pfSense: The Definitive Guide
The Definitive Guide to the pfSense Open Source Firewall and Router Distribution

Christopher M. Buechler
Jim Pingle

перевод: **Михайлов Алексей ака** iboxjo
20-08-2012
e-mail: iboxjo@yandex.ru
blog: iboxjo.livejournal.com

Глава 15 OpenVPN

OpenVPN является ещё одним решением SSL VPN с открытым исходным кодом, которое может использоваться для удалённого доступа клиента, так и для подключения site-to-site. Клиенты OpenVPN поддерживаются широким спектром операционных систем, в том числе, все BSD, Linux, Mac OS X, Solaris, Windows 2000 и новее. Каждое соединение OpenVPN, будь то удалённый доступ или соединение site-to-site, состоит из сторон сервера и клиента. В случает VPN site-to-site, один брандмауэр выступает в качестве сервера, а другой в качестве клиента. Не имеет значения, какой именно брандмауэр выступает в какой роли. Как правило, центральный брандмауэр обеспечивает подключения к серверу для всех удалённых мест, брандмауэры которых настраиваются в качестве клиентов. Эта функциональность эквивалентна противоположной конфигурации – центральный брандмауэр сконфигурирован как клиент соединяющийся с сервером запущенном на брандмауэре в удалённой локации.

Существует два типа методов аутентификации, которые могут использоваться в OpenVPN: общие ключи (shared keys) и X.509. Для использования общих ключей, вы генерируете ключ который будет использоваться на обеих сторонах. X.509 подробно описывается далее в этом разделе.

Обратите внимание, что хотя OpenVPN является SSL VPN, это не "clienless" SSL VPN, в том смысле, в котором его понимают производители коммерческих брандмауэров. Вам необходимо установить клиент OpenVPN на всех ваших клиентских устройствах. В действительности, не существует никакого VPN решения "без клиента", и терминология "clientless" – не более чем маркетинговый ход. Более подробную информацию по обсуждению SSL VPN предоставляет сообщение Мэтью Грумса (Matthew Grooms), разработчика pfSense и инструментов IPsec: http://marc.info/?l=pfsense-support&m=121556491024595&w=2. По вопросу общего рассмотрения различных типов VPN доступных в pfSense, их плюсов и минусов, обратитесь к главе 12, "Виртуальные частные сети".

15.1. Базовое введение в инфраструктуру открытых ключей X.509

Один из вариантов аутентификации OpenVPN позволяет использование ключей X.509. Подробное обсуждение X.509 и PKI выходит за рамки данной книги и является темой целого ряда специализированных изданий. Этот раздел содержит очень общее описание, которое необходимо для настройки OpenVPN. X.509 является предпочтительным методом запуска удалённого доступа VPN, поскольку позволяет ограничивать доступ индивидуальных машин.

При использовании общих ключей, вам необходимо либо создать уникальный сервер или порт для каждого клиента, либо передать один и тот же ключ всем клиентам. Первый способ является кошмаром в плане управления, а второй позволяет получить множество проблем в случае компрометации ключа. Если одна клиентская машина оказалась скомпрометирована или требуется отменить доступ

конкретного человека, придётся создавать новый ключ и изменять ключи на всех клиентских машинах. При развёртывании инфраструктуры открытого ключа, в случае компрометации клиента или при отзыве его доступа, можно просто отменить сертификат клиента. Другие клиенты при этом не пострадают.

При использовании PKI сначала создаётся Certificate Authority (CA). Затем, CA подписывает все индивидуальные сертификаты в вашем PKI. Сертификат CA используется на серверах OpenVPN и клиентах для проверки подлинности используемых сертификатов. CA можно использовать для проверки подписи сертификатов, но не для подписания сертификатов. Подписание сертификатов требует закрытый ключ CA (ca.key при использовании простых RSA, обсуждаемый далее в данной главе). Конфиденциальность закрытого ключа CA обеспечивает безопасность вашего PKI. Любой человек, имеющий доступ к закрытому ключу CA может создать сертификаты для использования на вашей PKI, и следовательно закрытые ключи должны быть хорошо защищены. Эти ключи никогда не распространяются на клиенты или сервера.

Убедитесь, что вы никогда не копируете клиенту больше файлов чем ему необходимо, так как это может привести к взлому вашей PKI. В последующих главах описывается, какие файлы требуются клиентам для подключения и как создавать сертификаты.

15.2. Генерация ключей и сертификатов OpenVPN

OpenVPN использует сертификаты и общие ключи для шифрования и де шифрования трафика. Этот раздел показывает, как генерировать общий ключ или сертификат используемый в OpenVPN. Последний раздел описывает, как использовать эти ключи и сертификаты.

15.2.1. Генерация общих ключей

Общие ключи – предпочтительный метод для соединения site-to-site с помощью OpenVPN. Для генерации общего ключа, перейдите на вкладку Diagnostics -> Command и выполните следующую команду:

```
# openvpn --genkey --secret /tmp/shared.key
```

Для отображения ключа выполните:

```
# cat /tmp/shared.key
```

Ключ будет выглядеть примерно следующим образом:

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
6ade12d55caacbbc5e086ccb552bfe14
4ca7f08230b7e24992685feba9842a03
44ee824c6ac4a30466aa85c0361c7d50
19878c55e6f3e7b552e03a807b21bad5
ce0ca22d911f08d16b21ea1114e69627
f9e8a6cd277ad13b794eef5e1862ea53
e7b0cba91e8f120fa983bdd8091281f6
610bf8c7eb4fed46875a67a30d25896f
0010d6d128ad607f3cbe81e2e257a48a
82abfca3f8f85c8530b975dca34bcfe4
69f0066a8abd114f0e2fbc077d0ea234
34093e7d72cc603d2f472075585f2bdec
ed663ad17db9841e881340c2b1f86d0a
45dc5b24823f47cc565196ceff4a46ca
34fc074959aa1ef988969cfdd6d37533
e5623222373d762a60e47165b04091c2
-----END OpenVPN Static key V1-----
```

Скопируйте ключ и вставьте его в вашу конфигурацию OpenVPN.

После копирования ключа, вам следует удалить его. Для этого выполните:

```
# rm /tmp/shared.key
```

15.2.2. Создание сертификатов

Для конфигурации OpenVPN с X.509, первоначально, необходимо сгенерировать сертификаты. Если у вас уже есть существующая PKI, и вы хотите её использовать, информация этого раздела к вам не относится. Большинство пользователей pfSense не имеют существующей PKI X.509, и простым средством её настройки является easy-rsa скрипт предоставляемый OpenVPN.

15.2.2.1. Местоположение easy-rsa

Если у вас есть система BSD или Linux, вы можете скачать последнюю версию OpenVPN для этой системы, распаковать дистрибутив и найти папку easy-rsa в извлечённой папке OpenVPN. Аналогично, для Windows, OpenVPN по умолчанию устанавливает easy-rsa в C:\Program Files\OpenVPN\easy-rsa. Кроме того, вы можете использовать easy-rsa непосредственно на pfSense.

Если вы предпочитаете запуск на виртуальной машине, pfSense Tools virtual appliance [http://www.pfsense.org/toolsvm], включает скрипт easy-rsa.

Наиболее серьёзные развертывания PKI обычно работают на выделенных системах находящихся в безопасной локации. В большинстве малых и средних сред большинство действий связанных с безопасностью PKI может оказаться непрактичными и редко применяются. Однако имейте в виду, что компрометация вашей PKI ставит под угрозу целостность всей инфраструктуры OpenVPN, а следовательно поддерживайте требуемый уровень безопасности.

15.2.2.2. Создание сертификатов с использованием pfSense

Вы можете использовать easy-rsa на pfSense для генерации ключей OpenVPN. Файлы easy-rsa, включённые в OpenVPN подразумевают наличие оболочки bash, которая не включается по умолчанию в системы BSD, поэтому требуется специальный пакет easy-rsa, предоставляемый разработчиками pfSense. Вам необходимо включить ssh на вашем брандмауэре, чтобы получить возможность использовать easy-rsa. Для установки просто выполните следующую команду в ssh сессии:

```
# fetch -o - http://files.pfsense.org/misc/easyrsa-setup.txt | /bin/sh
```

Команда позволит загрузить требуемые файлы. Распакуйте их и удалите загруженный файл. Затем, вам будет предложено выполнить следующий шаг вручную. Скопируйте и вставьте последнюю отображённую строку для генерации ваших сертификатов.

Замечание

Если вы выполняли этот процесс раньше, повтор приведёт к уничтожению всех существующих сертификатов!

```
# cd /root/easyrsa4pfsense && ./PFSENSE_RUN_ME_FIRST
```

Сначала вам предложат ввести ваше местоположение (location) и информацию о организации (organization information), которые будут использовать в дальнейшем по умолчанию при создании дополнительных сертификатов. Будет создан ваш CA, сертификат сервера и один клиентский сертификат. Эти файлы могут быть найдены в директории /root/easyrsa4pfsense/keys/.

15.2.2.2.1. Создание клиентских ключей

Для создания нового ключа клиента, выполните следующие команды, где username – имя клиента (замените username на соответствующее имя).

