동적 IP 주소의 피어로 Site-to-Site FlexVPN 터널 구성

목차

소개

이 문서에서는 원격 피어에 동적 IP 주소가 있는 경우 2개의 Cisco 라우터 간에 FlexVPN Site-to-Site VPN 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FlexVPN
- IKEv2 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CSR1000V 디바이스
- Cisco IOS® XE Software, 버전 17.3.4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

네트워크 다이어그램

동적 피어에 대한 토폴로지

이 예의 토폴로지는 Cisco 라우터와 공용 인터페이스에 동적 IP 주소가 있는 다른 Cisco 라우터를 보여줍니다.

설정

이 섹션에서는 원격 피어가 동적 IP 주소를 사용할 때 Cisco 라우터에서 사이트 대 사이트 FlexVPN 터널을 구성하는 방법에 대해 설명합니다.

이 컨피그레이션 예에서는 사용되는 인증 방법이 PSK(Pre-Shared-Key)이지만 PKI(Public Key Infrastructure)도 사용할 수 있습니다.

본사 라우터의 컨피그레이션

이 예에서는 라우터의 IKEv2 Smart Defaults가 사용되었습니다. IKEv2 Smart Defaults 기능은 대부분의 활용 사례를 지원하여 FlexVPN 컨피그레이션을 최소화합니다. IKEv2 스마트 기본값은 특정 활용 사례에 맞게 사용자 지정할 수 있지만 권장되지는 않습니다. 스마트 기본값에는 IKEv2 권한 부여 정책, IKEv2 제안, IKEv2 정책, IPsec(Internet Protocol Security) 프로파일 및 IPsec 변형 집합이 포함됩니다.

디바이스의 기본값을 검토하려면 아래 나열된 명령을 실행할 수 있습니다.

- show crypto ikev2 authorization policy default
- crypto ikev2 proposal default 표시
- show crypto ikev2 policy default
- 암호화 ipsec 프로필 기본값 표시
- crypto ipsec transform-set default 표시

1단계 IKEv2 키링을 구성합니다.

- 이 경우, 본사 라우터는 피어 IP가 동적이기 때문에 피어 IP를 알지 못하므로, ID가 어떤 IP 주소와도 매칭합니다.
- 원격 및 로컬 키도 구성됩니다.
- 취약성을 방지하기 위해 강력한 키를 사용하는 것이 좋습니다.

```
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
```

2단계 AAA(Authentication, Authorization and Accounting) 모델을 구성합니다.

- 이렇게 하면 이 인스턴스에 연결할 수 있는 사용자에 대한 관리 프레임워크가 생성됩니다.
- 이 디바이스에서 연결 협상이 시작되므로 모델은 권한 있는 사용자를 확인하기 위해 로컬 데이터베이스를 참조합니다.

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

3단계 IKEv2 프로파일을 구성합니다.

- 원격 피어 IP 주소가 동적이면 특정 IP 주소를 사용하여 피어를 식별할 수 없습니다.
- 그러나 피어 디바이스에 정의된 도메인, FQDN 또는 Key-id를 기준으로 원격 피어를 식별할 수 있습니다.

- PSK를 지정하는 프로파일의 권한 부여 방법을 위해 AAA(Authentication, Authorization and Accounting) 그룹을 추가해야 합니다.
- 인증 방법이 PKI인 경우 여기서 PKI 대신 cert로 지정됩니다.
- 이 프로필은 dVTI(Dynamic Virtual Tunnel Interface)를 만드는 데 목적이 있으므로 가상 템플릿에 연결됩니다

```
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
```

4단계 IPsec 프로필을 구성합니다.

- 기본 프로필을 사용하지 않는 경우 사용자 지정 IPsec 프로필을 구성할 수 있습니다.
- 3단계에서 생성한 IKEv2 프로파일은 이 IPsec 프로파일에 매핑됩니다.

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

5단계 루프백 인터페이스 및 가상 템플릿 인터페이스를 구성합니다.

- 원격 디바이스는 동적 IP 주소를 가지므로 템플릿에서 dVTI를 생성해야 합니다.
- 이 가상 템플릿 인터페이스는 동적 가상 액세스 인터페이스가 생성되는 컨피그레이션 템플릿입니다.

```
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
```

브랜치 라우터 컨피그레이션

브랜치 라우터의 경우, 이전 단계에서 설명한 대로 IKEv2 Keyring, AAA model, IPsec profile, IKEv2 profile을 필수 컨피그레이션 변경 사항과 다음에 설명된 대로 구성합니다.

1. 본사 라우터로 전송되는 로컬 ID를 식별자로 구성합니다.

```
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
```

5단계 고정 가상 터널 인터페이스를 구성합니다.

- Headquarter 라우터의 IP 주소가 알려져 있고 변경되지 않는 경우, Static VTI 인터페이스가 구성됩니다.

```
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
```

라우팅 컨피그레이션

이 예에서는 IKEv2 SA(Security Association)를 설정하는 동안 액세스 제어 목록 컨피그레이션과 함께 라우팅이 정의됩니다. 이는 VPN을 통해 전송할 트래픽을 정의합니다. 동적 라우팅 프로토콜을 구성할 수도 있지만 이 문서의 범위에 속하지 않습니다.

5단계. ACL을 정의합니다.

본사 라우터:

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

브랜치 라우터:

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

6단계. 각 라우터에서 IKEv2 권한 부여 프로파일을 수정하여 ACL을 설정합니다.

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

본사 라우터 컨피그레이션 완료

```
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
```

브랜치 라우터 전체 컨피그레이션

```
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
```

다음을 확인합니다.

터널을 확인하려면 1단계 및 2단계가 작동 중이고 제대로 작동하는지 확인해야 합니다.

```
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
```

2단계, 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:
```

또한 가상 액세스 인터페이스가 UP 상태인지 확인해야 합니다.

```
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
```

문제 해결

이 섹션에서는 터널 설정 문제를 해결하는 방법에 대해 설명합니다

IKE 협상이 실패할 경우 다음 단계를 완료합니다.

1. 다음 명령을 사용하여 현재 상태를 확인합니다.

- show crypto ikev2 sa
- 암호화 ipsec sa 표시
- 암호화 세션 표시

2. 터널 협상 프로세스를 디버깅하려면 다음 명령을 사용합니다.

- crypto ikev2 디버그
- 암호화 ipsec 디버그

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.