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

概要

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 またはそれ以降
- Cisco ASA バージョン 8.4(1) または それ 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

この資料はこれらのシナリオを説明します:

- シナリオ 1： 名前を挙げられたトンネル グループを使用し、ルータがダイナミックIPアドレスで設定される ASA は静的IP アドレスで設定されます。
- シナリオ 2： ASA はダイナミックIPアドレスで設定され、ルータはダイナミックIPアドレスで設定されます。
- シナリオ 3： このシナリオはここで説明されていません。 このシナリオでは、ASA は静的IPアドレスで設定されますが、DefaultL2LGroup トンネル グループを使用します。 これのための設定は説明があるものがに 2 ASA 設定例技術情報間のサイト IKEv2 VPN トンネルへのダイナミック サイトに類似したです。

シナリオ 1 および 3 間の最も大きいコンフィギュレーションの差はリモートルータによって使用される Internet Security Association and Key Management Protocol（ISAKMP） ID です。 DefaultL2LGroup が静的な ASA で使用されるとき、ルータのピアの ISAKMP ID は ASA のアドレスである必要があります。 ただし、名前を挙げられたトンネル グループが使用されれば、ルータのピアの ISAKMP ID は ASA で設定されるトンネル グループ名前と同じである必要があります。 これはルータのこのコマンドで達成されます:

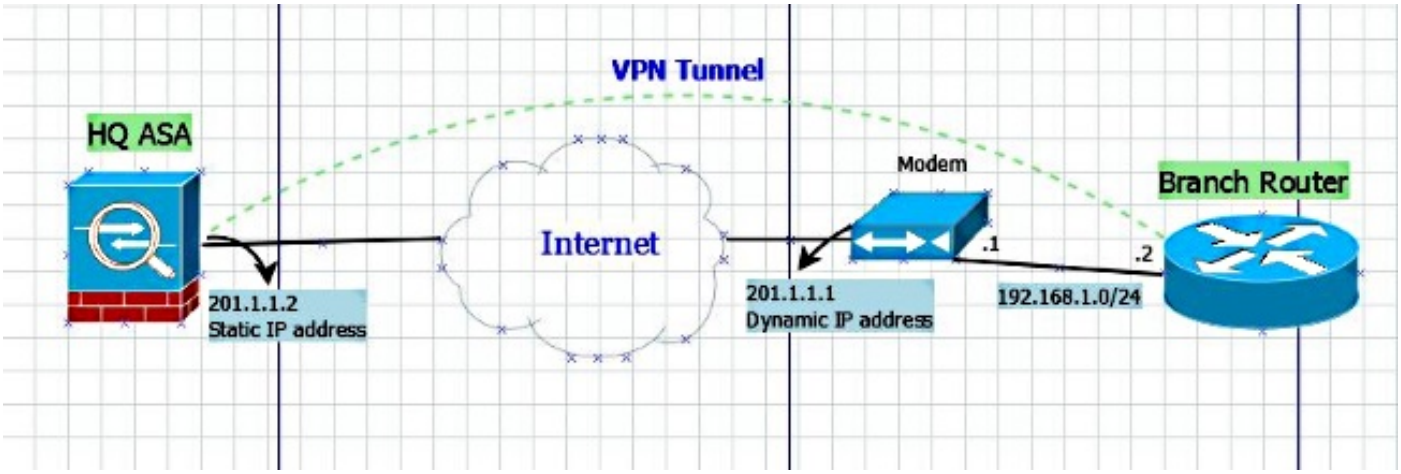
```
identity local key-id <name of the tunnel-group on the static ASA>
```

静的な ASA の名前を挙げられたトンネル グループを使用する長所は DefaultL2LGroup が使用されるときこと、事前共有キーが含まれているリモート ダイナミック ASA/ルータの設定同一である必要があるであり、ポリシーの設定の多くの細かさを可能にしません。

設定

シナリオ 1

ネットワーク図



設定

このセクションは指名されたトンネル グループ設定に基づいて ASA およびルータの設定を説明します。

静的な ASA 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 ルータコンフィギュレーション

ダイナミック ルータはルータがここに示されているように 1 つのコマンドの付加が付いている

IKEv2 L2L トンネルのためのダイナミック サイトなら普通設定するのと同じ方法ほとんど設定されます:

```
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
```

