EzVPN−NEM to FlexVPN Migration Guide

Document ID: 115950

Contributed by Praveena Shanubhogue and Atri Basu, Cisco TAC Engineers.

Mar 15, 2013

Contents

Introduction

This document provides assistance in the migration process from EzVPN (Internet Key Exchange v1 (IKEv1)) setup to FlexVPN (IKEv2) setup with as few issues as possible. Since IKEv2 Remote Access differs from IKEv1 Remote Access in certain ways that make migration a bit difficult, this document helps you choose different design approaches in the migration from the EzVPN model to the FlexVPN Remote Access model.

This document deals with the IOS FlexVPN client or the hardware client, this document does not discuss the software client. For more information on the software client please refer to:

- FlexVPN: IKEv2 with Built−in Windows Client and Certificate Authentication
- FlexVPN and Anyconnect IKEv2 Client Configuration Example
- FlexVPN Deployment: AnyConnect IKEv2 Remote Access with EAP−MD5

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- IKEv2
- Cisco FlexVPN
- Cisco AnyConnect Secure Mobility Client
- Cisco VPN Client

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

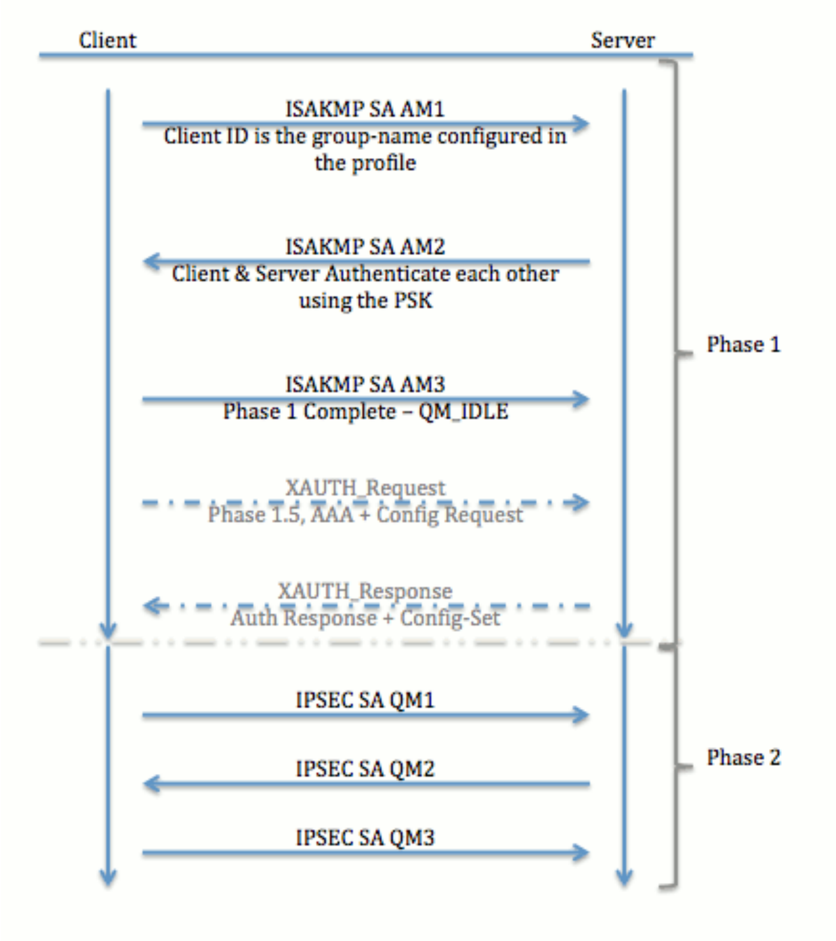
Refer to Cisco Technical Tips Conventions for more information on document conventions.

EzVPN versus FlexVPN

EzVPN Model − What Stands Out

As the name suggests, the objective of EzVPN is to make VPN configuration on the remote clients easy. In order to achieve this, the client is configured with minimal details needed to contact the correct EzVPN server, also known as the client profile.

