NEM EzVPN к руководству по переходу FlexVPN

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
EzVPN по сравнению с FlexVPN
Модель EzVPN - что выделяется
Согласование туннеля
Модель VPN для удаленного доступа FlexVPN
Сервер FlexVPN
Методы аутентификации клиента IOS FlexVPN
Согласование туннеля
Первоначальная конфигурация
Топология
Начальная конфигурация
EzVPN к подходу миграции FlexVPN
Перемещенная топология
!--- конфигурацию
Проверка операции FlexVPN
Сервер FlexVPN
Удаленный FlexVPN
Дополнительные сведения

Введение

Этот документ предоставляет помощь в процессе переноса от EzVPN (v1 обмена ключами между сетями (IKEv1)) настройка к FlexVPN (IKEv2) настройка с как можно меньшим количеством проблем. Так как Удаленный доступ IKEv2 отличается от Удаленного доступа IKEv1 определенными способами, которые делают миграцию немного трудной, этот документ помогает вам выбирать другие подходы дизайна в миграции от модели EzVPN до модели Удаленного доступа FlexVPN.

Соглашения об этом документе с клиентом IOS FlexVPN или аппаратным клиентом, этот документ не обсуждает клиентское программное обеспечение. Для получения дополнительной информации о клиентском программном обеспечении см.:

- FlexVPN: IKEv2 со встроенным Windows - клиентом и проверкой подлинности

сертификата
- FlexVPN и пример Anyconnect IKEv2 конфигурации клиента
- Развертывания FlexVPN: удаленный доступ AnyConnect IKEv2 с EAP-MD5

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- IKEv2
- Cisco FlexVPN
- Защищенный мобильный клиент Cisco AnyConnect Secure Mobility
- Cisco VPN Client

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

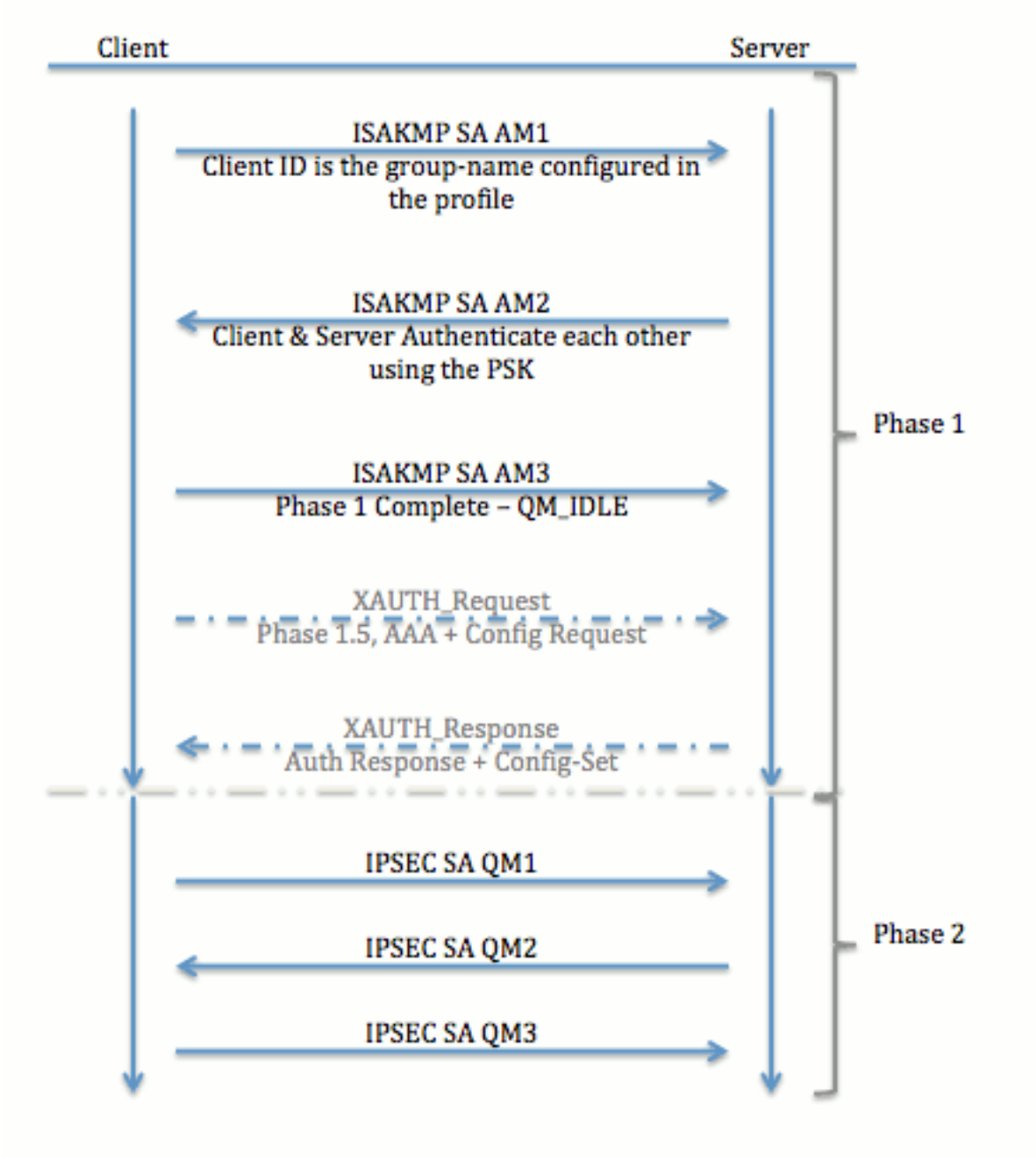
Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

