Migrationsleitfaden für EzVPN-NEM zu FlexVPN

Inhalt

Einführung

Dieses Dokument bietet Unterstützung bei der Migration von der EzVPN-Konfiguration (Internet Key Exchange v1 (IKEv1) zur FlexVPN-Konfiguration (IKEv2) mit möglichst wenigen Problemen. Da sich IKEv2 Remote Access in gewisser Weise von IKEv1 Remote Access unterscheidet, was die Migration etwas kompliziert macht, hilft Ihnen dieses Dokument bei der Auswahl verschiedener Design-Ansätze bei der Migration vom EzVPN-Modell zum FlexVPN Remote Access-Modell.

Dieses Dokument behandelt den IOS FlexVPN-Client oder den Hardware-Client. Der Software-Client wird in diesem Dokument nicht behandelt. Weitere Informationen zum Software-Client finden Sie unter:

- FlexVPN: IKEv2 mit integriertem Windows-Client und Zertifikatauthentifizierung
- Konfigurationsbeispiel für FlexVPN- und AnyConnect IKEv2-Client
- FlexVPN-Bereitstellung: AnyConnect IKEv2 Remote Access mit EAP-MD5

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

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

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

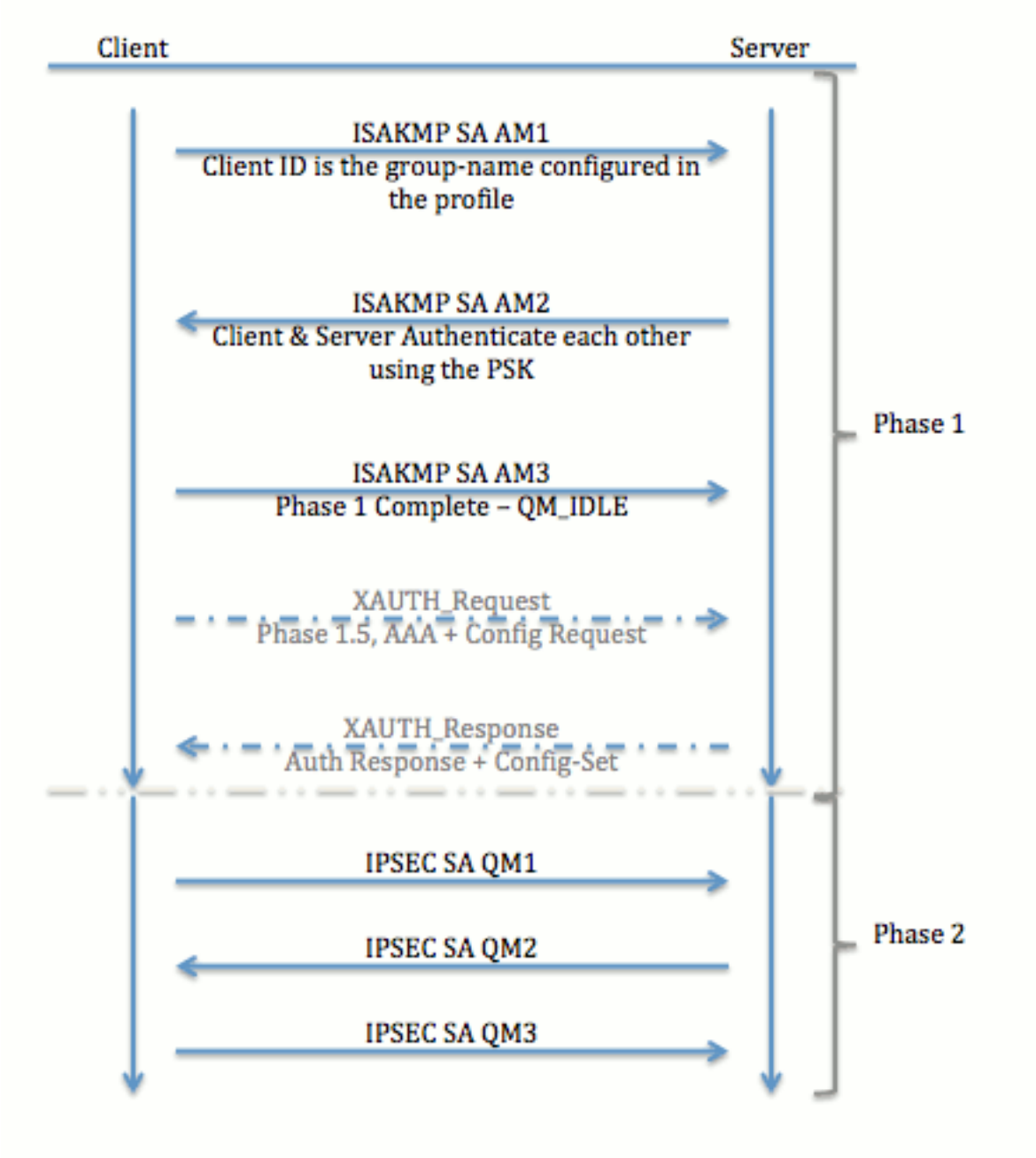
Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