```
# cd /root/easyrsa4pfsense
# source vars
# ./build-key username
```

15.2.2.2.2. Создание ключа клиента защищённого паролем

Процесс создание ключа клиента защищённого паролем примерно аналогичен. Для этого выполните следующие команды:

```
# cd /root/easyrsa4pfsense
# source vars
# ./build-key-pass username
```

Пароль указанный при создании ключа должен вводиться пользователем при каждом подключении к OpenVPN.

15.2.2.2.3. Копирование ключей с брандмауэра

После создания ключей, вам необходимо передать их для использования в конфигурациях сервера и клиента. Для ключей используемых на pfSense, будь то конфигурация сервера или клиента, простой способ заключается в использовании команды cat в ssh-сессии и копировании полученного результата. например, для получения содержимого сертификатов, выполните следующую команду:

```
# cat /root/easyrsa4pfsense/keys/ca.crt
```

Скопируйте вывод и вставьте его в поле CA certificate. То, какие файлы сертификатов вводятся в каждое поле ввода конфигурации OpenVPN, мы рассмотрим позже в этой главе.

Для не-pfSense клиентов, вам потребуется скачать соответствующие файлы сертификатов. Это можно сделать с помощью SCP, как описано в разделе 4.5.2., "Безопасная оболочка (SSH)", или посредством web-интерфейса, на странице Diagnostics -> Command. Заполните соответствующее имя файла в поле File to download, например /root/easyrsa4pfsense/keys/ca.crt для сертификата CA, и нажмите Download. Требуется повторить эту операцию для каждого файла.

Другим, альтернативным, способом является резервное копирование всего директория easy-rsa, как описано в следующем разделе, и извлечение резервной копии для получения необходимых файлов.

15.2.2.2.4. Резервное копирование easy-rsa

Папка easyrsa4pfsense не резервируется когда вы выполняете резервное копирование файла конфигурации. Вам необходимо создавать резервную копию

этой папки, поскольку потеря данных в директории ключей приведёт к невозможности создания новых ключей и отмене старых. Существующая конфигурация не станет неработоспособной, однако потеряет возможность добавления и отмены ключей, и вам придётся воссоздавать все ключи и заново передавать их клиентам. Самый простой способ резервного копирования easy-rsa — использование пакета Backup для резервного копирования пути /root/easyrsa4pfsense, как показано на рисунке 15.1., "Резервное копирование easy-rsa". Пакет Backup обсуждается в разделе 5.6., "Резервное копирование файлов и директориев с помощью пакета Backup".

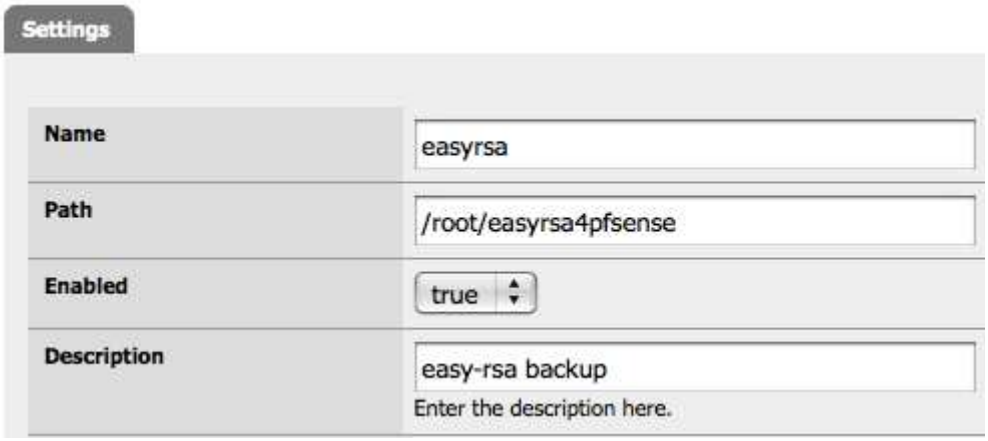

Рисунок 15.1. Резервное копирование easy-rsa

15.2.2.3. Использование easy-rsa

Если вы предпочитаете использовать easy-rsa на системе отличной от pfSense, вам требуется выполнить несколько дополнительных шагов. Эти шаги применимы к системам BSD и Linux, однако и на Windows они практически аналогичны. Если вы используете Windows, обратитесь к файлу README.txt в папке easy-rsa.

Для начала скачайте и распакуйте OpenVPN с http://openvpn.net. В извлечённой папке вы обнаружите папку easy-rsa. Для Windows, после установки OpenVPN, вы обнаружите папку easy-rsa в директории C:\Program Files\OpenVPN\.

15.2.2.3.1. Установка информации в vars

Существует файл названый vars который включён в папку easy-rsa. Откройте его в текстовом редакторе и перейдите в конец файла. Вы увидите нечто похожее:

```
export
export
export
```

```
export
KEY_COUNTRY=US
KEY_PROVINCE=Kentucky
KEY_CITY=Louisville
KEY_ORG="pfSense"
export KEY_EMAIL="pfsense@localhost"
```

Вы можете изменить эти значения на свою локацию (location), организацию (organization) и электронную почту (email), или оставить их по умолчанию, если хотите, чтобы ваши сертификаты были созданы с использованием данной информации. Сохраните vars после внесения необходимых изменений.

15.2.2.3.2. Создание своего CA

Сначала, выполните vars для загрузки переменных среды easy-rsa. Затем запустите ./clean-all для начальной очистки среды. после создания своего CA никогда не следует выполнять clean-all, поскольку она удалит все ваши CA и все сертификаты.

```
# source vars
NOTE: when you run ./clean-all, it will be doing a rm -rf on /home/cmb/easyr
# ./clean-all
#
```

Теперь вы готовы к запуску ./build-ca, команды которая создаёт ваш CA. Обратите внимание, что поля уже заполнены значениями введёнными в переменных. Вы можете просто нажимать Enter в ответ на запрос.

```
# ./build-ca
Generating a 1024 bit RSA private key
.....................................++++++
.....++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [Kentucky]:
```

```
Locality Name (eg, city) [Louisville]:
Organization Name (eg, company) [pfSense]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address [pfsense@localhost]:
#
```

15.2.2.3.3. Генерация DH ключа

Далее, следует сгенерировать DH-ключ, выполнив ./build-dh. Вас предупредят, что это займёт много времени, и оно зависит от быстродействия вашего процессора. На процессорах Intel Core2 Quad Q6600 эта процедура занимает 5 секунд, а на более медленных может растянуться до нескольких минут.

```
# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.............+.............+.........................................
..................... ..........................+.+.................
.....................+...............+... ..........................
.................+.............................................. ......
....+.++*++*++*
```

15.2.2.3.4. Генерация ключа и сертификата сервера

Теперь, вам необходимо создать сертификат и ключ сервера OpenVPN, используя команду ./build-key-server за которой следует имя по которому вы будете ссылаться на сервер (исключительно косметическое).

```
# ./build-key-server server
Generating a 1024 bit RSA private key
.................++++++
........++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [Kentucky]:
```

```
Locality Name (eg, city) [Louisville]:
Organization Name (eg, company) [pfSense]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: server
Email Address [pfsense@localhost]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /home/cmb/easyrsa4pfsense/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName
:PRINTABLE:'US'
stateOrProvinceName
:PRINTABLE:'Kentucky'
localityName
:PRINTABLE:'Louisville'
organizationName
:PRINTABLE:'pfSense'
commonName
:PRINTABLE:'server'
emailAddress
:IA5STRING:'pfsense@localhost'
Certificate is to be certified until Jan 18 07:18:22 2019 GMT (3650 days)
Sign the certificate? [y/n]: y
1 out of 1 certificate requests certified, commit? [y/n] y
Write out database with 1 new entries
Data Base Updated
#
```

15.2.2.3.5. Генерация сертификатов клиентов

Вам потребуется создать сертификат для каждого клиента используя команду biuild-key за которой следует ключевое имя. Следующий пример показывает создание ключа для пользователя cmb. вы можете использовать любое имя, однако использование имени пользователя которому будет принадлежать ключ будет вполне разумно. Для подключения клиентов которые находятся на брандмауэрах, вы можете использовать имя хоста брандмауэра использующего ключ.

```
# ./build-key cmb
Generating a 1024 bit RSA private key
.....................................................++++++
.........................++++++
writing new private key to 'cmb.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [Kentucky]:
Locality Name (eg, city) [Louisville]:
Organization Name (eg, company) [pfSense]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: cmb
Email Address [pfsense@localhost]:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /home/cmb/easyrsa4pfsense/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName
:PRINTABLE:'US'
stateOrProvinceName
:PRINTABLE:'Kentucky'
localityName
:PRINTABLE:'Louisville'
organizationName
:PRINTABLE:'pfSense'
commonName
:PRINTABLE:'cmb'
emailAddress
:IA5STRING:'pfsense@localhost'
Certificate is to be certified until Jan 18 07:21:04 2019 GMT (3650 days)
Sign the certificate? [y/n]: y
```

