Миграция FlexVPN: устаревший NEM EzVPN + и FlexVPN на том же сервере

Содержание

Введение

Этот документ описывает процесс переноса от EzVPN до FlexVPN. FlexVPN является новым унифицированным решением для VPN, предлагаемым Cisco. FlexVPN использует преимущества протокола IKEv2 и комбинирует удаленный доступ, от узла к узлу, концентратор и луч и развертывания VPN частичной сетки. С устаревшими технологиями как EzVPN Cisco строго поощряет вас мигрировать на FlexVPN для использования преимуществ с расширенными возможностями возможности.

Этот документ исследует существующие развертывания EzVPN, которые состоят из устаревших аппаратных клиентов EzVPN, которые завершаются, туннели на устаревшей криптокарте базировали устройство головной станции EzVPN. Цель состоит в том, чтобы мигрировать от этой конфигурации для поддержки FlexVPN с этими требованиями:

- Существующие устаревшие клиенты продолжат работать эффективно без любых

изменений конфигурации. Это позволяет поэтапную миграцию этих клиентов к FlexVPN в течение долгого времени.
- Устройство головной станции должно одновременно поддержать завершение новых клиентов FlexVPN.

Два ключевых компонента Конфигурации IPSec используются, чтобы помочь выполнять эти цели миграции: а именно, IKEv2 и Виртуальные туннельные интерфейсы (VTI). Эти цели кратко обсуждены в этом документе.

Другие Документы в этой Серии

- Руководство по развертыванию FlexVPN: AnyConnect к головному узлу IOS по IPsec с IKEv2 и сертификатами

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

Условные обозначения

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

IKEv1 по сравнению с IKEv2

FlexVPN основывается на протоколе IKEv2, который является протоколом управления ключами следующего поколения на основе RFC 4306 и усовершенствованием протокола IKEv1. FlexVPN не обратно совместим с технологиями, которые поддерживают только IKEv1 (например, EzVPN). Когда вы мигрируете от EzVPN до FlexVPN, это - одни из ключевых факторов. Для краткого описания протоколов на IKEv2 и сравнении с IKEv1, обратитесь к версии 2 IKE с первого взгляда.

Криптокарта по сравнению с Виртуальными туннельными интерфейсами

Виртуальный туннельный интерфейс (VTI) является новым методом задания конфигурации, используемым и для сервера VPN и для конфигураций клиента. VTI:

- Замена к динамическим криптокартам, которую теперь считают унаследованной конфигурацией.
- Поддерживает собственное Туннелирование IPSec.

- Не требует статического отображения Сеанса IPSec к физическому интерфейсу; поэтому, предоставляет гибкость, чтобы передать и получить зашифрованный поток данных на любом физическом интерфейсе (например, разнообразные пути).
- Минимальная настройка как по требованию виртуальный доступ клонирована от виртуального интерфейса.
- Когда прямым к/отом туннельный интерфейс и управляет таблица IP-маршрутизации (таким образом, играя важную роль в процессе шифрования), трафик шифруется/дешифруется.
- Функции могут или быть применены к пакетам открытого текста на интерфейсе VTI или зашифрованным пакетам на физическом интерфейсе.

Два типа доступного VTIs:

- Статичный (sVTI) — статический интерфейс виртуальных туннелей имеет неподвижный источник и место назначения туннеля и, как правило, используется в сценарии развертывания от узла к узлу. Вот пример sVTI конфигурации:
```
interface Tunnel2
 ip address negotiated
 tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile testflex
```
- Динамичный (dVTI) — динамический интерфейс виртуальных туннелей может использоваться для завершения динамических Туннелей IPSec, которые не имеют неподвижного назначения туннеля. На успешное согласование туннеля Интерфейсы виртуального доступа будут клонированы от Virtual-Template и наследуют все функции L3 на том Virtual-Template. Вот пример dVTI конфигурации:
```
interface Virtual-Template1
type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

См. эти документы для получения дополнительной информации о dVTI:

- Cisco Easy VPN Настройки с динамическим интерфейсом виртуальных туннелей (DVTI) IPSec
- Ограничения для интерфейса виртуальных туннелей IPsec
- Поддержка мультиSA Настройки динамических интерфейсов виртуальных туннелей Использование IKEv1

Для EzVPN и клиентов FlexVPN для сосуществования необходимо сначала переместить сервер EzVPN от устаревшей конфигурации криптокарты до dVTI конфигурации. Следующие разделы объясняют подробно обязательные действия.

Топология сети

Текущая конфигурация с устаревшим NEM + клиент EzVPN режима

Конфигурация клиента

Ниже типичная конфигурация маршрутизатора Клиента EzVPN. В этой конфигурации Расширении сети Плюс (NEM +) используется режим, который создает множественных пар

SA для обоих внутренние интерфейсы LAN, а также назначенный IP - адрес конфигурации режима для клиента.