Tunnel Negotiation


Client
Server
ISAKMP SA AM1
Client ID is the group-name configured in the profile
ISAKMP SA AM2
Client & Server Authenticate each other using the PSK
ISAKMP SA AM3
Phase 1 Complete – QM_IDLE
XAUTH_Request
Phase 1.5, AAA + Config Request
XAUTH_Response
Auth Response + Config-Set
Phase 1
IPSEC SA QM1
IPSEC SA QM2
IPSEC SA QM3
Phase 2

FlexVPN Remote Access VPN Model

FlexVPN Server

An important difference between normal FlexVPN and a FlexVPN Remote Access setup is that the server needs to authenticate itself to the FlexVPN clients through the use of the pre−shared keys and certificates (RSA−SIG) method only. FlexVPN allows you to decide which authentication methods the initiator and responder uses, independent of each other. In other words, they can be the same or they can be different. However, when it comes to FlexVPN Remote Access, the server does not have a choice.

IOS FlexVPN Client Authentication Methods

The client supports the these authentication methods:

- **RSA−SIG**   Digital Certificate Authentication.
- **Pre−Share**   Pre−Shared Key (PSK) Authentication.
- **Extensible Authentication Protocol (EAP)** − EAP Authentication. EAP−Support for IOS FlexVPN client was added in 15.2(3)T.

  Supported EAP methods by the IOS FlexVPN client include:

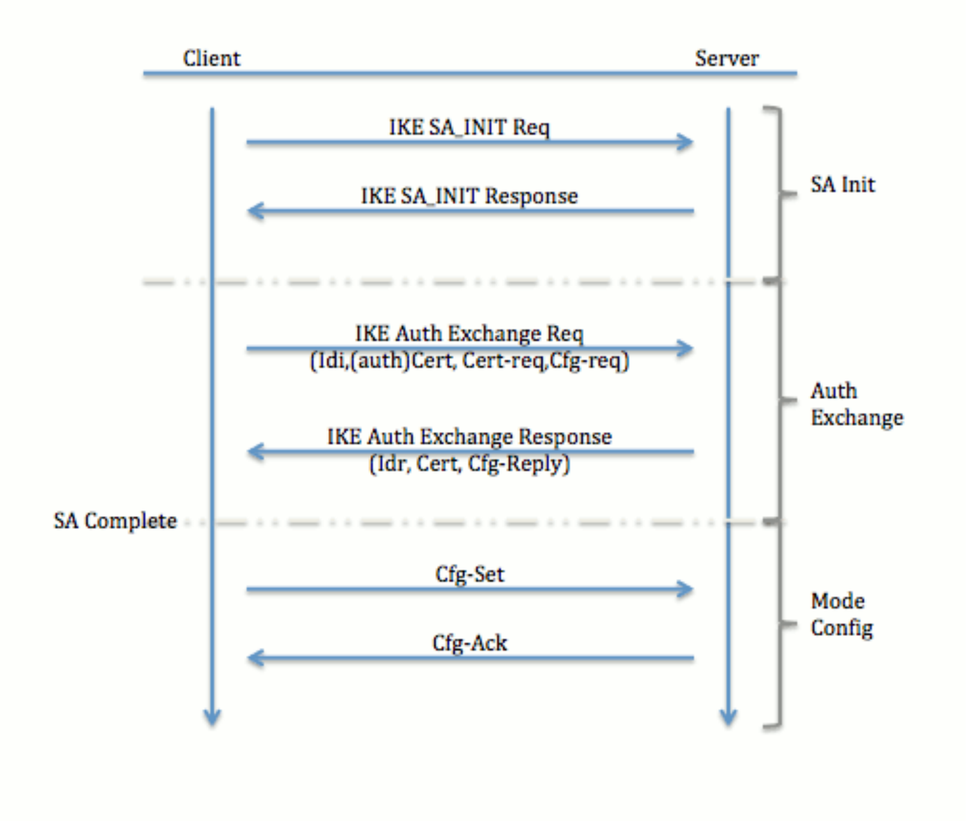
  - Extensible Authentication Protocol−Message Digest 5 (EAP−MD5),
  - Extensible Authentication Protocol−Microsoft Challenge Handshake Authentication Protocol Version 2 (EAP−MSCHAPv2), and
  - Extensible Authentication Protocol−Generic Token Card (EAP−GTC).

This document only describes the use of RSA−SIG authentication, for these reasons:

- **Scalable** Each client is given a certificate, and on the server, a generic part of client identity is authenticated against it.
- **Secure** More secure than a wildcard PSK (in case of local authorization). Although, in the case of AAA (authentication, authorization, and accounting) authorization, it is easier to write separate PSKs based on mangled IKE Identity.