```
1 out of 1 certificate requests certified, commit? [y/n] y
Write out database with 1 new entries
Data Base Updated
#
```

Вам придётся повторить данный процесс для каждого клиента. Для последующего добавления пользователей вы можете в любое время повторить данный процесс.

15.3. Параметры конфигурации OpenVPN

В этом разделе описаны доступные опции OpenVPN, которые вы можете или захотите использовать. Последующие разделы посвящены примерам настройки конфигурации site-to-site и удалённого доступа VPN с использованием наиболее распространённых вариантов минимальной конфигурации OpenVPN.

15.3.1. Параметры конфигурации сервера

В этом разделе описывается каждый из параметров конфигурации страницы OpenVPN Server Edit.

15.3.1.1. Disable this tunnel (**Отключить этот туннель**)

Установите этот флаг и нажмите кнопку Save, чтобы сохранить конфигурацию но не включать сервер.

15.3.1.2. Protocol (**Протокол**)

Здесь следует выбрать TCP или UDP. Если нет причины использовать TCP, например необходимости обхода брандмауэра путём запуска OpenVPN на TCP порту 443, вам следует использовать UDP. Когда используется туннелирование трафика, всегда предпочтительно использовать протоколы не устанавливающие соединения. TCP – ориентирован на соединение и обеспечивает гарантированную доставку. Любые потерянные пакеты будут передаваться повторно. Это может выглядеть хорошо, но на сильно загруженных соединениях может приводить к незначительной деградации производительности или постоянной потери пакетов из-за повторной передачи. Часто, вы будете передавать TCP трафик через туннель. Когда существует TCP обёртка вокруг TCP, при потере пакета будут повторно передаваться как внешние так и внутренние потерянные TCP-пакеты. В редких случая, это будет не проблемно, однако постоянно повторяющиеся потери пакетов приводят к заметному снижению производительности, сравнительно большему чем при использовании UDP. В действительности, вы не хотите осуществлять повторную отправку потерянных пакетов трафика инкапсулированного в VPN. Если трафику туннеля требуется надёжная доставка, он будет использовать протоколы подобные TCP которые обеспечивают надёжность и повтор передачи.

15.3.1.3. Dynamic IP (**Динамический IP**)

Установка данного флага добавляет некоторые опции конфигурации в конфигурацию OpenVPN. Опция позволяет подключенным клиентам сохранить соединения в случае если их IP изменился. Для клиентов, IP которых часто меняется, или для мобильных пользователей, которые часто перемещаются между различными подключениями, следует установить данную опцию. Если IP клиента статический или меняется редко, отключение данной опции позволяет незначительно повысить безопасность.

15.3.1.4. Local port (**Локальный порт**)

Локальный порт – номер порта на котором будет слушать OpenVPN. Правила вашего брандмауэра должны позволять трафик на этот порт, и он должен быть указан в конфигурации клиента. Порт для каждого сервера должен быть уникален.

15.3.1.5. Address pool (**Пул адресов**)

Пул адресов которые будут назначаться клиентам при подключении. Сервер OpenVPN будет использовать первый адрес пула для соединения и назначать дополнительные адреса присоединённым клиентам.

15.3.1.6. Use static IPs (**Использовать статические IP**)

Если вы включите этот флаг, то сервер не будет назначать IP клиентам. Как правила данная возможность не используется, хотя бывает полезна в сочетании с определёнными опциями для некоторых решений, таких как использование моста.

15.3.1.7. Local network (Локальная сеть)

В этом поле указывается маршрут, если имеется, которые направляют клиентов подключающихся к данному серверу. Если вам необходимо использовать маршруты для более чем одной подсети, введите здесь первую подсеть и изучите раздел 15.10, "Специальные параметры конфигурации" для получения информации о добавлении остальных подсетей.

15.3.1.8. Remote network (**Удалённая сеть**)

Если здесь указана подсеть, будет добавлен маршрут к этой подсети на другой стороне OpenVPN соединения. Эта опция используется только в соединениях типа site-to-site. но не для мобильных клиентов. Вы можете ввести только одну подсеть. Если вам необходимо добавить более одной удалённой сети, введите здесь первую подсеть и изучите раздел 15.10, "Специальные параметры конфигурации" для получения информации о добавлении остальных подсетей.

15.3.1.9. Client-to-client VPN (VPN **клиент-клиент**)

Если клиентам необходимо взаимодействовать друг с другом, установите данный

флаг. При сброшенном флаге, клиенты могут отправлять трафик только на сервер (и любые связанные сети, к которым имеется маршрут).

15.3.1.10. Cryptography (**Шифрование**)

Здесь можно выбрать криптографический шифр который будет использоваться для этого соединения. По умолчанию используется BF-CBC – Blowfish 128 bit Cipher Block Chaining. Это шифрование используется OpenVPN по умолчанию, и является прекрасным выбором в большинстве случаев. Одна из наиболее распространённых ситуаций, когда может понадобиться изменение алгоритма – использование аппаратного ускорителя шифрования, такого как glxsb построенного на оборудовании ALIX или карт hifn. В этих случаях, вы увидите значительное увеличение скорости шифрования. Для ALIX и иного оборудования glxsb, выберите метод AES-CBC-128. Для оборудования hifn выбрите 3DES или AES. Смотрите раздел 15.10.3., "Использование аппаратных крипто-ускорителей", для получения дополнительной информации о использовании данного оборудования.

15.3.1.11. Authentication method (**Способ аутентификации**)

Здесь можно выбрать PKI или общие ключи, в зависимости от того, что вы планируете использовать. Раздел 15.2. "Генерация ключей и сертификатов OpenVPN" более подробно рассматривает эти варианты.

15.3.1.12. Shared key (**Общий ключ**)

Когда используется аутентификация по общим ключам, сюда вставляется общий ключ.

15.3.1.13. **Параметры PKI**

Следующие пять опций относятся к использованию аутентификации с использованием PKI. Первые четыре опции являются обязательными.

15.3.1.13.1. CA certificate (**сертификат CA**)

Сюда следует вставить сертификат CA (при использовании easyrsa это ca.crt).

15.3.1.13.2. Server certificate (**сертификат сервера**)

Сюда вставляется сертификат сервера (server.crt при использовании easyrsa).

15.3.1.13.3. Server key (**ключ сервера**)

Вставьте сюда ключ сервера (server.key при использовании easyrsa).

15.3.1.13.4. DH parameters (**параметры DH**)

Сюда вставляются параметры DH (dh1024.pem при использовании easyrsa).

15.3.1.13.5. CRL

CRL – список отзыва сертификатов. Если вам необходимо отменить доступ к одному или нескольким сертификатам, создаётся файл crl.pem, который необходимо вставить в это поле. Этот файл представляет собой полный список отозванных сертификатов, поэтому содержимое поле должно заменяться, а не дополняться в случае отзыва сертификата.

15.3.1.14. DHCP options (**Параметры** DHCP)

Существует восемь параметров DHCP, которые можно настроить. Эти параметры ведут себя аналогично настройке любого DHCP сервера.

15.3.1.14.1. DNS Domain Name (**Имя домена** DNS)

В поле указывается имя домена DNS которое будет назначаться клиентам. Для обеспечения корректной работы разрешения имён компьютеров локальной сети, в которой используется разрешение имён DNS, необходимо указать DNS–имя внутреннего домена. В среде Microsoft AD, это, как правило, имя вашего домена AD.

15.3.1.14.2. DNS server (**сервер** DNS)

В этом поле указываются сервера DNS, которые будут использоваться клиентом при подключении к этому серверу. В среде Microsoft AD, здесь следует указывать DNS сервера вашего AD для целей разрешения имён и аутентификации при подключение посредством OpenVPN.

15.3.1.14.3. WINS server (**сервер** WINS)

В этом поле указываются WINS–сервера, которые предполагается использовать (если таковые имеются).

15.3.1.14.4. NBDD server (**сервер** NBDD)

Эта опция применяется для указания сервера распределения дейтаграмм NetBIOS (NetBIOS Datagram Distribution), который обычно не используется.

15.3.1.14.5. NTP server (**сервер** NTP)

Это поле определяет опцию 47 DHCP, основной NTP сервер. Это может быть IP адрес или FQDN (полное доменное имя).

15.3.1.14.6. NetBIOS node type (**тип узла** NetBIOS)

Тип узла NetBIOS контролирует, как Windows–системы будут функционировать при разрешении имён NetBIOS. Как правила, лучше оставить значение none по умолчанию.

15.3.1.14.7. NetBIOS scope (**область видимости** NetBIOS)

Введите область NetBIOS, если это возможно. Обычно поле оставляется пустым.