```
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-plus
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description EzVPN WAN interface
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description EzVPN LAN inside interface
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
```

Конфигурация сервера

На сервере EzVPN устаревшая конфигурация криптокарты используется в качестве основной конфигурации перед миграцией.

```
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network ezvpn-author local
!
username client1 password 0 client1
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address respond
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description EzVPN server WAN interface
 ip address 192.168.1.10 255.255.255.0
 crypto map client-map
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
```

```
!
ip access-list extended split-tunnel-acl
  remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
```

Миграция сервера к FlexVPN

Как описано в предыдущих разделах, FlexVPN использует IKEv2 в качестве протокола уровня управления и не обратно совместим с находящимся в IKEv1 решением для EzVPN. В результате общее представление этой миграции должно настроить существующий сервер EzVPN таким способом, которым это позволяет и устаревшему EzVPN (IKEv1) и FlexVPN (IKEv2) сосуществовать. Для достижения этой цели можно использовать этот двухступенчатый подход миграции:

1. Переместитесь устаревшая конфигурация EzVPN на головном узле от криптокарты базировала конфигурацию к dVTI.
2. Добавьте конфигурацию FlexVPN, которая является также на основе dVTI.

Переместите Устаревшую криптокарту в dVTI

Изменения конфигурации сервера

Сервер EzVPN, настроенный с криптокартой на физическом интерфейсе, включает несколько ограничений когда дело доходит до поддержки характеристик и гибкости. Если у вас есть EzVPN, Cisco строго поощряет вас использовать dVTI вместо этого. Как первый шаг для миграции на сосуществующий EzVPN и конфигурацию FlexVPN необходимо изменить его на dVTI конфигурацию. Это предоставит IKEv1 и разделение IKEv2 между другими виртуальными интерфейсами для размещения обоих типов клиентов.

Примечание: Для поддержки Расширения сети Плюс Режим операции EzVPN на Клиентах EzVPN маршрутизатор головной станции должен иметь поддержку много SA на dVTI функции. Это позволяет потокам множественного IP быть защищенными туннелем, который требуется для головного узла зашифровать трафик к внутренней сети Клиента EzVPN, а также IP-адрес, назначенный на клиента через настройку режима IKEv1. Для получения дополнительной информации о много поддержке SA на dVTI с IKEv1, обратитесь к Поддержке мультиSA Динамических интерфейсов виртуальных туннелей для IKEv1.

Выполните эти шаги для реализации изменения конфигурации на сервере:

Шаг 1 — Удаляет криптокарту из физического исходящего интерфейса, который завершает туннели Клиента EzVPN:

```
interface Ethernet0/0
 ip address 192.168.1.10 255.255.255.0
 no crypto map client-map
```

Шаг 2 — Создает виртуальный интерфейс, от которого будут клонированы интерфейсы виртуального доступа, как только установлены туннели:

```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
```

Шаг 3 — Партнер этот недавно созданный интерфейс виртуального шаблона к isakmp представляет для настроенной группы EzVPN:

```
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address initiate
   client configuration address respond
   virtual-template 1
```

Как только вышеупомянутые изменения конфигурации сделаны, проверяют, что существующие Клиенты EzVPN продолжают работать. Однако теперь их туннели завершены на динамично созданном интерфейсе виртуального доступа. Это может быть проверено с **командой show crypto session** как в данном примере:

```
PE-EzVPN-Server#show crypto session Crypto session current status Interface: Virtual-Access1
Username: client1 Profile: Group-One-Profile Group: Group-One Assigned address: 10.1.1.101
Session status: UP-ACTIVE Peer: 192.168.2.101 port 500 IKEv1 SA: local 192.168.1.10/500 remote
192.168.2.101/500 Active IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 host 10.1.1.101 Active
SAs: 2, origin: crypto map IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0
172.16.1.0/255.255.255.0 Active SAs: 2, origin: crypto map
```

Добавьте конфигурацию FlexVPN к серверу

Данный пример использует RSA-СИГНАЛ (т.е. Центр сертификации) на обоих клиент и сервер FlexVPN. Конфигурация в этом разделе предполагает, что сервер уже успешно аутентифицировался и зарегистрировался с сервером CA.

Шаг 1 — проверяет умную конфигурацию по умолчанию IKEv2.

С IKEv2 можно теперь использовать преимущества Умной Функции по умолчанию, представленной в 15.2 (1) T. Это используется для упрощения конфигурации FlexVPN. Вот некоторые конфигурации по умолчанию:

Политика авторизации IKEv2 по умолчанию:

