# Secure FirewallおよびCisco IOSでのDVTIの実装

## 内容



## 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)でEIGRPを使用してダイナミック仮想トンネルインターフェイス(DVTI)ハブアンドスポークソリューションを実装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。

- ASAの仮想トンネルインターフェイス(VTI)の基本的な知識
- ハブ/スポーク/ISP間の基本的なアンダーレイ接続
- EIGRPの基本的な知識

- 適応型セキュリティアプライアンスバージョン9.19(1)以降

### 使用するコンポーネント

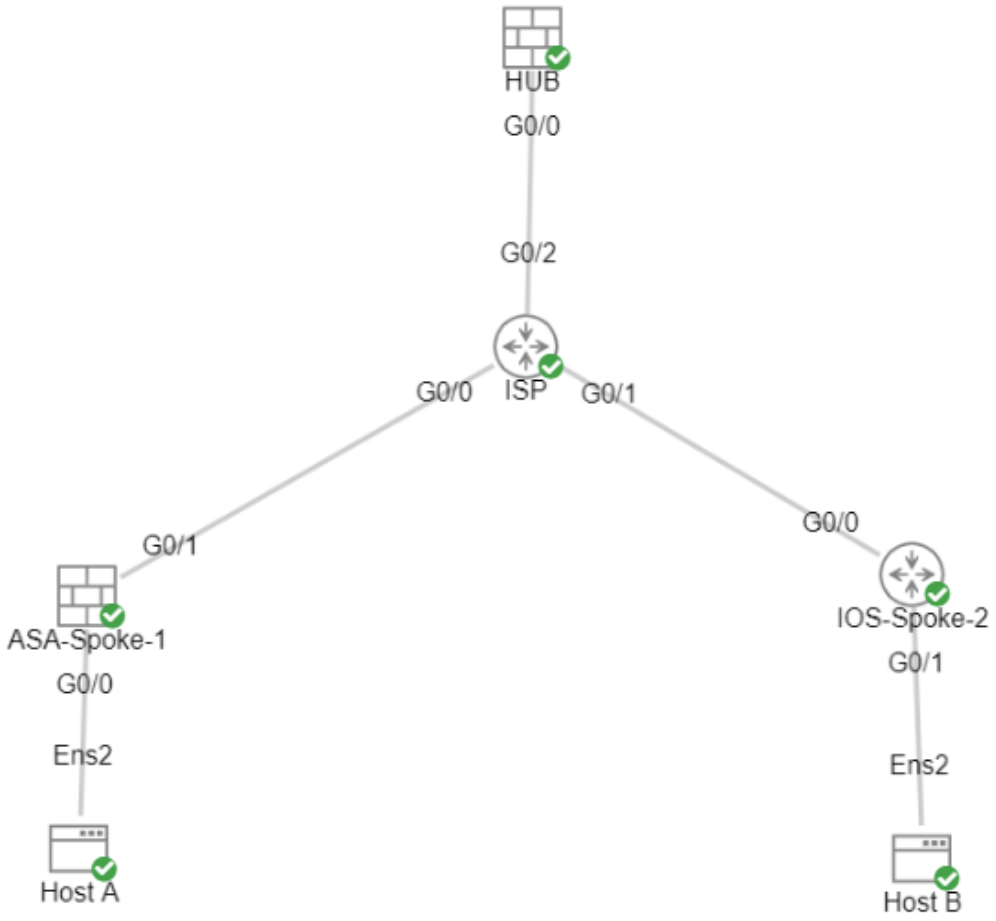
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 2台のASAvデバイス(両方ともバージョン9.19(1))スポーク1とハブで使用
- Cisco IOS® vデバイスバージョン15.9(3)M4 X 21つはISPデバイス用で、もう1つはスポーク2用です。
- トンネル用の汎用トラフィックに対する2つのUbuntuホスト

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。

## 設定

### ネットワーク図



# コンフィギュレーション

## ハブASAでのWANインターフェイスとIKEv2暗号化パラメータの設定

ハブで設定モードに入ります。

```
interface g0/0
ip address 198.51.100.1 255.255.255.0
nameif OUTSIDE
```

## ハブASAでのIKEv2パラメータの設定

IKE接続のフェーズ1パラメータを定義するIKEv2ポリシーを作成します。

```
crypto ikev2 policy 1      (The number is locally significant on the device, this determine the order i
encryption aes-256         (Defines the encryption parameter used to encrypt the initial communication
integrity sha256           (Defines the integrity used to secure the initial communication between the
group 21                   (Defines the Diffie-Hellman group used to protect the key exchange between d
prf sha256                 (Pseudo Random Function, an optional value to define, automatically chooses
lifetime seconds 86400     (Controls the phase 1 rekey, specified in seconds. Optional value, as the de
```