15.3.1.14.8. Disable NetBIOS (**отключить** NetBIOS)

Эта опция отключает NetBIOS через TCP/IP на клиенте, и как правило не устанавливается.

15.3.1.15. LZO Compression (**компрессия** LZO)

Этот флаг позволяет использовать LZO-компрессию для трафика OpenVPN. Если этот флаг установлен, трафик пересекающий ваши OpenVPN соединения будет сжиматься до его шифрования. Это позволяет экономить использование полосы пропускания для различных типов трафика за счёт повышения нагрузки на процессоры сервера и клиента. Как правило, влияние минимально, и я предполагаю, что данную опцию следует использовать для любых OpenVPN соединений проброшенных через Интернет.

Для высокоскоростных соединений, таких как OpenVPN через локальную сеть, высокоскоростные WAN или локальная беспроводная сеть, эта опция может оказаться нежелательной, поскольку задержка добавленная сжатием может оказаться выше чем задержки в передаче трафика. Если практически весь трафик проходящий через ваше OpenVPN-соединение уже зашифрован (например SSH, SCP и HTTPS), вы не должны использовать LZO-компрессию, поскольку шифрованные данные не сжимаются, и сжатие вызовет передачу большего объёма данных. То же верно, если ваш VPN трафик является уже сжатыми данными.

15.3.1.16. Custom options (**специальные опции**)

Хотя интерфейс pfSense поддерживает большинство наиболее общих опций, OpenVPN является весьма мощным и гибким, имея множество опций не доступных в Web-интерфейсе. Дополнительные опции могут быть введены в этом поле. Параметры опций описаны далее в разделе 15.10., "Специальные опции".

15.3.1.17. Description (**Описание**)

Здесь вводится описание для данной конфигурации сервера, имеющее справочное значение.

15.4. **Конфигурирование удалённого доступа**

В этом разделе описывается процесс настройки решения удалённого доступа VPN с использованием OpenVPN на основе X.509.

15.4.1. **Определение схемы IP адресации**

В дополнение к внутренней подсети к которой клиенты будут получать доступ, вам необходимо выьбрать IP подсеть для использования соединений OpenVPN. Эта подсеть заполняется в поле Interfaces IP в конфигурации сервера.

Подключающиеся клиенты будут получать IP адреса из этой подсети, и сервер на конце соединения также получит IP из этой подсети, когда клиент направляет трафик проходящий через соединение OpenVPN в подсеть. Как и в случае выбора внутренней подсети для единственной локации, эта подсеть должна подчиняться правилам CIDR суммаризации с вашей внутреней подсетью. Пример сети, приведённый в примере использует 172.31.54.0/24 для LAN и 172.31.55.0/24 для OpenVPN. Эти две подсети суммаризируются как 172.31.54.0/23, что позволяет легче управлять маршрутизацией. Суммаризация CIDR рассматривается в разделе 1.7.5., "Суммаризация CIDR".

15.4.2. Пример сети

Рисунок 15.2., "Пример удалённого доступа к сети с помощью OpenVPN", показывает сеть настроенную следующим образом:

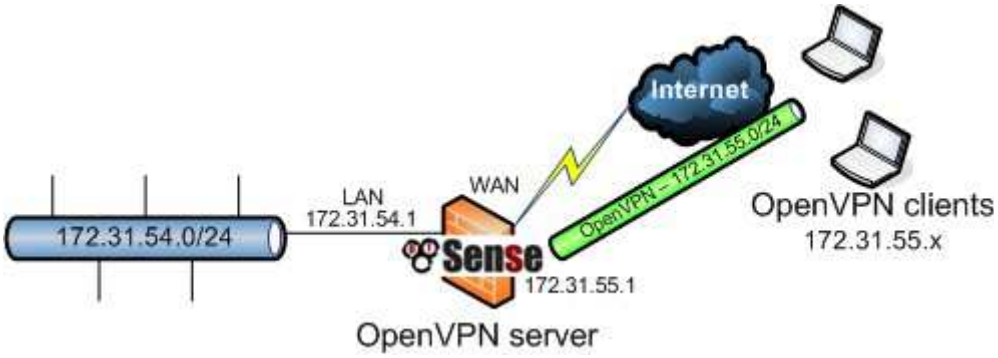

Рисунок 15.2., "Пример удалённого доступа к сети с помощью OpenVPN"

15.4.3. Конфигурация сервера

Перейдите на страницу VPN->OpenVPN и нажмите [+] на закладке Server для добавления нового сервера OpenVPN. Большинство опций будут установлены по умолчанию. Следующие опции необходимо сконфигурировать.

- Local Address (локальный адрес) – укажите здесь подсеть для использования клиентами OpenVPN. Для этого примера 172.31.55.0/24.
- Autentication method (метод аутентификации) – немного переместитесь вниз по странице и измените метод аутентификации с Shared key на PKI.
- Local Network (локальная сеть) – вернитесь по странице назад и укажите локальную сеть, как сеть достижимую для клиентов через VPN. В этом примере это будет LAN, так что укажем здесь 172.31.54.0/24. Дополнительные подсети могут указываться с использованием специальных опций описанных в разделе 15.10, "Настройка специальных опции".
- CA certificate – сюда вставьте содержимое ca.crt из easy-rsa
- Server certificate – вставьте содержимое server.crt из easy-rsa
- Server key – вставьте содержимое server.key из easy-rsa

- DH parameters – вставьте содержимое dh1024.pem из easy-rsa
- LZO compression – в том случае, если это не высокоскоростные соединения VPN с низкими задержками, такие как локальные проводные или беспроводные сети, вы можете включить LZO-компрессию.
- Description – заполните описание конфигурации сервера.

Это – конфигурационный минимум для большинства серверных конфигураций. По желанию (или необходимости) можно настроить дополнительные опции. Для получения дополнительной информации о других доступных опциях обратитесь к разделу 15.3., "Параметры настройки OpenVPN".

После завершения настройки нажмите кнопку Save для завершения конфигурирования сервера. После нажатия кнопки Save, pfSense запустит сервер OpenVPN.

15.4.3.1. Разрешение трафика к серверу OpenVPN

Далее, следует добавить правило брандмауэра, позволяющее трафик на сервер OpenVPN. Перейдите на страницу Firewall->Rules, и на закладке WAN нажмите [+]. Для данного примера конфигурации, выбран протокол UDP с любого источника, с адресом назначения WAN Address, и портом назначения 1194. Это правило показано на рисунке 15.3., "Правило WAN сервера OpenVPN".

Рисунок 15.3., "Правило WAN сервера OpenVPN".

Если вам известно, с каких адресов источников будут соединяться ваши клиенты, можно указать исходную подсеть или алиас, а не оставлять сервер открытым для всего Интернета. Как правило, это практически не возможно осуществить для мобильных клиентов. Существует не слишком много риска в открытие сервера, однако, вы можете снизить риск только при условии использования аутентификации на основе сертификатов, в то время как решения на основе паролей более восприимчивы к атакам подбора паролей. Всё это предполагает отсутствие дыр безопасности в самой OpenVPN, которая на сегодняшний день имеет приличный список отслеживания безопасности.

15.4.4. Установка на клиенте

Закончив с конфигурацией сервера, требуется установить OpenVPN на системы клиентов. Одна и та же инсталляция OpenVPN может работать в качестве клиента или сервера. В этом разделе предоставлен обзор установки для нескольких популярных операционных систем.

15.4.4.1. Установка на Microsoft Windows

Проект OpenVPN предоставляет установщик для Windows 2000 – Windows 7, который доступен для загрузки на http://openvpn.net/index.php/open-source/downloads.html. Во время написания этой главы лучшим вариантом загрузки для большинства пользователей Windows был релиз 2.1_rc19. Версия 2.1. в данный момент не классифицированная как стабильная, оказалась достаточно стабильной, широко используемой и включает в себя графический интерфейс.

Текущая стабильная версия 2.0.9 (та что работает на pfSense) не включает графического интерфейса Windows. Клиент 2.1. полностью совместим с версией 2.0.x работающей на pfSense. Установка достаточно прямолинейна – просто примите все настройки по умолчанию. Установка создаст новое локальное подключение на вашей системе для интерфейса tun. Этот интерфейс будет использоваться для VPN подключения, в противном случае он будет отключен. Никакой настройки данный интерфейс не требует, поскольку его конфигурация будет получена с сервера OpenVPN.

Замечание

В Windows Vista и Windows 7 с включенным UAC (управление аккаунтами пользователя), щёлкните правой кнопкой мыши на иконке OpenVPN GUI и выберите Запуск от имени администратора. Подключение может выполняться без прав администратора, однако не получится добавить маршрут для направления трафика через OpenVPN соединение, что сделает его непригодным для использования.

Аналогично, вы можете настроить свойства свойства ярлыка, чтобы всегда запускать программу от имени администратора. Эта опция доступна на вкладке Совместимость свойств ярлыка.

15.4.4.2. Клиенты Mac OS X

Существует три варианта клиентов Mac OS X. Одним из них, является простой клиент OpenVPN для командной строки. Большинство пользователей предпочитают графические клиенты для OS X представленные двумя вариантами. Tunnelblick – бесплатен и доступен для скачивания на сайте http://www.tunnelblick.net. В прошлом. я достаточно успешно его использовал. Другой вариант – использование коммерческого клиента Viscosity доступного на сайте http://www.viscosityvpn.com. На момент написания данной статьи он стоил 9 долларов за клиентское место. Если вы часто используете OpenVPN, Viscosity легко устанавливается и не требует дополнительных настроек.

15.4.4.3. Инсталляция на FreeBSD

Если у вас установлено FreeBSD, вы можете обнаружить OpenVPN в системе портов. Для установки просто выполните:

