Guida alla migrazione da EzVPN-NEM a FlexVPN

Sommario

Introduzione

Questo documento fornisce assistenza nel processo di migrazione dalla configurazione di EzVPN (Internet Key Exchange v1 (IKEv1)) alla configurazione di FlexVPN (IKEv2) con il minor numero di problemi possibile. Poiché l'accesso remoto IKEv2 si differenzia dall'accesso remoto IKEv1 per alcuni aspetti che rendono la migrazione un po' difficile, questo documento aiuta a scegliere diversi approcci di progettazione nella migrazione dal modello EzVPN al modello FlexVPN Remote Access.

Questo documento tratta il client IOS FlexVPN o il client hardware; non tratta il client software. Per ulteriori informazioni sul client software, consultare:

- FlexVPN: IKEv2 con autenticazione client Windows e certificato integrata
- Esempio di configurazione del client FlexVPN e Anyconnect IKEv2

- Installazione di FlexVPN: Accesso remoto AnyConnect IKEv2 con EAP-MD5

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

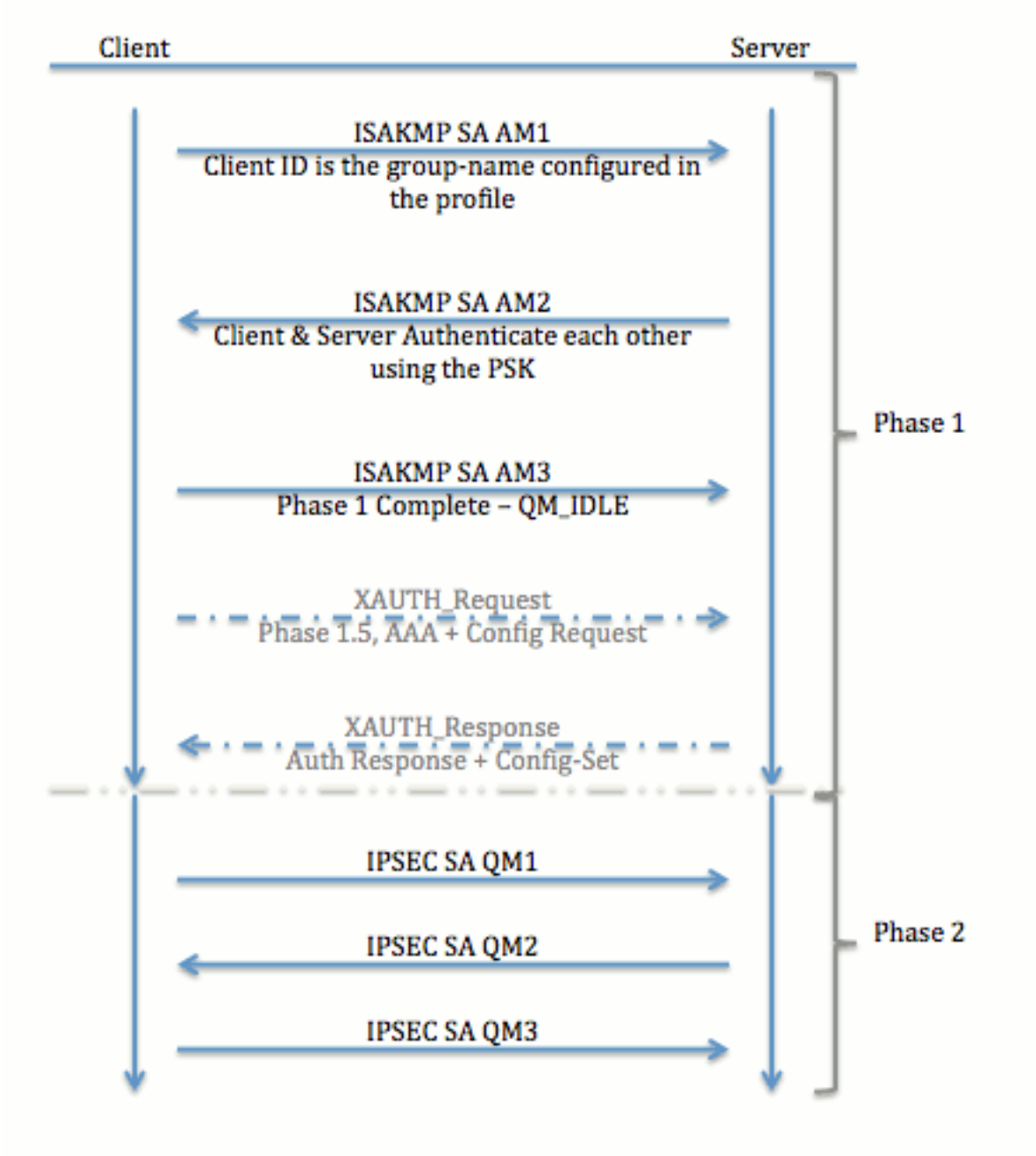
Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

EzVPN rispetto a FlexVPN

Modello EzVPN - Caratteristiche principali

Come suggerisce il nome, l'obiettivo di EzVPN è quello di semplificare la configurazione della VPN sui client remoti. Per ottenere questo risultato, il client è configurato con i dettagli minimi necessari per contattare il server EzVPN corretto, noto anche come profilo client.

Negoziazione tunnel



Modello VPN ad accesso remoto FlexVPN

Server FlexVPN

Una differenza importante tra la normale configurazione di FlexVPN e una configurazione di accesso remoto FlexVPN è che il server deve autenticarsi ai client FlexVPN solo tramite l'utilizzo del metodo RSA-SIG (Pre-Shared Key and Certificate). FlexVPN consente di decidere i metodi di autenticazione utilizzati dall'iniziatore e dal risponditore, indipendentemente l'uno dall'altro. In altre parole, possono essere uguali o diversi. Tuttavia, quando si tratta di accesso remoto FlexVPN, il server non ha scelta.

Metodi di autenticazione del client IOS FlexVPN

Il client supporta i seguenti metodi di autenticazione:

- **RSA-SIG**: autenticazione digitale dei certificati.

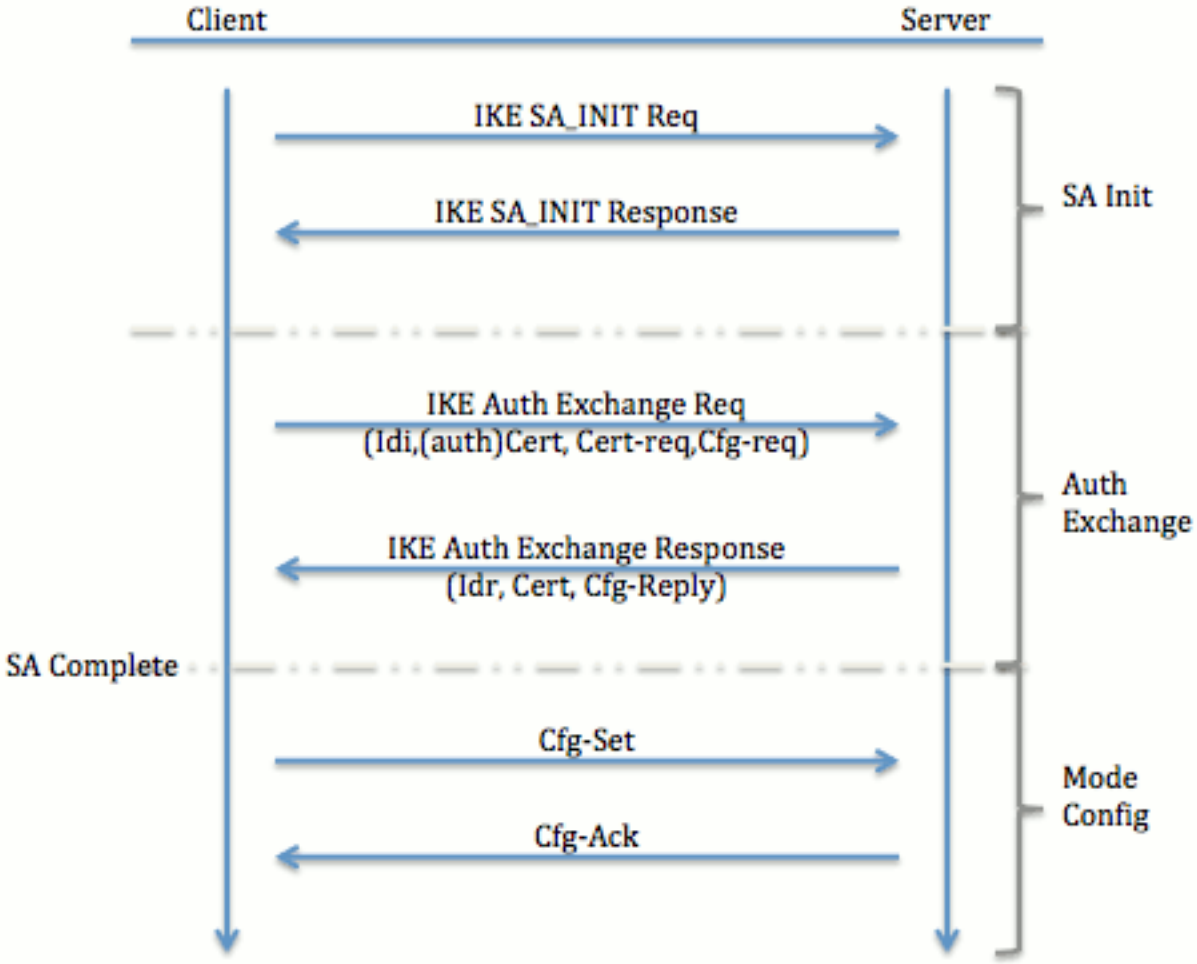
- **Pre-Share**: autenticazione con chiave già condivisa (PSK).
- **Extensible Authentication Protocol (EAP)** - Autenticazione EAP. Il supporto EAP per il client IOS FlexVPN è stato aggiunto nella versione 15.2(3)T.I metodi EAP supportati dal client IOS FlexVPN includono:Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol versione 2 (EAP-MSCHAPv2) eEAP-GTC (Extensible Authentication Protocol-Generic Token Card).

Questo documento descrive solo l'uso dell'autenticazione RSA-SIG, per i seguenti motivi:

- **Scalabile**: a ogni client viene assegnato un certificato e sul server viene autenticata una parte generica dell'identità del client.
- **Sicuro**: maggiore sicurezza rispetto a una chiave primaria con caratteri jolly (in caso di autorizzazione locale). Sebbene, nel caso dell'autorizzazione AAA (autenticazione, autorizzazione e accounting), sia più semplice scrivere PSK separati in base all'identità IKE modificata.

La configurazione del client FlexVPN mostrata in questo documento potrebbe sembrare poco esaustiva rispetto al client EasyVPN. Infatti, la configurazione include alcune parti che non devono essere configurate dall'utente a causa dei valori predefiniti. Smart defaults è il termine utilizzato per fare riferimento alla configurazione preconfigurata o predefinita per diversi elementi, ad esempio la proposta, il criterio, il set di trasformazioni IPSec e così via. A differenza dei valori predefiniti di IKEv1, i valori predefiniti intelligenti di IKEv2 sono elevati. Ad esempio, nelle proposte si fa uso di Advanced Encryption Standard (AES-256), Secure Hash Algorithm (SHA-512), e Group-5, e così via.

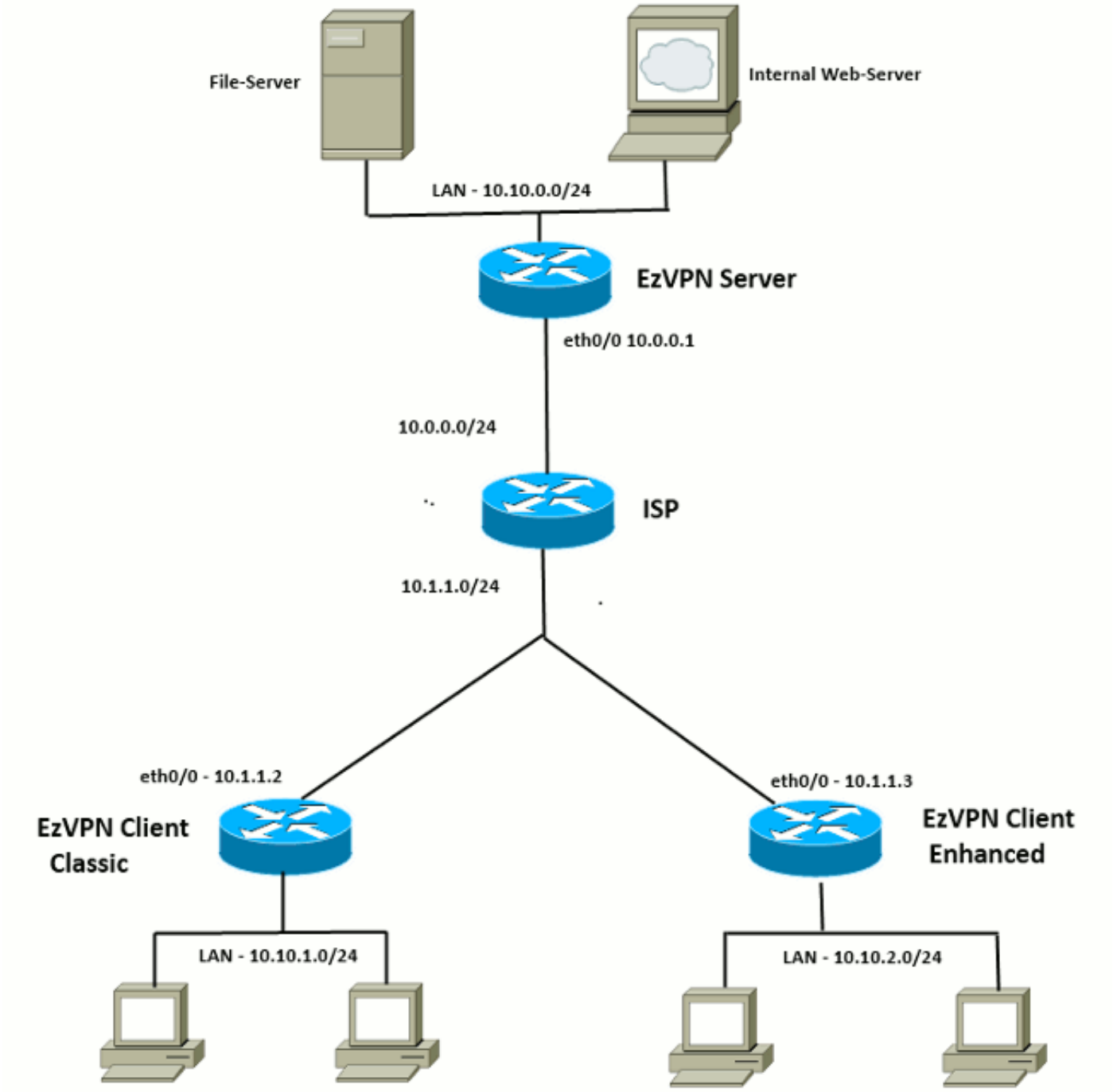
Negoziazione tunnel



Per ulteriori informazioni sullo scambio di pacchetti per uno scambio IKEv2, fare riferimento al debug a livello di protocollo e di scambio di pacchetti IKEv2.

Configurazione iniziale

Topologia



Configurazione iniziale

Hub EzVPN - Basato su 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
```

Client EzVPN - Classico (senza 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
```

Client EzVPN - Avanzato (basato su 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
```

Approccio alla migrazione da EzVPN a FlexVPN

Anche il server che funge da server EzVPN può fungere da server FlexVPN, a condizione che supporti la configurazione di accesso remoto IKEv2. Per il supporto completo della configurazione IKEv2, si consiglia un'opzione superiore a IOS v15.2(3)T. In questi esempi è stato utilizzato 15.2(4)M1.

Esistono due approcci possibili:

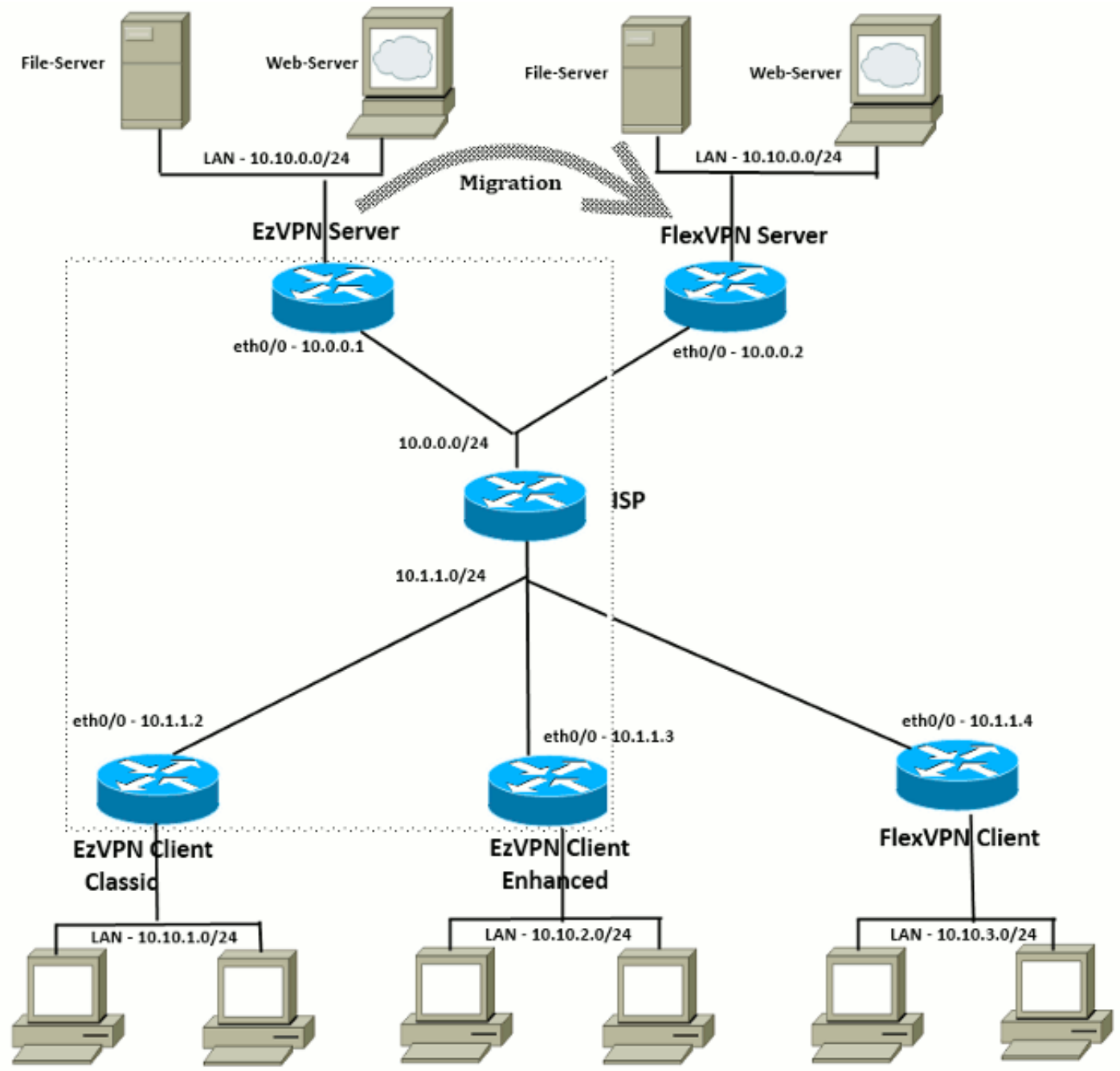
1. Configurare il server EzVPN come server FlexVPN, quindi eseguire la migrazione dei client EzVPN alla configurazione Flex.
2. Configurare un router diverso come server FlexVPN. I client EzVPN e i client FlexVPN migrati continuano a comunicare tramite la creazione di una connessione tra il server FlexVPN e il server EzVPN.

Questo documento descrive il secondo approccio e utilizza un nuovo spoke (ad esempio, Spoke3), come client FlexVPN. Questo spoke può essere utilizzato come riferimento per la migrazione di altri client in futuro.

Fasi della migrazione

Notare che quando si esegue la migrazione da EzVPN spoke a FlexVPN spoke, è possibile scegliere di caricare la **configurazione di FlexVPN** su EzVPN spoke. Tuttavia, durante il cut-over, potrebbe essere necessario un accesso di gestione fuori banda (non VPN) al dispositivo.

Topologia migrata



Configurazione

Hub FlexVPN

```
!! 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
```

Nota sui certificati server

L'utilizzo chiavi (KU, Key Usage) definisce lo scopo o l'utilizzo previsto della chiave pubblica. L'utilizzo chiavi avanzato/esteso (EKU) consente di perfezionare l'utilizzo chiavi. FlexVPN richiede che il certificato del server disponga di un EKU di **autenticazione server** (OID = 1.3.6.1.5.5.7.3.1) con gli attributi KU **Firma digitale** e **Crittografia chiave** affinché il certificato possa essere accettato dal 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>
```

Configurazione client FlexVPN

```
!! 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
```

Nota sui certificati client

FlexVPN richiede che il certificato client disponga di un EKU di **autenticazione client** (OID = 1.3.6.1.5.5.7.3.2) con gli attributi KU **Firma digitale** e **Crittografia chiave** affinché il certificato possa essere accettato dal 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>
```

Verifica dell'operazione FlexVPN

Server FlexVPN

```
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)
```

Informazioni correlate

- FlexVPN: Nota tecnica sull'autenticazione IKEv2 con client Windows e certificato integrati
- Note tecniche di esempio sulla configurazione del client FlexVPN e Anyconnect IKEv2
- Installazione di FlexVPN: Nota tecnica sull'accesso remoto AnyConnect IKEv2 con EAP-MD5
- Nota tecnica sul debug a livello di protocollo e di scambio pacchetti IKEv2
- Cisco FlexVPN

- Negoziazione IPSec/protocolli IKE
- Cisco AnyConnect Secure Mobility Client
- Cisco VPN Client
- Documentazione e supporto tecnico – Cisco Systems