FlexVPN Migration: Legacy EzVPN−NEM+ and FlexVPN on the Same Server

Document ID: 115013

Contributed by Wen Zhang, Cisco TAC Engineer.
Jan 25, 2013

Contents

Introduction

This document describes the migration process from EzVPN to FlexVPN. FlexVPN is the new unified VPN solution offered by Cisco. FlexVPN takes advantage of the IKEv2 protocol and combines remote access, site−to−site, hub and spoke, and partial mesh VPN deployments. With legacy technologies like EzVPN, Cisco strongly encourages you to migrate to FlexVPN in order to take advantage of its feature−rich capabilities.

This document examines an existing EzVPN deployment that consists of legacy EzVPN hardware clients that terminate tunnels on a legacy crypto map based EzVPN headend device. The goal is to migrate from this configuration to support FlexVPN with these requirements:

- Existing legacy clients will continue to work seamlessly without any configuration changes. This allows a phased migration of these clients to FlexVPN over time.
- The headend device should simultaneously support the termination of new FlexVPN clients.

Two key IPsec configuration components are used in order to help accomplish these migration goals: namely, IKEv2 and Virtual Tunnel Interfaces (VTI). These goals are briefly discussed in this document.

Other Documents in this Series

- FlexVPN Deployment Guide: AnyConnect to IOS Headend Over IPsec with IKEv2 and Certificates

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

IKEv1 vs IKEv2

FlexVPN is based on the IKEv2 protocol, which is the next−generation key management protocol based on RFC 4306, and an enhancement of the IKEv1 protocol. FlexVPN is not backward−compatible with technologies that support only IKEv1 (for example, EzVPN). This is one of the key considerations when you migrate from EzVPN to FlexVPN. For a protocol introduction on IKEv2 and comparison with IKEv1, refer to IKE version 2 at a glance.

Crypto map vs. Virtual Tunnel Interfaces

Virtual Tunnel Interface (VTI) is a new configuration method used for both VPN server and client configurations. VTI:

- Replacement to dynamic crypto maps, which is now considered legacy configuration.
- Supports native IPsec tunneling.
- Does not require a static mapping of an IPsec session to a physical interface; therefore, provides flexibility to send and receive encrypted traffic on any physical interface (for example, multiple paths).
- Minimal configuration as on−demand virtual access is cloned from virtual−template interface.
- Traffic is encrypted/decrypted when forward to/from the tunnel interface and is managed by the IP routing table (thereby, playing an important role in the encryption process).
- Features can either be applied to clear−text packets on the VTI interface, or encrypted packets on the physical interface.

The two types of VTIs available are:

- Static (sVTI) A static virtual tunnel interface has a fixed tunnel source and destination and is typically used in a site−to−site deployment scenario. Here is an example of an sVTI configuration:

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

- Dynamic (dVTI) A dynamic virtual tunnel interface can be used to terminate dynamic IPsec tunnels that do not have a fixed tunnel destination. Upon successful tunnel negotiation, Virtual−Access

interfaces will be cloned from a Virtual−Template and will inherit all L3 features on that Virtual−Template. Here is an example of a dVTI configuration:

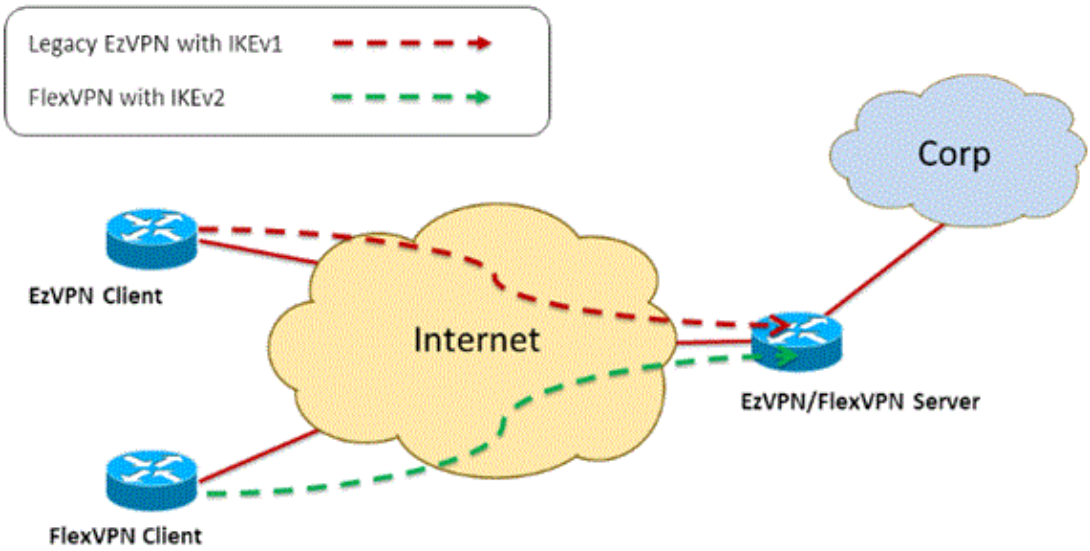
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Refer to these documents for more information on dVTI:

- Configuring Cisco Easy VPN with IPSec Dynamic Virtual Tunnel Interface (DVTI)
- Restrictions for IPsec Virtual Tunnel Interface
- Configuring Multi−SA Support for Dynamic Virtual Tunnel Interfaces Using IKEv1

In order for EzVPN and FlexVPN clients to coexist, you must first migrate the EzVPN server from the legacy crypto map configuration to a dVTI configuration. The following sections explain in detail the necessary steps.

