ASA와 IOS 라우터 간의 동적 사이트 대 사이트 IKEv2 VPN 터널 컨피그레이션 예

목차

소개

이 문서에서는 ASA(Adaptive Security Appliance)와 라우터에 동적 IP 주소가 있고 ASA에 공용 인터페이스에 고정 IP 주소가 있는 Cisco 라우터 간에 사이트 대 사이트 IKEv2(Internet Key Exchange Version 2) VPN 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 버전 15.1(1)T 이상
- Cisco ASA 버전 8.4(1) 이상

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

배경 정보

이 문서에서는 다음 시나리오에 대해 설명합니다.

- 시나리오 1:ASA는 명명된 터널 그룹을 사용하는 고정 IP 주소로 구성되고 라우터는 동적 IP 주소로 구성됩니다.
- 시나리오 2:ASA는 동적 IP 주소로 구성되고 라우터는 동적 IP 주소로 구성됩니다.
- 시나리오 3:이 시나리오는 여기에서 설명하지 않습니다. 이 시나리오에서 ASA는 고정 IP 주소로 구성되지만 DefaultL2LGroup 터널 그룹을 사용합니다.이 컨피그레이션은 두 ASAs 컨피그레이션 예제 기사 간 동적 사이트 대 사이트 IKEv2 VPN 터널에 설명된 것과 유사합니다.

시나리오 1과 3의 가장 큰 구성 차이는 원격 라우터에서 사용하는 ISAKMP(Internet Security Association and Key Management Protocol) ID입니다.고정 ASA에서 DefaultL2LGroup을 사용하는 경우 라우터의 피어의 ISAKMP ID가 ASA의 주소여야 합니다.그러나 명명된 터널 그룹을 사용하는 경우 라우터의 피어의 ISAKMP ID는 ASA에 구성된 터널 그룹 이름과 동일해야 합니다.이는 라우터에서 다음 명령을 사용하여 수행됩니다.

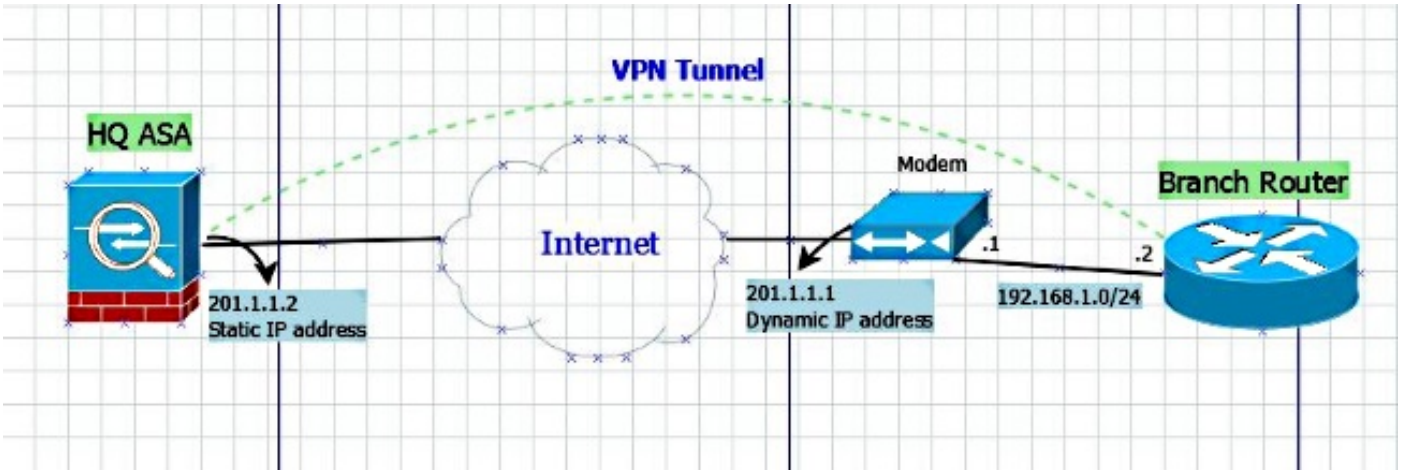
```
identity local key-id
```

고정 ASA에서 명명된 터널 그룹을 사용할 때의 장점은 DefaultL2LGroup을 사용할 때 사전 공유 키를 포함하는 원격 동적 ASA/라우터의 컨피그레이션이 동일해야 하며 정책 설정을 훨씬 세부적으로 조정할 수 없다는 것입니다.

구성

시나리오 1

네트워크 다이어그램



구성

이 섹션에서는 명명된 터널 그룹 컨피그레이션을 기반으로 ASA 및 라우터의 컨피그레이션에 대해 설명합니다.

