

```
crypto ikev2 keyring FLEXVPN_KEYRING
 peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123
```

手順2 AAA（認証、許可、アカウンティング）モデルを設定します。

- これにより、このインスタンスに接続できるユーザの管理フレームワークが作成されます。
- 接続ネゴシエーションはこのデバイスから開始されるため、モデルはローカルデータベースを参照して認証ユーザを決定します。

```
aaa new-model
aaa authorization network FLEXVPN local
```

手順3 IKEv2プロファイルを設定します。

- リモートピアのIPアドレスがダイナミックであるため、特定のIPアドレスを使用してピアを識別することはできません。
- ただし、ピアデバイスで定義されたドメイン、FQDN、またはキーIDによってリモートピアを識別できます。

- PSKを指定するプロファイルの許可方式で使用される方式は、Authentication, Authorization and Accounting(AAA)グループを追加する必要があります。
- ここで認証方式がPKIの場合は、PKIではなくcertとして指定されます。
- 目的はダイナミック仮想トンネルインターフェイス(dVTI)を作成することであるため、このプロファイルは仮想テンプレートにリンクされます

```
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote key-id Peer123
 identity local address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
 virtual-template 1
```

手順4 IPsecプロファイルを設定します。

- デフォルトプロファイルを使用しない場合は、カスタムIPsecプロファイルを設定できます。
- 手順3で作成したIKEv2プロファイルが、このIPsecプロファイルにマッピングされます。

```
crypto ipsec profile defualt
 set ikev2-profile FLEXVPN_PROFILE
```

手順5ループバックインターフェイスと仮想テンプレートインターフェイスを設定します。

- リモートデバイスにはダイナミックIPアドレスがあるため、dVTIはテンプレートから作成する必要があります。
- このバーチャルテンプレートインターフェイスは、ダイナミックバーチャルアクセスインターフェイスの作成元となる設定テンプレートです。

```
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
```

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel protection ipsec profile default
```

ブランチルータの設定

ブランチルータに対して、前の手順に示すようにIKEv2キーリング、AAAモデル、IPsecプロファイル、およびIKEv2プロファイルを設定し、必要な設定変更と次に説明する設定変更を行います。

1.本社のルータに送信されるローカルIDをIDとして設定します。

```
crypto ikev2 profile FLEXVPN_PROFILE
 identity local key-id Peer123
 match identity remote address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
```

手順5スタティック仮想トンネルインターフェイスを設定します。

- 本社ルータのIPアドレスが既知であり、変更されないことを前提として、スタティックVTIインターフェイスが設定されます。

```
interface Tunnel0
 ip address 192.168.1.10 255.255.255.0
 tunnel source GigabitEthernet0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default
```

ルーティング設定

この例では、アクセスコントロールリスト(ACL)の設定を使用したIKEv2セキュリティアソシエーション(SA)の確立中にルーティングが定義されます。VPN経由で送信されるトラフィックを定義します。ダイナミックルーティングプロトコルを設定することもできますが、このドキュメントでは説明しません。

ステップ 5：ACL を定義します。

本社ルータ：

```
ip access-list standard Flex-ACL
 permit 10.10.10.0 255.255.255.0
```

ブランチ ルータ:

```
ip access-list standard Flex-ACL
 permit 10.20.20.0 255.255.255.0
```

手順 6：各ルータのIKEv2許可プロファイルを変更して、ACLを設定します。

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL
```

本社ルータの完全な設定

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
 peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote key-id Peer123
 identity local address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
 virtual-template 1

crypto ipsec profile default
 set ikev2-profile FLEXVPN_PROFILE

interface Loopback1
 ip address 192.168.1.1 255.255.255.0

interface Loopback10
 ip address 10.10.10.10 255.255.255.255

interface GigabitEthernet0
 ip address 172.16.1.1 255.255.255.0

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel protection ipsec profile default

ip access-list standard Flex-ACL
 5 permit 10.10.10.0 255.255.255.0
```

ブランチルータの完全な設定

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
 peer HUB
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
```

```
 identity local key-id Peer123
 match identity remote address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default

crypto ipsec profile default
 set ikev2-profile FLEXVPN_PROFILE

interface Loopback20
 ip address 10.20.20.20 255.255.255.255

interface Tunnel0
 ip address 192.168.1.10 255.255.255.0
 tunnel source GigabitEthernet0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default

interface GigabitEthernet0
 ip address dhcp
 negotiation auto

ip access-list standard Flex-ACL
 10 permit 10.20.20.0 255.255.255.0
```

確認

トンネルを確認するには、フェーズ1とフェーズ2が正常に稼働していることを確認する必要があります。

```
Headquarter#show crypto ikev2 sa detail
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         172.16.1.1/500        172.16.2.1/500        none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: P
      Life/Active Time: 86400/74645 sec
      CE id: 61256, Session-id: 1
      Status Description: Negotiation done
      Local spi: D5129F36B1180175       Remote spi: F9298874F90BFEC7
      Local id: 172.16.1.1
      Remote id: 172.16.2.1
      Local req msg id:  16             Remote req msg id:  31
      Local next msg id: 16             Remote next msg id: 31
      Local req queued:  16             Remote req queued:  31
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: enabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
      Remote subnets:                  -------------> This section shows the traffic to be routed acros
      192.168.1.10 255.255.255.255
```

```
      10.20.20.20 255.255.255.255

 IPv6 Crypto IKEv2  SA
```

フェーズ2、Ipsec

```
Headquarter#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.1/255.255.255.255/47/0)
   current_peer 172.16.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 225, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 225, #pkts decrypt: 225, #pkts verify: 225
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.2.1
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
     current outbound spi: 0xC124D7C1(3240417217)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xC2AADCAB(3265977515)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2912, flow_id: CSR:912, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-he
        sa timing: remaining key lifetime (k/sec): (4607993/628)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC124D7C1(3240417217)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2911, flow_id: CSR:911, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-he
        sa timing: remaining key lifetime (k/sec): (4608000/628)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

仮想アクセスインターフェイスがUP状態であることも確認する必要があります。

```
show interface Virtual-Access1
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback1 (192.168.1.1)
  MTU 9934 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 172.16.1.1, destination 172.16.2.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1434 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "default")
  Last input 20:53:34, output 20:53:34, output hang never
  Last clearing of "show interface" counters 20:55:43
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     586 packets input, 149182 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     15 packets output, 1860 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

トラブルシュート

このセクションでは、トンネル確立のトラブルシューティング方法について説明します

IKE ネゴシエーションが失敗する場合、次の手順を実行します。

1. 次のコマンドで現在の状態を確認します。

- show crypto ikev2 sa
- show crypto ipsec sa
- show crypto session

2.トンネルネゴシエーションプロセスをデバッグするには、次のコマンドを使用します。

- debug crypto ikev2
- debug crypto ipsec

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。