EzVPN-NEM al Guía de migración de FlexVPN

Contenido

Introducción

Este documento proporciona la ayuda en el proceso de migración del EzVPN (v1 del intercambio de claves de Internet (IKEv1)) la configuración a FlexVPN (IKEv2) puso con como pocos problemas como sea posible. Puesto que el Acceso Remoto IKEv2 diferencia del Acceso Remoto IKEv1 de ciertas maneras que hagan migración un bit difícil, este documento le ayuda a elegir diversos acercamientos del diseño en la migración del modelo del EzVPN al modelo del Acceso Remoto de FlexVPN.

Este documento trata del cliente IOS FlexVPN o el hardware cliente, este documento no discute al software cliente. Para más información sobre el software cliente refiérase por favor:

- FlexVPN: IKEv2 con el cliente de Windows incorporado y la autenticación certificada
- Ejemplo de la configuración del cliente de FlexVPN y de Anyconnect IKEv2
- Despliegue de FlexVPN: Acceso Remoto de AnyConnect IKEv2 con el EAP-MD5

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- IKEv2
- Cisco FlexVPN
- Cliente de movilidad Cisco AnyConnect Secure
- Cliente de Cisco VPN

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

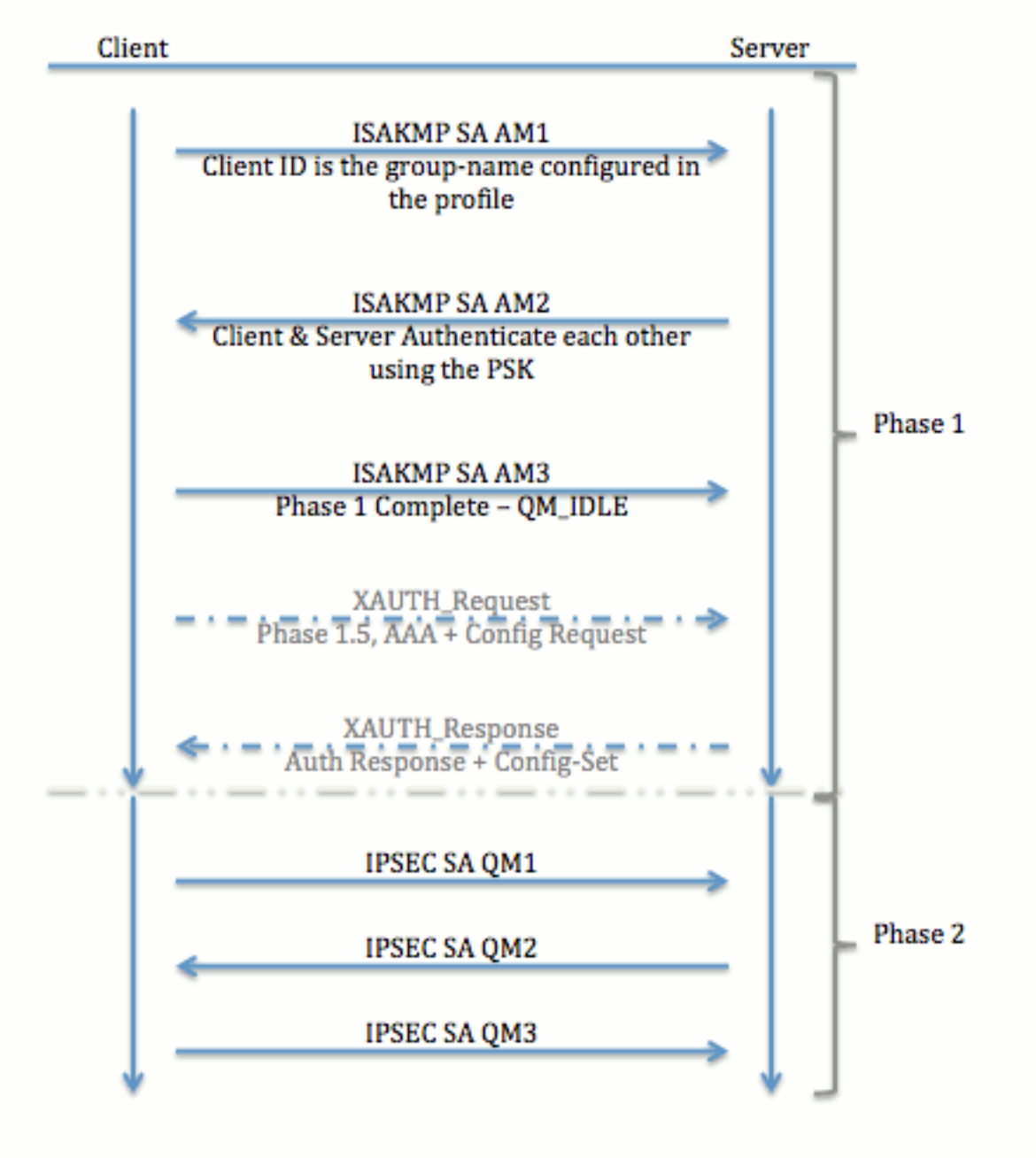
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

