Динамическая конфигурация FlexVPN с локальными списками атрибутов AAA

Содержание

Введение

Этот пример конфигурации демонстрирует, как использовать локальную проверку подлинности, Авторизацию, и Бухгалтерский (AAA) список атрибутов для выполнения динамичный и потенциально усовершенствованная конфигурация без использования внешнего сервера Сервиса RADIUS.

Когда быстрое развертывание или тест требуются, это желаемо в определенных сценариях, особенно. Такие развертывания являются, как правило, тестовыми лабораторными работами, новым тестированием развертываний или устранением проблем.

Динамическая конфигурация важна на концентраторе/стороне концентратора, где другая политика или атрибуты должны быть применены на для каждого пользователя, на клиента, для каждого сеанса основание.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются, но не ограниченные, эти версии программного и аппаратного обеспечения. Этот список не выделяет минимальные требования, но отражает состояние устройства всюду по этапу тестирования этой функции.

Аппаратные средства

- Маршрутизаторы агрегации (ASR) - ASR 1001 - названный "bsns-asr1001-4"
- Поколение 2 Маршрутизаторов ISR (ISR G2) - 3925e - названный "bsns-3925e-1"
- Поколение 2 Маршрутизаторов ISR (ISR G2) - 3945e - названный "bsns-3945e-1"

Программное обеспечение

- Выпуск 3.8 - 15.3 (1) S Cisco IOS XE
- Выпуск 15.2 (4) M1 и 15.2 (4) M2 программного обеспечения Cisco IOS

Лицензии

- Маршрутизаторы ASR имеют **adventerprise**, и характеристики лицензирования **ipsec** включили.
- Маршрутизаторы ISR G2 имеют **ipbasek9**, **securityk9**, и **hseck9** характеристики лицензирования включили.

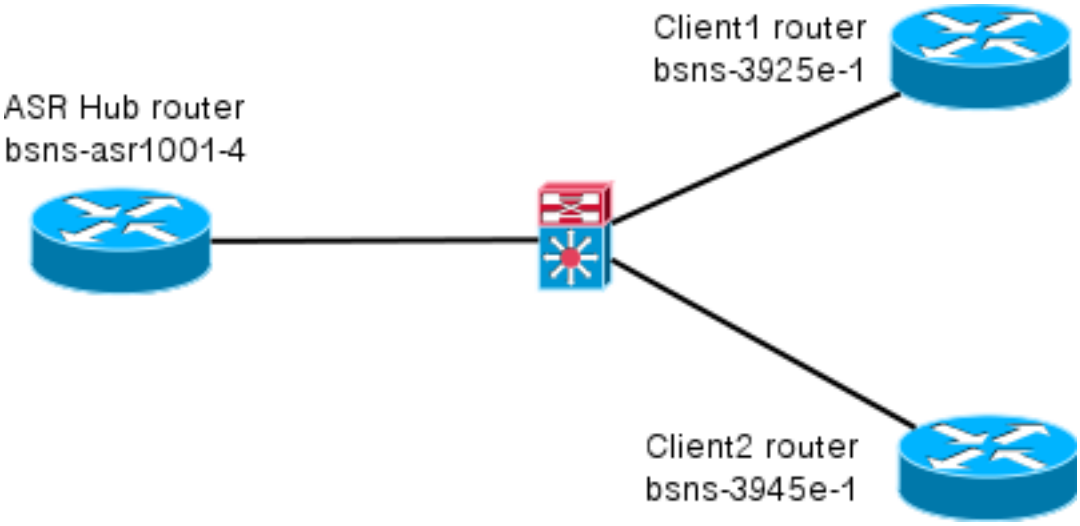
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

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

Топология

Топология, используемая в этом осуществлении, является основной. Маршрутизатор концентратора (ASR) и два маршрутизатора на конце луча (ISR) используется, которые моделируют клиентов.



Конфигурации

Конфигурации в этом документе предназначены для показа базовой настройки с умными настройками по умолчанию как можно больше. Для Рекомендаций Cisco на криптографии посетите страницу Encryption Следующего поколения на cisco.com.

