レガシーEzVPN-NEM+から同じサーバ上のFlexVPNへの移行

内容

概要

このドキュメントでは、EzVPN から FlexVPN への移行プロセスについて説明します。FlexVPN は Cisco によって提供される新しいユニファイド VPN ソリューションです。FlexVPN は、IKEv2 プロトコルを活用して、リモート アクセス、サイト間、ハブとスポーク、および部分メッシュの VPN 導入を結合します。EzVPN のような従来のテクノロジーを使用する場合、Cisco では、豊富な機能を活用するために、FlexVPN に移行することを強くお勧めします。

このドキュメントでは、レガシー クリプト マップ ベースの EzVPN ヘッドエンド デバイスでトンネルを終端するレガシー EzVPN ハードウェア クライアントからなる既存の EzVPN の導入について説明します。目標は、この設定から移行して、次の要件を持つ FlexVPN をサポートすることです。

- 既存のレガシー クライアントは、設定の変更なしで引き続きシームレスに機能します。これによって、時間の経過とともにこれらのクライアントを FlexVPN に段階的に移行できます。

- ヘッドエンド デバイスは、新しい FlexVPN クライアントの終了を同時にサポートします。

これらの移行の目標を達成するために、2 つの主要な IPsec 設定コンポーネントを使用します。つまり、IKEv2 と仮想トンネル インターフェイス（VTI）です。 このドキュメントでは、これらの目標について簡単に説明します。

このシリーズの他のドキュメント

- 『FlexVPN 導入ガイド』：「IKEv2 と証明書を使用した IPsec 経由での IOS ヘッドエンドへの AnyConnect」

前提条件

要件

このドキュメントに特有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内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

IKEv1 対 IKEv2

FlexVPN は IKEv2 プロトコルに基づいています。このプロトコルは、RFC 4306 に基づいた次世代のキー管理プロトコルであり、IKEv1 プロトコルの拡張機能です。FlexVPN には、IKEv1 のみをサポートするテクノロジー（たとえば、EzVPN）との後方互換性はありません。 これは、EzVPN から FlexVPN に移行する際の重要な考慮事項の 1 つです。IKEv2 でのプロトコルの概要と IKEv1 との比較については、『IKE バージョン 2 の概要』を参照してください。

暗号マップと仮想トンネルインターフェイス

仮想トンネル インターフェイス（VTI）は、VPN サーバとクライアントの両方の設定に使用される新しい設定方法です。VTI：

- 現在はレガシー設定であると見なされる、ダイナミック クリプト マップの代替品。
- ネイティブ IPsec トンネリングをサポートします。
- IPsec セッションの物理インターフェイスへのスタティック マッピングは必要ありません。そのため、暗号化されたトラフィックを物理インターフェイスで柔軟に送受信できます（複数のパスなど）。
- オンデマンドの仮想アクセスは仮想テンプレート インターフェイスからクローニングされるため、設定は最小限で済みます。
- トラフィックは、トンネル インターフェイス間の転送時に暗号化または復号化され、IP ルーティング テーブルによって管理されます（そのため、暗号化プロセスで重要な役割を果たし

ます）。
- 機能は、VTI インターフェイスでクリア テキストのパケットに適用することも、物理インターフェイスで暗号化されたパケットに適用することもできます。

次の 2 つのタイプの VTI が使用可能です。

- スタティック（sVTI）：スタティック仮想トンネル インターフェイスは、固定のトンネルの送信元と宛先を持ち、通常はサイト間の導入シナリオで使用されます。次に、sVTI の設定例を示します。

```
interface Tunnel2
 ip address negotiated
 tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile testflex
```

- ダイナミック（dVTI）：ダイナミック仮想トンネル インターフェイスは、固定のトンネルの宛先を持たないダイナミック IPsec トンネルを終端するために使用されます。トンネルのネゴシエーションの成功時に、仮想アクセス インターフェイスが仮想テンプレートからクローニングされ、その仮想テンプレートですべての L3 機能を継承します。次に、dVTI の設定例を示します。