```
# cd /usr/ports/security/openvpn && make install clean
```

15.4.4.4. Установка на Linux

Установка на Linux будет различаться в зависимости от выбранного дистрибутива и способа управления установкой ПО. OpenVPN входит в репозиторий пакетов всех основных дистрибутивов Linux. Множество доступной информации можно обнаружить в Интернет.

15.4.5. Конфигурирование клиента

После установки OpenVPN, вам необходимо скопировать сертификаты клиентов и создать файл конфигурации клиента.

15.4.5.1. Копирование сертификатов

Для каждого клиента необходимы три файла easy-rsa: сертификат CA, сертификат клиента и ключ клиента. Сертификат CA – ca.key в директории easy-rsa. Клиентский сертификат и ключ клиента представлены с именем клиента использованным при генерации сертификатов пользователей. Для пользователя jdoe – это jdoe.crt и ключ jdoe.key. Скопируйте ca.crt, <имя пользователя>.crt и <имя пользователя>.key в директорий конфигурации OpenVPN на клиенте.

15.4.5.2. Создание конфигурации

После копирования сертификатов на клиента, должен быть создан клиентский файл конфигурации OpenVPN. Это можно сделать с помощью любого текстового редактора. Ниже приведён пример наиболее часто используемой конфигурации.

```
client
dev tun
proto udp
remote openvpn.example.com 1194
ping 10
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert username.crt
key username.key
pull
verb 3
comp-lzo
```

Строка remote определяет хост и порт удалённого сервера OpenVPN. Здесь может быть указан IP-адрес или полное доменное имя. Строка proto указывает

протокол используемый соединением OpenVPN. Измените данную строку на proto tcp, если вы для работы протокол TCP вместо UDP. Строки ca, cert и key необходимо изменить соответственно для каждого клиента.

15.4.5.2.1. Распространение конфигурации и ключей для клиентов

Самый простой способ распространения ключей и конфигурации OpenVPN для клиентов — их упаковка в zip архив или самораспаковывающийся архив с автоматическим извлечением в C:\Program Files\OpenVPN\config (для Windows). Он должен быть безопасно передан конечным пользователям и никогда не должен передаваться через не надёжные сети в не зашифрованном виде.

15.4.5.3. Конфигурирование Viscosity

При использовании данного клиента вам нет необходимости вручную создавать клиентский файл конфигурации OpenVPN, как это было описано в предыдущем разделе. Viscosity представляет собой графический инструмент конфигурации, который используется для формирования основной конфигурации клиента OpenVPN. Сначала, следует скопировать CA сертификат, сертификат клиента и ключ клиента в выбранный директорий на Mac. Эти файлы будут импортированы в Viscosity, а затем удалены. Затем запустите Viscosity чтобы приступить к созданию конфигурации.

Нажмите кнопку [Lock] на панели меню в верхней части экрана, и нажмите Preferences для начала конфигурирования, как показано на рисунке 15.4., "Настройка Viscosity".

Нажмите значок [+] в нижнем правом углу экрана Preferences, и щёлкните New Connection как показано на рисунке 15.5. "Добавление соединений в Viscosity". На первом экране конфигурации (Рисунок 15.6, "Конфигурирование Viscosity: Основное"), введите имя вашего соединения, IP адрес или имя хоста сервера OpenVPN, используемый порт и протокол. Отметьте Enable DNS support, если вы указали DNS сервера в конфигурации своего сервера. Щёлкните вкладку Certificates когда закончите.

На вкладке Cetrtificates (рисунок 15.7, "Конфигурирование Viscosity: Сертификаты"), должны быть указаны CA, сертификаты пользователей и ключи пользователей. Эти файл могут быть загружены в любую папку на Mac OS. После загрузки файлов, нажмите Select рядом с каждым полем и выберите соответствующие файлы. Поле TLS-Auth оставьте пустым. Когда закончите, нажмите закладку Options.

На закладке Options (рисунок 15.8, "Конфигурирование Viscosity: Параметры"), установите флаг Use LZO Compression если вы включили LZO компрессию на

стороне сервера. Остальные параметры можно оставить по умолчанию. Теперь перейдите на закладку Networking.

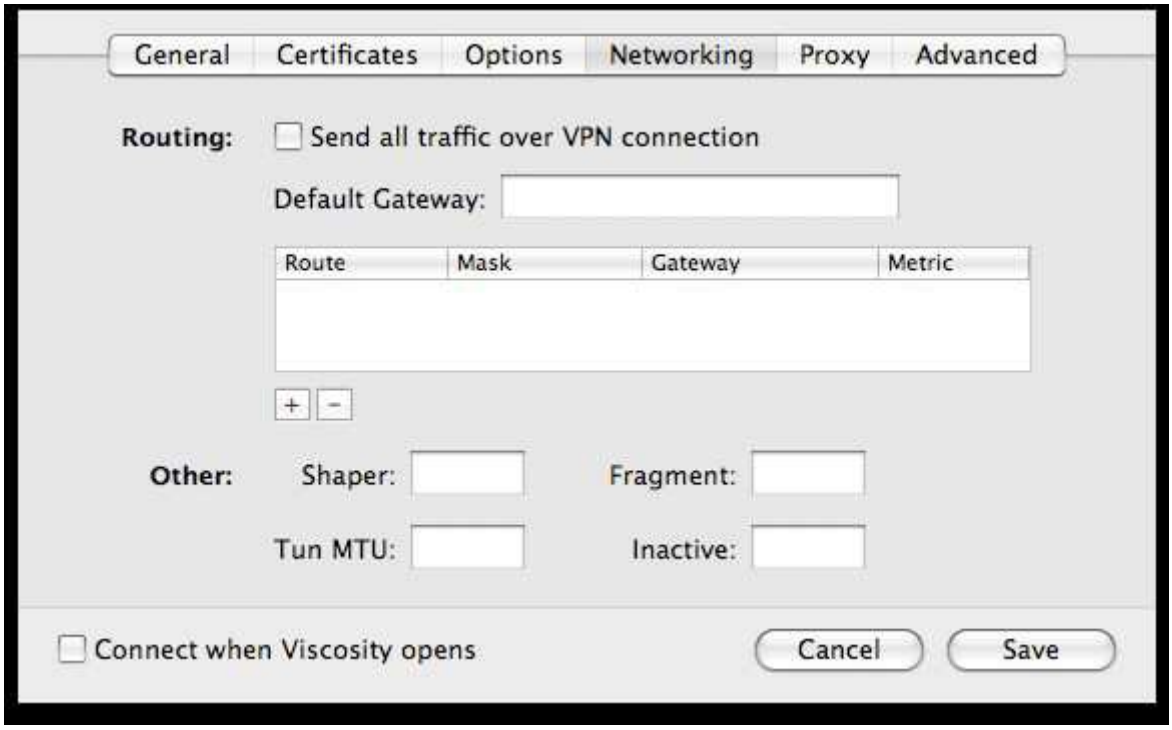

Рисунок 15.9. Конфигурирование Viscosity: работа с сетью.

На закладке Networking (Рисунок 15.9. "Конфигурирование Viscosity: работа с сетью"), основной интерес представляет опция Send all traffic over VPN connection. Если вы хотите направлять весь трафик через VPN – установите этот флаг. Остальные вкладки конфигурирования можно оставить по умолчанию практически во всех конфигурациях. Когда завершите настройку, нажмите кнопку Save для завершения конфигурирования.

Закройте экран настройки, и нажмите кнопку [Lock] и имя вашего VPN соединения для установки соединения, как показано на рисунке 15.10, "Соединение Viscosity".

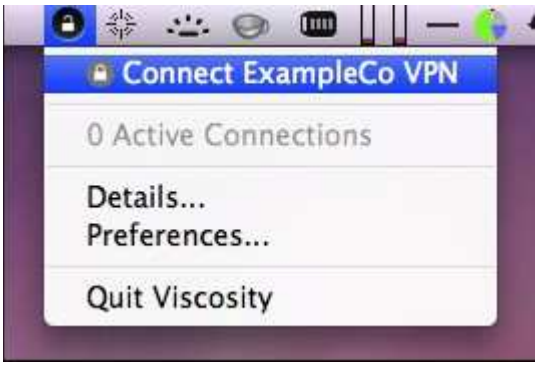

Рисунок 15.10, "Соединение Viscosity".

Через несколько секунд кнопка [Lock] станет зелёной, что говорит об успешности соединения. Нажмите на неё, и щёлкните Details, как показано на рисунке 15.11, "Меню Viscosity", чтобы посмотреть информацию о соединении. На первом экране (Рисунок 15.12, "Детали соединения Viscosity"), вы увидите статус соединения, время соединения, IP адрес назначенный клиенту и IP адрес сервера. В верхней части экрана отображается график использования полосы пропускания. При нажатии стрелок вверх/вниз в середине информационного экрана, вы можете увидеть статистику сетевого трафика. Она показывает трафик передаваемый через туннель (TUN/TAP In and Out), а так же общий TCP/UDP трафик включая накладные расходы на туннелирование и шифрование. Для соединений использующих в основном небольшие пакеты, накладные расходы значительны для всех решений VPN.

Если у вас возникают проблемы, вы можете посмотреть журналы Viscosity или обратиться к разделу 15.11, "Устранение неполадок OpenVPN".

15.5. Пример конфигурации OpenVPN Site-to-Site

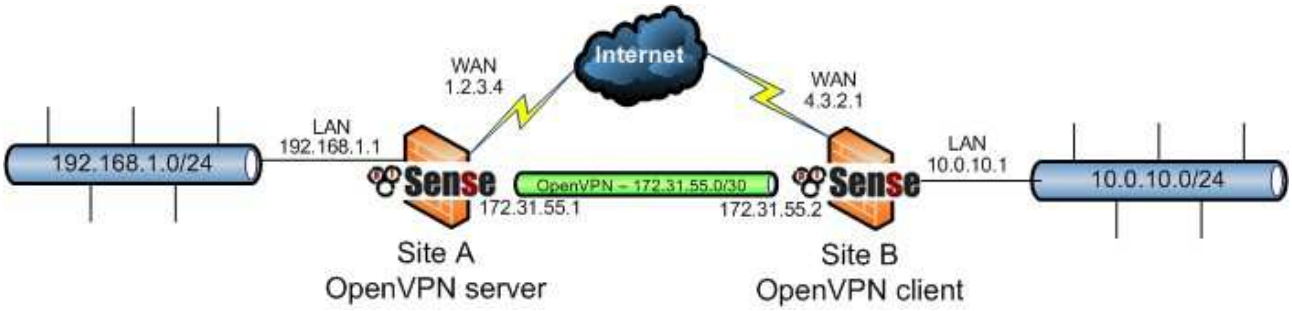

Рисунок 15.15. Пример OpenVPN сети site-to-site

Этот раздел описывает процесс настройки соединений site-to-site использующим общие ключи. При настройке соединения OpenVPN в такой схеме, один брандмауэр является сервером, а другой клиентом. Обычно, головной офис является сервером, а удалённый выступает в качестве клиента, хотя обратная конфигурация будет равнозначной. Дополнительно, к подсетям обеих сторон соединения, конфигурация удалённого доступа OpenVPN будет использовать выделенную подсеть для соединения OpenVPN между сетями. Пример конфигурации изображён на рисунке 15.15., "Пример OpenVPN сети site-to-site". 172.31.55.0/30 используется в качестве адресного пула. Туннель OpenVPN между двумя брандмауэрами получает IP адреса из этой подсети на каждом конце, что и показано на рисунке. Следующий раздел описывает процесс настройки сервера и клиента соединения.

15.5.1. Конфигурирование на стороне сервера

На странице VPN->OpenVPN нажимаем [+] на закладке Server. Конфигурируем следующие поля (пропущенные оставляем по умолчанию):

- Address pool (Адресный пул) – Здесь вводим 172.31.55.0/30
- Remote network (Удалённая сеть) – Вводим 10.0.10.0/24
- Shared key (Общий ключ) – Вставьте общий ключ для этого соединения. Инструкции по генерации общего ключа предоставлены в разделе 15.2.1., "Генерация общих ключей".
- Description (Описание) – Введите понятное описание соединения.

Это все настройки, которые требуется произвести на сервере OpenVPN для работы данного сценария. Нажмите кнопку Save.

Далее, вам необходимо добавить правила брандмауэра для WAN, позволяющие доступ к серверу OpenVPN. Укажите протокол UDP, IP источника как IP адрес клиента если он имеет статический IP, или any, если IP клиента динамический. Назначением является WAN адрес и порт назначения 1194.

Рисунок 15.16., "Пример правил брандмауэра для WAN в конфигурации site-to-site OpenVPN", демонстрирует правило брандмауэра использованное в данном примере.

Рисунок 15.16., "Пример правил брандмауэра для WAN в конфигурации site-to-site OpenVPN"

После добавления правила брандмауэра примените изменения. На этом конфигурация сервера завершается.

15.5.2. Конфигурирование стороны клиента

На стороне клиента, перейдите на страницу VPN->OpenVPN и нажмите [+] на закладке Client. Конфигурируем следующие поля (пропущенные оставляем по умолчанию):

- Server address (Адрес сервера) – Введите публичный IP адрес или имя хоста для сервера OpenVPN.
- Remote Network (Удалённая сеть) – Введите 192.168.1.0/24
- Shared key (Общий ключ) – Вставьте общий ключ для соединения, используя тот же ключ что и на стороне сервера.
- Description (Описание) – Введите понятное описание для соединения.