EzVPN und FlexVPN

EzVPN-Modell - Was steht da?

Wie der Name schon sagt, besteht das Ziel von EzVPN darin, die VPN-Konfiguration auf den Remote-Clients zu vereinfachen. Um dies zu erreichen, wird der Client mit minimalen Details konfiguriert, die erforderlich sind, um den richtigen EzVPN-Server zu kontaktieren, der auch als Client-Profil bezeichnet wird.

Tunnelaushandlung



FlexVPN Remote Access VPN-Modell

FlexVPN-Server

Ein wichtiger Unterschied zwischen normalen FlexVPN- und FlexVPN Remote Access-Konfigurationen besteht darin, dass sich der Server nur mithilfe der vorinstallierten Schlüssel und Zertifikate (RSA-SIG) bei den FlexVPN-Clients authentifizieren muss. Mit FlexVPN können Sie unabhängig voneinander entscheiden, welche Authentifizierungsmethoden der Initiator und der Responder verwendet. Mit anderen Worten, sie können gleich sein oder anders sein. Beim FlexVPN Remote Access hat der Server jedoch keine Wahl.

Authentifizierungsmethoden des IOS FlexVPN-Clients

Der Client unterstützt die folgenden Authentifizierungsmethoden:

- **RSA-SIG** - Digitale Zertifikatauthentifizierung.

