EzVPN-NEM naar FlexVPN-migratiegids

Inhoud

Inleiding

Dit document biedt ondersteuning bij het migratieproces van EzVPN (Internet Key Exchange v1 (IKEv1)) naar FlexVPN (IKEv2) instellingen met zo weinig mogelijk problemen. Aangezien IKEv2 Remote Access op bepaalde manieren verschilt van IKEv1 Remote Access waardoor migratie een beetje moeilijk wordt, helpt dit document u bij het kiezen van verschillende ontwerpbenaderingen in de migratie van het EzVPN-model naar het FlexVPN Remote Access-model.

Dit document behandelt de IOS FlexVPN-client of de hardwareclient. Dit document bespreekt de softwareclient niet. Raadpleeg voor meer informatie over de softwareclient:

- FlexVPN: IKEv2 met ingebouwde Windows-client en certificaatverificatie
- Configuratievoorbeeld van FlexVPN- en AnyConnect IKEv2-client
- FlexVPN-implementaties: AnyConnect IKEv2 externe toegang met EAP-MD5

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IKEv2
- Cisco FlexVPN
- Cisco AnyConnect beveiligde mobiliteit-client
- Cisco VPN-client

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

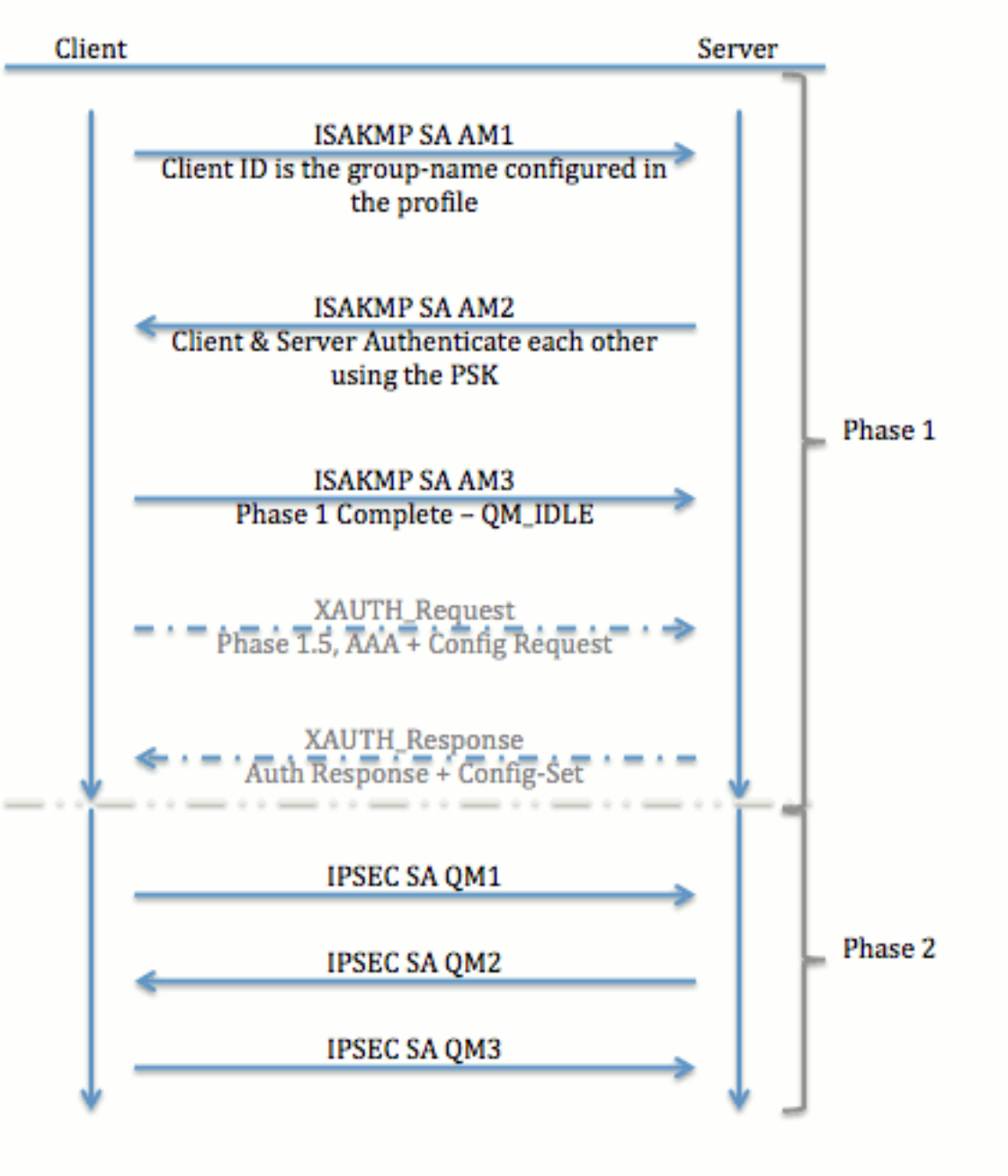
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