После заполнения всех полей нажмите Save. Конфигурирование клиента завершено. На стороне клиента нет необходимости в добавлении правил брандмауэра, поскольку клиент только инициирует исходящие соединения. Сервер никогда не инициирует соединение с клиентом.

Примечание

При конфигурации PKI удалённого доступа, часто не определяют маршруты и другие параметры конфигурации на стороне клиента, а предоставляют эти опции клиенту с сервера. При развёртывании с общими ключами, вам необходимо (по мере необходимости) определить маршруты и иные параметры на обоих концах (как описано ниже в разделе 15.10., "Специальные опции конфигурации"), поскольку вы не сможете передать эти параметры с клиента серверу при использовании общих ключей.

15.5.3. Тестирование соединения

Конфигурирование завершено и соединение должно активироваться сразу после сохранения конфигурации на стороне клиента. Попробуйте выполнить ping с удалённого конца подключения. Если возникают проблемы обратитесь к разделу 15.11., "Устранение неполадок OpenVPN".

15.6. Фильтрация и NAT с OpenVPN соединениями

По умолчанию, pfSense добавляет правила для интерфейсов tun или tap используемыми OpenVPN для разрешения всего трафика к/от клиентов OpenVPN. Если вы планируете фильтровать трафик клиентов OpenVPN, вам необходимо отметить флаг Disable all auto-added VPN rules (Отключить все автоматически добавляемые правила VPN) на странице System->Advanced (смотрите раздел 12.3., "Правила VPN и Брандмауэра" прежде чем произвести это изменение настройки). Затем, вы назначаете интерфейс OpenVPN на интерфейс OPT и соответственно конфигурируете его. Этот раздел описывает, как выполнить фильтрацию и NAT для клиентов OpenVPN.

15.6.1. Назначение и конфигурирование интерфейса

Перейдите на страницу Interfaces->Assign и назначьте соответствующий tun или tap интерфейс в качестве интерфейса OPT. Если у вас имеется только одно подключение OpenVPN и вы не используете мост, как описано в разделе 15.9., "Мост OpenVPN соединений", ваш интерфейс OpenVPN – tun0. Если у вас несколько соединений, и требуется NAT или фильтрация входящего трафика клиентов OpenVPN, вам необходимо указать устройство которое будет использоваться для каждого соединения в поле специальных настроек, как описано в разделе 15.10.2., "Указание интерфейса". У вас будет один настроенный OPT интерфейс на каждый сервер и клиент OpenVPN. Рисунок 15.17., "Назначение интерфейса tun0", показывает назначение tun0 на OPT.

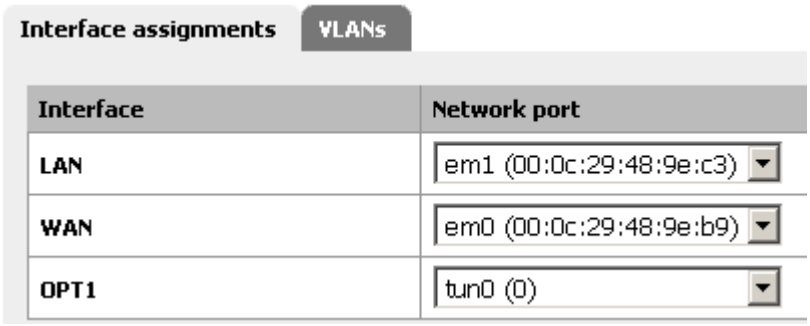

Рисунок 15.17., "Назначение интерфейса tuno"

Теперь перейдите на страницу интерфейса для ранее назначенного интерфейса, Interfaces->OPT1 для примера показанного на рисунке 15.17, "Назначение интерфейса tuno". Сначала отметьте флаг Enable interfaces в верхней части страницы, и введите соответствующее описание в поле Description. В поле IP address введите none. Эта уловка позволяет не конфигурировать любую информацию IP для интерфейса, поскольку OpenVPN самостоятельно должен конфигурировать эти настройки на интерфейсе tuno. Нажмите Save для применения этих изменений. Это не повлечёт никаких изменений в функционировании OpenVPN, а просто сделает интерфейс доступным для правил брандмауэра и целей NAT.

15.6.2. Фильтрация с OpenVPN

Теперь, когда у вас есть назначенный интерфейс OpenVPN, перейдите на страницу Firewall->Rules и нажмите на закладку назначенного интерфейса OpenVPN. Здесь вы можете добавить правила брандмауэра аналогично любому другому интерфейсу, которые будут распространяться на трафик клиентов OpenVPN. Помните, что если вы не установили флаг Disable all auto-added VPN rules на странице System->Advanced, вы позволите автоматически добавлять правила для интерфейса, которые будут перекрывать любые правила используемые нами. Более подробную информацию о правилах брандмауэра вы можете найти в главе 6, "Брандмауэр".

15.6.3. NAT с OpenVPN

Если вы хотите использовать NAT для ваших клиентов OpenVPN к вашему WAN IP, так чтобы они могли получать доступ в Интернет используя соединение OpenVPN, вам необходимо включить Advanced Outbound NAT и указать правило Outbound NAT для адресного пула подсети(ей). смотрите раздел 7.6., "Исходящий NAT" для получения большей информации о исходящем NAT.

Когда интерфейс OpenVPN назначен, правила NAT могут применяться так же как и для любых других интерфейсов. Это полезно, когда необходимо соединить две конфликтующие сети. Если у вас имеются две сети использующие подсети LAN

192.168.1.0/24 которые необходимо соединить в конфигурации VPN site-to-site, они не смогут взаимодействовать через VPN без NAT (или моста, как рассматривалось в разделе 15.9., "Мост соединений OpenVPN", который в реальности может использоваться только для мобильных клиентов, а не в конфигурации site-to-site). Хосты подсети 192.168.1.0/24 никогда не достигнут другого конца соединения с удалённой подсетью 192.168.1.0/24, поскольку сеть всегда рассматривается как локальная. Однако используя NAT, вы можете заставить функционировать удалённую сторону так, как будто она находится в отличной IP подсети.

Замечание

Всё это будет прекрасно работать для множества протоколов, но для некоторых, как правило желательных для соединения VPN, и прежде всего общих файлов SMB/CIFS, это не будет работать в комбинации с NAT. Если вы используете протокол, который не может функционировать с NAT – данное решение является не приемлемым. Рисунок 15.18., "Site-to-site для конфликтных подсетей" показывает пример где обе конечные подсети используют ту же самую подсеть. После назначения интерфейса tun на интерфейс OPT на обеих сторонах, как описано в разделе 15.6.1., "Назначение и конфигурирование интерфейса", может быть применён NAT 1:1.

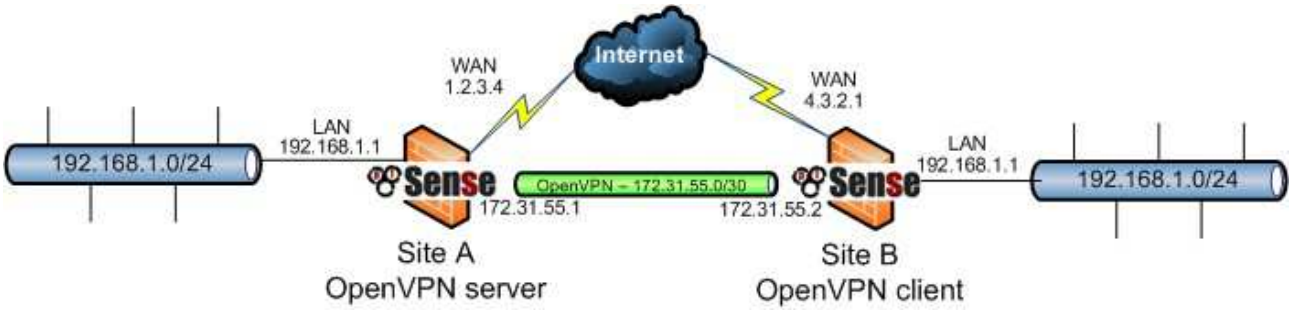

Рисунок 15.18., "Site-to-site для конфликтных подсетей"

Трафик Site A будет транслироваться в 172.16.1.0/24, а Site B будет транслироваться в 172.17.1.0/24. запись 1:1 NAT будет добавлена на каждый конец соединения для трансляции всего диапазона /24. Для достижения Site A с Site B будут использоваться адреса 172.16.1.x. Последний октет в 192.168.1.x будет транслироваться в последний октет 172.16.1.x, следовательно, чтобы попасть на 192.168.1.10 Site A с Site B, вы должны использовать 172.16.1.10. Для достижения 192.168.1.50 Site B с Site A, вы должны использовать 172.17.1.50. рисунок 15.19., "Конфигурация Site A 1:1 NAT" и рисунок 15.20., "Конфигурация Site B 1:1 NAT", показывают конфигурацию 1:1 NAT для каждой из сторон, где интерфейс tun назначен на OPT2.

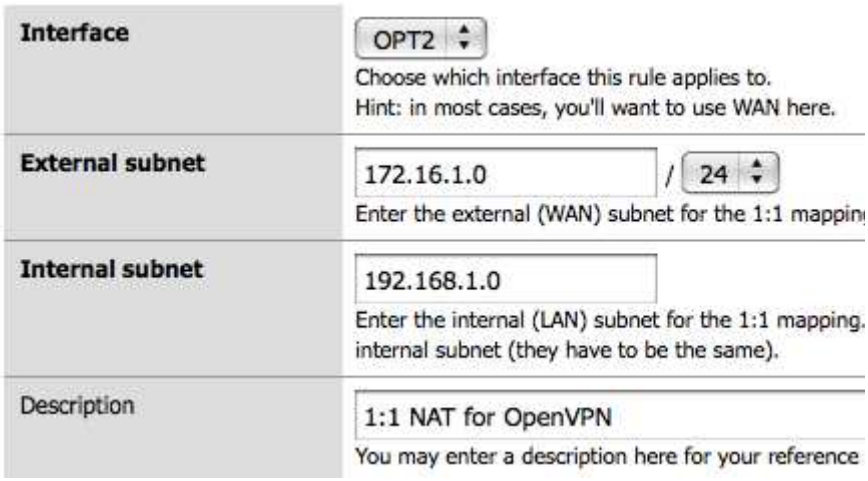

Рисунок 15.19., "**Конфигурация** Site A 1:1 NAT"

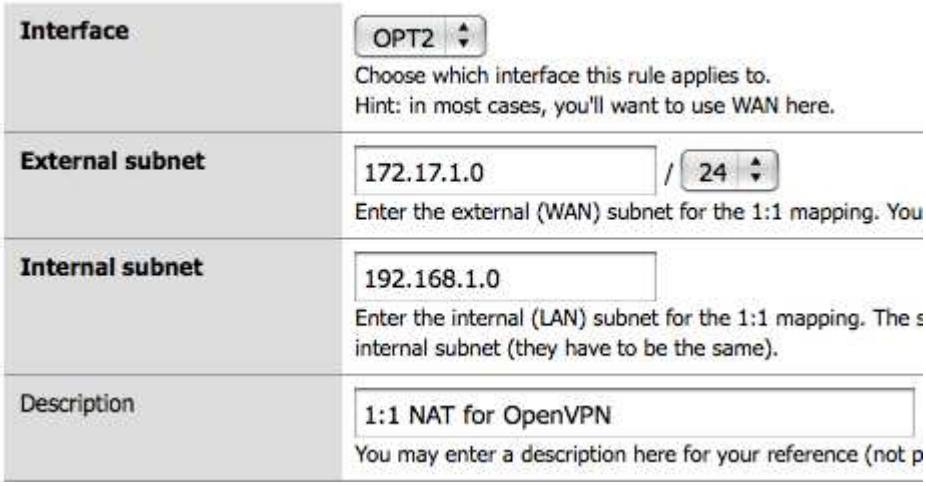

Рисунок 15.20., "**Конфигурация** Site B 1:1 NAT"

В конфигурации OpenVPN для обеих сторон, должны быть указаны Remote network как транслируемые IP подсети, а не как 192.168.1.0/24. В данном примере, Remote network на Site A – 172.17.1.0/24, а на Site B – 172.16.1.0/24. после применения изменений конфигурации NAT и соответствующей настройке Remote Network с обеих сторон, сети смогут взаимодействовать используя транслируемые подсети.

15.7. OpenVPN и multi-WAN

OpenVPN совместим с multi-WAN, с рядом оговорок при некоторых обстоятельствах. Этот раздел рассматривает некоторые соображения относящиеся к конфигурированию сервера OpenVPN при использовании множества WAN и конфигурированию клиента.

15.7.1. Сервер OpenVPN и multi-WAN

Сервер OpenVPN может использоваться с любым соединением WAN, хотя возможности этого будут варьироваться в зависимости от вашей конкретной конфигурации.

15.7.1.1. Сервер OpenVPN использующий TCP

Поскольку, TCP, как правило, не является предпочтительным протоколом для OpenVPN, о чем мы уже говорили в данной главе, использование TCP упрощает настройку OpenVPN для multi-WAN. OpenVPN сервер использующий TCP будет работать на всех WAN, для которых правила брандмауэра позволяют трафик OpenVPN сервера. Вам потребуется правило для каждого WAN интерфейса.

15.7.1.2. Сервер OpenVPN использующий UDP

Сервер OpenVPN использующий UDP так же способен работать с multi-WAN, но с некоторыми оговорками, которые не применимы к TCP, поскольку multi-WAN использует функции маршрутизации PF. Каждый WAN должен иметь свой сервер OpenVPN. Вы можете использовать одни и те же сертификаты для всех серверов. Изменяются только две части конфигурации OpenVPN.

15.7.1.2.1. Address Pool(Адресный пул)

Каждый сервер должен иметь уникальный адресный пул, не пересекающийся с любыми другими пулами адресов или внутренними подсетями.

15.7.1.2.2. Локальные специальные настройки (Custom Option)

Каждому серверу OpenVPN в специальных настройках необходимо указать IP WAN интерфейса с которым он будет использоваться. Следующий пример показывает, как сконфигурировать OpenVPN для WAN IP 1.2.3.4.

