对FlexVPN迁移指南的EzVPN NEM

目录

简介

本文提供在迁移进程的援助从EzVPN (互联网密钥交换v1 (IKEv1))对FlexVPN (IKEv2)的设置设置与作为少量问题尽可能。因为IKEv2远程访问与IKEv1远程访问有所不同用使迁移有点困难的某些方式，本文帮助您选择在迁移的不同的设计方法从EzVPN型号到FlexVPN远程访问型号。

本文处理IOS FlexVPN客户端或硬件客户端，本文不讨论软件客户端。关于软件客户端的更多信息请参考：

- FlexVPN ：与内置的Windows客户端和证书验证的IKEv2
- FlexVPN和Anyconnect IKEv2客户端配置示例
- FlexVPN部署：与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

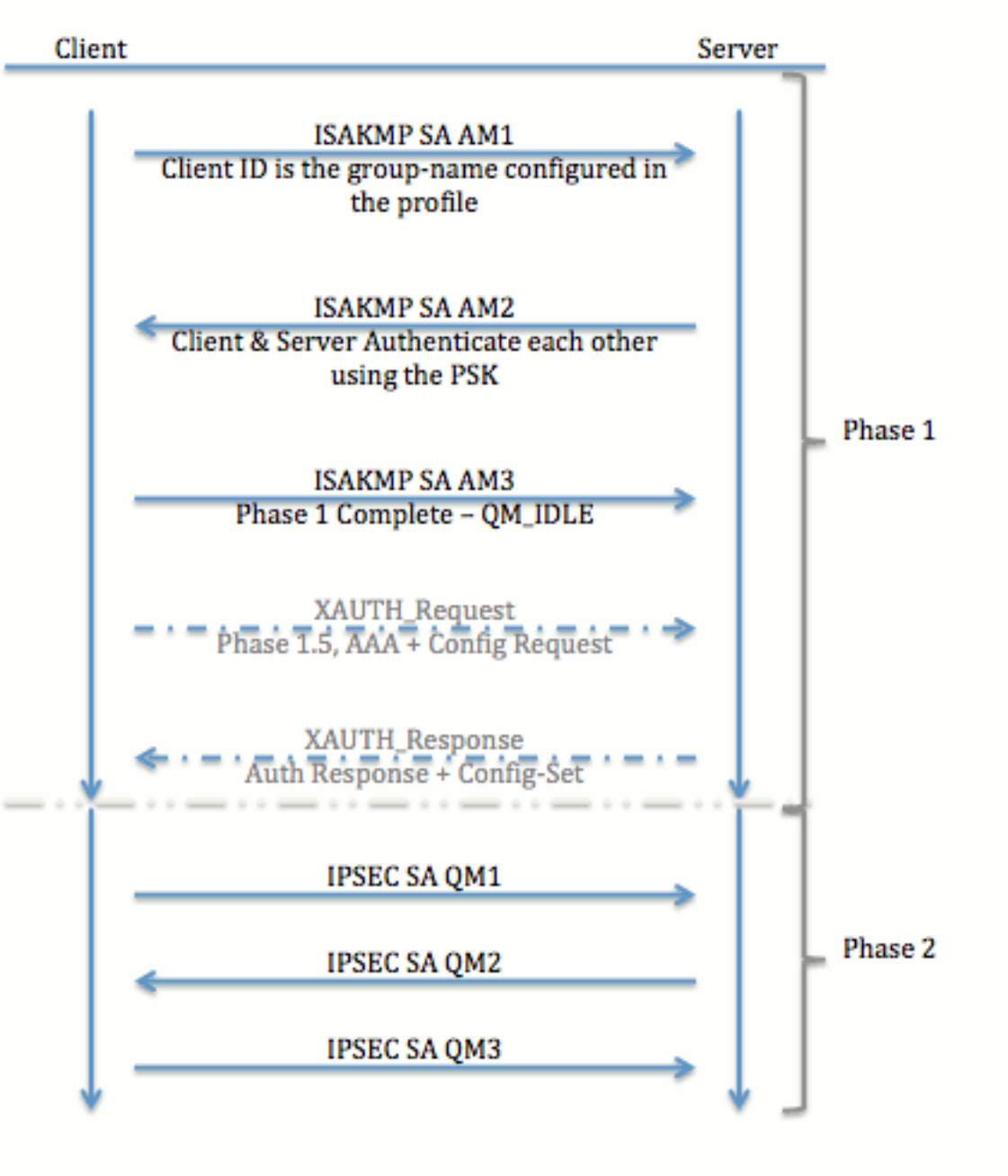
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

EzVPN与FlexVPN

EzVPN型号-什么引人注意

因为名称建议， EzVPN目标将使VPN配置在远程客户端变得容易。为了达到此，客户端配置与必要的最小详细信息与正确EzVPN服务器，亦称客户端配置文件联系。

隧道协商



FlexVPN远程访问VPN型号

FlexVPN服务器

在正常FlexVPN和FlexVPN远程访问设置之间的一个重要区别是服务器需要验证对FlexVPN客户端通过使用仅预先共享密钥和证书(RSA-SIG)方法。FlexVPN允许您决定哪些认证方法发起者和响应方用途，对立于彼此。换句话说，他们可以是相同的或他们可以不同的。然而，当谈到FlexVPN远程访问，服务器没有一选择。

IOS FlexVPN客户端验证方法

客户端支持这些认证方法：

- **RSA-SIG** —数字证书验证。
- **预共用**—预先共享密钥(PSK)验证。
- **可扩展的认证协议(EAP)** - EAP验证。IOS FlexVPN客户端的EAP支持在15.2(3)T被添加了。由

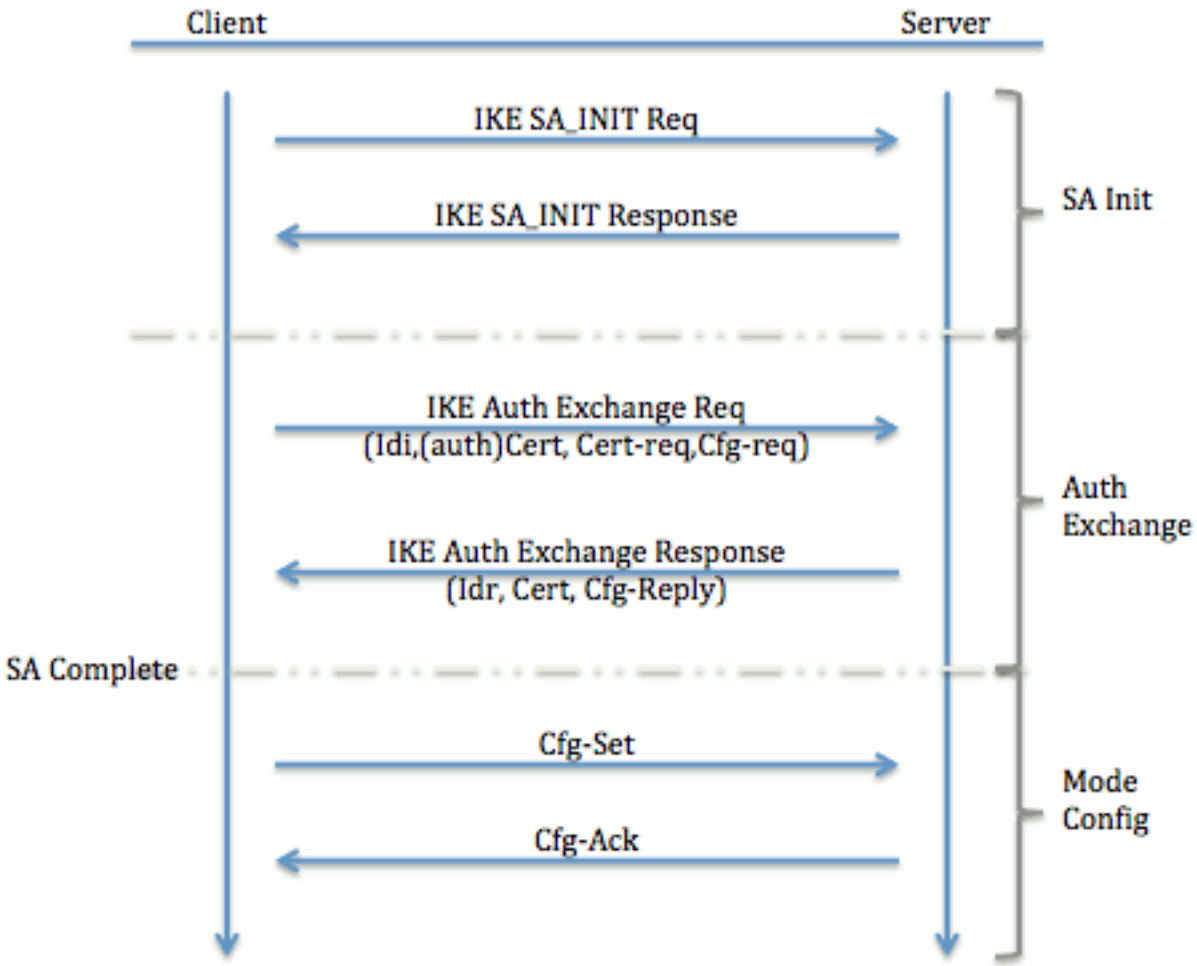
IOS FlexVPN客户端的支持的EAP方法包括：扩展验证消息摘要5 (EAP-MD5)，扩展验证协议Microsoft挑战握手验证协议版本2 (EAP-MSCHAPv2)，和扩展验证协议通用的令牌卡(EAP-GTC)。

本文只描述使用RSA-SIG验证，对于这些原因：

- **可扩展**—每个客户端给证书，并且在服务器，客户端标识的一个通用的部分验证它。
- **安全**—安全的更多比通配符PSK (在本地授权的情况下)。虽然，一旦AAA (认证、授权和记帐)授权，写入根据被损坏的IKE标识的分开的PSKs是更加容易的。

FlexVPN客户端配置显示在本文也许似乎少许详尽与EasyVPN比较客户端。这是因为配置包括不需要由用户配置由于聪明的默认配置的一些部分。聪明的默认是参考多种事的预先配置或默认配置的此术语用于类似建议，策略， IPSec转换集，等等。并且不同于IKEv1默认值， IKEv2聪明的默认值强。例如，它利用高级加密标准(AES-256)，在建议的安全散列算法(SHA-512)和Group-5，等等。

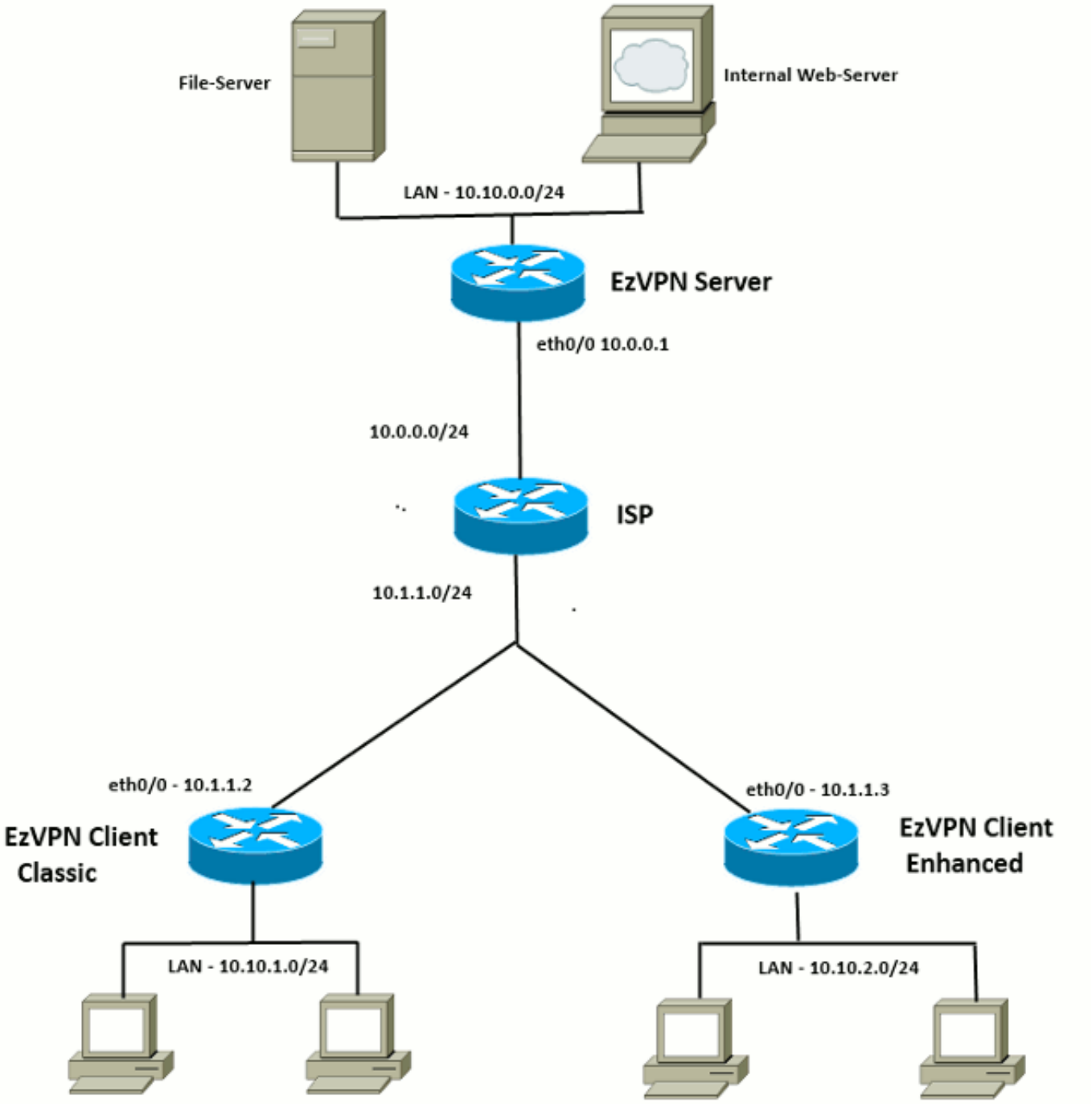
隧道协商



关于数据包的更多信息交换IKEv2交换的，参考IKEv2信息包交换和协议级调试。

初始设置

拓扑



初始配置

EzVPN集线器-基于的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-经典之作(没有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-提高(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
```

对FlexVPN迁移方法的EzVPN

作为EzVPN服务器的服务器能也作为FlexVPN服务器，只要支持IKEv2远程访问配置。对于一最大的IKEv2配置支持，在IOS v15.2(3)T上推荐任何。在这些示例中使用了15.2(4)M1。

有两个可能的途径：

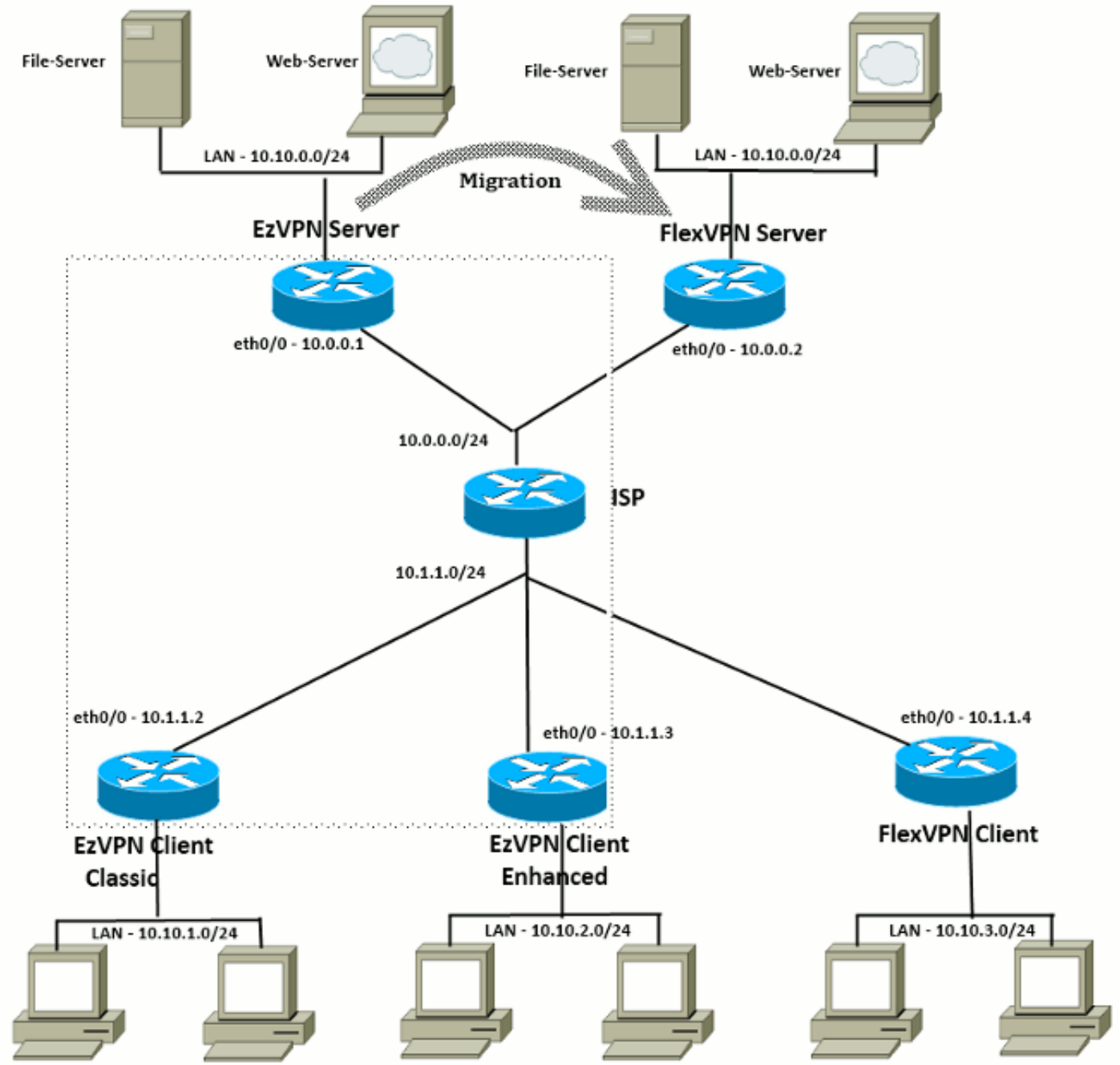
1. 设置EzVPN服务器作为FlexVPN服务器，然后移植EzVPN客户端屈曲配置。
2. 设置一个不同的路由器作为FlexVPN服务器。EzVPN客户端和被移植的FlexVPN客户端继续通过一连接的创建FlexVPN服务器和EzVPN服务器之间的通信。

本文描述第二方法并且使用一新的分支(例如， Spoke3)，作为FlexVPN客户端。此分支可以作为参考用于为了在将来移植其他客户端。

迁移步骤

注意，当您从EzVPN移植与FlexVPN谈了话发言，您能选择装载在EzVPN分支的**FlexVPN设置**。然而，在割接中，您也许需要一次带外(Non-VPN)管理访问到方框。

已迁移拓扑



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意

密钥用法(KU)定义了目的或公共密钥的目标使用。提高/扩展了密钥用法(EKU)完善密钥用法。FlexVPN需要服务器证书有**服务器验证**(OID EKU = 1.3.6.1.5.5.7.3.1)与**数字签名**和**密钥编码**KU属性

为了客户端能将接受的证书。

```
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意

FlexVPN需要客户端证书有**客户端验证**(OID EKU = 1.3.6.1.5.5.7.3.2)与**数字签名**和**密钥编码**KU属性为了服务器能将接受的证书。

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远程

```
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 ：与内置的Windows客户端和证书验证TechNote的IKEv2
- FlexVPN和Anyconnect IKEv2客户端配置示例TechNote
- FlexVPN部署：与EAP-MD5 TechNote的AnyConnect IKEv2远程访问
- IKEv2信息包交换和协议级调试TechNote

- 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