トラフィックの保護に使用するフェーズ2パラメータを定義するIKEv2 IPsecプロポーザルを作成します。

```
crypto ipsec ikev2 ipsec-proposal NAME                (Name is locally signicant and is used as a refer
protocol esp encryption aes-256                       (specifies that Encapsulating Security Payload an
protocol esp integrity sha-256                        (specifies that Encapsulating Security Payload an
```

IPsecプロポーザルを含むIPsecプロファイルを作成します。

```
crypto ipsec profile NAME                    (This name is referenced on the Virtual-Template Interface
set ikev2 ipsec-proposal NAME                (This is the name previously used when creating the ipsec-
```

## ループバックおよび仮想テンプレートインターフェイスの作成

```
interface loopback 1
ip address 172.16.50.254 255.255.255.255        (This IP address is used for all of the Virtual-Access
```

```
nameif LOOP1



interface Virtual-Template 1 type tunnel
ip unnumbered LOOP1                                (Borrows the IP address specified in Loopback1 for a
nameif DVTI
tunnel source Interface OUTSIDE                    (Specifies the Interface that the tunnel terminates
tunnel mode ipsec ipv4                             (Specifies that the mode uses ipsec, and uses ipv4)
tunnel protection ipsec profile NAME               (Reference the name of the previously created ipsec
```

## トンネルグループを作成し、IKEv2交換によってトンネルインターフェイスIPをアドバタイズする

トンネルグループを作成して、トンネルのタイプと認証方法を指定します。

```
tunnel-group DefaultL2LGroup ipsec-attributes              ('DefaultL2LGroup' is a default tunnel-group
virtual-template 1                                         (This command ties the Virtual-Template previ
ikev2 remote-authentication pre-shared-key cisco123        (This specifies the remote authentication as
ikev2 local-authentication pre-shared-key cisco123         (This specifies the local authentication as a
ikev2 route set Interface                                  (Advertises the VTI Interface IP over IKEv2 e
```

## ハブASAでのEIGRPルーティングの設定

```
router eigrp 100
network 172.16.50.254 255.255.255.255         (Advertise the IP address of the Loopback used for the Vi
```

## スポークASAのインターフェイスの設定

WANインターフェイスを設定します。

```
interface g0/1
ip address 203.0.113.1 255.255.255.0
nameif OUTSIDE-SPOKE-1
```

LANインターフェイスを設定します。

```
interface g0/0
ip address 10.45.0.4 255.255.255.0
nameif INSIDE-SPOKE-1
```

ループバックインターフェイスを設定します。

```
interface loopback1
ip address 172.16.50.1 255.255.255.255
nameif Loop1
```

## スポークASAでのIKEv2暗号化パラメータの設定

ハブのパラメータと一致するIKEv2ポリシーを作成します。

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 21
prf sha256
lifetime 86400
```

ハブのパラメータに一致するIKEv2 IPsecプロポーザルを作成します。

```
crypto ipsec ikev2 ipsec-proposal NAME           (Name is locally signicant, this does not need to matc
protocol esp encryption aes-256
protocol esp integrity sha-256
```

IPsecプロポーザルを含むIPsecプロファイルを作成します。

```
crypto ipsec profile NAME               (This name is locally significant and is referenced in the SVTI
set ikev2 ipsec-proposal NAME           (This is the name previously used when creating the ipsec-propo
```

## スポークASAでのスタティック仮想トンネルインターフェイスの設定

ハブをポイントするスタティック仮想トンネルインターフェイス(VTI)を設定します。 スポークのデバイスは、ハブへの通常の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。仮想テンプレートを必要とするのはハブだけです。

```
interface tunnel1
ip unnumbered loopback1
nameif ASA-SPOKE-SVTI
tunnel destination  198.51.100.254          (Tunnel destination references the Hub ASA tunnel source. C
```

```
tunnel mode ipsec ipv4
tunnel protection ipsec profile NAME
```

## トンネルグループを作成し、IKEv2交換によってトンネルインターフェイスIPをアドバタイズする

```
tunnel-group 198.51.100.1 type ipsec-l2l                    (This specifies the connection type as ipsec
tunnel-group 198.51.100.1 ipsec-attributes                  (Ipsec attributes allows you to make changes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
ikev2 route set Interface
```

## スポークASAでのEIGRPルーティングの設定

EIGRP自律システムを作成し、アドバタイズする必要なネットワークを適用します。

```
router eigrp 100
network 10.45.0.0 255.255.255.0        (Advertises the Host-A network to the hub. This allows the hub t
network 172.16.50.1 255.255.255.255    (Advertises and utilizes the tunnel IP address to form an EIGRP
```

## スポークルータのインターフェイスの設定

```
interface g0/0
ip address 192.0.2.1 255.255.255.0
no shut
```

```
interface g0/1
ip address 10.12.0.2
no shut
```

```
interface loopback1
ip address 172.16.50.2 255.255.255.255
```

## スポークルータでのIKEv2パラメータとAAAの設定

ASAのフェーズ1パラメータに一致するIKEv2プロポーザルを作成します。

```
crypto ikev2 proposal NAME       (These parameters must match the ASA IKEv2 Policy.)
encryption aes-cbc-256           (aes-cbc-256 is the same as the ASA aes-256. However, AES-GCM of any v
                                  and is not a matching parameter with plain AES.)
integrity sha256
group 21
```

提案を添付するIKEv2ポリシーを作成します。

```
crypto ikev2 policy NAME
proposal NAME               (This is the name of the IKEv2 proposal created in the step ikev2.)
```

IKEv2許可ポリシーを作成します。

```
crypto ikev2 authorization policy NAME   (IKEv2 authorization policy serves as a container of IKEv2 loc
route set Interface
```

デバイスでAAAを有効にします。

```
aaa new-model
```

AAA認可ネットワークを作成します。

```
aaa authorization network NAME local    (Creates a name and method for aaa authorization that is refere
```

ローカルまたはリモートのIDや認証方式など、IKE SAのネゴシエートできないパラメータのリポジトリを含むIKEv2プロファイルを作成します。

```
crypto ikev2 profile NAME
match identity remote address  198.51.100.1    (Used to match the address of the Hub VTI source Interfa
identity local address  192.0.2.1              (Defines the local IKE-ID of the router for this IKEv2 p
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
no config-exchange request                     (Applies to Cisco IOS, Cisco IOS-XE devices do this by d
                                                which is unsupported on the ASA.)
aaa authorization group psk list NAME NAME     (Specifies an AAA method list and username for group. Th
```

トランスフォームセットを作成して、トンネル化されたトラフィックの保護に使用する暗号化パラメータとハッシュパラメータを定義します。

```
crypto ipsec transform-set NAME esp aes 256 esp-sha256-hmac
```

トランスフォームセットとIKEv2プロファイルを格納する暗号化IPsecプロファイルを作成します。

```
crypto ipsec profile NAME                  (Define the name of the ipsec-profile.)
set transform-set NAME                     (Reference the name of the created transform set.)
set ikev2-profile NAME                     (Reference the name of the created IKEv2 profile.)
```

## スポークルータでのスタティック仮想トンネルインターフェイスの設定

ハブをポイントするスタティック仮想トンネルインターフェイス(VTI)を設定します。

```
interface tunnel1
ip unnumbered loopback1
tunnel source g0/0
tunnel mode ipsec ipv4
tunnel destination 198.51.100.1
tunnel protection ipsec profile NAME      (Reference the name of the created ipsec profile. This applies
                                           and transform set parameters to the tunnel Interface.)
```

## スポークルータでのEIGRPルーティングの設定

EIGRP自律システムを作成し、アドバタイズする必要なネットワークを適用します。

```
router eigrp 100
network 172.16.50.2 0.0.0.0     (Routers advertise EIGRP networks with the wildcard mask.
                                 This advertises the tunnel IP address to allow the device to form an E
network 10.12.0.0 0.0.0.255      (Advertises the Host-B network to the hub. This allows the hub to noti
```

# 確認

ここでは、設定が正常に機能しているかどうかを確認します。

ASAルーティング：

```
show run router

show eigrp topology

show eigrp neighbors

show route [eigrp]
```

ASA暗号化：

```
show run crypto ikev2

show run crypto ipsec

show run tunnel-group [NAME]

show crypto ikev2 sa

show crypto ipsec sa peer X.X.X.X
```

ASAバーチャルテンプレートとバーチャルアクセス：

```
show run interface virtual-template # type tunnel

show interface virtual-access #
```

Cisco IOSルーティング：

```
show run | sec eigrp

show ip eigrp topology

show ip eigrp neighbors

show ip route

show ip route eigrp
```

Cisco IOS暗号化：

```
show run | sec cry

show crypto ikev2 sa
```

```
show crypto ipsec sa peer X.X.X.X
```

Cisco IOSトンネルインターフェイス：

```
show run interface tunnel#
```

# トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ASA Debugs:

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug ip eigrp #
debug ip eigrp neighbor X.X.X.X
```

Cisco IOSデバッグ：

```
debug crypto ikev2
debug crypto ikev2 error
debug crypto ikev2 packet
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
debug ip eigrp #
debug ip eigrp neighbor X.X.X.X
```

# 関連情報

- シスコテクニカルサポートおよびダウンロード

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。