```
VPN-Server#show crypto ikev2 authorization policy default IKEv2 Authorization Policy : default
route set interface route accept any tag : 1 distance : 1
```

Предложение IKEv2 по умолчанию:

```
VPN-Server#show crypto ikev2 proposal default IKEv2 proposal: default Encryption : AES-CBC-256
AES-CBC-192 AES-CBC-128 Integrity : SHA512 SHA384 SHA256 SHA96 MD596 PRF : SHA512 SHA384 SHA256
SHA1 MD5 DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

Политика IKEv2 по умолчанию:

```
VPN-Server#show crypto ikev2 policy default IKEv2 policy : default Match fvrf : any Match
address local : any Proposal : default
```

Профиль IPSec по умолчанию:

```
VPN-Server#show crypto ipsec profile default IPSEC profile default Security association
lifetime: 4608000 kilobytes/3600 seconds Responder-Only (Y/N): N PFS (Y/N): N Transform sets={
default: { esp-aes esp-sha-hmac } , }
```

Набор преобразований IPSec по умолчанию:

```
VPN-Server#show crypto ipsec transform default { esp-aes esp-sha-hmac } will negotiate = {
Transport, },
```

Для получения дополнительной информации об Умной Функции по умолчанию IKEv2 обратитесь к Умным Настройкам по умолчанию IKEv2 (только зарегистрированные клиенты).

Шаг 2 — Модифицирует политику авторизации IKEv2 по умолчанию и добавляет профиль IKEv2 по умолчанию для клиентов FlexVPN.

Профиль IKEv2, созданный здесь, будет совпадать на идентификаторе равноправного узла на основе cisco.com доменного имени, и интерфейсы виртуального доступа, созданные для клиентов, будут порождены прочь виртуального шаблона 2. Также обратите внимание, что политика авторизации определяет пул IP-адреса, используемый для присвоения IP - адресов адресуемых точки, а также маршрутов, которыми обменяются через режим конфигурации IKEv2:

```
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
```

Шаг 3 — Создает интерфейс виртуального шаблона, используемый для клиентов FlexVPN:

```
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
```

Конфигурация клиента FlexVPN

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
```

Законченная конфигурация

Завершите гибридную конфигурацию сервера

```
hostname VPN-Server
```

```
!
!
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network default local
aaa authorization network ezvpn-author local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=vpn-server.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 07
 certificate ca 01
username client1 password 0 client1
username cisco password 0 cisco
!
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
 save-password
crypto isakmp profile Group-One-Profile
 match identity group Group-One
 client authentication list client-xauth
 isakmp authorization list ezvpn-author
 client configuration address initiate
 client configuration address respond
 virtual-template 1
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
```

```
!
crypto ipsec profile default
 set ikev2-profile default
!
crypto ipsec profile legacy-profile
 set transform-set aes-sha
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description WAN
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.0.1 255.255.255.0
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
ip local pool flexvpn-pool 10.1.1.201 10.1.1.250
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip access-list extended split-tunnel-acl
 remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
!
access-list 1 permit 172.16.0.0 0.0.0.255
```

Завершите конфигурацию клиента EzVPN IKEv1

```
hostname Client1
!
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-extension
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description LAN
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
!
```

```
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

Завершенная конфигурация клиента IKEv2 FlexVPN

```
hostname Client2
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 redundancy
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=Client2.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 06
 certificate ca 01
!
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.102 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
!
```

```
access-list 1 permit 172.16.2.0 0.0.0.255
```

Проверка конфигурации

Вот некоторые команды, используемые для проверки операций EzVPN/FlexVPN на маршрутизаторе:

```
show crypto session

show crypto session detail

show crypto isakmp sa

show crypto ikev2 sa

show crypto ipsec sa detail

show crypto ipsec client ez (for legacy clients)

show crypto socket

show crypto map
```

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация