FlexVPN и пример Anyconnect IKEv2 конфигурации клиента

Содержание

Введение

Этот документ описывает, как настроить защищенный мобильный клиент Cisco AnyConnect Secure Mobility для использования Сервиса RADIUS и атрибутов локальной проверки подлинности для аутентификации против Microsoft Active Directory.

> **Примечание:** В настоящее время использование базы локальных пользователей для аутентификации не функционирует на устройствах Cisco IOS®. Это вызвано тем, что Cisco IOS не функционирует как средство проверки подлинности EAP. Запрос на расширение CSCui07025 был подан для добавления поддержки.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия Cisco IOS 15.2 (T) или позже
- Версия 3.0 Защищенного мобильного клиента Cisco AnyConnect Secure Mobility или позже
- Microsoft Active Directory

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В этом разделе приводятся сведения о настройке функций, описанных в данном документе.

Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация концентратора
- Конфигурация сервера Microsoft Active Directory
- Конфигурация клиента

Конфигурация концентратора

1. Настройте RADIUS для аутентификации только и определите локальную проверку подлинности.

```
aaa new-model
aaa group server radius FlexVPN-AuthC-Server-Group-1
server-private 10.7.7.129 key Cisco123
```

```
aaa authentication login FlexVPN-AuthC-List-1 group
FlexVPN-AuthC-Server-Group-1
aaa authorization network FlexVPN-AuthZ-List-1 local
```

Команда **списка aaa authentication login** обращается к группе аутентификации, авторизации и учета (AAA) (который определяет сервер RADIUS). Состояния команды **списка сети с проверкой подлинности AAA**, что должны использоваться локально определенные пользователи/группы. Конфигурация на сервере RADIUS должна быть изменена для разрешения запросов аутентификации от этого устройства.

2. Настройте политику локальной проверки подлинности.

```
ip local pool FlexVPN-Pool-1 10.8.8.100 10.8.8.200
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
pool FlexVPN-Pool-1
dns 10.7.7.129
netmask 255.255.255.0
def-domain example.com
```

Команда ip local pool используется для определения IP-адресов, которые назначены на клиента. Политика авторизации определена с именем пользователя *FlexVPN-Local-Policy-1* и приписывает для клиента (Серверы DNS, маска подсети, раздельный список, доменное имя, и т.д) настроены здесь.

3. Гарантируйте, что сервер использует сертификат (rsa-сигнал) для аутентификации себя.

Защищенный мобильный клиент Cisco AnyConnect Secure Mobility требует, чтобы сервер аутентифицировал себя с помощью сертификата (rsa-сигнал). Маршрутизатор должен иметь сертификат *Web-сервера* (т.е. сертификат с 'проверкой подлинности сервера' в расширенном ключевом расширении использования) от доверенного центра сертификации (CA).

См. шаги 1 - 4 в ASA 8.x Вручную Сертификаты Поставщика третьей стороны Установки для использования с Примером конфигурации WebVPN и изменение все экземпляры *крипто-CA* к *крипто-pki*.

```
crypto pki trustpoint FlexVPN-TP-1
enrollment url
serial-number none
fqdn flex-hub.example.com
ip-address none
subject-name cn=flex-hub.example.com
revocation-check crl
rsakeypair FlexVPN-TP-1-Key 2048
```

4. Настройте параметры настройки для этого соединения.

```
crypto ikev2 profile FlexVPN-IKEv2-Profile-1
match identity remote key-id example.com
identity local dn
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint FlexVPN-TP-1
dpd 60 2 on-demand
aaa authentication eap FlexVPN-AuthC-List-1
aaa authorization group eap list FlexVPN-AuthZ-List-1
```

```
FlexVPN-Local-Policy-1
virtual-template 10
```

Крипто-ikev2 profilec ontains большинство соответствующих параметров настройки для этого соединения: **match identity удаленный ключевой идентификатор** - Обращается к идентичности IKE, используемой клиентом. Это строковое значение настроено в профиле XML AnyConnect.**идентичность локальный dn** - Определяет идентичность IKE, используемую концентратором FlexVPN. Это значение использует значение из используемого сертификата.**удаленная аутентификация** - Состояния, что EAP должен использоваться для аутентификации клиента.**опознавательная локальная переменная** - Состояния, что сертификаты должны использоваться для локальной аутентфикации.**eap aaa authentication** - Состояния для использования списка FlexVPN-AuthC-List-1 aaa authentication login , когда EAP используется для authentiation.**список eap группы aaa authorization** - Состояния для использования списка FlexVPN-AuthZ-List-1 сети с проверкой подлинности AAA с именем пользователя *FlexVPN-Local-Policy-1* для атрибутов полномочий.**virtual-template 10** - Определяет, какой шаблон использовать, когда клонирован интерфейс виртуального доступа.

5. Настройте Профиль IPSEC, который связывается назад с профилем IKEv2, определенным в шаге 4.

```
crypto ipsec profile FlexVPN-IPsec-Profile-1
set ikev2-profile FlexVPN-IKEv2-Profile-1
```

Примечание: Cisco IOS использует Умные Настройки по умолчанию. В результате набор преобразований не должен быть явно определен.