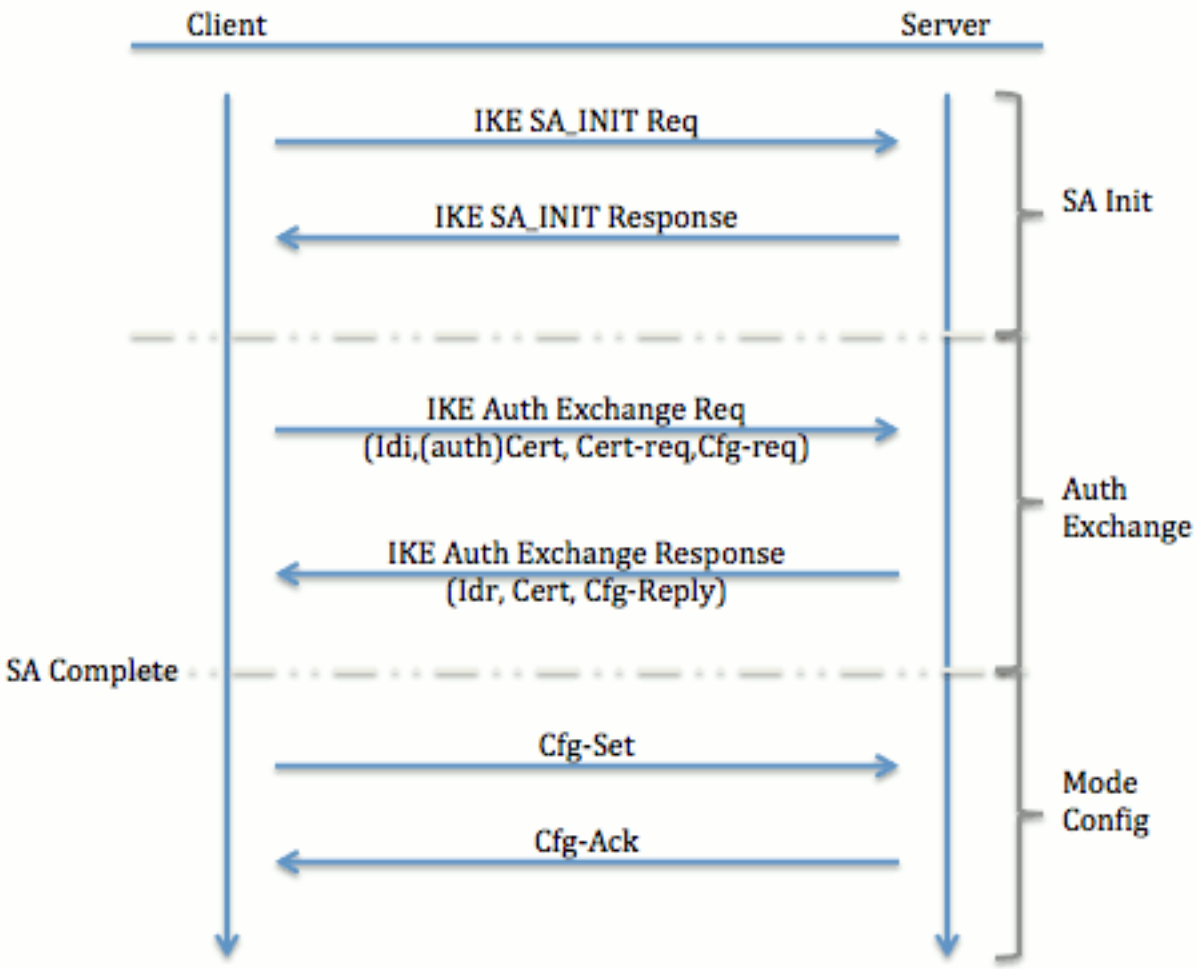
- **Pre-Share** - PSK-Authentifizierung (Pre-Shared Key).
- **Extensible Authentication Protocol (EAP)** - EAP-Authentifizierung EAP-Unterstützung für IOS FlexVPN-Client wurde in 15.2(3)T hinzugefügt.Die vom IOS FlexVPN-Client unterstützten EAP-Methoden umfassen:Extensible Authentication Protocol-Message Digest 5 (EAP-MD5),Extensible Authentication Protocol - Microsoft Challenge Handshake Authentication Protocol Version 2 (EAP-MSCHAPv2) undExtensible Authentication Protocol - Generic Token Card (EAP-GTC).

In diesem Dokument wird nur die Verwendung der RSA-SIG-Authentifizierung aus folgenden Gründen beschrieben:

- **Skalierbar** - Jeder Client erhält ein Zertifikat, und auf dem Server wird ein generischer Teil der Client-Identität damit authentifiziert.
- **Sicher** - Sicherer als ein Platzhalter-PSK (bei lokaler Autorisierung). Obwohl es bei der AAA-Autorisierung (Authentifizierung, Autorisierung und Abrechnung) einfacher ist, separate PSKs auf der Grundlage einer verwalteten IKE-Identität zu schreiben.

Die in diesem Dokument gezeigte FlexVPN-Client-Konfiguration scheint im Vergleich zum EasyVPN-Client kaum vollständig zu sein. Dies liegt daran, dass die Konfiguration einige Teile der Konfiguration umfasst, die aufgrund intelligenter Standardwerte nicht vom Benutzer konfiguriert werden müssen. Unter "Smart Default" (Intelligente Standardwerte) wird der Begriff zur Bezugnahme auf die vorkonfigurierte oder Standardkonfiguration für verschiedene Aspekte wie das Angebot, die Richtlinie, das IPSec-Transformationssatz usw. verstanden. Im Gegensatz zu IKEv1-Standardwerten sind die Smart Default-Werte für IKEv2 stark. Beispielsweise werden in den Vorschlägen Advanced Encryption Standard (AES-256), Secure Hash Algorithm (SHA-512) und Group-5 verwendet usw.