The FlexVPN client configuration shown in this document might seem little exhaustive compared to EasyVPN client. This is because the configuration includes some parts of the configuration that do not need to be configured by the user due to smart defaults. Smart defaults is the term used to refer to the pre−configured or default configuration for various things like the proposal, policy, IPSec transform set, and so on. And unlike IKEv1 default values, IKEv2 smart default values are strong. For example, it makes use of Advanced Encryption Standard (AES−256), Secure Hash Algorithm (SHA−512), and Group−5 in the proposals, and so forth.

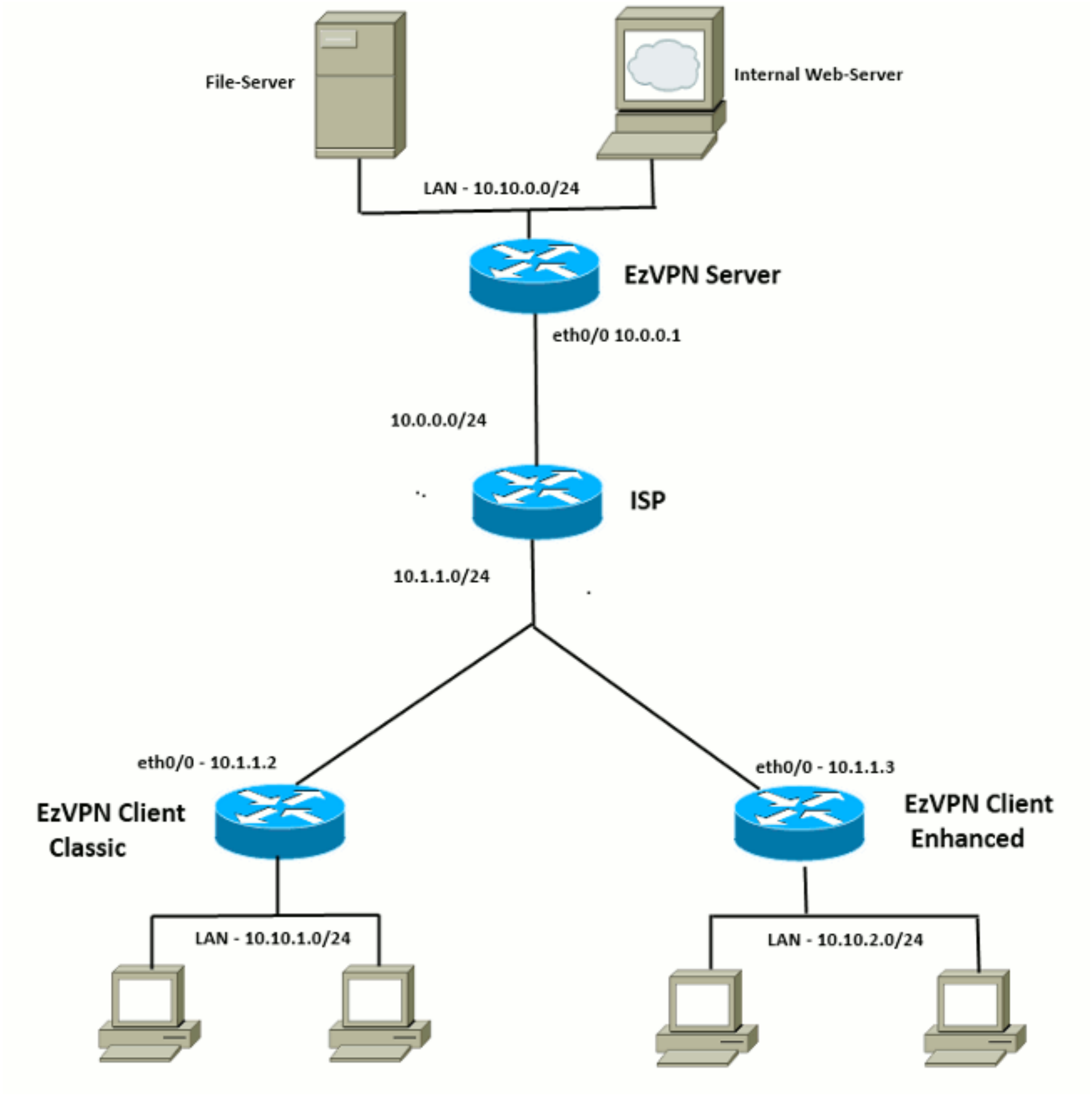
Tunnel Negotiation



For more information on the exchange of packets for an IKEv2 exchange, refer to IKEv2 Packet Exchange and Protocol Level Debugging.