```
local 1.2.3.4
```

Для соединения с динамическим IP, альтернативно можно указать имя хоста. Следующий пример показывает как это сделать для мени хоста openvpn.example.com.

```
local openvpn.example.com
```

15.7.1.2.3. Автоматическая отказоустойчивость для клиентов (Automatic Failover for Clients)

На клиентах OpenVPN могут быть настроены несколько удалённых серверов. Если первый сервер не может быть разрешён, будет использован второй. Это может использоваться в комбинации с развёртыванием multi-WAN OpenVPN для предоставления автоматической отказоустойчивости для клиентов. Если ваши сервера OpenVPN работают на IP 1.2.3.4 и 4.3.2.1, и оба используют порт 1194, строки remote в конфигурации клиента должны быть следующие:

```
remote 1.2.3.4 1194
```

remote 4.3.2.1 1194

Для клиентов настроенных на pfSense, первая строка remote настраивается посредством GUI. Вторая строка remote указывается в поле Custom options.

15.7.2. Клиенты OpenVPN и multi-WAN

Клиенты OpenVPN, настроенные на брандмауэре, при подключении к серверу OpenVPN, будут следовать системной таблице маршрутизации. Это означает, что по умолчанию, все клиенты будут использовать интерфейс WAN. Для использования интерфейса OPT WAN, необходимо ввести статический маршрут, для направления трафика на удалённый конец соединения OpenVPN. Рисунок 15.21., "Пример статического маршрута для клиента OpenVPN на OPT WAN" показывает статический маршрут, необходимый для использования интерфейса WAN2 для доступа на сервер OpenVPN, работающий на IP 1.2.3.4, когда шлюз интерфейса WAN2 – 172.31.1.1.

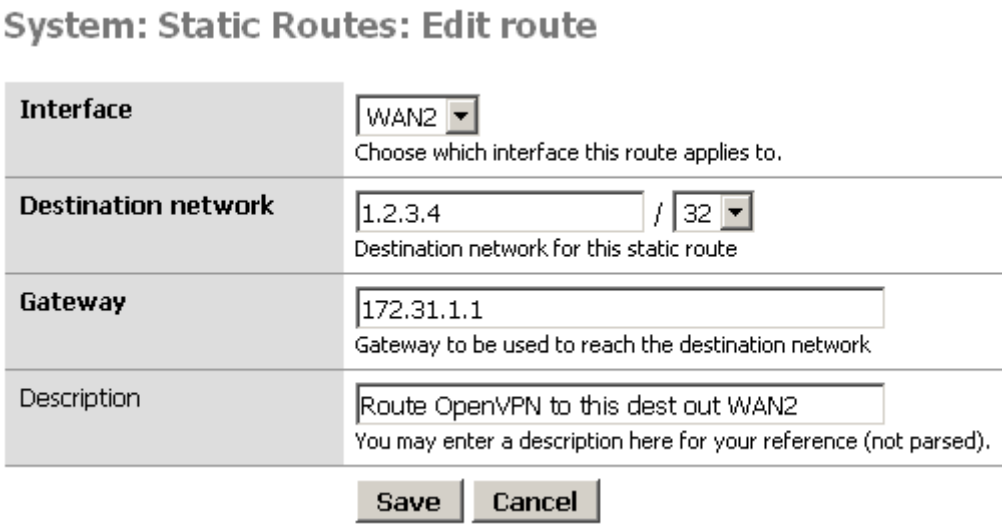

Рисунок 15.21., "Пример статического маршрута для клиента OpenVPN на OPT WAN"

15.8 OpenVPN и CARP

OpenVPN совместим с CARP. Для обеспечения высокой доступности решением OpenVPN с CARP, сконфигурируйте своих клиентов для соединения с CARP VIP, и сконфигурируйте сервер OpenVPN для использования CARP IP с локальными настройками. В pfSense 1.2.x., конфигурация OpenVPN не может синхронизироваться с резервным брандмауэром, следовательно вам необходимо вручную ввести её на оба брандмауэра. Состояние соединения между хостами не удерживается, поэтому клиенты должны переподсоединиться после сбоя, однако OpenVPN будет обнаруживать ошибки соединения и переподключаться после сбоя, через минуту или около того. Более детально, CARP обсуждается в главе 20, "Брандмауэр, избыточность/высокая доступность".

15.9. Мост соединений OpenVPN

Конфигурации OpenVPN обсуждаемые до данного момента были маршрутизируемыми, и использовали интерфейс tun. Как правило, это предпочтительный способ подключения клиентов VPN, но кроме этого, OpenVPN имеет возможность использования tap-интерфейса и мостового подключения клиентов непосредственно в вашу LAN или другие внутренние сети. Это позволит удалённым клиентам непосредственно оказаться в вашей локальной сети. Однако, GUI pfSense не был расчитан на подобный сценарий. Существовал хак, который некоторые использовали, однако он имел серьёзные проблемы. В какой то момент такая возможность будет доступна – обратитесь на http://doc.pfsense.org/index.php/OpenVPN_Bridging для получения свежей информации по мостам OpenVPN.

15.10 Специальные настройки конфигурации (Custom configuration options)

OpenVPN предоставляет множество вариантов конфигурации, выходящие за ограничения доступных полей GUI. Именно по этой причине существует поле специальной конфигурации (custom configuration). Вы можете использовать неограниченное количество дополнительных опций конфигурации, разделяя их запятой.

В этом разделе мы рассмотрим наиболее часто используемые пользовательские опции. Существует и множество других возможностей, но они используются более редко. Более подробно изучить дополнительные возможности можно на странице руководства OpenVPN, [http://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x-manpage.html]. При добавлении специальных опций следует соблюдать осторожность, поскольку входящие данные не проверяются на достоверность. Если опция используется не корректно, клиент или сервер OpenVPN могут не запуститься.

На закладке OpenVPN страницы Status->System logs, вы можете просматривать журналы OpenVPN, чтобы убедиться, что ваши опции корректны. Любые неверные опции приведут к возникновению ошибок в журнале, например: Unrecognized option or missing parameter(s), с последующей опцией, вызвавшей ошибку.

15.10.1. Опции маршрутизации

Для добавления дополнительных маршрутов конкретному клиенту или серверу OpenVPN, вы можете использовать пользовательскую конфигурацию маршрутов. Следующий пример добавляет маршрут для 10.50.0.0/24.

```
route 10.50.0.0 255.255.255.0
```

Для добавления нескольких маршрутов, их следует разделять точкой с запятой:

route 10.50.0.0 255.255.255.0;route 10.254.0.0 255.255.255.0

Опции конфигурирования маршрутов используются для локального добавления маршрутов. Для сервера OpenVPN использующего PKI, вы можете добавить маршруты для клиентов. Для передачи маршрутов 10.50.0.0/24 и 10.254.0.0/24 всем клиентам, используйте следующие опции специальной конфигурации:

push "route 10.50.0.0 255.255.255.0";push "route 10.254.0.0 255.255.255.0"

15.10.1.1. Перенаправление шлюза по умолчанию

OpenVPN позволяет изменять шлюз по умолчанию для клиента соединения OpenVPN, следовательно, весь трафик клиента будет проталкиваться через VPN. Это отличная возможность для ненадёжных локальных сетей, подобных беспроводным точкам доступа, поскольку она предоставляет защиту от многочисленных атак, являющихся значимой опасностью для ненадёжных сетей. Чтобы произвести перенаправление, добавьте следующие специальные опции:

push "redirect-gateway def1"

Так же, вы можете ввести эти опции на стороне клиента использующего перенаправленный шлюз def1 без опции push. (Обратите внимание, что после "def" следует цифра 1 а не буква "L").

15.10.2. Спецификация интерфейса

Сервера и клиенты OpenVPN используют интерфейс туннельного типа для каждого соединения. Все они автоматически управляются pfSense, но вы можете указать имя устройства которое будет использоваться. Некоторые пользователи предпочитают указывать устройство, например для назначения интерфейса OpenVPN на интерфейс OPT, чтобы иметь возможность применить правила фильтрации для входящего трафика OpenVPN. Что бы сделать это, добавьте специальные опции, такие как dev tun0. Каждый клиент и сервер OpenVPN должен использовать уникальное устройство, поэтому, для следующей конфигурации OpenVPN необходимо указать dev tun1, приращивая единицу для каждого дополнительного сервера или клиента.

15.10.3. Использование аппаратного криптоускорителя

Если у вас есть аппаратный криптоускоритель, подобный Hifn или строенному glxsb для платформы ALIX, добавьте специальную опцию engine cryptodev для его поддержки с OpenVPN. Кроме того, вы должны использовать криптографический алгоритм поддерживаемый ускорителем. Для glxsb – только AES-128-CBC. Современные карты Hifn, подобне Soekris vpn1411, поддерживают

3DES 128, 192 и 256 бит AES.

15.10.4. Указание используемого IP адреса

Локальные специальные опции позволяют указать IP-адрес сервиса OpenVPN, который будет использоваться в дальнейшем. Это может быть либо IP адрес, такой как локальный 1.2.3.4, или FQDN – local myopenvpn.dyndns.org. В основном, это используется для сценария multi-WAN, как было описано в разделе 15.7., "OpenVPN и multi-WAN" или в сочетании с CARP VIP.

15.11. Поиск и устранение неисправностей OpenVPN

Если у вас возникают некоторые проблемы при использовании OpenVPN, этот раздел содержит некоторую информацию по решению наиболее распространённых проблем с которыми сталкиваются пользователи.

15.11.1. Некоторые хосты работают, но не все

Если трафик между некоторыми хостами связанными через VPN движется нормально, а между некоторыми нет, обычно это одна из четырёх следующих проблем:

1. Отсутствуют, некорректны или проигнорированы шлюзы по умолчанию – Если устройство не имеет шлюза по умолчанию или имеет указание к чемуто иному, чем pfSense, оно не знает, как корректно двигаться к удалённой сети по VPN. Некоторые устройства, даже при указанном шлюзе по умолчанию, не используют этот шлюз. Это замечено на различных встраиваемых устройствах, в том числе IP камерах и некоторых принтерах. В данном случае, нет другого решения как поиск исправленного ПО для этих устройств. Вы можете произвести проверку, запустив tcpdump на внутреннем интерфейсе брандмауэра, к которому подключено устройство. Поиск проблем с помощью tcpdump описан в разделе 25.5., "Использование tcpdump в командной строке". Если вы наблюдаете трафик из внутреннего интерфейса, однако не наблюдаете обратных ответов – устройство не правильно маршрутизирует ответный трафик (или он может блокироваться брандмауэром).
2. Неверная маска подсети – Если на одном конце подсеть 10.0.0.0/24 а на другом 10.254.0.0/24, и хост имеет не корректную маску подсети 255.0.0.0 или /8, он никогда не сможет взаимодействовать по VPN, поскольку считает, что удалённая подсеть VPN является частью местной сети, и, следовательно, маршрутизация не будет работать должным образом.
3. Брандмауэр – Если на целевом компьютере присутствует брандмауэр, он может запрещать соединения.
4. Правила брандмауэра на pfSense – корректные правила на обоих концах соединения позволят желаемый трафик.

15.11.2. Проверяйте журналы OpenVPN

Перейдите на страницу Status->System logs и нажмите закладку OpenVPN для просмотра журналов OpenVPN. После подключения, OpenVPN будет регистрировать записи следующего вида (нумерация openvpn может отличаться ID процесса создаваемого при соединение OpenVPN):

```
openvpn[32194]: UDPv4 link remote: 1.2.3.4:1194
openvpn[32194]: Peer Connection Initiated with 192.168.110.2:1194
openvpn[32194]: Initialization Sequence Completed
```

Если, при попытке подключения, вы не видите сообщения link remote и Peer Connection Initialized, причина, скорее всего кроется в неправильной настройке клиента, и клиент не пытается подключиться к нужному серверу, или соединения блокируют некорректные настройки брандмауэра клиента.

15.11.3. Убедитесь что нет перекрытия соединениями IPsec

Из-за способа связи IPsec в ядре FreeBSD, любые включенные соединения IPsec совпадающие с локальными или удалёнными подсетями, существующими когда включается IPsec (даже если он не поднят), приводит к тому, что трафик, никогда не будет двигаться через соединение OpenVPN. Любые IPsec соединения указанные для той же локальной и удалённой сетей должны быть отключены.

15.11..4. Проверьте системную таблицу маршрутизации

Перейдите не страницу Diagnostics->Routes для просмотра добавленных маршрутов. Для VPN site-to-site, ы должны видеть маршруты для удалённой сети (сетей) на соответствующем tun или tap интерфейсе. Если маршруты отсутствуют или не корректны, ваши параметры Local Network, Remote Network или специальные настройки неверны. Если вы используете установку с общими ключами, а не PKI, убедитесь, что вы не использовали команду push вместо добавления маршрутов на обоих концах, а использовали route, как описано в разделе 15.10.1., "Опции маршрутизации".

15.11.5. Тестирование с различных точек

Если соединение показано в журналах как поднятое, но не работает из LAN, попробуйте проверить его с помощью ping с брандмауэра, сначала с внутреннего интерфейса, используемого для соединения OpenVPN (обычно LAN). Если это не работает, зайдите на брандмауэр по SSH и выберите опцию 8 для перехода в режим командной строки. Запустите ping x.x.x.x из командной строки, заменив x.x.x.x на IP удалённой стороны VPN. Это поможет сузить поиск проблем с маршрутизацией на удалённой сети.

15.11.6. Отслеживание трафика с помощью tcpdump

Использование tcpdump позволяет увидеть трафик и является одним из самых полезных методом устранения неполадок. Начните с внутреннего интерфейса (обычно LAN) на стороне инициирующей трафик, затем на tun интерфейсе этого брандмауэра, далее на tun интерфейсе удалённого брандмауэра, и наконец на внутреннем интерфейсе удалённого брандмауэра. Захват пакетов подробно описан в главе 25, "Захват пакетов".