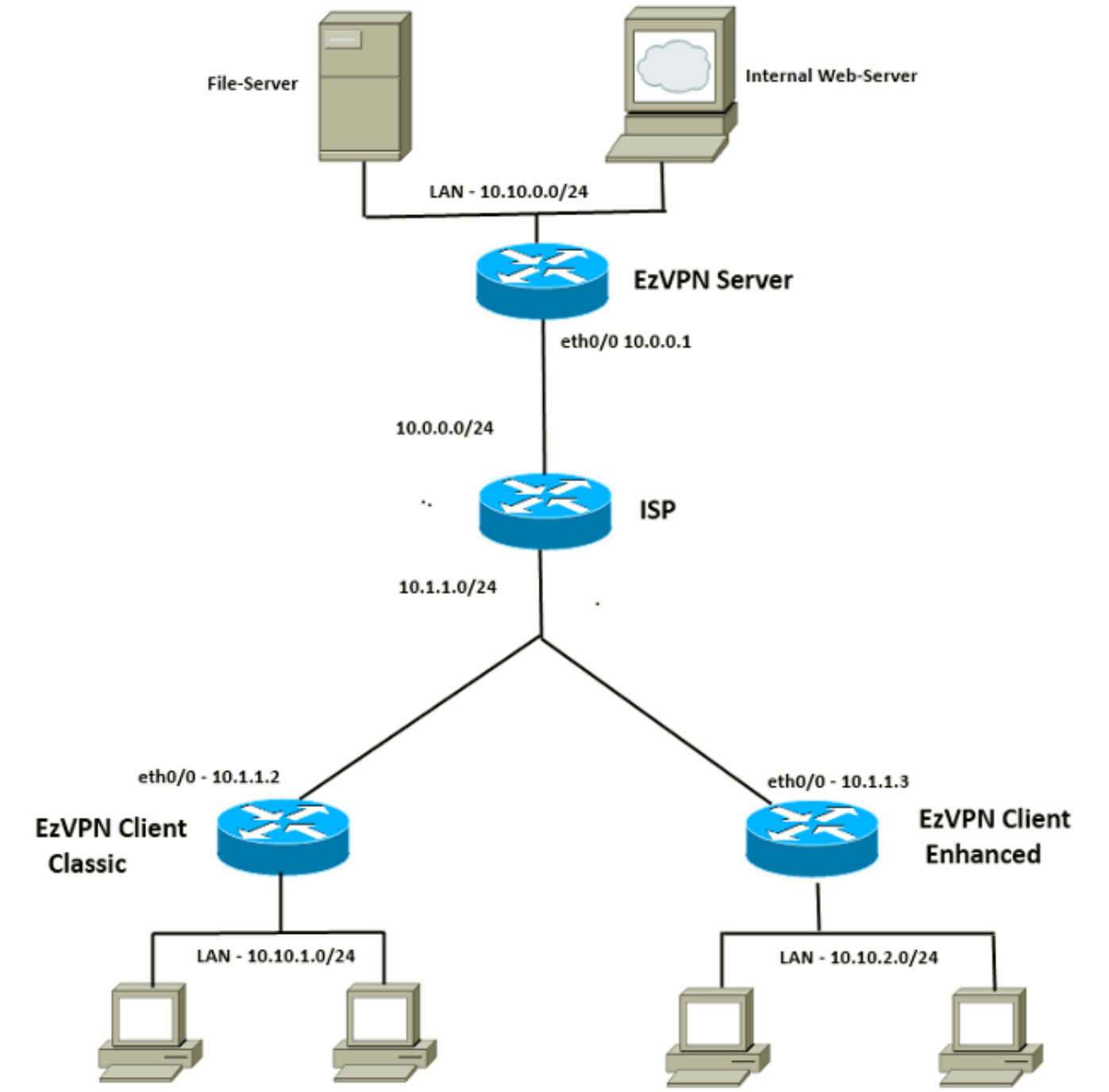
Tunnelaushandlung



Weitere Informationen zum Austausch von Paketen für einen IKEv2-Austausch finden Sie unter Debuggen auf IKEv2-Paketaustausch und Protokollebene.

Ersteinrichtung

Topologie



Erstkonfiguration

EzVPN-Hub - dVTI-basiert

```
!! 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 (ohne 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 - Erweitert (VTI-basiert)

```
!! 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
```

Migration von EzVPN zu FlexVPN

Der Server, der als EzVPN-Server fungiert, kann auch als FlexVPN-Server fungieren, sofern er die IKEv2-Remote-Zugriffskonfiguration unterstützt. Für eine vollständige Unterstützung der IKEv2-Konfiguration wird alles über IOS v15.2(3)T hinausgehende empfohlen. In diesen Beispielen wurde 15.2(4)M1 verwendet.

Es gibt zwei mögliche Ansätze:

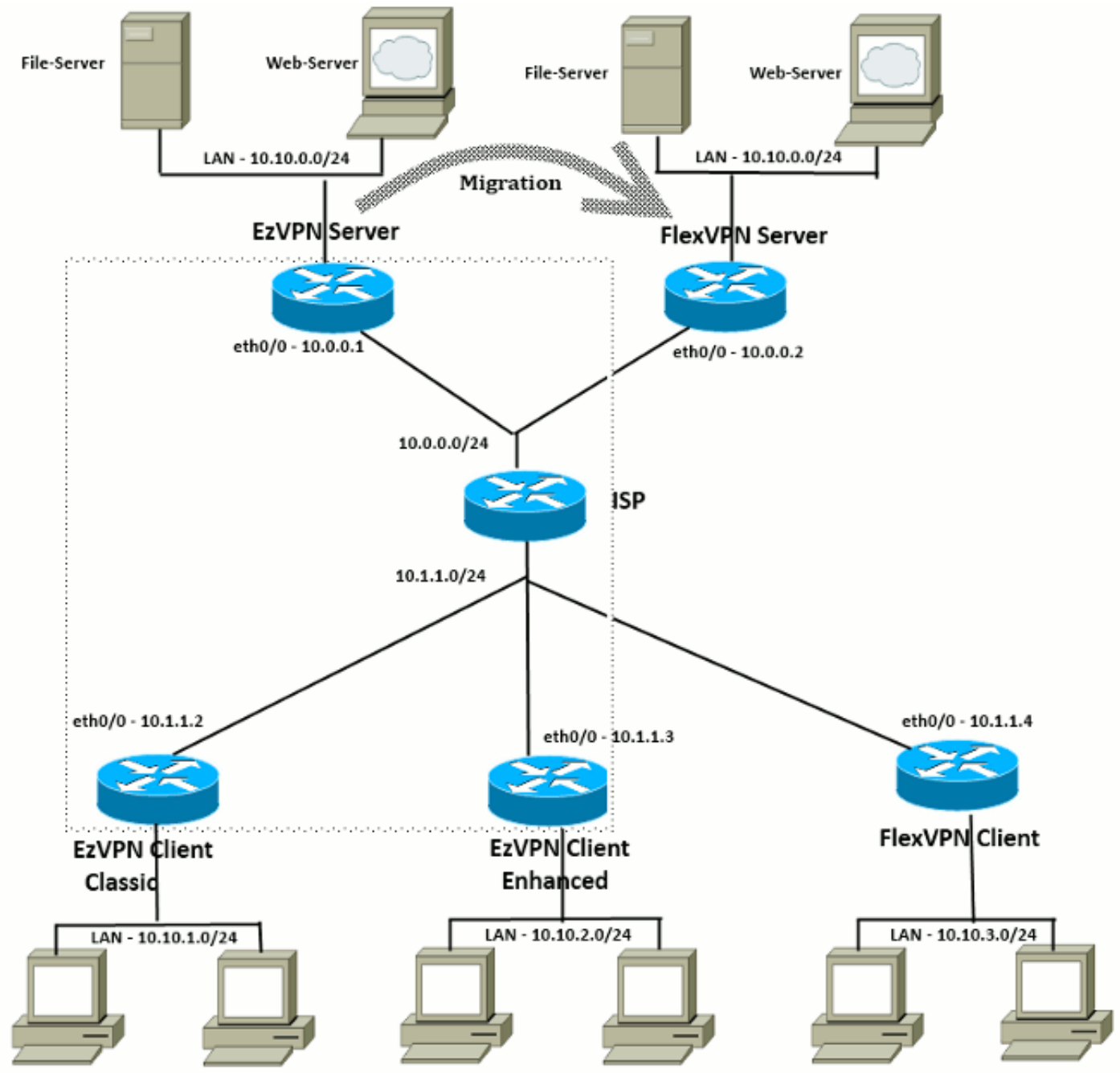
1. Einrichtung des EzVPN-Servers als FlexVPN-Server und Migration der EzVPN-Clients zur Flex-Konfiguration
2. Einrichten eines anderen Routers als FlexVPN-Server. EzVPN-Clients und migrierte FlexVPN-Clients kommunizieren weiterhin durch die Herstellung einer Verbindung zwischen dem FlexVPN-Server und dem EzVPN-Server.

Dieses Dokument beschreibt den zweiten Ansatz und verwendet einen neuen Spoke-Ansatz (z. B. Spoke3) als FlexVPN-Client. Dieser Spoke kann als Referenz für die zukünftige Migration anderer Clients verwendet werden.

Migrationsschritte

Beachten Sie, dass Sie bei der Migration von einem EzVPN-Spoke zu einem FlexVPN-Spoke die **FlexVPN-Konfiguration** in das EzVPN-Spoke laden können. Während des Umstiegs ist jedoch möglicherweise ein Out-of-Band-Verwaltungszugriff (kein VPN) erforderlich.

Migrierte Topologie



Konfiguration

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
```