EzVPN по сравнению с FlexVPN

Модель EzVPN - что выделяется

Как название предполагает, цель EzVPN состоит в том, чтобы сделать конфигурацию VPN на удаленных клиентах легкой. Для достижения этого клиент настроен с минимальными подробными данными, должен был связаться с корректным сервером EzVPN, также известным как клиентский профиль.

Согласование туннеля



Модель VPN для удаленного доступа FlexVPN

Сервер FlexVPN

Важное различие между обычным FlexVPN и настройкой Удаленного доступа FlexVPN - то, что сервер должен аутентифицировать себя на клиентах FlexVPN с помощью предварительных общих ключей и сертификатов (RSA-СИГНАЛ) метод только. FlexVPN позволяет вам решать который методы аутентификации использование инициатора и респондента, независимое друг от друга. Другими словами, они могут быть тем же, или они могут быть другими. Однако когда дело доходит до Удаленного доступа FlexVPN, сервер не имеет выбора.

Методы аутентификации клиента IOS FlexVPN

Поддержки клиентов эти методы аутентификации:

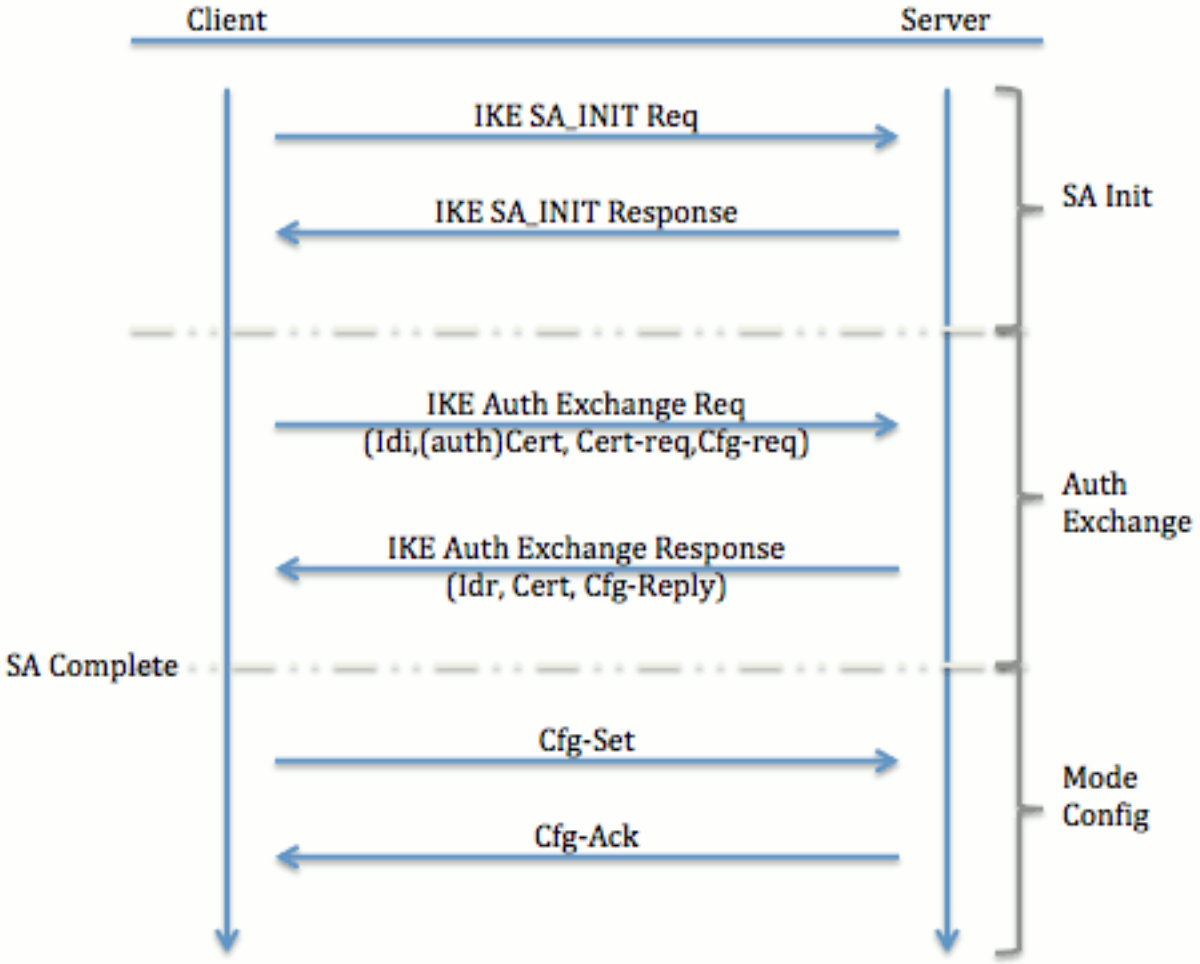
- **RSA-SIG** — Аутентификация цифрового сертификата.
- **Pre-Share** — Аутентификация предварительного общего ключа (PSK).
- **Протокол EAP** - Аутентификация eap. Поддержка EAP клиента IOS FlexVPN была добавлена в 15.2 (3) T.Поддерживаемые методы EAP клиентом IOS FlexVPN включают:Дайджест 5 (EAP-MD5) сообщения протокола расширенной проверки подлинности,Версия протокола 2 (EAP-MSCHAPv2) квитирования с аутентификацией Microsoft расширяемого протокола аутентификации, иКарта с переменым паролем общего назначения расширяемым протоколом аутентификации (EAP-GTC).

Этот документ только описывает использование аутентификации RSA-СИГНАЛА по этим причинам:

- **Масштабируемый** — Каждому клиенту дают сертификат, и на сервере, часть общего назначения клиентской идентичности аутентифицируется против него.
- **Безопасный** — более безопасный, чем PSK подстановочного знака (в случае локальной проверки подлинности). Несмотря на то, что, в случае AAA (аутентификация, авторизация и учет) авторизация, легче записать отдельные PSK на основе искаженной Идентичности IKE.

Конфигурация клиента FlexVPN, показанная в этом документе, могла бы казаться мало исчерпывающей по сравнению с клиентом EasyVPN. Это вызвано тем, что конфигурация включает некоторые части конфигурации, которые не должны быть настроены пользователем из-за умных настроек по умолчанию. Умные настройки по умолчанию являются термином, использованным для обращения к предварительно сконфигурированному или конфигурации по умолчанию для различных вещей как предложение, политика, Команда IPsec transform set, и так далее. И в отличие от значений по умолчанию IKEv1, IKEv2 умные значения по умолчанию сильны. Например, это использует Расширенный стандарт шифрования (AES 256), Защищенный алгоритм хэширования (SHA 512) и Группа 5 в предложениях, и т.д.

