EzVPN-NEM到FlexVPN迁移指南

目录

简介

本文档在从EzVPN(互联网密钥交换v1(IKEv1))设置到FlexVPN(IKEv2)设置的迁移过程中提供帮助，尽可能少的问题。由于IKEv2远程访问与IKEv1远程访问在某些方面不同，使迁移有些困难，因此本文档可帮助您在从EzVPN模式迁移到FlexVPN远程访问模式时选择不同的设计方法。

本文档涉及IOS FlexVPN客户端或硬件客户端，本文档不讨论软件客户端。有关软件客户端的详细信息，请参阅：

- FlexVPN:带内置Windows客户端和证书身份验证的IKEv2
- FlexVPN和Anyconnect IKEv2客户端配置示例
- FlexVPN部署：使用EAP-MD5的AnyConnect IKEv2远程访问

先决条件

要求

Cisco 建议您了解以下主题：

- IKEv2
- 思科FlexVPN
- Cisco AnyConnect 安全移动客户端
- Cisco VPN 客户端

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

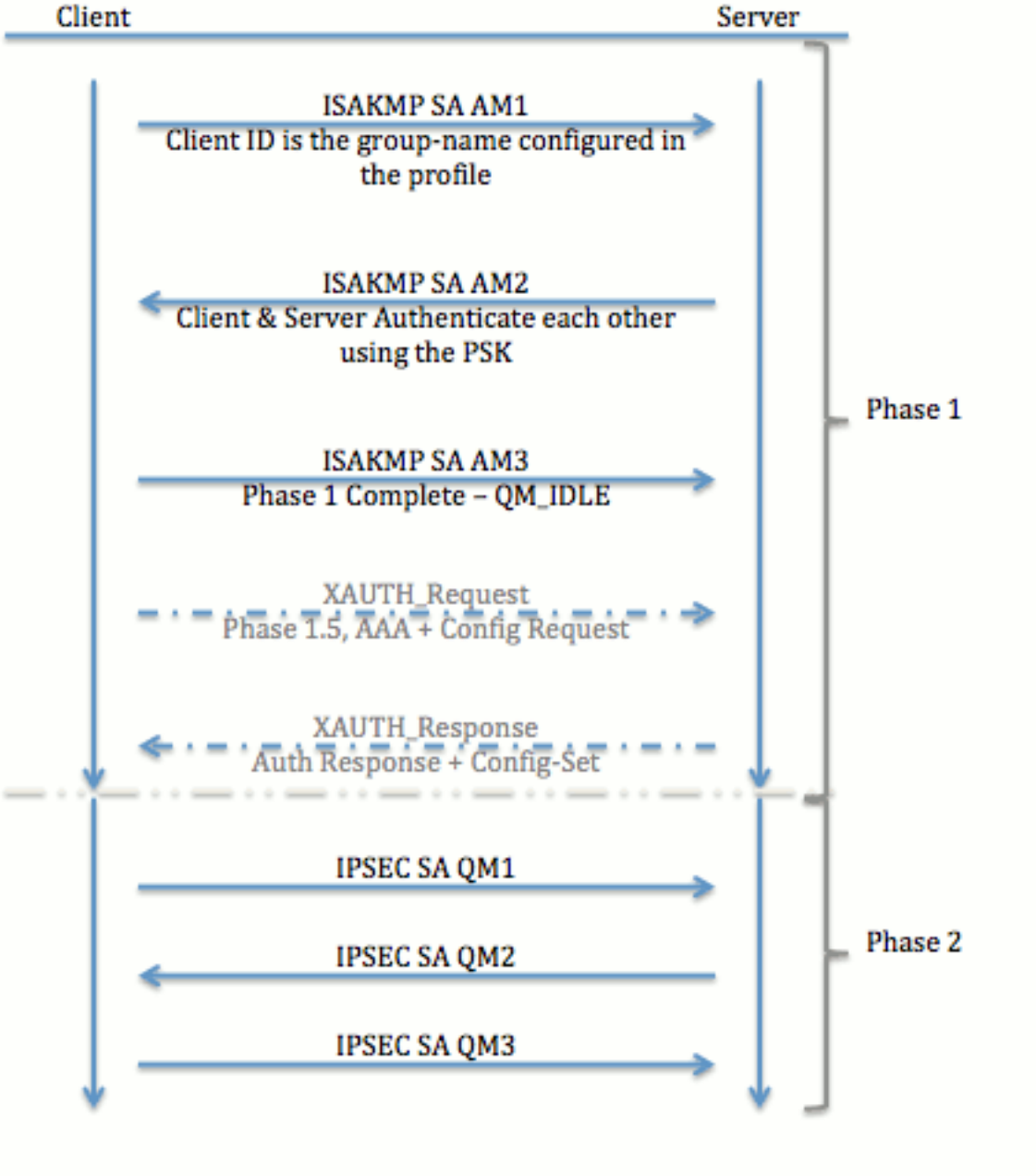
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

EzVPN与FlexVPN

EzVPN型号 — 突出之处

如名称所示，EzVPN的目标是使远程客户端上的VPN配置变得简单。为了实现此目的，客户端配置了联系正确的EzVPN服务器（也称为客户端配置文件）所需的最少详细信息。

隧道协商



FlexVPN远程访问VPN型号

FlexVPN服务器

正常FlexVPN和FlexVPN远程访问设置之间的一个重要区别是服务器需要仅通过使用预共享密钥和证书(RSA-SIG)方法向FlexVPN客户端验证自身。FlexVPN允许您决定发起方和响应方使用哪些身份验证方法，它们彼此独立。换句话说，它们可以是相同的，也可以是不同的。但是，在FlexVPN远程访问方面，服务器没有选择。

IOS FlexVPN客户端身份验证方法

客户端支持以下身份验证方法：

- **RSA-SIG** — 数字证书身份验证。
- **预共享** — 预共享密钥(PSK)身份验证。
- **可扩展身份验证协议(EAP)**- EAP身份验证。在15.2(3)T中添加了对IOS FlexVPN客户端的

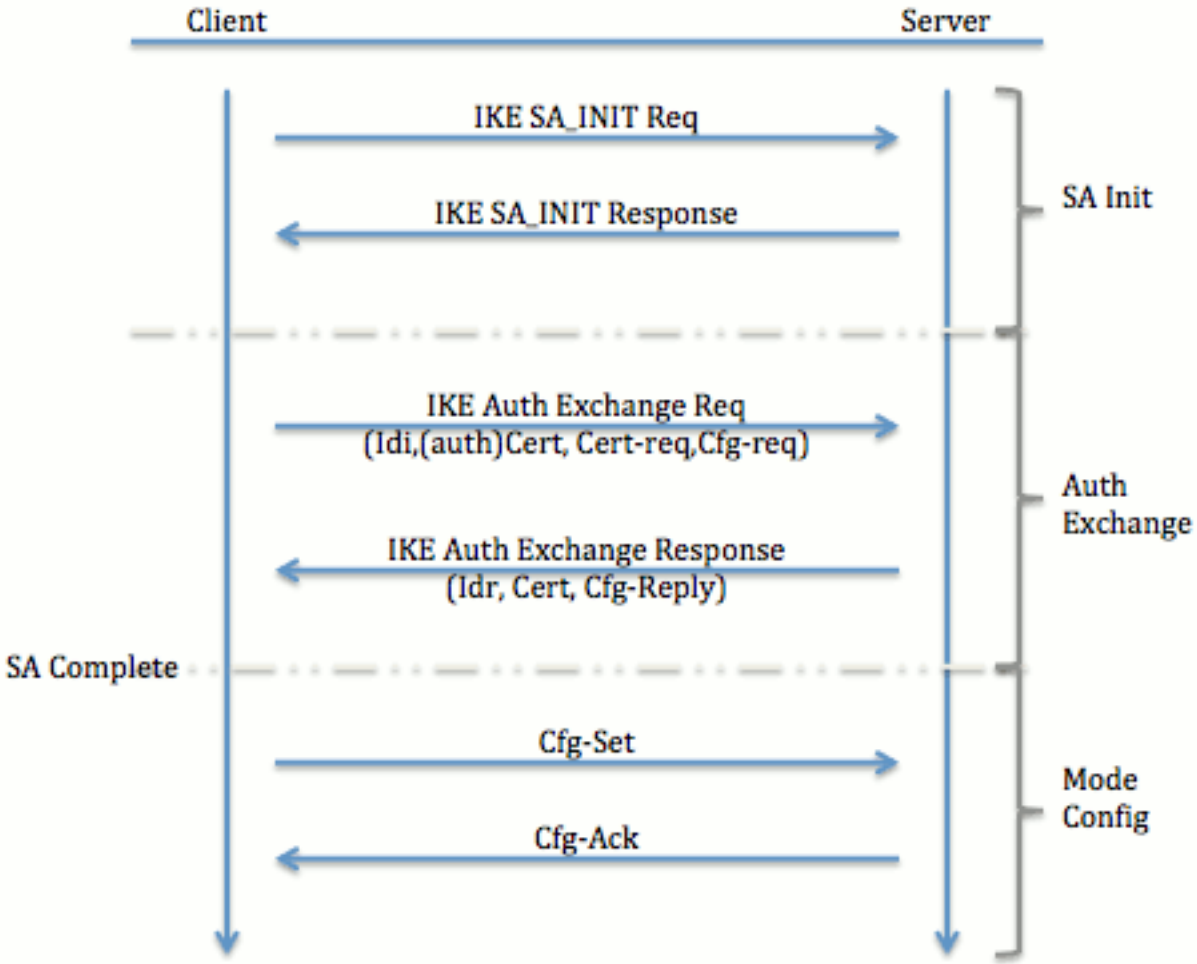
EAP支持。IOS FlexVPN客户端支持的EAP方法包括：可扩展身份验证协议 — 消息摘要5(EAP-MD5),可扩展身份验证协议 — Microsoft质询握手身份验证协议版本2(EAP-MSCHAPv2)，以及可扩展身份验证协议 — 通用令牌卡(EAP-GTC)。

本文档仅介绍RSA-SIG身份验证的使用，原因如下：

- **可扩展** — 为每个客户端都提供证书，并且在服务器上，客户端身份的通用部分会根据证书进行身份验证。
- **安全** — 比通配符PSK更安全（在本地授权情况下）。 虽然在AAA（身份验证、授权和记帐）授权的情况下，基于损坏的IKE身份编写单独的PSK会更容易。

与EasyVPN客户端相比，本文档中显示的FlexVPN客户端配置可能看起来并不详尽。这是因为配置包含由于智能默认值而不需要由用户配置的部分配置。智能默认值是指预配置或默认配置的术语，用于指建议、策略、IPSec转换集等各种配置。与IKEv1默认值不同，IKEv2智能默认值很强。例如，它在建议中使用高级加密标准(AES-256)、安全散列算法(SHA-512)和组5等。

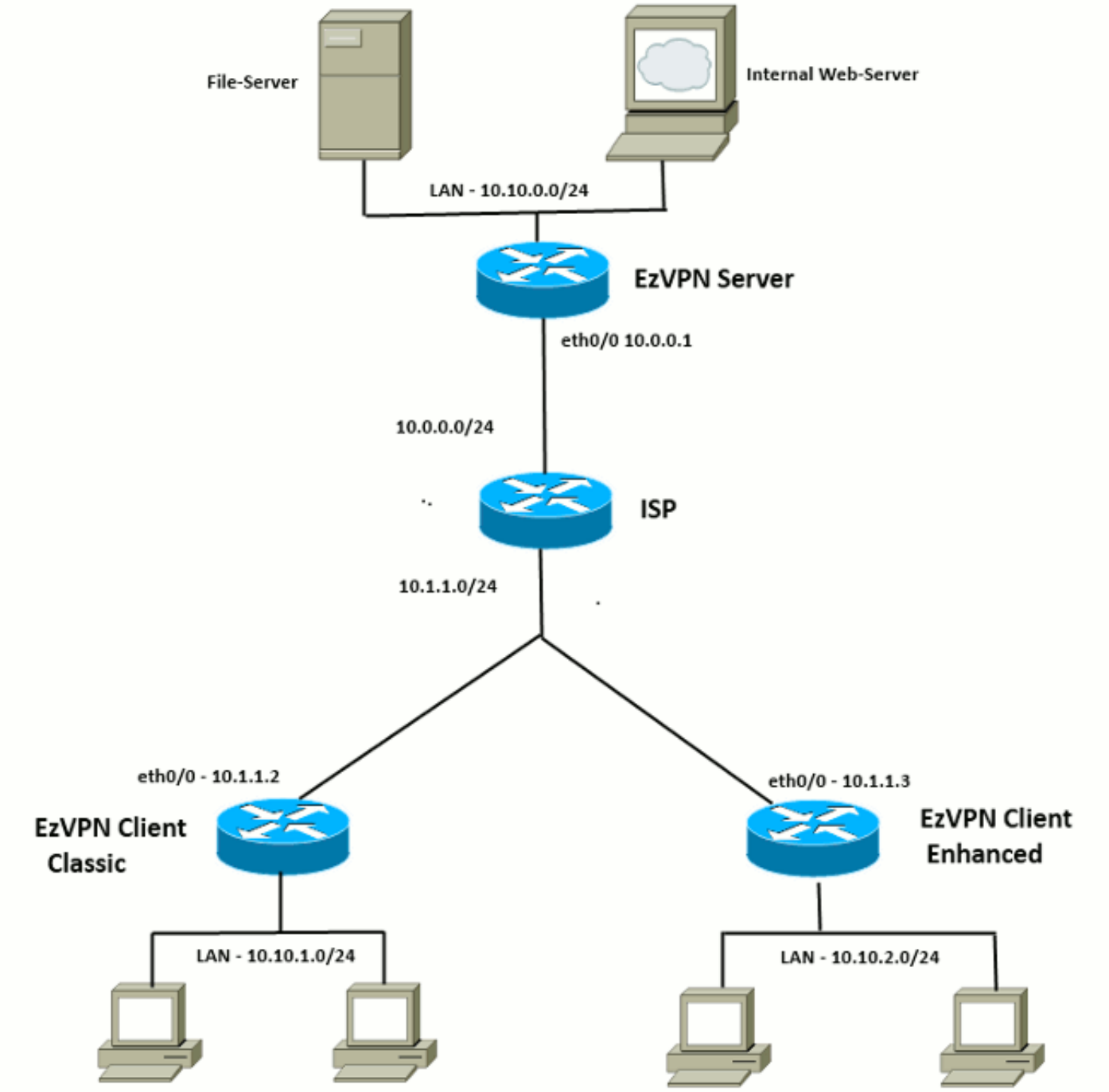
隧道协商



有关为IKEv2交换交换数据包的详细信息，请参阅IKEv2数据包交换和协议级调试。

初始设置

拓扑



初始配置

EzVPN集线器 — 基于dVTI

```
!! 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客户端 — 传统（无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客户端 — 增强型（基于VTI）

```
!! 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到FlexVPN的迁移方法

充当EzVPN服务器的服务器也可充当FlexVPN服务器，只要它支持IKEv2远程访问配置。要获得完整的IKEv2配置支持，建议使用高于IOS v15.2(3)T的任何内容。在本例中，使用了15.2(4)M1。

有两种可能的方法：

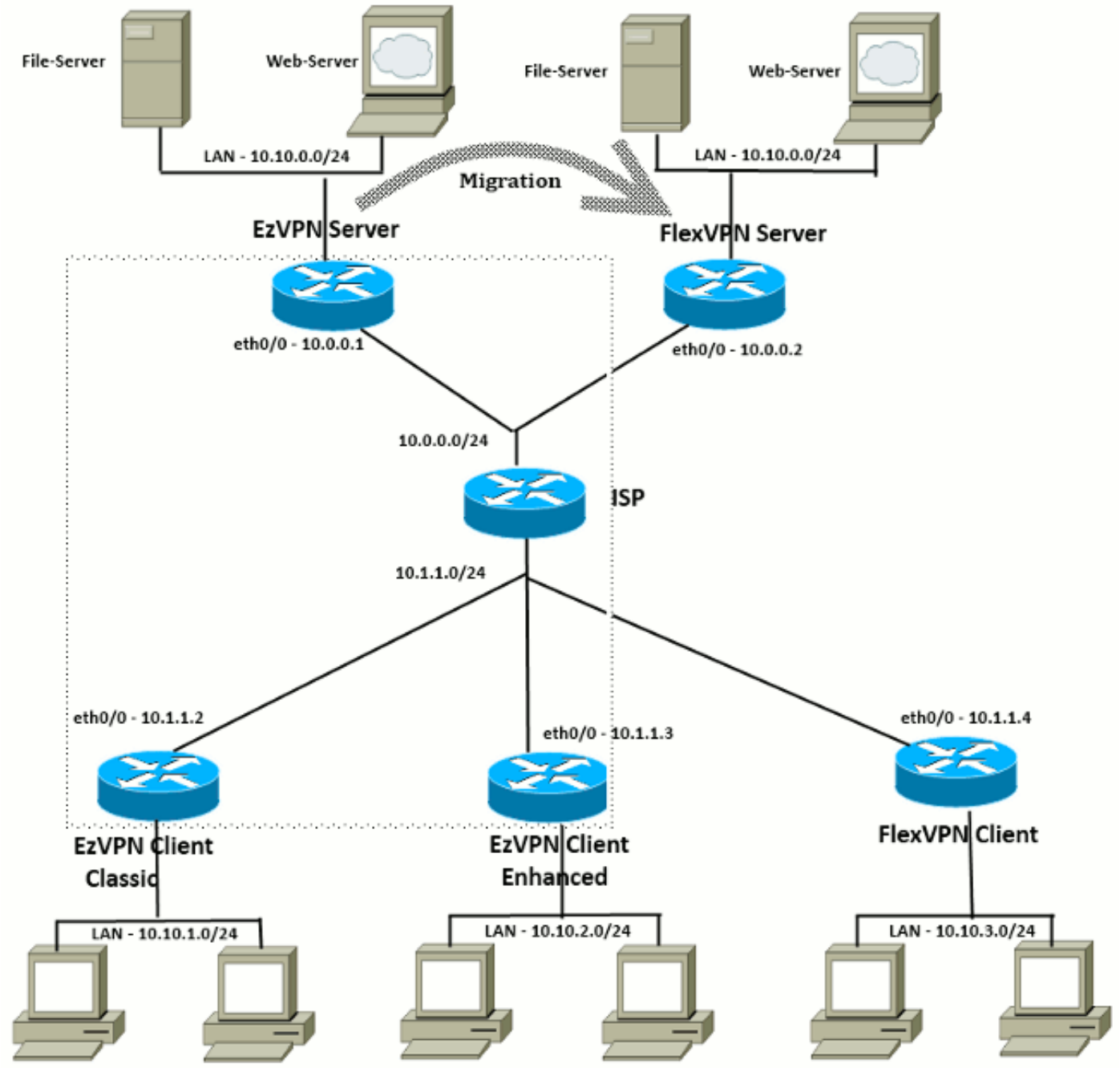
1. 将EzVPN服务器设置为FlexVPN服务器，然后将EzVPN客户端迁移到Flex配置。
2. 将另一台路由器设置为FlexVPN服务器。EzVPN客户端和迁移的FlexVPN客户端通过在FlexVPN服务器和EzVPN服务器之间创建连接继续通信。

本文档介绍第二种方法，并使用新的分支（例如Spoke3）作为FlexVPN客户端。此分支可用作将来迁移其他客户端的参考。

迁移步骤

请注意，从EzVPN分支迁移到FlexVPN分支时，可以选择在EzVPN分支**上加**载FlexVPN配置。但是，在整个切换过程中，您可能需要对设备进行带外（非VPN）管理访问。

迁移的拓扑



配置

FlexVPN集线器

```
!! 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
```

关于服务器证书的注释

密钥使用(KU)定义公钥的用途或目标用途。增强/扩展密钥使用(EKU)改进了密钥使用。FlexVPN要求服务器证书具有EKU(服务器**身份验证**(OID = 1.3.6.1.5.5.7.3.1))和**数字签名**和**密钥加密**的KU属性，以便客户端接受证书。

```
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客户端配置

```
!! 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
```

关于客户端证书的注释

FlexVPN要求客户端证书具有**客户端**身份验证(OID = 1.3.6.1.5.5.7.3.2)的KU属性(**数字签名**和**密钥加密**)，以便服务器接受证书。

```
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操作验证

FlexVPN服务器

```
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)
```

相关信息

- FlexVPN:带内置Windows客户端和证书身份验证的IKEv2技术说明
- FlexVPN和Anyconnect IKEv2客户端配置示例TechNote
- FlexVPN部署：使用EAP-MD5的AnyConnect IKEv2远程访问技术说明
- IKEv2数据包交换和协议级调试技术说明
- 思科FlexVPN
- IPsec 协商/IKE 协议
- Cisco AnyConnect 安全移动客户端
- Cisco VPN 客户端
- 技术支持和文档 - Cisco Systems