Hinweis zu Serverzertifikaten

Key Usage (KU) definiert den Zweck oder die beabsichtigte Verwendung des öffentlichen Schlüssels. Enhanced/Extended Key Usage (EKU) verfeinert die Schlüsselverwendung. FlexVPN erfordert, dass das Serverzertifikat über ein EKU der **Serverauth** (OID = 1.3.6.1.5.7.3.1) mit den KU-Attributen **Digital Signature** und **Key Encipherment** verfügt, damit das Zertifikat vom Kunden akzeptiert werden kann.

```
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>
```

Konfiguration des FlexVPN-Clients

```
!! 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
```

Hinweis zu Client-Zertifikaten

FlexVPN erfordert, dass das Client-Zertifikat über ein EKU von **Client Auth** (OID = 1.3.6.1.5.7.3.2) mit den KU-Attributen **Digital Signature** und **Key Encipherment** verfügt, damit das Zertifikat vom Server akzeptiert werden kann.

```
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>
```

Überprüfung des FlexVPN-Betriebs

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 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)
```

Zugehörige Informationen

- FlexVPN: IKEv2 mit integriertem Windows-Client und ZertifikatauthentifizierungHinweis
- FlexVPN und AnyConnect IKEv2 Client - Konfigurationsbeispiel TechHinweis
- FlexVPN-Bereitstellung: AnyConnect IKEv2 Remote Access mit EAP-MD5 TechHinweis
- Technischer Hinweis zum Debuggen von IKEv2-Paketen für Exchange und Protokollebene
- Cisco FlexVPN

- IPSec-Aushandlung/IKE-Protokolle
- Cisco AnyConnect Secure Mobility Client
- Cisco VPN-Client
- Technischer Support und Dokumentation - Cisco Systems