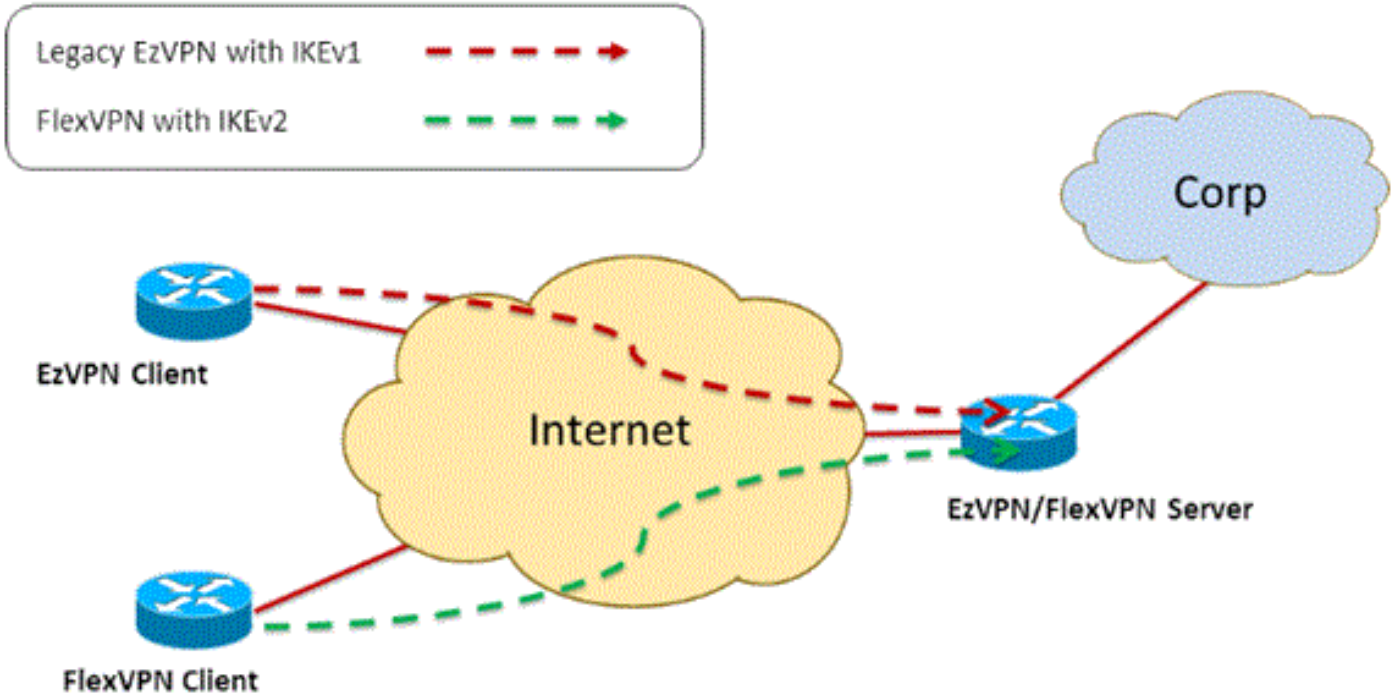
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

dVTI の詳細については、次のドキュメントを参照してください。

- IPSec ダイナミック仮想トンネル インターフェイス（DVTI）を使用した Cisco Easy VPN の設定
- IPsec 仮想トンネル インターフェイスの制約事項
- IKEv1 を使用したダイナミック仮想トンネル インターフェイスのマルチ SA サポートの設定

EzVPN および FlexVPN クライアントが共存するためには、最初に EzVPN サーバをレガシー クリプト マップ設定から dVTI 設定に移行する必要があります。次のセクションでは、必要な手順を詳細に説明します。

Network Topology



レガシー NEM+ モード EzVPN クライアントの現在の設定

クライアント設定

次に、一般的な EzVPN クライアントのルータ設定を示します。この設定では、Network Extension Plus (NEM+) モードが使用されます。このモードでは、両方の LAN 内部インターフェイス用に複数の SA ペアと、クライアント用にモード設定によって割り当てられた IP アドレスが作成されます。

```
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-plus
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description EzVPN WAN interface
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description EzVPN LAN inside interface
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
```

サーバ設定

EzVPN サーバでは、レガシー クリプト マップ設定が、移行前の基本設定として使用されます。

```
aaa new-model
!
```

```
aaa authentication login client-xauth local
aaa authorization network ezvpn-author local
!
username client1 password 0 client1
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address respond
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description EzVPN server WAN interface
 ip address 192.168.1.10 255.255.255.0
 crypto map client-map
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
!
ip access-list extended split-tunnel-acl
  remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
```

サーバの FlexVPN への移行

前のセクションで説明したように、FlexVPN は IKEv2 をコントロール プレーン プロトコルとして使用し、IKEv1 ベースの EzVPN ソリューションとの後方互換性を持ちません。その結果、この移行の一般概念は、レガシー EzVPN (IKEv1) と FlexVPN (IKEv2) の両方が共存できるような方法で既存の EzVPN サーバを設定することです。この目標を達成するには、次の 2 つの手順の移行方法を使用できます。

1. ヘッドエンドのレガシー EzVPN 設定をクリプト マップ ベースの設定から dVTI に移行します。
2. dVTI に基づく FlexVPN 設定を追加します。

レガシー クリプト マップの dVTI への移行

サーバ設定の変更

物理インターフェイスでクリプト マップを使用して設定された EzVPN サーバには、機能のサポートと柔軟性の点でいくつかの制約事項があります。EzVPN がある場合、Cisco では、代わりに

dVTI を使用することを強くお勧めします。EzVPN と FlexVPN が共存する設定に移行するための最初の手順では、これを dVTI 設定に変更する必要があります。これによって、両方のタイプのクライアントに対応するために、さまざまな仮想テンプレート インターフェイス間で IKEv1 と IKEv2 が区別されます。

注：EzVPNクライアントでNetwork Extension Plus(NEM)モードのEzVPN動作をサポートするには、ヘッドエンドルータがdVTI機能のマルチSAをサポートしている必要があります。これによって、複数の IP フローをトンネルによって保護できます。これは、ヘッドエンドが EzVPN クライアントの内部ネットワークへのトラフィック、および IKEv1 モードの設定によってクライアントに割り当てられた IP アドレスを暗号化するために必要です。IKEv1 を使用した dVTI でのマルチ SA サポートの詳細については、『IKEv1 のダイナミック仮想トンネル インターフェイスのマルチ SA サポート』を参照してください。

サーバで設定変更を実装するには、次の手順を実行します。

手順 1：EzVPN クライアント トンネルを終端する物理出力インターフェイスからクリプト マップを削除します。

```
interface Ethernet0/0
 ip address 192.168.1.10 255.255.255.0
 no crypto map client-map
```

手順 2：トンネルの確立後に、仮想アクセス インターフェイスのクローニング元の仮想テンプレート インターフェイスを作成します。

```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
```

手順 3：新たに作成されたこの仮想テンプレート インターフェイスを、設定済みの EzVPN グループの isakmp プロファイルに関連付けます。

```
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address initiate
   client configuration address respond
   virtual-template 1
```

上の設定変更を行ったら、既存の EzVPN クライアントが引き続き機能することを確認します。ただし、今回トンネルは、ダイナミックに作成された仮想アクセス インターフェイスで終端します。これは、次の例のように **show crypto session** コマンドを使用して確認できます。

```
PE-EzVPN-Server#show crypto session
Crypto session current status
Interface: Virtual-Access1
Username: client1
Profile: Group-One-Profile
Group: Group-One
Assigned address: 10.1.1.101
Session status: UP-ACTIVE
Peer: 192.168.2.101 port 500
  IKEv1 SA: local 192.168.1.10/500 remote 192.168.2.101/500 Active
```

```
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 host 10.1.1.101
        Active SAs: 2, origin: crypto map
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 172.16.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

FlexVPN 設定のサーバへの追加

この例では、FlexVPN クライアントとサーバの両方で RSA-SIG (つまり、認証局) を使用します。このセクションの設定では、サーバがすでに正常に認証され、CA サーバに登録されていることを前提としています。

手順 1：IKEv2 スマート デフォルト設定を確認します。

IKEv2 を使用して、15.2(1)T で導入されたスマート デフォルト機能を活用できるようになりました。これは、FlexVPN 設定を単純化するために使用されます。次に、いくつかのデフォルト設定を示します。

デフォルトの IKEv2 許可ポリシー：