Initial Setup

Topology



Initial Configuration

EzVPN Hub − dVTI Based

```
!! AAA Config for EzVPN clients. We are using Local AAA Server.
aaa new−model
aaa authentication login default local
aaa authorization network default local

!! ISAKMP Policy
crypto isakmp policy 1
 encr 3des
 authentication pre−share
 group 2

!! ISAKMP On−Demand Keep−Alive
crypto isakmp keepalive 10 2

!! EzVPN Split ACL
access−list 101 permit ip 10.10.0.0 0.0.0.255 any
```

```
!! EzVPN Client Group Configuration. This is what holds all the config attributes
crypto isakmp client configuration group cisco
 key cisco
 dns 6.0.0.2
 wins 7.0.0.1
 domain cisco.com
 acl 101
 save−password

!! ISAKMP Profile. This ties Client IKE identity to AAA.
!! And since this is dVTI setup, ISAKMP Profile tells the IOS
!!   from which Virtual−Template (VT1) to clone the Virtual Access interfaces
crypto isakmp profile vi
   match identity group cisco
   client authentication list default
   isakmp authorization list default
   virtual−template 1

!! IPSec Transform Set.
crypto ipsec transform−set set esp−3des esp−sha−hmac

!! IPSec Profile. This ties Transform set and ISAKMP Profile together.
crypto ipsec profile vi
 set transform−set set
 set isakmp−profile vi

!! The loopback interface. And virtual−template borrows the address from here.
interface Loopback0
 ip address 10.10.10.1 255.255.255.252

!! dVTI interface.
interface Virtual−Template1 type tunnel
 ip unnumbered Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
```

EzVPN Client − Classic (No VTI)

```
!! ISAKMP On−Demand Keep−Alive
crypto isakmp keepalive 10 2

!! EzVPN Client − Group Name and The key (as configured on the Server),
!!   Peer address and XAUTH config go here.
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 local−address Ethernet0/0
 mode network−extension
 peer 10.0.0.1
 username cisco password cisco
 xauth userid mode local

!! EzVPn outside interface − i.e. WAN interface
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 crypto ipsec client ezvpn ez

!! EzVPN inside interface
!! Traffic sourced from this LAN is sent over established Tunnel
interface Ethernet0/1
 ip address 10.10.1.1 255.255.255.0
 crypto ipsec client ezvpn ez inside
```

EzVPN Client − Enhanced (VTI−based)

```
!! VTI −
interface Virtual−Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4

!! ISAKMP On−Demand Keep−Alive
crypto isakmp keepalive 10 2

!! EzVPN Client − Group Name and The key (as configured on the Server),
!!   Peer address and XAUTH config go here.
!! Also this config says which Virtual Template to use.
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 local−address Ethernet0/0
 mode network−extension
 peer 10.0.0.1
 virtual−interface 1
 username cisco password cisco
 xauth userid mode local

!! EzVPn outside interface − WAN interface
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 crypto ipsec client ezvpn ez

!! EzVPN inside interface −
!! Traffic sourced from this LAN is sent over established Tunnel
interface Ethernet0/1
 ip address 10.10.2.1 255.255.255.0
 crypto ipsec client ezvpn ez inside
```

EzVPN to FlexVPN Migration Approach

The server that acts as an EzVPN server can also act as a FlexVPN server as long as it supports IKEv2 Remote Access configuration. For a full IKEv2 configuration support, anything above IOS v15.2(3)T is recommended. In these examples 15.2(4)M1 has been used.

There are two possible approaches:

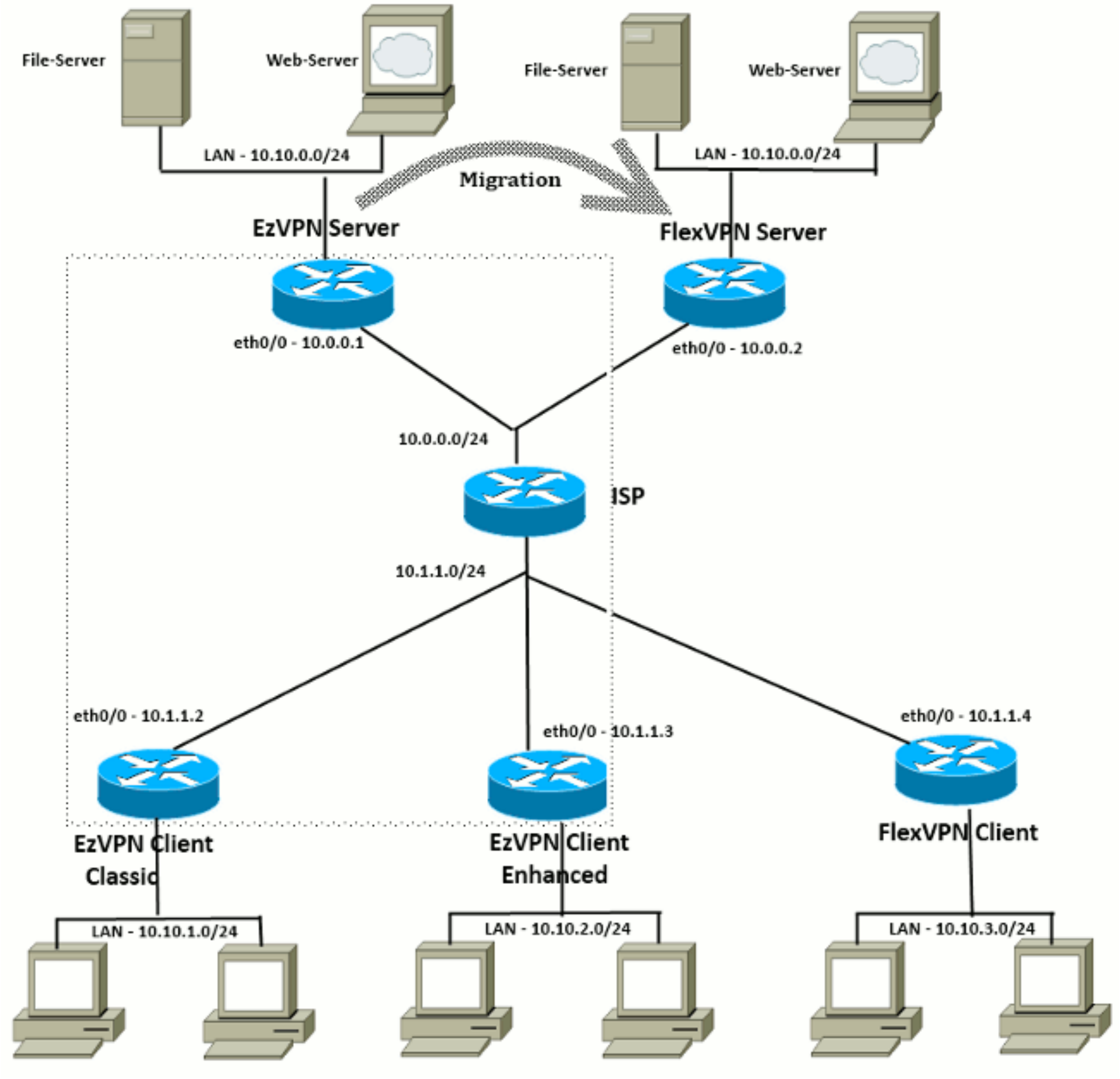
1. Setup EzVPN server as FlexVPN server, then migrate the EzVPN clients to Flex configuration.
2. Setup a different router as a FlexVPN server. EzVPN clients and migrated FlexVPN clients continue to communicate through the creation of a connection between the FlexVPN server and the EzVPN server.

This document describes the second approach and uses a new spoke (for instance, Spoke3), as the FlexVPN client. This spoke can be used as a reference in order to migrate other clients in the future.

Migration Steps

Note that when you migrate from an EzVPN spoke to a FlexVPN spoke, you can choose to load **FlexVPN config** on the EzVPN spoke. However, throughout the cut−over, you might need an out−of−band (non−VPN) management access to the box.

Migrated Topology



Configuration

FlexVPN Hub

```
!! AAA Authorization done Locally
aaa new-model
aaa authorization network Flex local

!! PKI TrustPoint to Sign and Validate Certificates.
!! Contains Identity Certificate and CA Certificate
crypto pki trustpoint FlexServer
 enrollment terminal
 revocation-check none
 rsakeypair FlexServer
 subject-name CN=flexserver.cisco.com,OU=FlexVPN

!! Access-list used in Config-Reply in order to push routes
access-list 1 permit 10.10.0.0 0.0.0.255

!! IKEv2 Authorization done locally. Used in Config-Set.
```

```
crypto ikev2 authorization policy FlexClient-Author
 def-domain cisco.com
 route set interface
 route set access-list 1

!! IKEv2 Proposal. Optional Config. Smart-Default takes care of this.
crypto ikev2 proposal FlexClient-Proposal
 encryption aes-cbc-128 aes-cbc-192 3des
 integrity sha256 sha512 sha1
 group 5 2

!! If IKEv2 Proposal was left out default, then IKEv2 Policy can be left out too.
!! Ties Proposal to Peer address/fvrf
crypto ikev2 policy FlexClient-Policy
 match fvrf any
 proposal FlexClient-Proposal

!! IKEv2 Profile. This is the main Part
!! Clients are configured to send their FQDN. And we match the domain 'cisco.com'
!! We are sending 'flexserver.cisco.com' as the fqdn identity.
!! Local and Remote authentication is RSA-SIG
!! Authorization (config-reply) is done locally with the user-name
!!   'FlexClient-Author'
!! This whole profile is tied to Virtual-Template 1
crypto ikev2 profile FlexClient-Profile
 match identity remote fqdn domain cisco.com
 identity local fqdn flexserver.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint FlexServer
 aaa authorization group cert list Flex FlexClient-Author
 virtual-template 1

!! IPSec Transform set. Optional Config, since Smart Default takes care of this.
crypto ipsec transform-set ESP-AES-SHA1 esp-aes esp-sha-hmac

!! IPSec Profile ties default/Configured transform set with the IKEv2 Profile
crypto ipsec profile FlexClient-IPSec
 set transform-set ESP-AES-SHA1
 set ikev2-profile FlexClient-Profile

!! Loopback interface lends ip address to Virtual-template and
!!   eventually to Virtual-Access interfaces spawned.
interface Loopback0
 ip address 10.10.10.1 255.255.255.252

!! The IKEv2 enabled Virtual-Template
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel protection ipsec profile FlexClient-IPSec

!! WAN interface
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0

!! LAN interfaces
interface Ethernet0/1
 ip address 10.10.0.1 255.255.255.0
```

Note about Server Certificates

Key Usage (KU) defines the purpose or the intended usage of the public key. Enhanced/Extended Key Usage (EKU) refines the key usage. FlexVPN requires that the server certificate has an EKU of **server auth** (OID = 1.3.6.1.5.5.7.3.1) with the KU attributes of **Digital Signature** and **Key Encipherment** in order for the certificate to be accepted by the client.

```
FlexServer#show crypto pki certificates verbose
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 09
  Certificate Usage: General Purpose
  Issuer:
    l=lal-bagh
    c=IN
    o=Cisco
    ou=TAC
    cn=Praveen
  Subject:
    Name: flexserver.cisco.com
    ou=FlexVPN
    cn=flexserver.cisco.com
  CRL Distribution Points:
    http://10.48.67.33:80/Praveen/Praveen.crl
<snip>
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: F3646C9B 1CC26A81 C3CB2034 061302AA
  Fingerprint SHA1: 7E9E99D4 B66C70E3 CBA8C4DB DD94629C 023EEBE7
  X509v3 extensions:
    X509v3 Key Usage: E0000000
      Digital Signature
      Non Repudiation
      Key Encipherment
<snip>
    Authority Info Access:
    Extended Key Usage:
        Client Auth
        Server Auth
  Associated Trustpoints: FlexServer
  Storage: nvram:lal-bagh#9.cer
  Key Label: FlexServer
  Key storage device: private config



CA Certificate
<snip>
```

FlexVPN Client Configuration

```
!! AAA Authorization done Locally
aaa new-model
aaa authorization network Flex local

!! PKI TrustPoint to Sign and Validate Certificates.
!! Contains Identity Certificate and CA Certificate
crypto pki trustpoint Spoke3-Flex
 enrollment terminal
 revocation-check none
 subject-name CN=spoke3.cisco.com,OU=FlexVPN
 rsakeypair Spoke3-Flex

!! Access-list used in Config-Set in order to push routes
access-list 1 permit 10.10.3.0 0.0.0.255

!! IKEv2 Authorization done locally. Used in Config-Set.
crypto ikev2 authorization policy FlexClient-Author
 route set interface
 route set access-list 1


!! IKEv2 Proposal. Optional Config. Smart-Default takes care of this.
```

```
crypto ikev2 proposal FlexClient−Proposal
 encryption aes−cbc−128 aes−cbc−192 3des
 integrity sha256 sha512 sha1
 group 5 2


!! If IKEv2 Proposal was left out default, then IKEv2 Policy can be left out too.
!! Ties Proposal to Peer address/fvrf
crypto ikev2 policy FlexClient−Policy
 match fvrf any
 proposal FlexClient−Proposal

!! IKEv2 Profile. This is the main Part
!! Server is configured to send its FQDN type IKE−ID,
!!    and we match the domain 'cisco.com'
!! (If the IKE−ID type is DN (extracted from the certificate),
!!    we will need a certificate map)
!! We are sending 'spoke3.cisco.com' as the IKE−identity of type fqdn.
!! Local and Remote authentication is RSA−SIG
!! Authorization (config−set) is done locally using the user−name filter
!!    'FlexClient−Author'
crypto ikev2 profile FlexClient−Profile
 match identity remote fqdn flexserver.cisco.com
 identity local fqdn spoke3.cisco.com
 authentication remote rsa−sig
 authentication local rsa−sig
 pki trustpoint Spoke3−Flex
 aaa authorization group cert list Flex FlexClient−Author

!! IPSec Transform set. Optional Config, since Smart Default takes care of this.
crypto ipsec transform−set ESP−AES−SHA1 esp−aes esp−sha−hmac

!! IPSec Profile ties the transform set with the IKEv2 Profile
crypto ipsec profile FlexClient−IPSec
 set transform−set ESP−AES−SHA1
 set ikev2−profile FlexClient−Profile

!! FlexVPN Client Tunnel interface.
!! If IP−Address of the tunnel is negotiated,
!!   FlexVPN server is capable of assigning an IP through Config−Set
interface Tunnel0
 ip unnumbered Ethernet0/1
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel protection ipsec profile FlexClient−IPSec

!! Final FlexVPN client Part.
!! Multiple backup Peer and/or Multiple Tunnel source interfaces can be configured
crypto ikev2 client flexvpn FlexClient
  peer 1 10.0.0.2
  client connect Tunnel0

!! WAN interface
interface Ethernet0/0
 ip address 10.1.1.4 255.255.255.248

!! LAN Interface
interface Ethernet0/1
 ip address 10.10.3.1 255.255.255.0
```

Note about Client Certificates

FlexVPN requires that the client certificate has an EKU of **Client Auth** (OID = 1.3.6.1.5.5.7.3.2) with the KU attributes of **Digital Signature** and **Key Encipherment** in order for the certificate to be accepted by the server.

```
Spoke3#show crypto pki certificates verbose
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 08
  Certificate Usage: General Purpose
  Issuer:
    l=lal-bagh
    c=IN
    o=Cisco
    ou=TAC
    cn=Praveen
  Subject:
    Name: spoke3.cisco.com
    ou=FlexVPN
    cn=spoke3.cisco.com
 <snip>
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: 2381D319 906177E1 F45019BC 61059BD5
  Fingerprint SHA1: D81FD705 653547F2 D0916710 E6B096A1 23F6C467
  X509v3 extensions:
    X509v3 Key Usage: E0000000
      Digital Signature
      Non Repudiation
      Key Encipherment
 <snip>
    Extended Key Usage:
        Client Auth
        Server Auth
  Associated Trustpoints: Spoke3-Flex
  Storage: nvram:lal-bagh#8.cer
  Key Label: Spoke3-Flex
  Key storage device: private config



CA Certificate
<snip>
```

FlexVPN Operation Verification

FlexVPN Server

```
FlexServer#show crypto ikev2 session
 IPv4 Crypto IKEv2 Session
Session-id:5, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.0.0.2/500          10.1.1.4/500          none/none            READY
    Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth verify:
   RSA
    Life/Active Time: 86400/7199 sec
Child sa: local selector  10.0.0.2/0 - 10.0.0.2/65535
          remote selector 10.1.1.4/0 - 10.1.1.4/65535
          ESP spi in/out: 0xA9571C00/0x822DDAAD


FlexServer#show crypto ikev2 session detailed

 IPv4 Crypto IKEv2 Session
```

```
Session-id:5, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.0.0.2/500          10.1.1.4/500          none/none            READY

    Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth verify:
   RSA
    Life/Active Time: 86400/7244 sec
    CE id: 1016, Session-id: 5
    Status Description: Negotiation done
    Local spi: 648921093349609A       Remote spi: 1C2FFF727C8EA465
    Local id: flexserver.cisco.com
    Remote id: spoke3.cisco.com
    Local req msg id:  2              Remote req msg id:  5
    Local next msg id: 2              Remote next msg id: 5
    Local req queued:  2              Remote req queued:  5
    Local window:      5              Remote window:      5
    DPD configured for 0 seconds, retry 0
    NAT-T is not detected
    Cisco Trust Security SGT is disabled
    Initiator of SA : No
    Remote subnets:
    10.10.3.0 255.255.255.0


  Child sa: local selector  10.0.0.2/0 - 10.0.0.2/65535
            remote selector 10.1.1.4/0 - 10.1.1.4/65535
        ESP spi in/out: 0xA9571C00/0x822DDAAD
        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 transport


FlexServer#show ip route static
      10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
S        10.10.3.0/30 is directly connected, Virtual-Access1

FlexServer#ping 10.10.3.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.10.3.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/5/13 ms


FlexServer#show crypto ipsec sa | I ident|caps|spi
 local  ident (addr/mask/prot/port): (10.0.0.2/255.255.255.255/47/0)
 remote ident (addr/mask/prot/port): (10.1.1.4/255.255.255.255/47/0)
  #pkts encaps: 205, #pkts encrypt: 205, #pkts digest: 205
  #pkts decaps: 200, #pkts decrypt: 200, #pkts verify: 200
   current outbound spi: 0x822DDAAD(2184043181)
    spi: 0xA9571C00(2841058304)
    spi: 0x822DDAAD(2184043181)
```

FlexVPN Remote

```
Spoke3#show crypto ikev2 session
 IPv4 Crypto IKEv2 Session
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
```

```
1         10.1.1.4/500          10.0.0.2/500          none/none            READY
    Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth verify:
   RSA
    Life/Active Time: 86400/7621 sec
Child sa: local selector  10.1.1.4/0 - 10.1.1.4/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
          ESP spi in/out: 0x822DDAAD/0xA9571C00


Spoke3#show crypto ikev2 session detailed

 IPv4 Crypto IKEv2 Session
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.1.1.4/500          10.0.0.2/500          none/none            READY

    Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth verify:
   RSA
    Life/Active Time: 86400/7612 sec
    CE id: 1016, Session-id: 4
    Status Description: Negotiation done
    Local spi: 1C2FFF727C8EA465       Remote spi: 648921093349609A
    Local id: spoke3.cisco.com
    Remote id: flexserver.cisco.com
    Local req msg id:  5              Remote req msg id:  2
    Local next msg id: 5              Remote next msg id: 2
    Local req queued:  5              Remote req queued:  2
    Local window:      5              Remote window:      5
    DPD configured for 0 seconds, retry 0
    NAT-T is not detected
    Cisco Trust Security SGT is disabled
    Initiator of SA : Yes
    Default Domain: cisco.com
    Remote subnets:
    10.10.10.1 255.255.255.255
    10.10.0.0 255.255.255.0


Child sa: local selector  10.1.1.4/0 - 10.1.1.4/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
         ESP spi in/out: 0x822DDAAD/0xA9571C00
         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 transport


Spoke3#ping 10.10.0.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.10.0.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/5/12 ms

Spoke3#show crypto ipsec sa | I ident|caps|spi
  local  ident (addr/mask/prot/port): (10.1.1.4/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (10.0.0.2/255.255.255.255/47/0)
   #pkts encaps: 300, #pkts encrypt: 300, #pkts digest: 300
   #pkts decaps: 309, #pkts decrypt: 309, #pkts verify: 309
    current outbound spi: 0xA9571C00(2841058304)
     spi: 0x822DDAAD(2184043181)
     spi: 0xA9571C00(2841058304)
```

Related Information

- **FlexVPN: IKEv2 with Built−in Windows Client and Certificate Authentication TechNote**
- **FlexVPN and Anyconnect IKEv2 Client Configuration Example TechNote**
- **FlexVPN Deployment: AnyConnect IKEv2 Remote Access with EAP−MD5 TechNote**
- **IKEv2 Packet Exchange and Protocol Level Debugging TechNote**
- **Cisco FlexVPN**
- **IPSec Negotiation/IKE Protocols**
- **Cisco AnyConnect Secure Mobility Client**
- **Cisco VPN Client**
- **Technical Support & Documentation − Cisco Systems**

Updated: Mar 15, 2013 Document ID: 115950