EzVPN contra FlexVPN

Modelo del EzVPN - Qué se destaca

Pues el nombre sugiere, el objetivo del EzVPN es hacer la configuración VPN en los clientes remotos fácil. Para alcanzar esto, configuran al cliente con los detalles mínimos necesarios para entrar en contacto al servidor EzVPN correcto, también conocido como el perfil del cliente.

Negociación de túnel



Modelo del VPN de acceso remoto de FlexVPN

Servidor de FlexVPN

Una diferencia importante entre FlexVPN normal y una configuración del Acceso Remoto de FlexVPN es que el servidor necesita autenticarse a los clientes de FlexVPN con el uso de las claves previamente compartidas y certifica el método (RSA-SIG) solamente. FlexVPN permite que usted decida a qué métodos de autentificación las aplicaciones del iniciador y del respondedor, independiente de uno a. Es decir pueden ser lo mismo o pueden ser diferentes. Sin embargo, cuando se trata del Acceso Remoto de FlexVPN, el servidor no tiene una opción.

Métodos de autenticación de cliente IOS FlexVPN

Los soportes de cliente los estos métodos de autentificación:

- **RSA-SIG** — Autenticación del certificado digital.

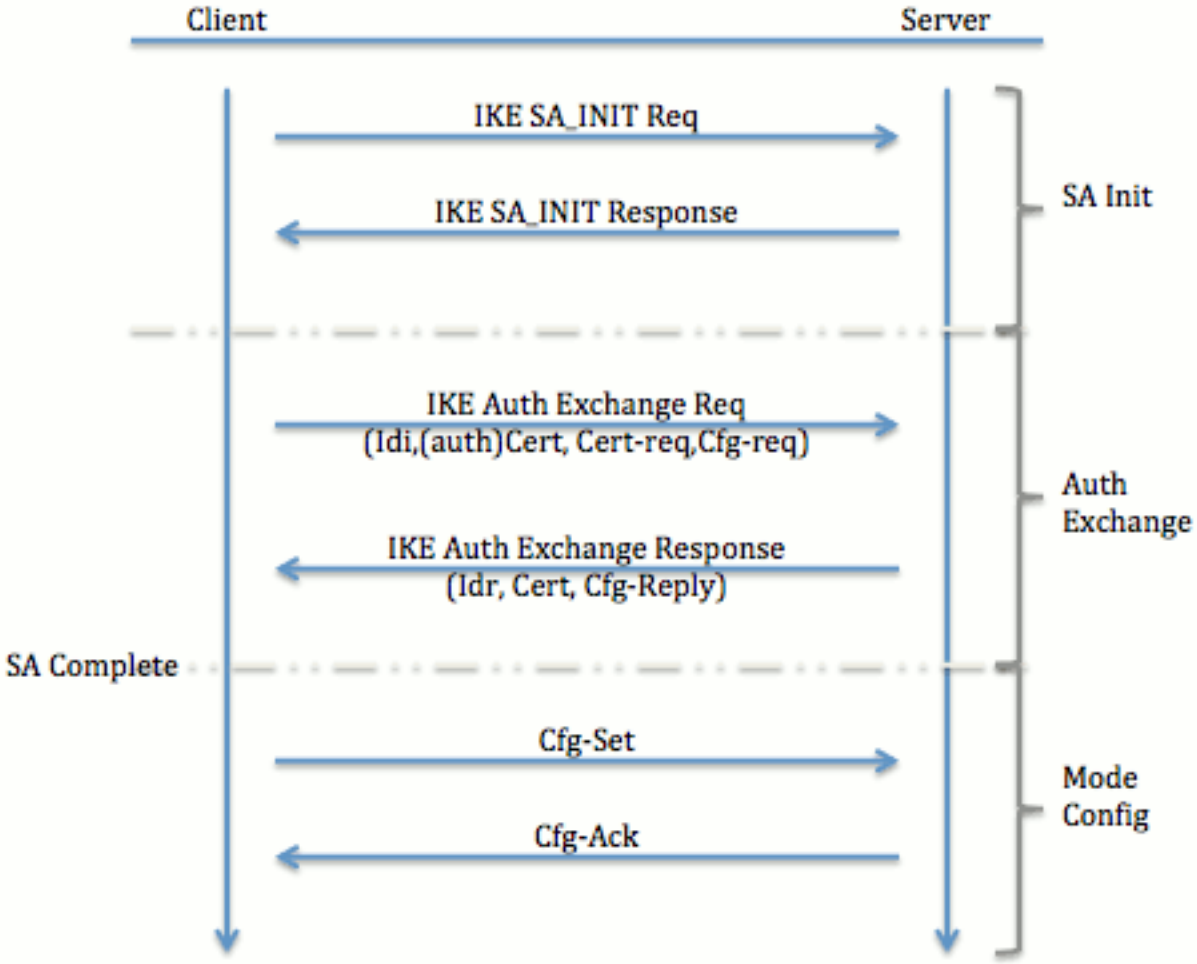
- **PRE-parte** — Autenticación de la clave previamente compartida (PSK).
- **Protocolo de Autenticación Extensible (EAP)** - Autenticación EAP. El EAP-soporte para el cliente IOS FlexVPN fue agregado en 15.2(3)T.Los métodos EAP soportados del cliente IOS FlexVPN incluyen:Extensible Authentication Protocol Message Digest 5 (EAP-MD5),Challenge Handshake Authentication Protocol de Protocolo-Microsoft de la autenticación ampliable versión 2 (EAP MSCHAPv2), yPlaca Token Protocolo-genérica de la autenticación ampliable (EAP-GTC).

Este documento describe solamente el uso de la autenticación RSA-SIG, por estas razones:

- **Scalable** — Dan cada cliente un certificado, y en el servidor, una identidad genérica del cliente de la parte de se autentica contra ella.
- **Asegure** — Más seguro que un PSK del comodín (en caso de la autorización local). Aunque, en el caso de la autorización AAA (autenticación, autorización y contabilidad), sea más fácil escribir PSKs separado basado en la identidad destrozada IKE.

La configuración del cliente de FlexVPN mostrada en este documento pudo parecer poco exhaustiva comparada al EasyVPN el cliente. Esto es porque la configuración incluye a algunas partes de la configuración que no necesiten ser configuradas por el usuario debido a los valores por defecto elegantes. Los valores por defecto elegantes son el término usado para referir al haber preconfigurado o la configuración predeterminada para las diversas cosas como la oferta, directiva, IPSec transforma el conjunto, y así sucesivamente. Y a diferencia de los valores predeterminados IKEv1, los valores predeterminados elegantes IKEv2 son fuertes. Por ejemplo, hace uso del Advanced Encryption Standard (AES-256), del algoritmo de troceo seguro (SHA-512), y de Group-5 en las ofertas, y así sucesivamente.