Конфигурация оконечного устройства

Как упомянуто ранее, большинство действий в этой документации выполнено на концентраторе. Конфигурация оконечного устройства здесь для ссылки. В этой конфигурации заметьте, что только изменение является идентичностью между Client1 и Client2 (отображенный полужирным).

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
 !!
crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 identity local email Client1@cisco.com authentication remote pre-share authentication local
pre-share keyring local Flex_key aaa authorization group psk list default default virtual-
template 1 crypto logging session crypto ipsec profile default set ikev2-profile Flex_IKEv2
interface Tunnel1 ip address negotiated ip mtu 1400 ip nhrp network-id 2 ip nhrp shortcut
virtual-template 1 ip nhrp redirect ip tcp adjust-mss 1360 tunnel source GigabitEthernet0/0
tunnel destination 172.25.1.1 tunnel path-mtu-discovery tunnel protection ipsec profile default
interface Virtual-Template1 type tunnel ip unnumbered Tunnel1 ip mtu 1400 ip nhrp network-id 2
ip nhrp shortcut virtual-template 1 ip nhrp redirect ip tcp adjust-mss 1360 tunnel path-mtu-
discovery tunnel protection ipsec profile default
```

Конфигурация концентратора

Конфигурация концентратора разделена на две части:

1. **Конфигурация основного подключения**, которая выделяет конфигурацию, необходимую для основного подключения.

2. **Расширенная конфигурация**, которая выделяет изменения конфигурации, необходимые, чтобы продемонстрировать, как администратор может использовать AAA attribute list для выполнения для каждого пользователя или для каждого сеанса изменения конфигурации.

Базовая конфигурация связности

Эта конфигурация для ссылки только и не предназначена, чтобы быть оптимальной, только функциональной.

Самое большое ограничение этой конфигурации является использованием предварительного общего ключа (PSK) как метод аутентификации. Cisco рекомендует использование сертификатов каждый раз, когда применимо.

```
aaa new-model
aaa authorization network default local

aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
 route set interface

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
 !!
 peer Client1
 identity email Client1@cisco.com
 pre-shared-key cisco
 !!
 peer Client2
 identity email Client2@cisco.com
 pre-shared-key cisco

crypto ikev2 profile Flex_IKEv2
 match fvrf any
 match identity remote address 0.0.0.0
 match identity remote email domain cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

no crypto ikev2 http-url cert

crypto logging session

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Virtual-Template1 type tunnel
 vrf forwarding IVRF
 ip unnumbered Loopback100
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp redirect
 ip tcp adjust-mss 1360
```

```
 tunnel path-mtu-discovery
 tunnel vrf INTERNET
 tunnel protection ipsec profile default
```

Расширенная конфигурация

Существует несколько вещей, должен был назначить атрибуты AAA на отдельный сеанс. Данный пример показывает завершенную работу для client1; тогда это показывает, как добавить другого клиента/пользователя.

Расширенная конфигурация концентратора для Client1

1. Определите AAA attribute list.`aaa attribute list Client1`
   ```
    attribute type interface-config "ip mtu 1300" protocol ip
    attribute type interface-config "service-policy output TEST" protocol ip
   ```
   Примечание: Помните, что объект, назначенный через атрибуты, должен существовать локально. В этом случае **policy-map** был ранее настроен.`policy-map TEST`
   ```
    class class-default
    shape average 60000
   ```
2. Назначьте AAA attribute list на **политику авторизации.**`crypto ikev2 authorization policy` **`Client1`** `pool FlexSpokes aaa attribute list Client1 route set interface`
3. Гарантируйте что эта новая политика, используемая клиентами то подключение. В этом случае извлеките часть **имени пользователя** идентичности, передаваемой клиентами. Клиенты должны использовать адрес электронной почты ClientX@cisco.com (X, 1 или 2, зависящий от клиента). **mangler** разделяет адрес электронной почты на имя пользователя и доменную часть и использует только одного из них (имя пользователя в этом случае) для выбора названия политики авторизации.`crypto ikev2 name-mangler GET_NAME`
   ```
    email username

   crypto ikev2 profile Flex_IKEv2
    aaa authorization group psk list default name-mangler GET_NAME
   ```
   Когда client1 в рабочем состоянии, client2 может быть добавлен относительно легкий.

Расширенная конфигурация концентратора для Client2

Гарантируйте, что существуют политика и отдельный набор атрибутов, в случае необходимости.

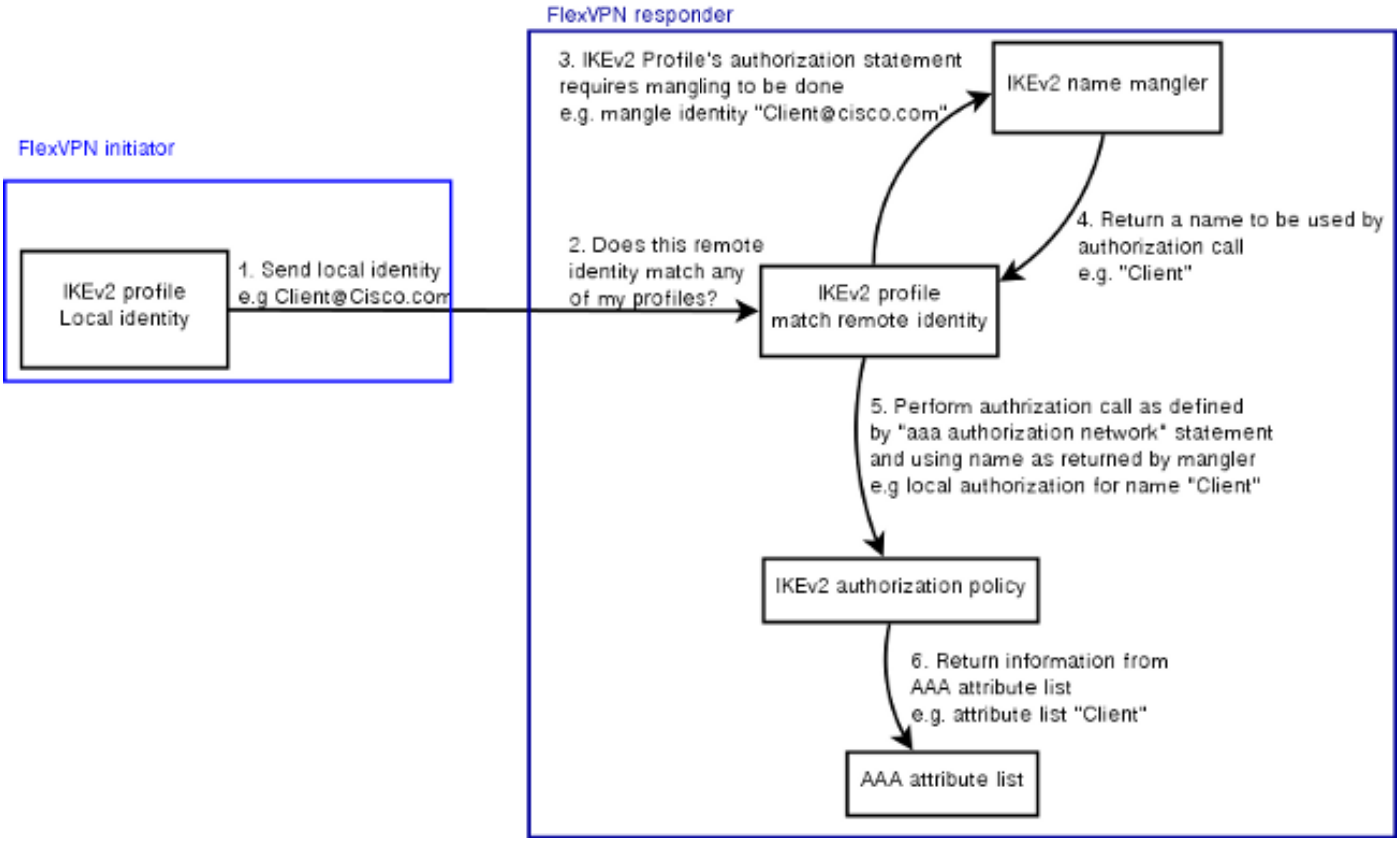
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

crypto ikev2 authorization policy Client2
 pool FlexSpokes
 aaa attribute list Client2
 route set interface
```

В данном примере, обновленном значении Maximum Segment Size (MSS) и списке доступа на вход для работы для этого клиента применен. Другие параметры настройки могут быть легко выбраны. Типичный параметр должен назначить другую виртуальную маршрутизацию и передачу (VRF) для других клиентов. Как отмечалось ранее, любой объект, назначенный на список атрибутов, такой как access-list 133 в этом сценарии, должен уже существовать в конфигурации.