EzVPN versus FlexVPN

EZVPN-model - Wat uitkomt

Zoals de naam al zegt, is het doel van EzVPN om VPN-configuratie op de externe clients gemakkelijk te maken. Om dit te bereiken, wordt de client geconfigureerd met minimale informatie die nodig is om contact op te nemen met de juiste EzVPN-server, ook bekend als het clientprofiel.

Tunnelonderhandeling



FlexVPN Remote Access VPN-model

FlexVPN-server

Een belangrijk verschil tussen normale FlexVPN en een FlexVPN externe toegangsinstelling is dat de server zichzelf aan de FlexVPN-clients moet authenticeren door gebruik te maken van alleen de vooraf gedeelde sleutels en certificaten (RSA-SIG) methode. FlexVPN stelt u in staat te beslissen welke authenticatiemethoden de initiator en de responder gebruiken, onafhankelijk van elkaar. Met andere woorden, ze kunnen hetzelfde zijn of anders. Wanneer FlexVPN Remote Access wordt geleverd, heeft de server echter geen keuze.

IOS FlexVPN-clientverificatiemethoden

De cliënt steunt deze authenticatiemethoden:

- **RSA-SIG** — Digitale certificaatverificatie.

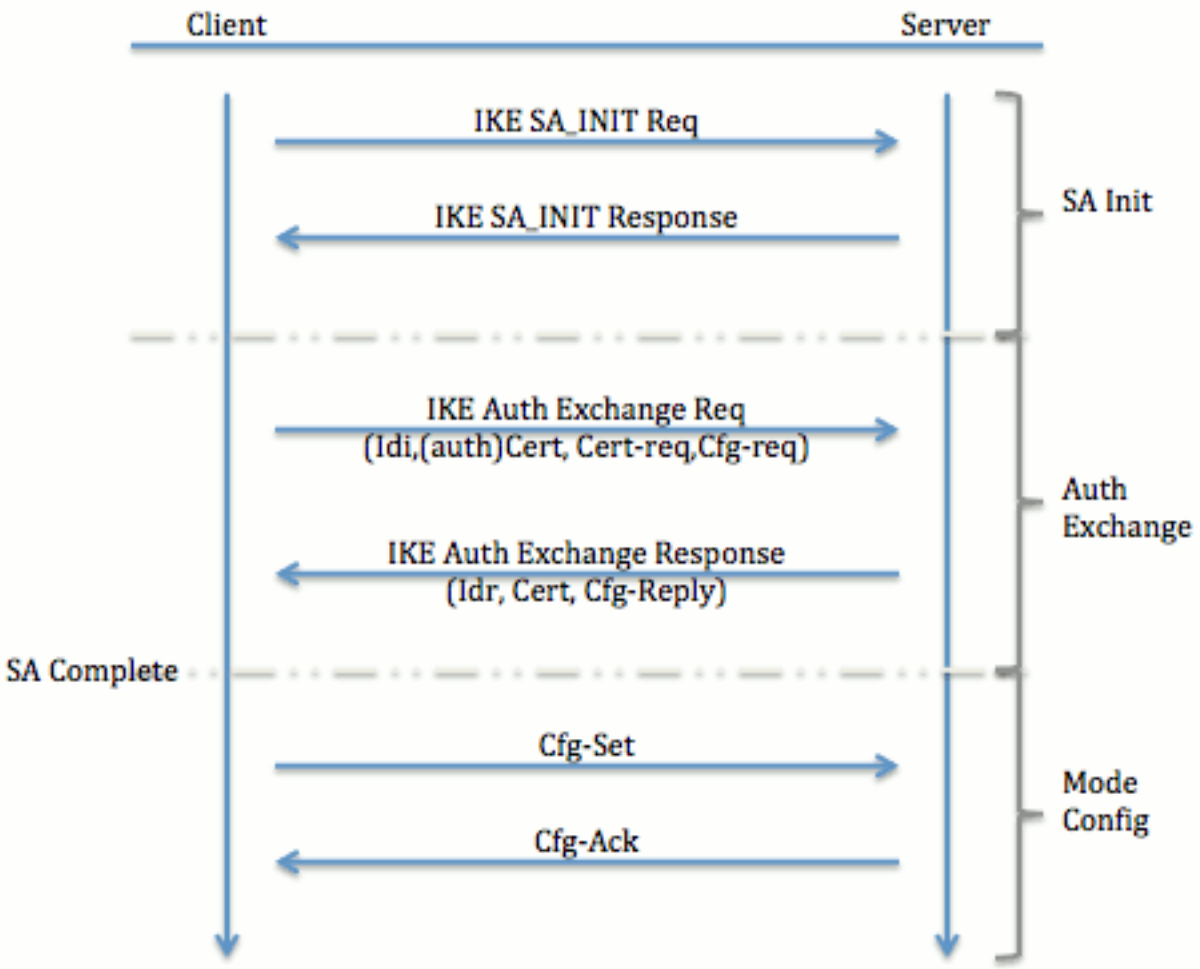
- **Pre-Share** — Pre-Shared Key (PSK) verificatie.
- **Extensible Authentication Protocol (EAP)** - EAP-verificatie. EAP-ondersteuning voor IOS FlexVPN-client werd toegevoegd in 15.2(3)T.Ondersteunde EAP-methoden door de IOS FlexVPN-client zijn onder meer:Extensible Authentication Protocol-Message Digest 5 (EAP-MD5),Uitbreidbare verificatie Protocol-Microsoft Challenge Handshake Authentication Protocol, versie 2 (EAP-MSCHAPv2) enUitbreidbare verificatieprotocol-generieke Token Card (EAP-GTC).