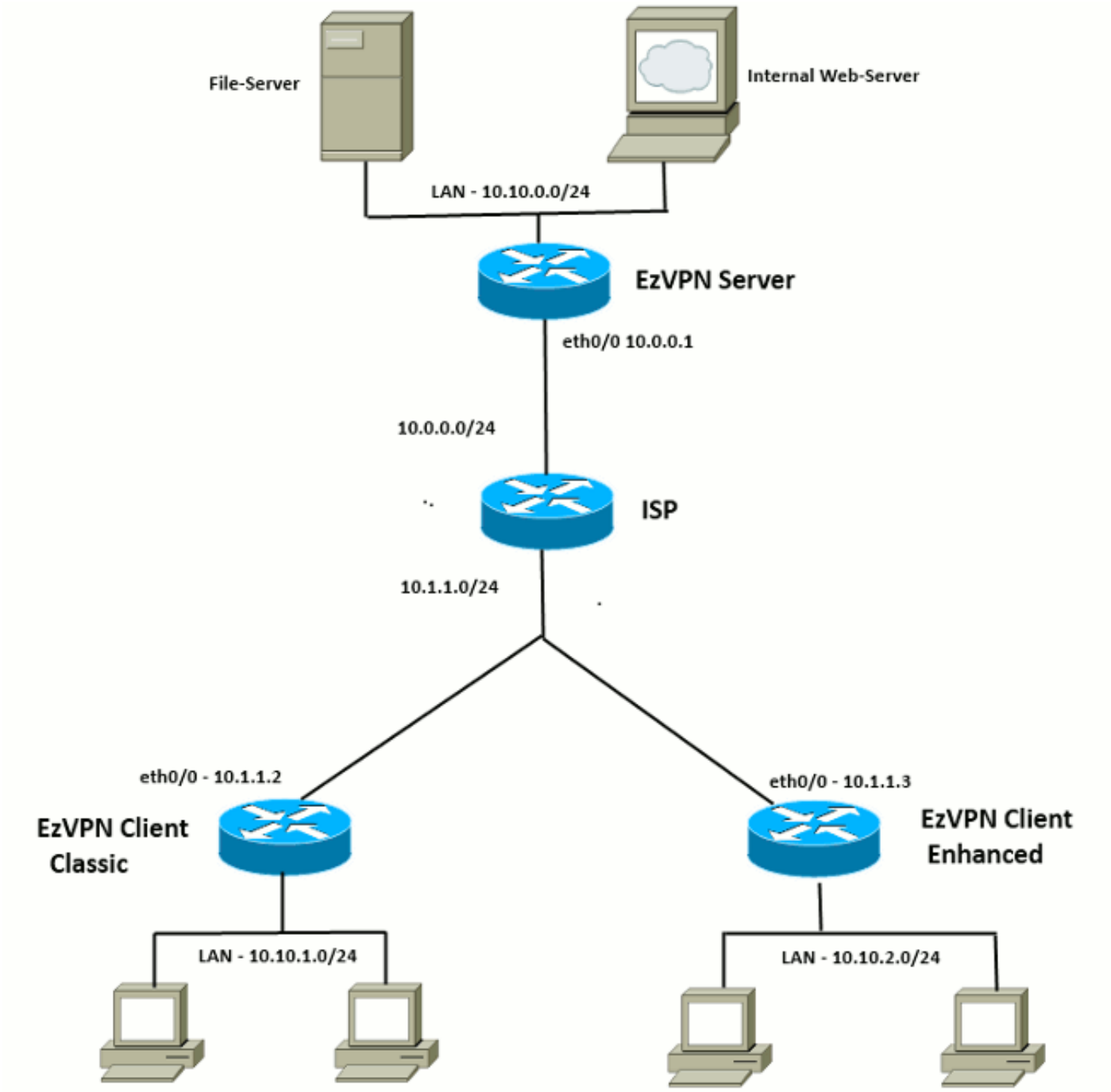
Negociación de túnel



Para más información sobre el intercambio de los paquetes para un intercambio IKEv2, refiera al intercambio de paquetes IKEv2 y al debugging del nivel del protocolo.

Configuración inicial

Topología



Configuración inicial

Concentrador del EzVPN - dVTI basado

```
!! 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
```

Cliente EzVPN - Obra clásica (ningún 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
```

Cliente EzVPN - Aumentado (VTI-basado)

```
!! 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 al acercamiento de la migración de FlexVPN

El servidor que actúa como servidor EzVPN puede también actuar como servidor de FlexVPN mientras soporte la configuración del Acceso Remoto IKEv2. Para un soporte completo de la configuración IKEv2, cualquier cosa sobre IOS v15.2(3)T se recomienda. En estos ejemplos se ha utilizado 15.2(4)M1.

Hay dos acercamientos posibles:

1. El servidor EzVPN de la configuración como servidor de FlexVPN, entonces emigra a los clientes EzVPN para doblar la configuración.
2. Ponga a un diverso router como servidor de FlexVPN. Los clientes EzVPN y los clientes emigrados de FlexVPN continúan comunicando a través de la creación de una conexión entre el servidor de FlexVPN y el servidor EzVPN.

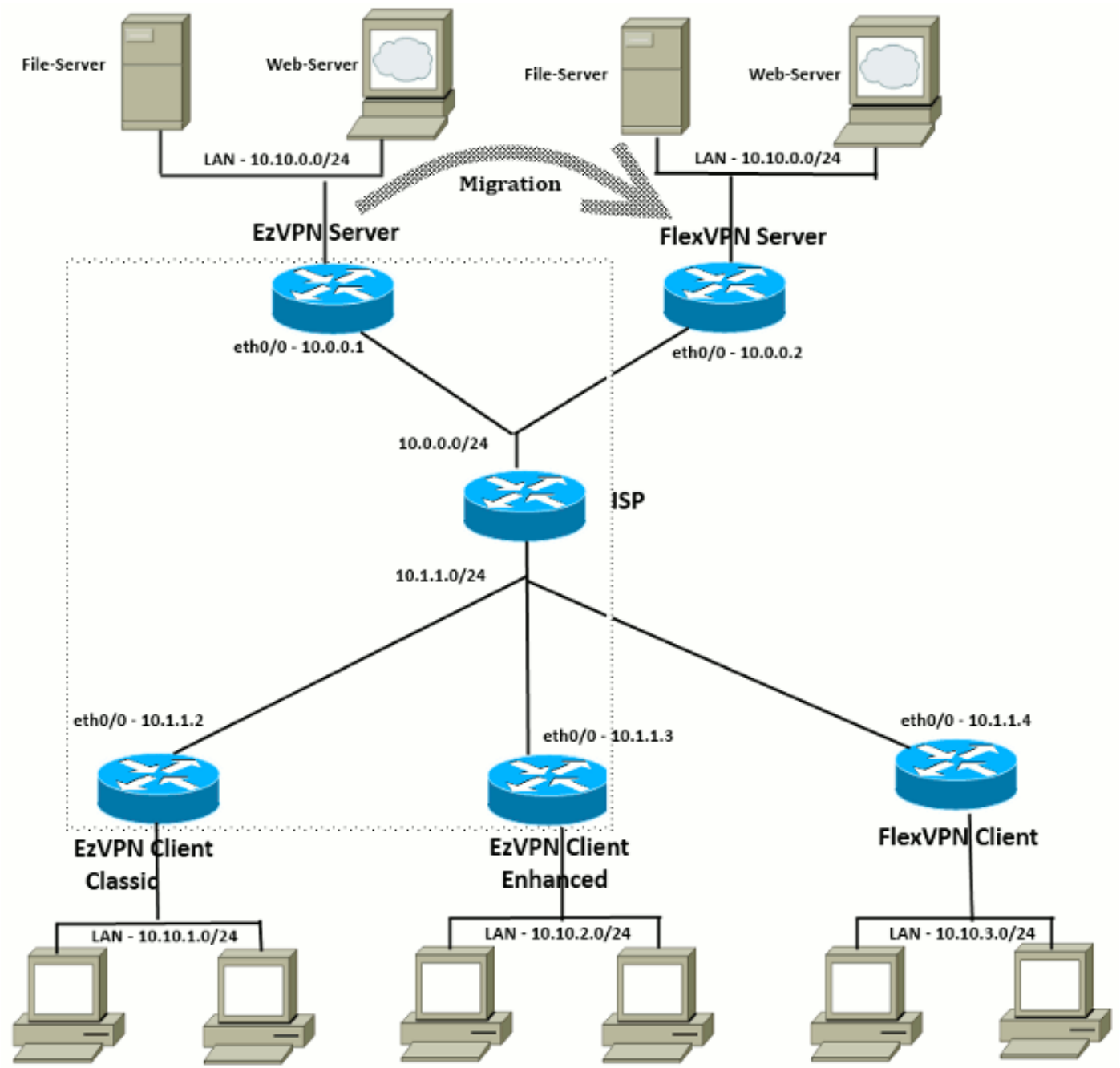
Este documento describe el segundo acercamiento y utiliza un nuevo spoke (por ejemplo, Spoke3), como el cliente de FlexVPN. Este spoke se puede utilizar como referencia para emigrar a otros clientes en el futuro.