```
VPN-Server#show crypto ikev2 authorization policy default
 IKEv2 Authorization Policy : default
 route set interface
 route accept any tag : 1 distance : 1
```

デフォルトの IKEv2 提案：

```
VPN-Server#show crypto ikev2 proposal default
 IKEv2 proposal: default
 Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
 Integrity : SHA512 SHA384 SHA256 SHA96 MD596
 PRF : SHA512 SHA384 SHA256 SHA1 MD5
 DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

デフォルトの IKEv2 ポリシー：

```
VPN-Server#show crypto ikev2 policy default
 IKEv2 policy : default
 Match fvrf : any
 Match address local : any
 Proposal : default
```

デフォルトの IPsec プロファイル：

```
VPN-Server#show crypto ipsec profile default
IPSEC profile default
 Security association lifetime: 4608000 kilobytes/3600 seconds
 Responder-Only (Y/N): N
 PFS (Y/N): N
 Transform sets={
 default: { esp-aes esp-sha-hmac } ,
 }
```

デフォルトの IPsec トランスフォーム セット：

```
VPN-Server#show crypto ipsec transform default
{ esp-aes esp-sha-hmac }
```

```
 will negotiate = { Transport, },
```

IKEv2 スマート デフォルト機能の詳細については、『IKEv2 スマート デフォルト』（登録ユーザ専用）を参照してください。

手順 2：デフォルトの IKEv2 許可ポリシーを変更して、FlexVPN クライアントのデフォルトの IKEv2 プロファイルを追加します。

ここで作成したIKEv2プロファイルは、ドメイン名cisco.comに基づくピアIDと一致し、クライアント用に作成した仮想アクセスインターフェイスが仮想テンプレート2から生成されます。また、認証ポリシーは、ピアIPアドレスの割り当てに使用するルートを定義します。

```
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
```

手順 3：FlexVPN クライアントに使用される仮想テンプレート インターフェイスを作成します。

```
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
```

FlexVPN Client の設定

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
```

詳細な設定

完全なハイブリッド サーバ設定

```
hostname VPN-Server
!
!
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network default local
aaa authorization network ezvpn-author local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=vpn-server.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 07
 certificate ca 01
username client1 password 0 client1
username cisco password 0 cisco
!
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
 save-password
```

```
crypto isakmp profile Group-One-Profile
 match identity group Group-One
 client authentication list client-xauth
 isakmp authorization list ezvpn-author
 client configuration address initiate
 client configuration address respond
 virtual-template 1
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto ipsec profile default
 set ikev2-profile default
!
crypto ipsec profile legacy-profile
 set transform-set aes-sha
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description WAN
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.0.1 255.255.255.0
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
ip local pool flexvpn-pool 10.1.1.201 10.1.1.250
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip access-list extended split-tunnel-acl
 remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
!
access-list 1 permit 172.16.0.0 0.0.0.255
```

完全な IKEv1 EzVPN クライアント設定

```
hostname Client1
!
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-extension
 peer 192.168.1.10
 username client1 password client1
```

```
 xauth userid mode local
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description LAN
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

完全な IKEv2 FlexVPN クライアント設定

```
hostname Client2
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 redundancy
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=Client2.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 06
 certificate ca 01
!
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
```

```
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.102 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
!
access-list 1 permit 172.16.2.0 0.0.0.255
```

設定の確認

次に、ルータでの EzVPN/FlexVPN の動作を確認するために使用されるいくつかのコマンドを示します。

```
show crypto session

show crypto session detail

show crypto isakmp sa

show crypto ikev2 sa

show crypto ipsec sa detail

show crypto ipsec client ez (for legacy clients)

show crypto socket

show crypto map
```

関連情報

- テクニカル サポートとドキュメント – Cisco Systems