In dit document wordt alleen het gebruik van RSA-SIG-authenticatie beschreven, om deze redenen:

- **Schaalbaar** — Elke cliënt krijgt een certificaat, en op de server wordt een generiek deel van de identiteit van de cliënt ertegen geauthentificeerd.
- **Beveiliging** — veiliger dan een jokerbrochure PSK (in het geval van plaatselijke toestemming). Hoewel het in het geval van een vergunning voor AAA (authenticatie, autorisatie en accounting) gemakkelijker is om afzonderlijke PSK's te schrijven op basis van een beheerde IKE Identity.

De FlexVPN-clientconfiguratie die in dit document wordt getoond, lijkt mogelijk weinig limitatief vergeleken met EasyVPN-client. Dit komt doordat de configuratie bepaalde delen van de configuratie bevat die niet door de gebruiker hoeven te worden geconfigureerd vanwege slimme standaardinstellingen. Smart default is de term die wordt gebruikt om te verwijzen naar de vooraf ingestelde of standaard configuratie voor verschillende zaken zoals het voorstel, het beleid, de IPSec transformatie set enzovoort. En in tegenstelling tot IKEv1 standaardwaarden zijn IKEv2 slimme standaardwaarden sterk. Bijvoorbeeld, het maakt gebruik van Advanced Encryption Standard (AES-256), Secure Hash Algorithm (SHA-512) en Group-5 in de voorstellen, enzovoort.

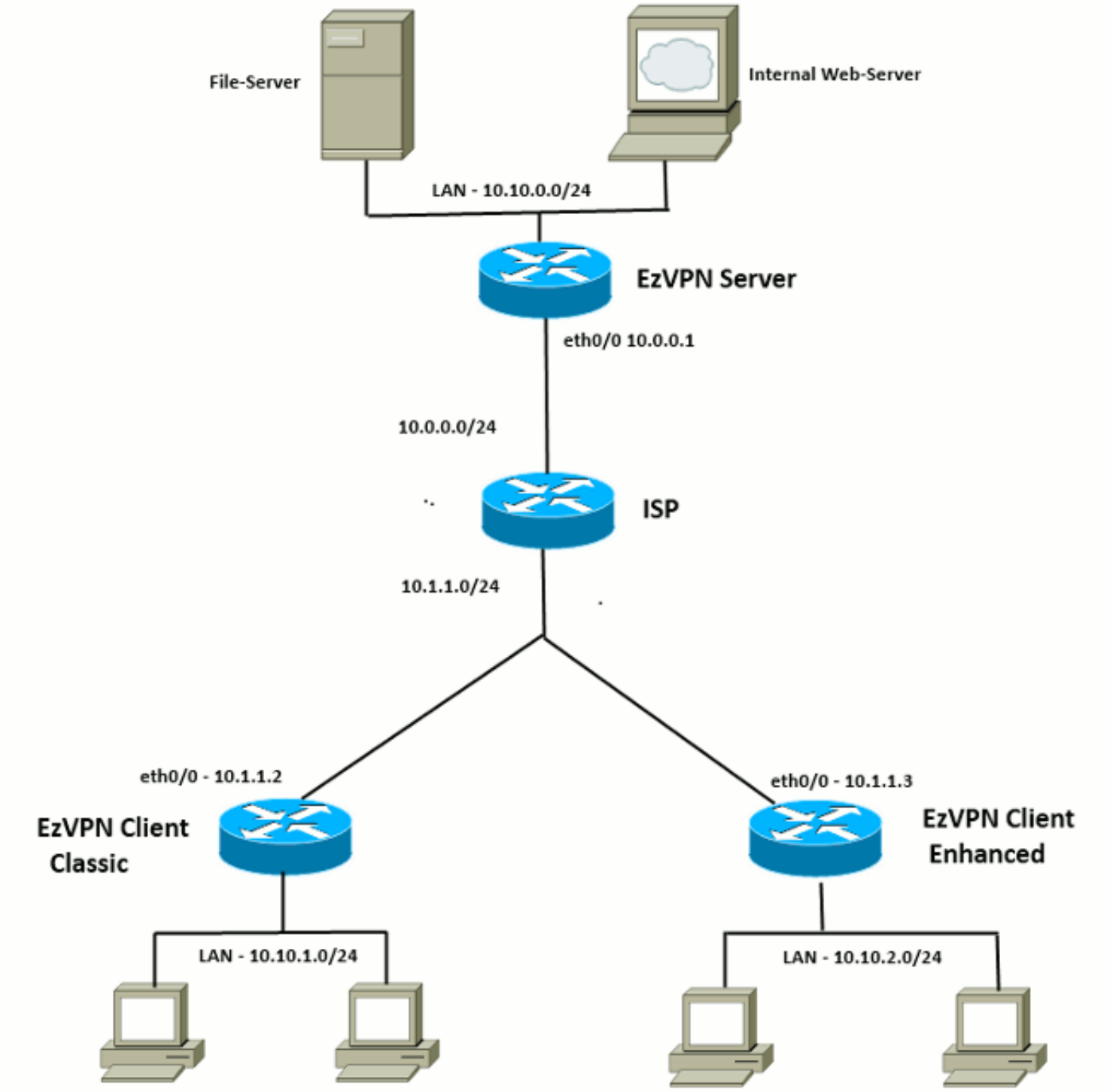
Tunnelonderhandeling



Voor meer informatie over de uitwisseling van pakketten voor een IKEv2 uitwisseling, zie IKEv2 Packet Exchange en Protocol Level Debugging.

Eerste instelling

Topologie



Eerste configuratie

EZVPN-hub - VTI-gebaseerd

```
!! 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-client - Classic (geen 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-client - uitgebreid (VTI-gebaseerd)

```
!! 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-to-FlexVPN-migratiebenadering

De server die als een EzVPN-server fungeert kan ook als een FlexVPN-server fungeren zolang de server IKEv2 Remote Access-configuratie ondersteunt. Voor een volledige IKEv2-configuratieondersteuning wordt alles boven IOS v1.2(3)T aanbevolen. In deze voorbeelden is 15.2(4)M1 gebruikt.

Er zijn twee mogelijke benaderingen:

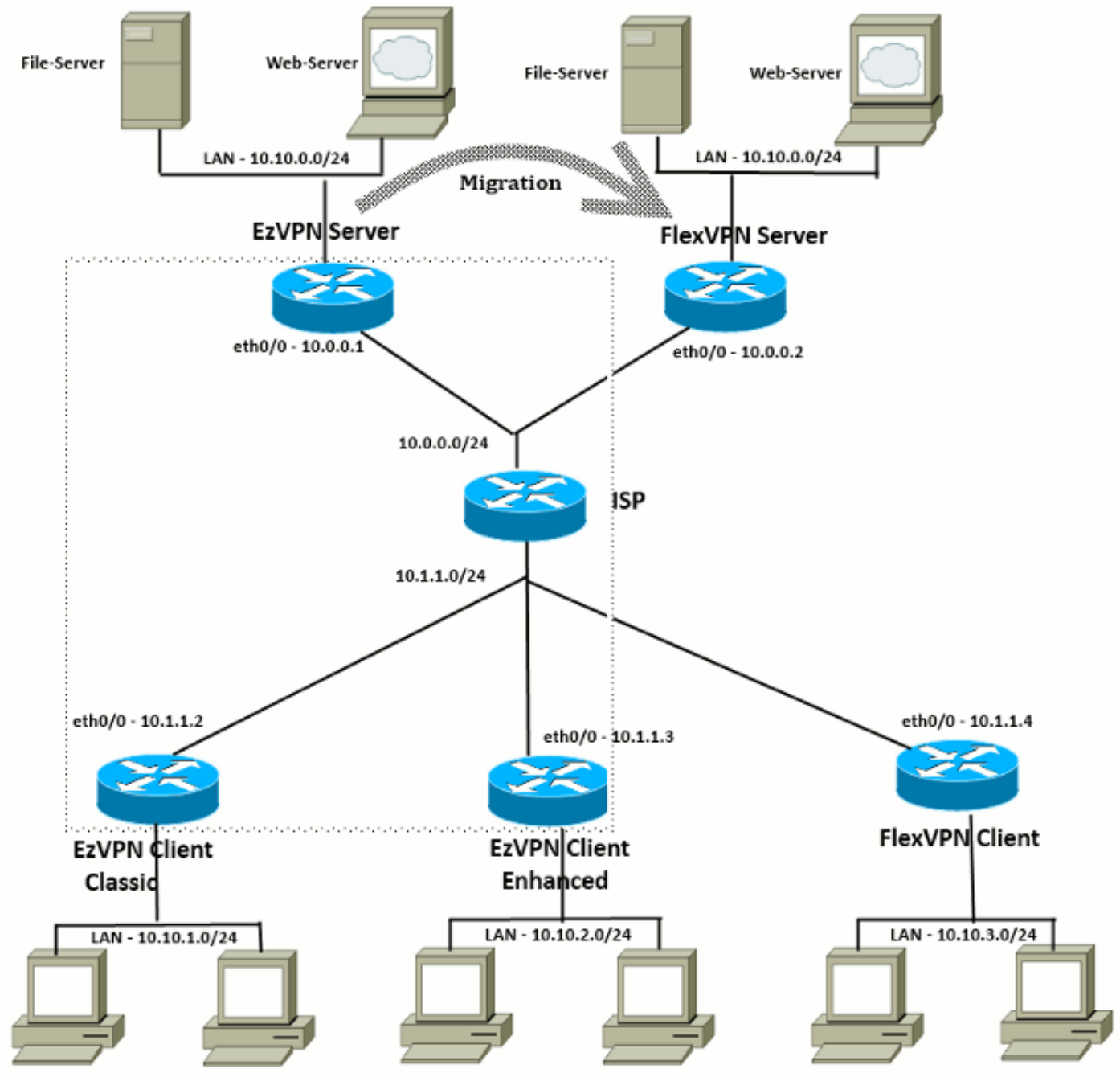
1. Setup EzVPN-server als FlexVPN-server en migreren vervolgens de EzVPN-clients naar Flex-configuratie.
2. Stel een andere router in als een FlexVPN-server. EzVPN-clients en gemigreerde FlexVPN-clients blijven via de verbinding tussen de FlexVPN-server en de EzVPN-server communiceren.