6. Настройте виртуальный шаблон, от которого клонированы интерфейсы виртуального доступа:

ненумерованный IP- Не пронумеруйте интерфейс от *Внутреннего интерфейса* , таким образом, маршрутизация IPv4 может быть включена на интерфейсе.**ipv4 ipsec туннельного режима -** Определяет интерфейс, чтобы быть туннелем типа VTI.

```
interface Virtual-Template10 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

7. Ограничьте согласование SHA-1. Дополнительно

Должный дезертировать CSCud96246 (только зарегистрированные клиенты) , клиент AnyConnect мог бы быть не в состоянии правильно проверять сертификат Концентратора FlexVPN. Эта проблема происходит из-за IKEv2, выполняющего согласование о функции SHA 2 для Псевдослучайной функции (PRF), тогда как сертификат FlexVPN-концентратора был подписан с помощью SHA-1. Конфигурация ниже ограничивает согласование SHA-1:

```
crypto ikev2 proposal SHA1-only
encryption aes-cbc-256
integrity sha1
group 5
crypto ikev2 policy SHA1-only
match fvrf any
proposal SHA1-only
```

Конфигурация сервера Microsoft Active Directory

1. В Менеджере Windows Server разверните **Роли> Сетевая политика и Сервер доступа> NMPS (Локальный)> Клиенты RADIUS и Серверы**, и нажмите **RADIUS Clients**.

   Диалоговое окно New RADIUS Client появляется.

2. В диалоговом окне New RADIUS Client добавьте маршрутизатор Cisco IOS как Клиента RADIUS:
   Нажмите **Enable этот** флажок **Клиента RADIUS**.Введите имя в Дружественном поле имени. Данный пример использует *FlexVPN-концентратор*.Введите IP-адрес маршрутизатора в Поле адреса.В области Shared Secret нажмите кнопку с зависимой фиксацией **Manual**, и введите общий секретный ключ в Общий секретный ключ и Подтвердите поля общего секретного ключа.**Примечание:** Общий секретный ключ должен совпасть с общим секретным ключом, настроенным на маршрутизаторе. **Нажмите кнопку ОК.**

3. В интерфейсе Диспетчера серверов разверните **Политику** и выберите **Network Policies**.

   Диалоговое окно New Network Policy появляется.

4. В диалоговом окне New Network Policy добавьте новую сетевую политику:

   Введите имя в поле имени Политики. Данный пример использует *FlexVPN*.Нажмите кнопку с зависимой фиксацией **сервера доступа Типа сети** и выберите **Unspecified** из выпадающего списка. **Нажмите кнопку Next.**В диалоговом окне New Network Policy **нажмите Add** для добавления нового условия.В Избранном диалоговом окне условия выберите условие **Адреса IPv4 NAS** и **нажмите Add**.

   Диалоговое окно NAS IPv4 Address появляется.

   В диалоговом окне NAS IPv4 Address введите адрес IPv4 сервера доступа к сети для ограничения сетевой политики только запросами, которые происходят из этого маршрутизатора Cisco IOS.

   Нажмите кнопку ОК.

   В новом диалоговом окне Network Policy нажмите **доступ** , предоставленный кнопка с зависимой фиксацией для разрешения доступа клиента сети (если учетные данные, предоставленные пользователем, допустимы), и нажмите **Next**.

Гарантируйте только Microsoft: Безопасный пароль (MSCHAP EAP v2) появляется в области EAP Types, чтобы позволить EAP-MSCHAPv2 использоваться в качестве метода подключения между устройством Cisco IOS и Active Directory, и нажимать **Next**.

Примечание: Оставьте все опции 'Less secure authentication methods' неконтролируемыми.

Продолжите через мастера и примените любые дополнительные ограничения или параметры настройки, как определено вашей организационной политикой безопасности. Кроме того, гарантируйте, что политика перечислена сначала в порядке обработки как показано в этом образе:

Конфигурация клиента

1. Создайте профиль XML в текстовом редакторе и назовите его *flexvpn.xml*.

   Данный пример использует этот профиль XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true
</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true
</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false
</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true
</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false
</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">false
</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
```

```
<AutoUpdate UserControllable="true">false</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
Automatic
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon
</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly
</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false">
</PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="true">true
<TerminateScriptOnNextEvent>true
</TerminateScriptOnNextEvent>
<EnablePostSBLOnConnectScript>true
</EnablePostSBLOnConnectScript>
</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20
</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4
</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>FlexVPN Hub</HostName>
<HostAddress>flexvpn-hub.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>EAP-MSCHAPv2</AuthMethodDuringIKENegotiation>
<IKEIdentity>example.com</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

<hostname> является текстовой строкой, которая появляется в клиенте.**<HostAddress>** является полным доменным именем (FQDN) концентратора FlexVPN.**<PrimaryProtocol>** настраивает соединение для использования IKEv2/IPsec, а не SSL (по умолчанию в AnyConnect).**<AuthMethodDuringIKENegotiation>** настраивает соединение для использования MSCHAPv2 в EAP. Это значение требуется для аутентификации против Microsoft Active Directory.**<IKEIdentity>** определяет строковое значение, которое совпадает с клиентом к определенному профилю IKEv2 на концентраторе (см. шаг 4 выше).
Примечание: Клиентский профиль - что-то, что только используется клиентом. Рекомендуется, чтобы администратор использовал редактора Профиля Anyconnect для создания клиентского профиля.

2. Сохраните flexvpn.xml файл к соответствующему каталогу, как перечислено в этой таблице:

3. Закройте и перезапустите клиента AnyConnect.

4. В диалоговом окне Cisco AnyConnect Secure Mobility Client выберите **FlexVPN Hub** и нажмите **Connect**.

   AnyConnect Cisco | диалоговое окно FlexVPN Hub появляется.

5. Введите имя пользователя и пароль и нажмите **OK**.

Проверка

Для проверки соединения используйте **удаленную клиентскую-ipaddress** команду **подробности show crypto session**. См. show crypto session для получения дополнительной информации об этой команде.

> **Примечание:** Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Устранение неполадок

Для устранения проблем соединения соберите и проанализируйте журналы DART от клиента и используйте эти команды отладки на маршрутизаторе: **debug crypto ikev2 пакет** и **debug crypto ikev2 внутренний**.

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация