EzVPN-NEM到FlexVPN遷移指南

目錄

簡介

本文檔在從EzVPN(Internet Key Exchange v1(IKEv1)設定)遷移到FlexVPN(IKEv2)設定的過程中提供幫助，儘可能減少問題。由於IKEv2遠端訪問與IKEv1遠端訪問在某些方面有所不同，因此遷移變得有點困難，本文檔將幫助您在從EzVPN模型遷移到FlexVPN遠端訪問模型時選擇不同的設計方法。

本文檔涉及IOS FlexVPN客戶端或硬體客戶端，本文檔不討論軟體客戶端。有關軟體客戶端的詳細資訊，請參閱：

- FlexVPN:具有內建Windows客戶端和證書身份驗證的IKEv2
- FlexVPN和Anyconnect IKEv2客戶端配置示例
- FlexVPN部署：採用EAP-MD5的AnyConnect IKEv2遠端存取

必要條件

需求

思科建議您瞭解以下主題：

- IKEv2
- Cisco FlexVPN
- Cisco AnyConnect Security Mobility Solution — 遠端存取
- Cisco VPN使用者端

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

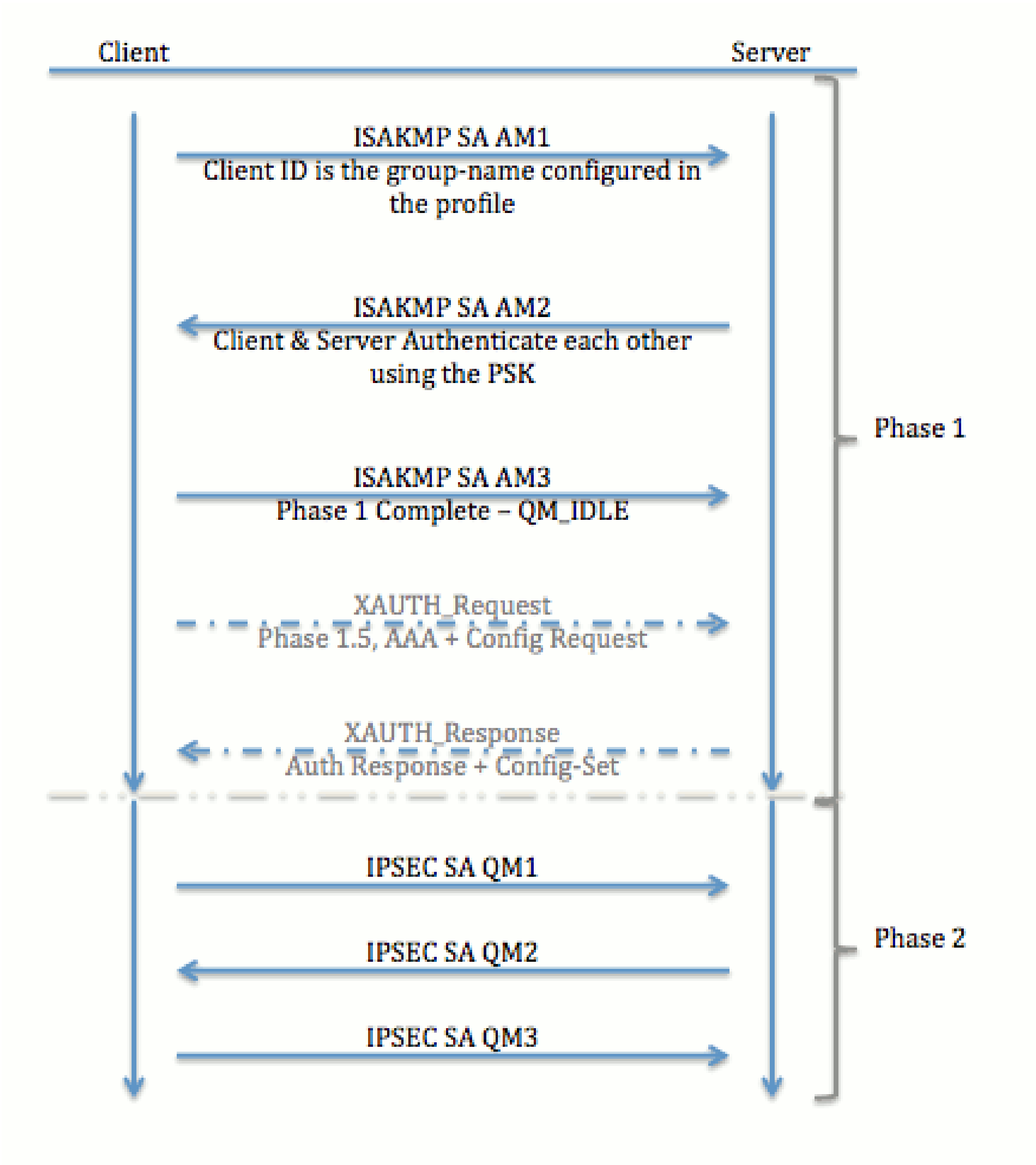
如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

EzVPN與FlexVPN

EzVPN型號 — 特別之處

顧名思義，EzVPN的目標是簡化遠端客戶端上的VPN配置。為了達到此目的，客戶端配置為聯絡正確的EzVPN伺服器（也稱為客戶端配置檔案）所需的最少詳細資訊。

通道交涉


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遠端存取VPN型號

FlexVPN伺服器

普通FlexVPN和FlexVPN遠端訪問設定的一個重要區別在於，伺服器需要僅通過使用預共用金鑰和證書(RSA-SIG)方法向FlexVPN客戶端驗證其自身。FlexVPN允許您決定發起方和響應方使用的身份驗證方法，彼此獨立。換句話說，它們可以相同或不同。但是，對於FlexVPN遠端訪問，伺服器沒有選擇。

IOS FlexVPN使用者端驗證方法

客戶端支援以下身份驗證方法：

- **RSA-SIG — 數**字證書身份驗證。
- **預共用 —** 預共用金鑰(PSK)身份驗證。
- **可擴展身份驗證協定(EAP)**- EAP身份驗證。15.2(3)T中增加了對IOS FlexVPN客戶端的EAP支

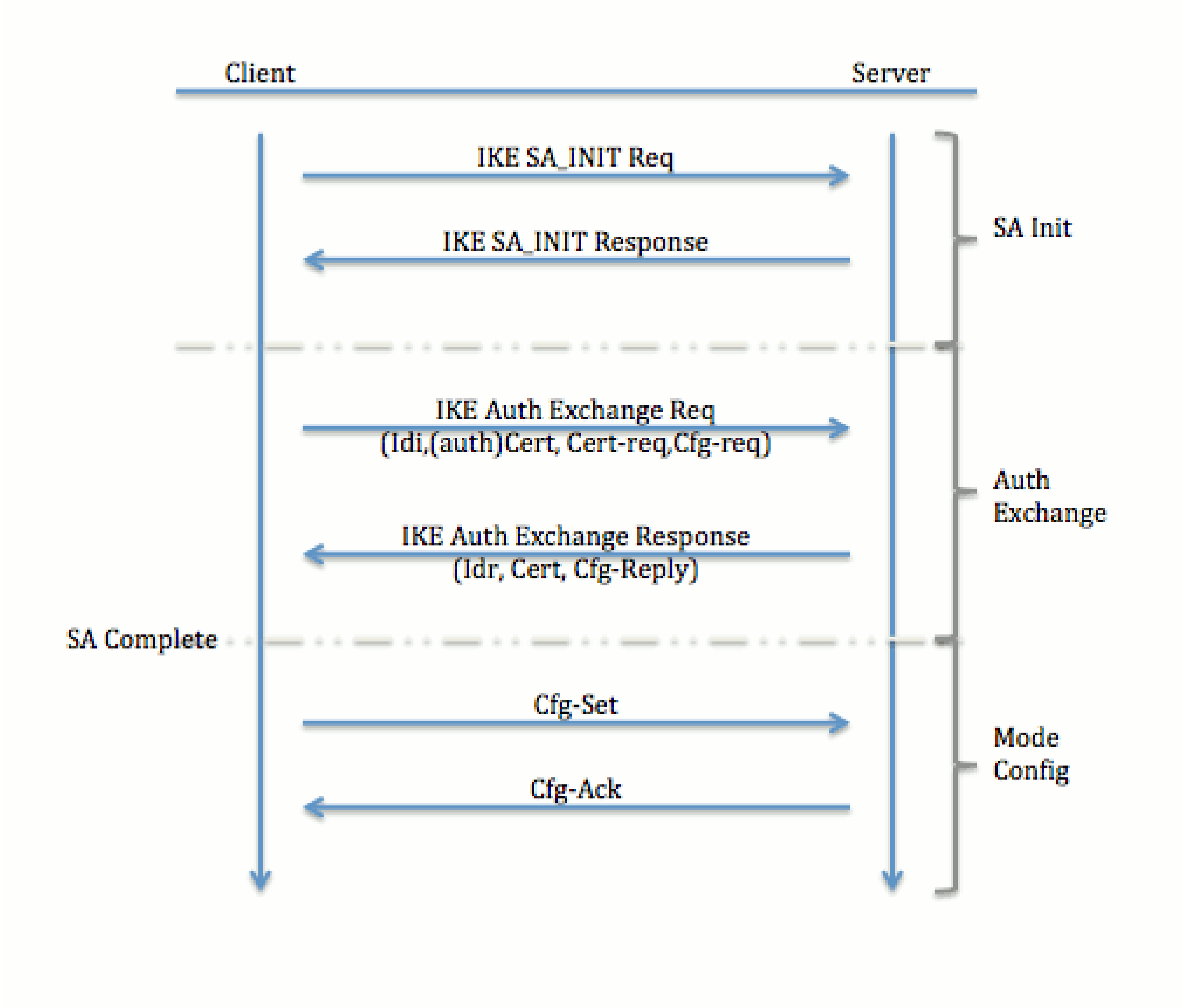
援。IOS FlexVPN客戶端支援的EAP方法包括：可擴展身份驗證協定 — 消息摘要5(EAP-MD5)、可擴展身份驗證協定 — Microsoft質詢握手身份驗證協定版本2(EAP-MSCHAPv2)，以及可擴充驗證通訊協定 — 通用權杖卡(EAP-GTC)。

本文檔僅介紹使用RSA-SIG身份驗證，原因如下：

- **可擴**展 — 每個客戶端都獲得一個證書，並且在伺服器上，客戶端標識的通用部分會根據它進行身份驗證。
- **安全** — 比萬用字元PSK更安全（在本地授權的情況下）。 雖然在AAA（身份驗證、授權和記帳）授權的情況下，基於損壞的IKE標識寫入獨立的PSK較為容易。

與EasyVPN客戶端相比，本文檔中顯示的FlexVPN客戶端配置看起來並不詳盡。這是因為配置中包含一些由於智慧預設值不需要由使用者配置的部分。智慧預設值是用來指預配置或預設配置的術語，用於各種事項，如建議、策略、IPSec轉換集等。與IKEv1預設值不同，IKEv2智慧預設值是強的。例如，它在建議書中使用了高級加密標準(AES-256)、安全雜湊演算法(SHA-512)和Group-5等。

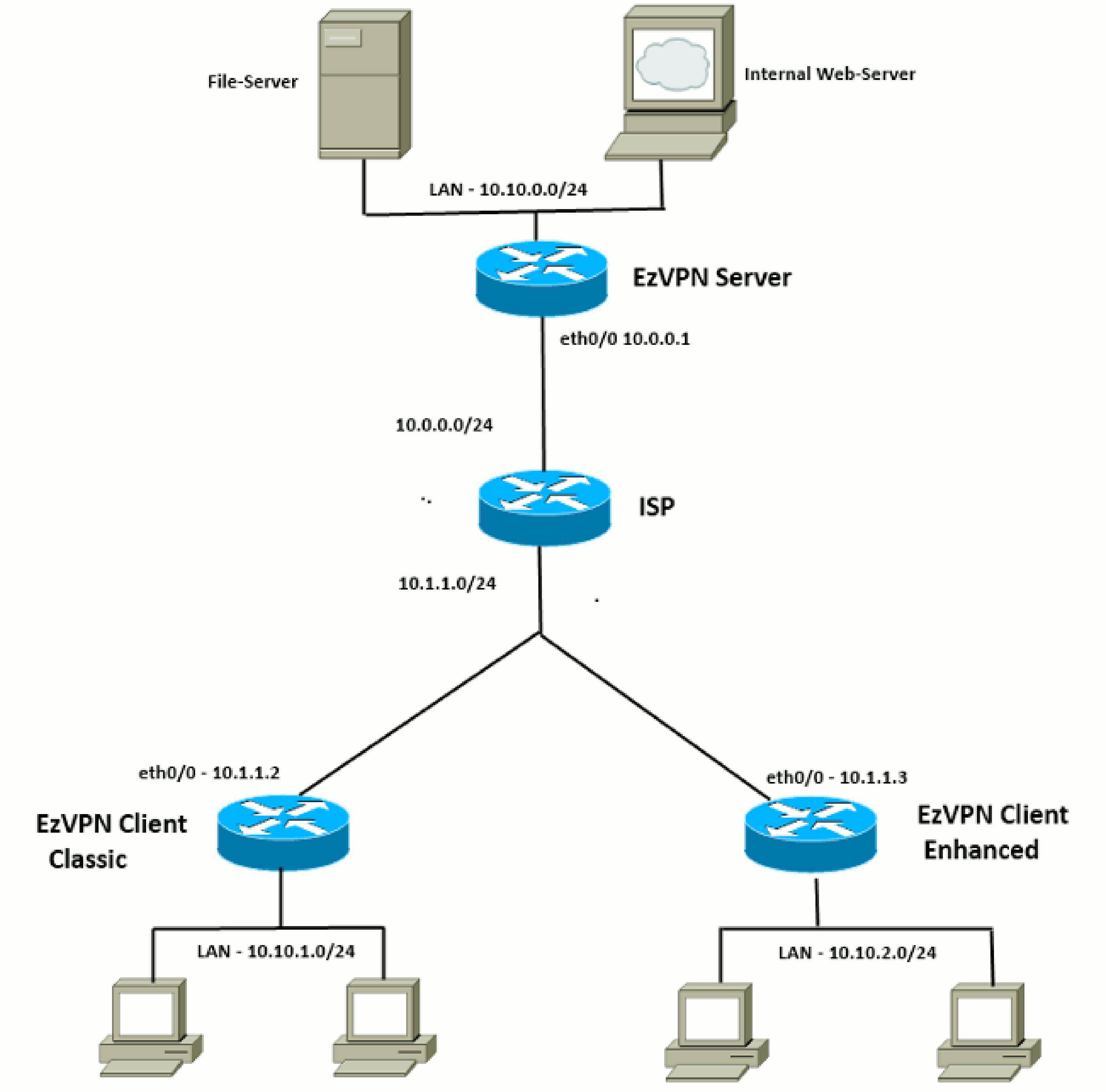
通道交涉



有關為IKEv2交換交換的資料包的詳細資訊，請參閱IKEv2資料包交換和協定級別調試。

初始設定

拓撲



初始配置

EzVPN中心 — 基於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客戶端 — 傳統（無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客戶端 — 增強型（基於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遷移方法

充當EzVPN伺服器的伺服器也可以充當FlexVPN伺服器，只要其支援IKEv2遠端訪問配置。如需完整的IKEv2配置支援，建議使用高於IOS v15.2(3)T的任何配置。在這些示例中，使用了15.2(4)M1。

有兩種可能的方法：

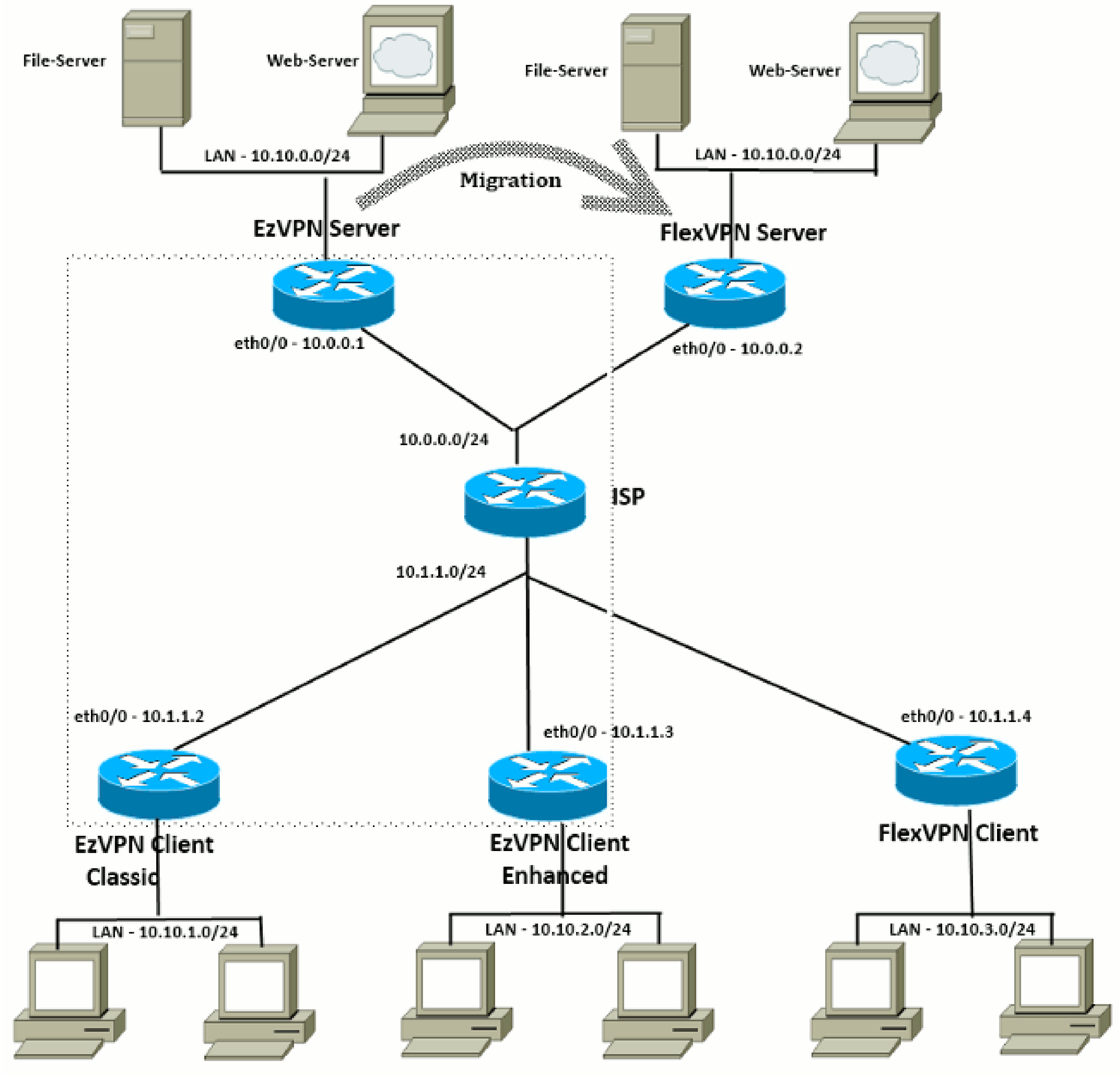
1. 將EzVPN伺服器設定為FlexVPN伺服器，然後將EzVPN客戶端遷移到Flex配置。
2. 將不同的路由器設定為FlexVPN伺服器。EzVPN客戶端和遷移的FlexVPN客戶端通過建立FlexVPN伺服器與EzVPN伺服器之間的連線繼續通訊。

本文檔介紹第二種方法並使用新的分支（例如Spoke3）作為FlexVPN客戶端。此分支可用作將來遷移其他客戶端的參考。

遷移步驟

請注意，從EzVPN分支遷移到FlexVPN分支時，您可以選擇在EzVPN分支**上加**載FlexVPN配置。但是，在整個轉換過程中，您可能需要對裝置的帶外（非VPN）管理訪問。

遷移的拓撲



組態

FlexVPN中心

```
!! 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
```

有關伺服器證書的說明

金鑰用法(KU)定義了公鑰的用途或預期用途。增強型/擴展金鑰使用(EKU)最佳化金鑰使用。FlexVPN要求伺服器憑證具有**伺服器驗證**(OID = 1.3.6.1.5.7.3.1)的EKU，以及具有**Digital Signature**和**Key Encipherment**的KU屬性，以便使用者端接受憑證。

```
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客戶端配置

```
!! 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
```

有關客戶端證書的說明

FlexVPN要求客戶端證書具有**Client Auth**(OID = 1.3.6.1.5.7.3.2)的EKU屬性，以及**Digital Signature**和**Key Encipherment**的KU屬性，以便伺服器接受證書。

```
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操作驗證

FlexVPN伺服器

```
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)
```

相關資訊

- FlexVPN:帶內建Windows客戶端和證書身份驗證的IKEv2技術說明
- FlexVPN和Anyconnect IKEv2客戶端配置示例技術說明
- FlexVPN部署：採用EAP-MD5的AnyConnect IKEv2遠端訪問技術說明
- IKEv2封包交換和通訊協定層級偵錯技術說明
- Cisco FlexVPN
- IPSec 協商/IKE 通訊協定
- Cisco AnyConnect Security Mobility Solution — 遠端存取
- Cisco VPN使用者端
- 技術支援與文件 - Cisco Systems