Network Topology



Current Configuration with Legacy NEM+ Mode EzVPN Client

Client configuration

Below is a typical EzVPN client router configuration. In this configuration, Network Extension Plus (NEM+)mode is used, which creates multiple SA pairs for both the LAN inside interfaces as well as the mode configuration assigned IP address for the client.

```
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
```

Server configuration

On the EzVPN server, a legacy crypto map configuration is used as the base configuration before the migration.

```
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
```

Migration of Server to FlexVPN

As described in the previous sections, FlexVPN uses IKEv2 as the control plane protocol and is not backward compatible with an IKEv1−based EzVPN solution. As a result, the general idea of this migration is to configure the existing EzVPN server in such a way that it allows both legacy EzVPN (IKEv1) and FlexVPN (IKEv2) to coexist. In order to achieve this goal, you can use this two−step migration approach:

1. Move the legacy EzVPN configuration on the headend from a crypto map based configuration to dVTI.
2. Add the FlexVPN configuration, which is also based on dVTI.

Move Legacy crypto map to dVTI

Server configuration changes

An EzVPN server configured with crypto map on the physical interface includes several limitations when it comes to feature support and flexibility. If you have EzVPN, Cisco strongly encourages you to use dVTI instead. As a first step to migrate to a coexisting EzVPN and FlexVPN configuration, you must change it to a dVTI configuration. This will provide IKEv1 and IKEv2 separation between the different virtual−template interfaces in order to accommodate both types of clients.

Note: In order to support the Network Extension Plus Mode of EzVPN operation on the EzVPN clients, the headend router must have support for the multi SA on dVTI feature. This allows multiple IP flows to be protected by the tunnel, which is required for the headend to encrypt traffic to the inside network of the EzVPN client, as well as the the IP address assigned to the client through IKEv1 mode config. For more information about multi SA support on dVTI with IKEv1, refer to Multi−SA Support for Dynamic Virtual Tunnel Interfaces for IKEv1.

Complete these steps in order to implement the configuration change on the server:

Step 1 Remove the crypto map from the physical egress interface that terminates the EzVPN client tunnels:

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

Step 2 Create a virtual−template interface from which virtual access interfaces will be cloned once the tunnels are established:

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

Step 3 Associate this newly created virtual template interface to the isakmp profile for the configured EzVPN group:

```
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
```

Once the above configuration changes are made, verify that the existing EzVPN clients continue to work. However, now their tunnels are terminated on a dynamically created virtual access interface. This can be verified with the **show crypto session** command as in this example:

```
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
```

Add the FlexVPN Configuration to the Server

This example uses RSA-SIG (that is, Certificate Authority) on both the FlexVPN client and server. The configuration in this section assumes that the server has already successfully authenticated and enrolled with the CA server.

Step 1 Verify the IKEv2 Smart Default Configuration.

With IKEv2, you can now take advantage of the Smart Default feature introduced in 15.2(1)T. It is used to simplify a FlexVPN configuration. Here are some default configurations:

Default IKEv2 authorization policy:

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

Default IKEv2 proposal:

```
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
```

Default IKEv2 policy:

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

Default IPsec profile:

```
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 } ,
 }
```

Default IPsec transform set:

```
VPN-Server#show crypto ipsec transform default
{ esp-aes esp-sha-hmac }
 will negotiate = { Transport, },
```

For more information on the IKEv2 Smart Default feature, refer to IKEv2 Smart Defaults (registered customers only) .

Step 2 Modify the default IKEv2 authorization policy and add a default IKEv2 profile for the FlexVPN clients.

The IKEv2 profile created here will match on a peer ID based on the domain name cisco.com and the virtual access interfaces created for the clients will be spawned off of virtual template 2. Also note the authorization policy defines the IP address pool used for assigning peer IP addresses as well as routes to be exchanged via IKEv2 configuration mode:

```
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
```

Step 3 Create the virtual template interface used for the FlexVPN clients:

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

FlexVPN Client Configuration

```
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
```

Complete Configuration

Complete Hybrid Server Configuration

```
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
```

Complete IKEv1 EzVPN Client Configuration

```
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
```

Complete IKEv2 FlexVPN Client Configuration

```
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
```

Configuration Verification

Here are some of the commands used to verify the EzVPN/FlexVPN operations on a router:

```
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
```

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 25, 2013 Document ID: 115013