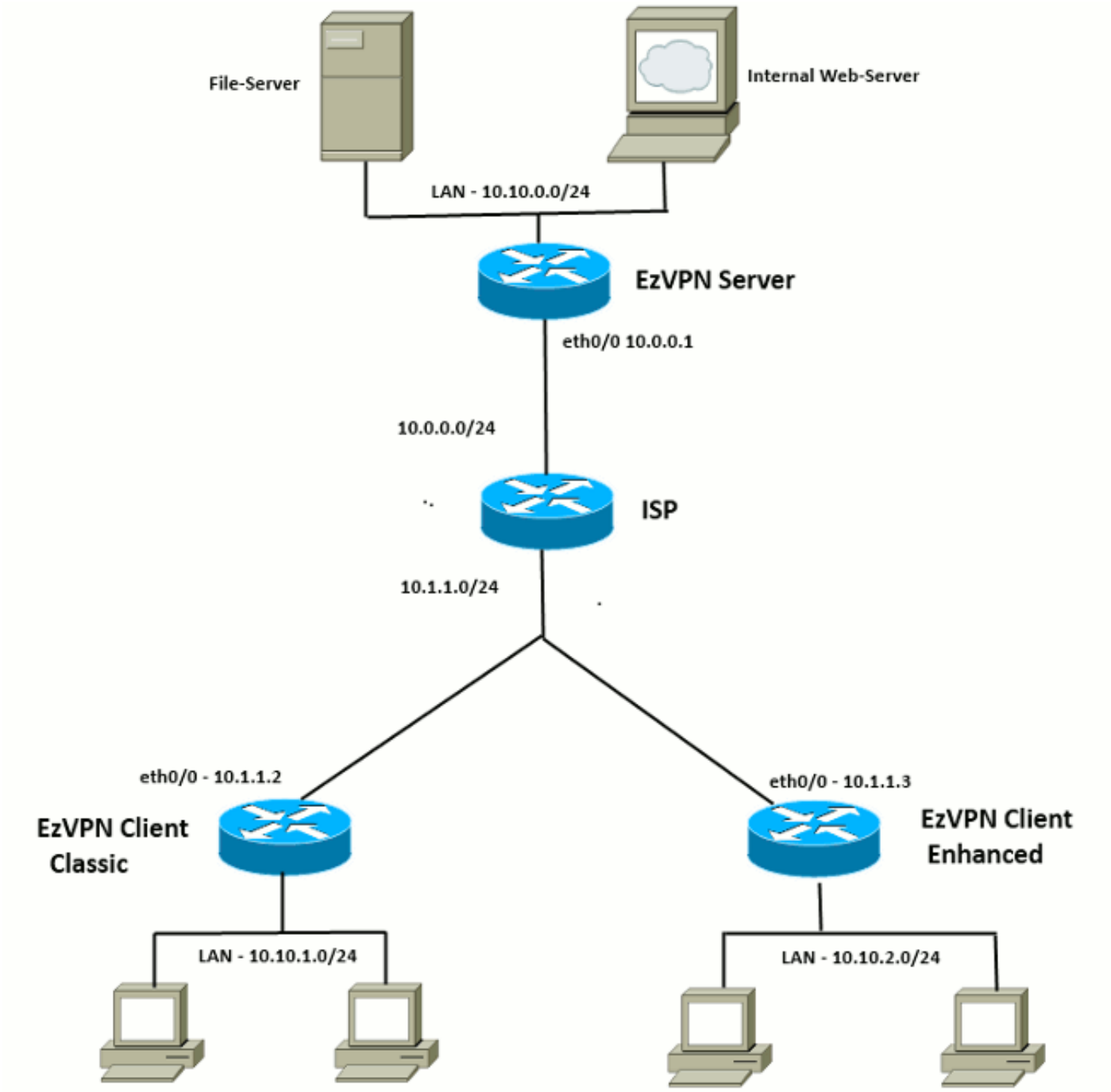
Согласование туннеля



Для получения дополнительной информации об обмене пакетами для обмена IKEv2 обратитесь к Отладке Обмена пакетами и Уровня протокола IKEv2.