Dit document beschrijft de tweede benadering en gebruikt een nieuw gesproken (bijvoorbeeld Spoke3), als de FlexVPN-client. Dit woord kan worden gebruikt als referentie voor de migratie van andere cliënten in de toekomst.

Migratiestappen

Merk op dat wanneer u vanuit een EzVPN naar een FlexVPN-onderwerp migreert, u kunt kiezen om **FlexVPN-configuratie** te laden op het door EzVPN opgeroepen adres. Maar door de cut-over heb je mogelijk een out-of-band (niet-VPN) beheertoegang tot het vak nodig.

Gecumuleerde topologie



Configuratie

FlexVPN-hub

```
!! 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
```

Opmerking over servercertificaten

Key Gebruik (KU) definieert het doel of het beoogde gebruik van de openbare sleutel. Uitgebreid/uitgebreid Key Gebruik (EKU) verfijnt het hoofdgebruik. FlexVPN vereist dat het servercertificaat beschikt over een EKU **server-auth** (OID = 1.3.6.1.5.7.3.1) met de KU-eigenschappen van **digitale handtekening** en **Key Encipherment** om het certificaat door de client te kunnen aanvaarden.

```
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-clientconfiguratie

```
!! 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
```

Opmerking over clientcertificaten

FlexVPN vereist dat het clientcertificaat beschikt over een EKU **Client Audio** (OID = 1.3.6.1.5.7.3.2) met de KU-eigenschappen van **Digitale Handtekening** en **Key Encipherment** om het certificaat door de server te laten aanvaarden.

```
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-toepassingsverificatie

FlexVPN-server

```
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-afstandsbediening

```
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)
```

Gerelateerde informatie

- FlexVPN: IKEv2 met ingebouwde Windows-client- en certificaatverificatie-technische opmerking
- TechNotes over clientconfiguratie van FlexVPN en AnyConnect IKEv2
- FlexVPN-implementaties: AnyConnect IKEv2 externe toegang met EAP-MD5-technische opmerking

- TechNotes op pakketuitwisseling en protocolniveau
- Cisco FlexVPN
- IPsec-onderhandeling/IKE-protocollen
- Cisco AnyConnect beveiligde mobiliteit-client
- Cisco VPN-client
- Technische ondersteuning en documentatie – Cisco Systems