고정 ASA 컨피그레이션

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
crypto map vpn 1 ipsec-isakmp dynamic dmap
crypto map vpn interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

group-policy Site-to-Site internal
group-policy Site-to-Site attributes
 vpn-tunnel-protocol ikev2
tunnel-group S2S-IKEv2 type ipsec-l2l
tunnel-group S2S-IKEv2 general-attributes
 default-group-policy Site-to-Site
tunnel-group S2S-IKEv2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco321
 ikev2 local-authentication pre-shared-key cisco123
```

동적 라우터 컨피그레이션

동적 라우터는 IKEv2 L2L 터널을 위한 동적 사이트이며 여기에 표시된 명령 하나를 추가하는 경우

일반적으로 구성하는 것과 거의 동일한 방식으로 구성됩니다.

```
ip access-list extended vpn
 permit ip host 10.10.10.1 host 201.1.1.2

crypto ikev2 proposal L2L-Prop
 encryption 3des
 integrity sha1
 group 2 5
!
crypto ikev2 policy L2L-Pol
 proposal L2L-Prop
!
crypto ikev2 keyring L2L-Keyring
 peer vpn
 address 201.1.1.2
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
 match identity remote address 201.1.1.2 255.255.255.255
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map vpn 10 ipsec-isakmp
 set peer 201.1.1.2
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
```

따라서 모든 동적 피어에서 key-id는 다르며 적절한 이름을 사용하여 Static ASA에 해당 터널 그룹을 생성해야 합니다. 이는 ASA에서 구현되는 정책의 세분성도 증가시킵니다.

시나리오 2

> **참고**: 이 컨피그레이션은 하나 이상의 면이 라우터인 경우에만 가능합니다.양쪽이 모두 ASA인 경우 이 설정은 현재 작동하지 않습니다.버전 8.4에서 ASA는 **set peer** 명령과 함께 FQDN(Fully Qualified Domain Name)을 사용할 수 없지만 CSCus37350의 향상된 기능이 향후 릴리스에 대해 요청되었습니다.

원격 ASA의 IP 주소가 동적이기는 하지만 VPN 인터페이스에 대해 Fully Qualified Domain Name이 할당된 경우 원격 ASA의 IP 주소를 정의하지 않고 원격 ASA의 FQDN을 라우터에서 이 명령으로 정의합니다.

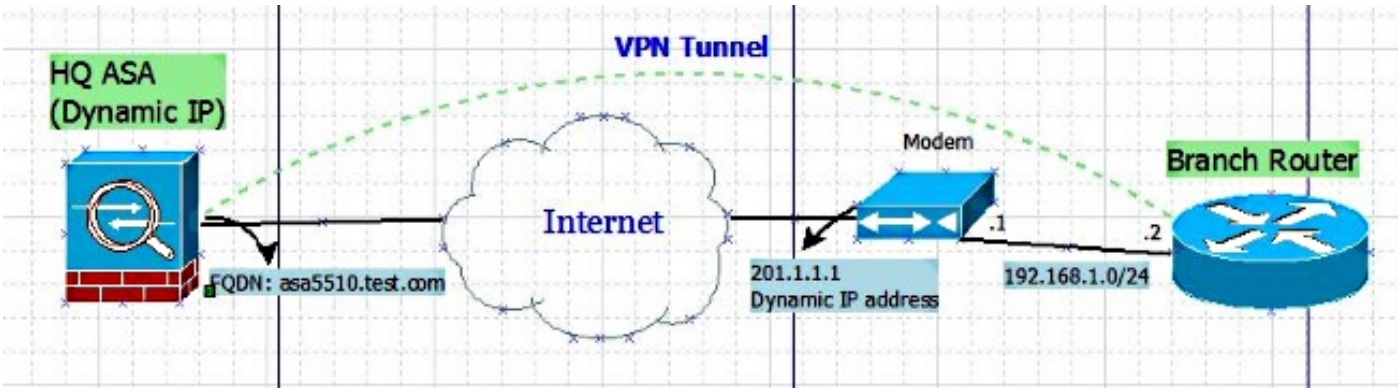
```
C1941(config)#do show run | sec crypto map
```

```
crypto map vpn 10 ipsec-isakmp
 set peer <FQDN> dynamic
```

팁:dynamic 키워드는 선택 사항입니다. set **peer** 명령을 통해 원격 IPsec 피어의 호스트 이름을 지정하는 경우 dynamic 키워드를 실행할 수 있습니다. 이 키워드는 IPsec 터널이 설정되기 바로 전까지의 호스트 이름의 DNS(Domain Name Server) 확인을 지연시킵니다.

지연 해결을 통해 Cisco IOS 소프트웨어는 원격 IPsec 피어의 IP 주소가 변경되었는지 여부를 탐지할 수 있습니다.따라서 소프트웨어는 새 IP 주소의 피어에 연결할 수 있습니다. dynamic 키워드가 발급되지 않으면 호스트 이름이 지정된 직후 확인됩니다.따라서 Cisco IOS 소프트웨어는 IP 주소 변경을 탐지할 수 없으므로 이전에 확인한 IP 주소에 연결을 시도합니다.

네트워크 다이어그램



구성

동적 ASA 컨피그레이션

ASA의 컨피그레이션은 물리적 인터페이스의 IP 주소가 정적으로 정의되지 않는다는 한 가지 예외와 함께 Static ASA Configuration과 동일합니다.

라우터 컨피그레이션

```
crypto ikev2 keyring L2L-Keyring
 peer vpn
 hostname asa5510.test.com
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
 !
crypto ikev2 profile L2L-Prof
 match identity remote fqdn domain test.com
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
```

```
crypto map vpn 10 ipsec-isakmp
 set peer asa5510.test.com dynamic
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

고정 ASA

- 다음은 show crypto IKEv2 sa det 명령의 결과입니다.

```
IKEv2 SAs:

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote     Status          Role
120434199        201.1.1.2/4500        201.1.1.1/4500      READY    RESPONDER
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/915 sec
     Session-id: 23
     Status Description: Negotiation done
     Local spi: 97272A4B4DED4A5C       Remote spi: 67E01CB8E8619AF1
     Local id: 201.1.1.2
      Remote id: S2S-IKEv2
     Local req mess id: 43             Remote req mess id: 2
     Local next mess id: 43            Remote next mess id: 2
     Local req queued: 43              Remote req queued: 2
     Local window: 1                   Remote window: 5
     DPD configured for 10 seconds, retry 2
     NAT-T is detected  outside
Child sa: local selector  201.1.1.2/0 - 201.1.1.2/65535
          remote selector 10.10.10.1/0 - 10.10.10.1/65535
          ESP spi in/out: 0x853c02/0x41aa84f4
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

- 다음은 show crypto ipsec sa 명령의 결과입니다.

```
interface: outside
   Crypto map tag: dmap, seq num: 1, local addr: 201.1.1.2

     local ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
     remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
     current_peer: 201.1.1.1


     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
```

```
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 201.1.1.2/4500, remote crypto endpt.: 201.1.1.1/4500
    path mtu 1500, ipsec overhead 82(52), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 41AA84F4
    current inbound spi : 00853C02

  inbound esp sas:
    spi: 0x00853C02 (8731650)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
       slot: 0, conn_id: 94208, crypto-map: dmap
       sa timing: remaining key lifetime (kB/sec): (4101119/27843)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x0000001F
  outbound esp sas:
    spi: 0x41AA84F4 (1101694196)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
       slot: 0, conn_id: 94208, crypto-map: dmap
       sa timing: remaining key lifetime (kB/sec): (4055039/27843)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

동적 라우터

- 다음은 show crypto IKEv2 sa detail 명령의 결과입니다.

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1013 sec
     CE id: 1023, Session-id: 23
     Status Description: Negotiation done
     Local spi: 67E01CB8E8619AF1       Remote spi: 97272A4B4DED4A5C
      Local id: S2S-IKEv2
     Remote id: 201.1.1.2
     Local req msg id:  2              Remote req msg id:  48
     Local next msg id: 2              Remote next msg id: 48
     Local req queued:  2              Remote req queued:  48
     Local window:      5              Remote window:      1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes
```

```
 IPv6 Crypto IKEv2  SA
```

- 다음은 show crypto ipsec sa 명령의 결과입니다.

```
interface: GigabitEthernet0/0
   Crypto map tag: vpn, local addr 192.168.1.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
  current_peer 201.1.1.2 port 4500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
   #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.: 192.168.1.2, remote crypto endpt.: 201.1.1.2
    plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0x853C02(8731650)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x41AA84F4(1101694196)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x853C02(8731650)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

동적 라우터(원격 동적 ASA 사용)

- 다음은 show crypto IKEv2 sa detail 명령의 결과입니다.

```
C1941#show cry ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1516 sec
      CE id: 1034, Session-id: 24
      Status Description: Negotiation done
      Local spi: 98322AED6163EE83       Remote spi: 092A1E5620F6AA9C
       Local id: S2S-IKEv2
       Remote id: asa5510.test.com
      Local req msg id:  2              Remote req msg id:  73
      Local next msg id: 2              Remote next msg id: 73
      Local req queued:  2              Remote req queued:  73
      Local window:      5              Remote window:      1
      DPD configured for 0 seconds, retry 0
      Fragmentation not configured.
      Extended Authentication not configured.
      NAT-T is detected inside
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes

 IPv6 Crypto IKEv2  SA
```

참고:이 출력의 원격 및 로컬 ID는 올바른 터널 그룹에 속하는지 확인하기 위해 ASA에 정의한 **명명된 터널 그룹입니다**.두 끝 중 하나에서 IKEv2를 디버깅하는 경우에도 이를 확인할 수 있습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령**을** 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

Cisco IOS 라우터에서 다음을 사용합니다.

```
deb crypto ikev2 error
deb crypto ikev2 packet
deb crypto ikev2 internal
```

ASA에서 다음을 사용합니다.

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```