Первоначальная конфигурация

Топология



Начальная конфигурация

Концентратор EzVPN - dVTI Базирующийся

```
!! 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
```

Клиент EzVPN - классика (никакой 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
```

Клиент EzVPN - расширенный (основанный на VTI)

```
!! VTI -
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4

!! ISAKMP On-Demand Keep-Alive
crypto isakmp keepalive 10 2

!! EzVPN Client - Group Name and The key (as configured on the Server),
!!   Peer address and XAUTH config go here.
!! Also this config says which Virtual Template to use.
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 local-address Ethernet0/0
 mode network-extension
 peer 10.0.0.1
 virtual-interface 1
 username cisco password cisco
 xauth userid mode local

!! EzVPn outside interface - WAN interface
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 crypto ipsec client ezvpn ez

!! EzVPN inside interface -
!! Traffic sourced from this LAN is sent over established Tunnel
interface Ethernet0/1
 ip address 10.10.2.1 255.255.255.0
 crypto ipsec client ezvpn ez inside
```

EzVPN к подходу миграции FlexVPN

Сервер, который действует как сервер EzVPN, может также действовать как сервер FlexVPN, пока он поддерживает конфигурацию Удаленного доступа IKEv2. Для полной поддержки конфигурации IKEv2 чего-либо выше IOS v15.2 (3) рекомендуется T. В этих примерах 15.2 (4) использовался M1.

Существует два возможных подхода:

1. Сервер EzVPN настройки как сервер FlexVPN, затем переместите Клиенты EzVPN на конфигурацию Flex.
2. Установите другой маршрутизатор как сервер FlexVPN. Клиенты EzVPN и перемещенные клиенты FlexVPN продолжают связываться посредством создания соединения между сервером FlexVPN и сервером EzVPN.

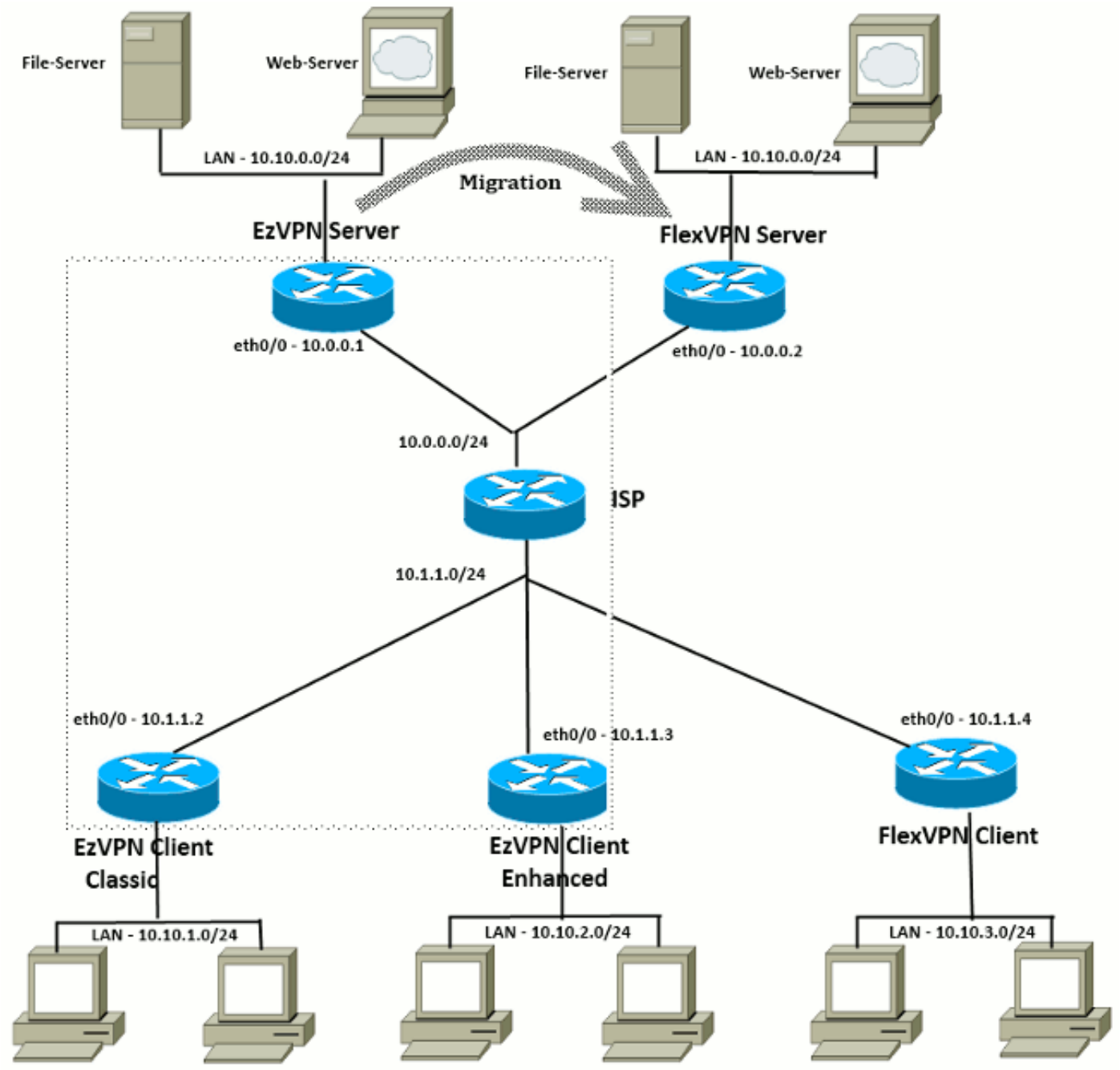
Этот документ описывает второй подход и использует новый луч (например, Spoke3), как клиент FlexVPN. Этот луч может использоваться в качестве ссылки для миграции других клиентов в будущем.

Шаги миграции

Обратите внимание на то, что то, когда вы мигрируете от EzVPN, говорило с лучом

FlexVPN, можно принять решение загрузиться, config FlexVPN на EzVPN говорил. Однако всюду по переключению, вам, возможно, понадобилось бы внеполосное (не-VPN) управляющий доступ к коробке.

Перемещенная топология



!--- конфигурацию

Концентратор 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
```

Обратите внимание о серверных сертификатах

Ключевое использование (KU) определяет цель или предполагаемое использование открытого ключа. Расширенное / Расширенное использование ключа (EKU) совершенствовало ключевое использование. FlexVPN требует, чтобы серверный сертификат имел EKU **аутентификации сервера** (OID = 1.3.6.1.5.5.7.3.1) с атрибутами KU **Цифровой подписи** и **Ключевой Шифровки** для сертификата, который будет принят клиентом.

```
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>
```

Конфигурация клиента 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
```

Обратите внимание о сертификатах клиента

FlexVPN требует, чтобы сертификат клиента имел EKU **Клиентской Аутентификации** (OID = 1.3.6.1.5.5.7.3.2) с атрибутами KU **Цифровой подписи** и **Ключевой Шифровки** для сертификата, который будет принят сервером.

```
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>
```

Проверка операции FlexVPN

Сервер 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)
```

Удаленный 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)
```

Дополнительные сведения

- FlexVPN: IKEv2 со встроенным Windows - клиентом и проверкой подлинности сертификата TechNote
- FlexVPN и пример конфигурации клиента TechNote Anyconnect IKEv2
- Развертывания FlexVPN: удаленный доступ AnyConnect IKEv2 с EAP-MD5 TechNote
- Обмен пакетами IKEv2 и отладка уровня протокола TechNote
- Cisco FlexVPN
- Согласование IPsec/Протоколы IKE
- Защищенный мобильный клиент Cisco AnyConnect Secure Mobility
- Cisco VPN Client
- Cisco Systems – техническая поддержка и документация