ASA と IOS ルータの間の動的サイト間 IKEv2 VPN トンネルの設定例

目次

はじめに

このドキュメントでは、適応型セキュリティ アプライアンス (ASA) と Cisco ルータ間にサイト間インターネットキーエクスチェンジ バージョン 2 (IKEv2) VPN トンネルを設定する方法について説明します。ここでは、公共へのインターフェイスでルータにダイナミック IP アドレスが設定されており、ASA に静的 IP アドレスが設定されています。

前提条件

要件

このドキュメントに関しては個別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くものです。

- Cisco IOS®バージョン15.1(1)T以降
- Cisco ASA バージョン 8.4(1) 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

このドキュメントでは次のシナリオについて説明します。

- シナリオ 1：ASA には静的 IP アドレスが設定されており、名前付きトンネル グループを使用します。ルータにはダイナミック IP アドレスが設定されています。
- シナリオ 2：ASA にはダイナミック IP アドレスが設定されており、ルータにもダイナミック IP アドレスが設定されています。
- シナリオ 3：このシナリオについては説明しません。このシナリオでは、ASAは静的IPアドレスで構成されますが、DefaultL2LGroupトンネルグループを使用します。この設定は、『2 つの ASA 間でのダイナミックサイト間 IKEv2 VPN トンネルの設定例』で説明する設定に似ています。

シナリオ 1 と 3 の設定における最も大きな違いは、リモート ルータが使用する Internet Security Association and Key Management Protocol（ISAKMP）ID です。スタティック ASA で DefaultL2LGroup を使用する場合、ルータでのピアの ISAKMP ID は ASA のアドレスでなければなりません。ただし、名前付きトンネル グループを使用する場合は、ルータでのピアの ISAKMP ID は、ASA で設定されているトンネル グループ名と同一でなければなりません。このためにはルータで次のコマンドを実行します。

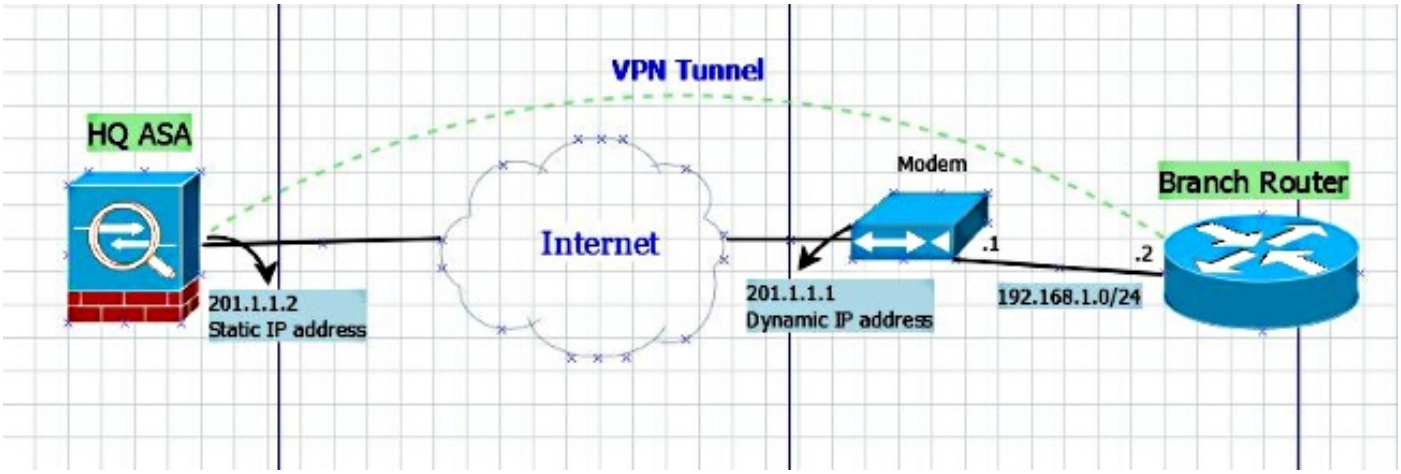
```
identity local key-id
```

スタティック ASA で名前付きトンネル グループを使用する利点は、DefaultL2LGroup を使用すると、リモート ダイナミック ASA/ルータでは、事前共有キーを含む設定が同一である必要があり、ポリシーの設定でそれほど粒度を持たせることができない点です。

設定

シナリオ 1

ネットワーク図



コンフィギュレーション

このセクションでは、名前付きトンネル グループの設定に基づく ASA とルータの設定について説明します。

スタティック ASA の設定

```
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
```

ダイナミック ルータの設定

ダイナミック ルータは、ルータが IKEv2 L2L トンネルのダイナミック サイトである場合の通常

の設定方法とほぼ同じ方法で設定され、次に示す 1 つの追加コマンドが使用されます。

```
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
```

したがって各ダイナミック ピアでは key-id が異なり、対応するトンネルグループをスタティック ASA で正しい名前を使用して作成する必要があります。これにより、ASA に導入されるポリシーの粒度がさらに細かくなります。

シナリオ 2

> **注**：この設定は、少なくとも1つの側がルータである場合にのみ可能です。現時点では、両側が ASA の場合はこのセットアップは機能しません。バージョン 8.4 では ASA は set peer コマンドに完全修飾ドメイン名（FQDN）を使用できませんが、CSCus37350 機能拡張のために今後のリリースが必要とされています。

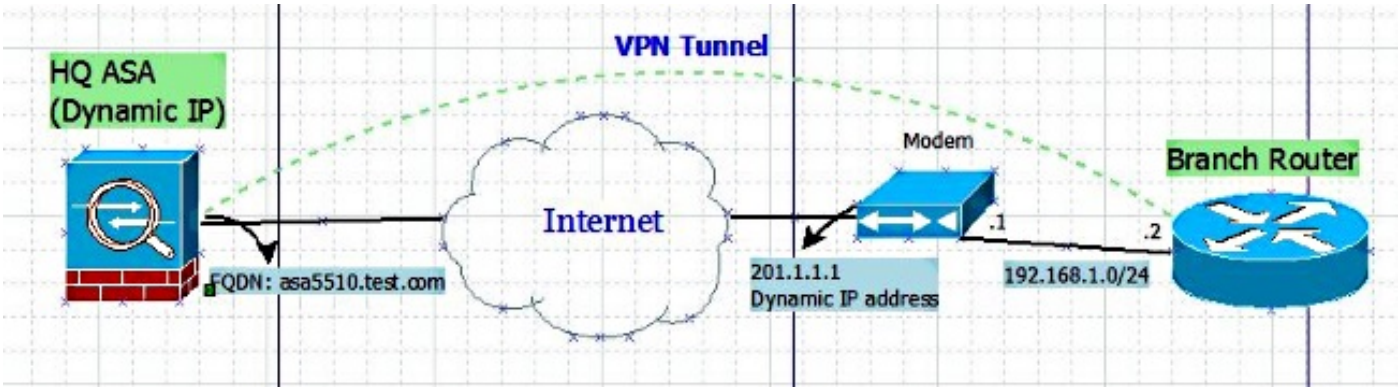
リモート ASA の IP アドレスがダイナミック IP アドレスであるものの、その VPN インターフェイスに完全修飾ドメイン名が割り当てられている場合、リモート ASA の IP アドレスを定義する代わりに、ルータで次のコマンドを使用してリモート ASA の FQDN を定義するようになりました。

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

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

> **ヒント**：**dynamic**キーワードはオプションです。**set** peerコマンドでリモートIPsecピアのホスト名を指定する場合は、dynamicキーワードを発行して、IPsecトンネルが確立される直前までホスト名のドメインネームサーバ(DNS)解決を延期します。
>
> 解決が遅れることで、Cisco IOS ソフトウェアはリモート IPsec ピアの IP アドレスが変更されたかどうかを検出できます。したがって、ソフトウェアは新しいIPアドレスでピアに接続できます。dynamicキーワードが発行されない場合、ホスト名は指定された直後に解決されます。このため、Cisco IOS ソフトウェアは IP アドレスの変更を検知できず、以前に解決した IP アドレスに対して接続を試みます。

ネットワーク図



コンフィギュレーション

ダイナミック ASA の設定

この ASA の設定は[スタティック ASA の設定とほぼ同一ですが、唯一異なる点として、物理インターフェイスの IP アドレスが静的に定義されないことがあります。]

ルータの設定

```
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
```

確認

このセクションでは、設定が正常に機能していることを確認します。

スタティック ASA

- 次に **show crypto IKEv2 sa det** コマンドの結果を示します。

```
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
```

- 次に **show crypto ipsec sa** コマンドの結果を示します。

```
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
```

ダイナミック ルータ

- 次に **show crypto IKEv2 sa detail** コマンドの結果を示します。

```
 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
```

- 次に **show crypto ipsec sa** コマンドの結果を示します。

```
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:
```

ダイナミック ルータ (リモート ダイナミック ASA 付)

- 次に **show crypto IKEv2 sa detail コマンドの結果を示します。**

```
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
```

注：この出力のリモート ID とローカル ID は、正しいトンネル グループに含まれるかどうかを確認するために ASA で定義した名前付きトンネル グループです。いずれかの側で IKEv2 をデバッグする場合にもこれを確認できます。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

注：debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

Cisco IOS ルータでは次のコマンドを使用します。

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

ASA では次のコマンドを使用します。

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