Pasos de la migración

Observe que cuando usted emigra de un EzVPN habló a un FlexVPN habló, usted puede elegir

cargar los **config de FlexVPN** en el spoke del EzVPN. Sin embargo, en el cortado, usted puede ser que necesite un Acceso de administración fuera de banda (NON-VPN) al cuadro.

Topología emigrada



Configuración

Concentrador de 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
```

Observe sobre los certificados de servidor

El uso dominante (KU) define el propósito o el Uso previsto de la clave pública. Aumentado/amplió el uso dominante (EKU) refina el uso dominante. FlexVPN requiere que el certificado de servidor tenga un EKU del **auth del servidor** (OID = 1.3.6.1.5.5.7.3.1) con los atributos KU de la **firma digital** y de la **estenografía de la clave** para que el certificado sea validado por el cliente.

```
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>
```

Configuración del cliente de 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
```

Observe sobre los certificados del cliente

FlexVPN requiere que el certificado del cliente tenga un EKU del **auth del cliente** (OID = 1.3.6.1.5.5.7.3.2) con los atributos KU de la **firma digital** y de la **estenografía de la clave** para que el certificado sea validado por el servidor.

```
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>
```

Verificación de la operación de FlexVPN

Servidor de 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)

Telecontrol de FlexVPN

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)
```

Información Relacionada

- FlexVPN: IKEv2 con la Nota Técnica incorporada del cliente de Windows y de la autenticación certificada
- Nota Técnica del ejemplo de la configuración del cliente de FlexVPN y de Anyconnect IKEv2
- Despliegue de FlexVPN: Acceso Remoto de AnyConnect IKEv2 con la Nota Técnica del EAP-MD5
- Nota Técnica del intercambio de paquetes IKEv2 y del debugging del nivel del protocolo
- Cisco FlexVPN
- IPSec Negotiation/IKE Protocols
- Cliente de movilidad Cisco AnyConnect Secure
- Cliente de Cisco VPN
- Soporte Técnico y Documentación - Cisco Systems