従って各ダイナミック ピアで、キー ID は異なって、対応するトンネル グループはまた ASA で設定される polocies の細かさを高める右の名前で静的な ASA で作成する必要があります。

シナリオ2

> **注:** この設定は少なくとも一方がルータのときだけ可能性のあるです。 両側が ASA である場合、この設定は現時点ではたらきません。 バージョン 8.4 では、ASA は **set peer コマンド**で完全修飾ドメイン名（FQDN）を使用できませんが CSCus37350 機能拡張は未来のリリースのために要求されました。

しかしリモート ASA の IP アドレスがダイナミック同様に持っていたら VPN インターフェイスに割り当てられるドメイン ネームの絶対表記をよりもむしろリモート ASA の IP アドレスを、今定義しますルータのこのコマンドでリモート ASA の FQDN を定義して下さい:

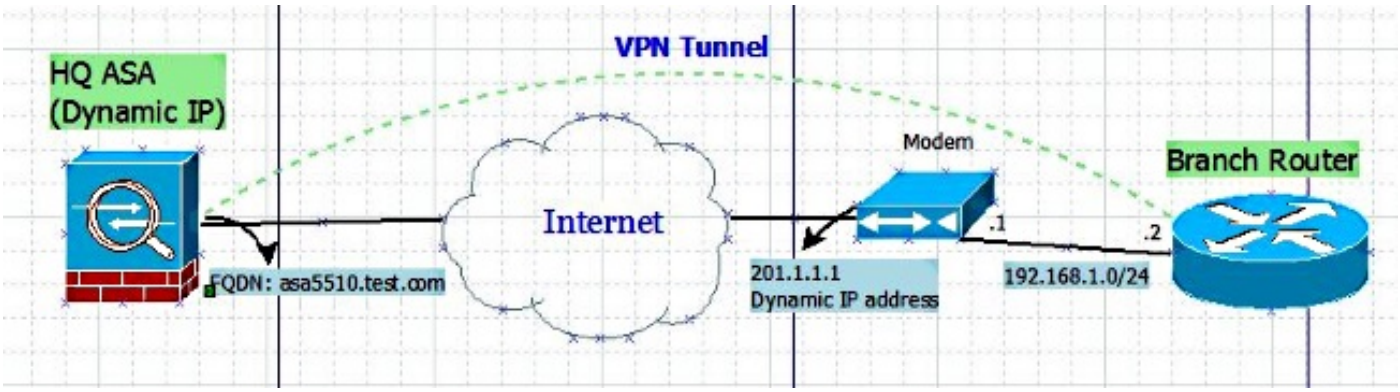
```
C1941(config)#do show run | sec crypto map

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

ヒント： **ダイナミック キーワードは**オプションです。 - **set peer コマンド**によるリモート IPSec ピアのホスト名を規定 するとき、またホスト名の Domain Name Server （ DNS ）解像度を延期するダイナミック キーワードを発行できます-まで IPSecトンネルの前に確立される。

延期解決はリモート IPSec ピアの IP アドレスが変更されたかどうか検出することを Cisco IOSソフトウェアが可能にします。 従って、ソフトウェアは新しい IP アドレスでピアに接触できます。 ダイナミック キーワードが発行されない場合、ホスト名は規定 される直後に解決されます。 このように、Cisco IOSソフトウェアは IP アドレス変更を検出できないし、従ってその IP アドレスに接続する試み以前に解決しました。

ネットワーク図



設定

ダイナミック ASA 設定

ASA の設定は物理インターフェイスの IP アドレスは統計的に定義されないことの 1 つの例外だけを除く静的な ASA 設定と同じです。

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。

静的な ASA

- 提示暗号 IKEv2 sa det コマンドの結果はここにあります:

```
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
```

- show crypto ipsec sa コマンドの結果はここにあります:

```
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
```

ダイナミック ルータ

- 提示暗号 IKEv2 sa detail コマンドの結果はここにあります:

```
  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
```

- show crypto ipsec sa コマンドの結果はここにあります:

```
  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
```

ダイナミック ルータ (リモート ダイナミック ASA と)

- **提示暗号 IKEv2 sa detail コマンド**の結果はここにあります:

```
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およびローカル ID は右のトンネル グループでころぶかどうか確認するために ASA で定義した**指名されたトンネル グループ**です。 これはまたどちらかの端の IKEv2 をデバッグする場合確認することができます。

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。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 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、使用して下さい:

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

ASA で、使用して下さい:

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