Обзор процесса

Когда авторизация AAA обработана через профиль второй версии протокола Internet Key Exchange (IKEv2) и содержит информацию, определенную для этого примера конфигурации, этот рисунок выделяет заказ операции.



Проверка

Этот раздел показывает, как проверить, что параметры настройки, ранее назначенные, были применены к клиентам.

Клиент 1

Вот команды, которые проверяют, что были применены параметры настройки максимальных размеров передаваемого блока данных (MTU), а также политика обслуживания.

```
bsns-asr1001-4#show cef int virtual-access 1 (...) Hardware idb is Virtual-Access1 Fast
switching type 14, interface type 21 IP CEF switching enabled IP CEF switching turbo vector IP
Null turbo vector VPN Forwarding table "IVRF" IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
Tunnel VPN Forwarding table "INTERNET" (tableid 2) Input fast flags 0x0, Output fast flags
0x4000 ifindex 16(16) Slot unknown (4294967295) Slot unit 1 VC -1 IP MTU 1300 Real output
interface is GigabitEthernet0/0/0 bsns-asr1001-4#show policy-map interface virtual-access1
Virtual-Access1 Service-policy output: TEST Class-map: class-default (match-any) 5 packets, 620
bytes 5 minute offered rate 0000 bps, drop rate 0000 bps Match: any Queueing queue limit 64
packets (queue depth/total drops/no-buffer drops) 0/0/0 (pkts output/bytes output) 5/910 shape
(average) cir 60000, bc 240, be 240 target shape rate 60000
```

Клиент 2

Вот команды, которые проверяют, что параметры настройки MSS были выдвинуты и что access-list 133 был также применен как входящий фильтр на эквивалентном интерфейсе виртуального доступа.

```
bsns-asr1001-4#show cef int virtual-access 2 Virtual-Access2 is up (if_number 18) Corresponding hwidb fast_if_number 18 Corresponding hwidb firstsw->if_number 18 Internet address is 0.0.0.0/0 Unnumbered interface. Using address of Loopback100 (192.168.1.1) ICMP redirects are never sent Per packet load-sharing is disabled IP unicast RPF check is disabled Input features: Access List, TCP Adjust MSS (...) bsns-asr1001-4#show ip interface virtual-access2 Virtual-Access2 is up, line protocol is up Interface is unnumbered. Using address of Loopback100 (192.168.1.1) Broadcast address is 255.255.255.255 MTU is 1400 bytes Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is 133, default is not set (...)
```

.debug

Существует два главных блока для отладки. Когда необходимо открыть кэйс TAC (Центра технической поддержки) и получить вещи, на ходу более быстрые, это полезно.

Отладка IKEv2

Начните с этой главной команды отладки:

```
debug crypto ikev2 [internal|packet]
```

Затем введите эти команды:

```
show crypto ikev2 sa show crypto ipsec sa peer a.b.c.d
```

Присвоение атрибута Debug AAA

Если вы хотели бы к присвоению debug AAA атрибутов, эти отладки могут быть полезными.

```
debug aaa authorization
debug aaa attr
debug aaa proto local
```

Заключение

Этот документ демонстрирует, как использовать AAA attribute list для разрешения добавленной гибкости в развертываниях FlexVPN, где сервер RADIUS не мог бы быть доступен или не желаем. AAA attribute list предлагает включенные параметры конфигурации для каждого сеанса, каждая группа по отдельности, если это требуется.

Дополнительные сведения

- FlexVPN и руководство по конфигурации версии 2 обмена ключами между сетями, Cisco IOS Release 15M&T
- Сервисы RADIUS
- Запросы комментариев (RFC)
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация