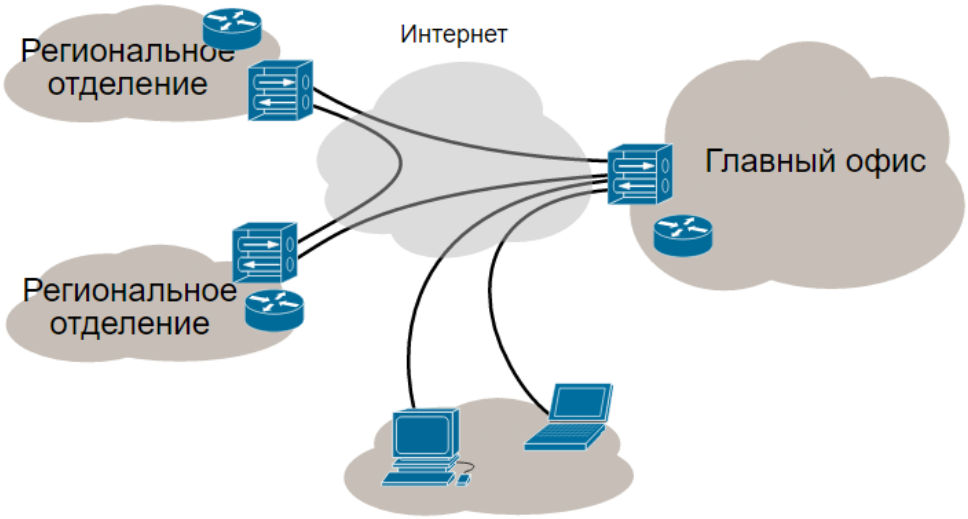
SMART-SOFT
ГРУППА КОМПАНИЙ

TRAFFIC INSPECTOR NEXT GENERATION

Настройка виртуальных частных сетей (VPN)

www.smart-soft.ru

1. Вступление



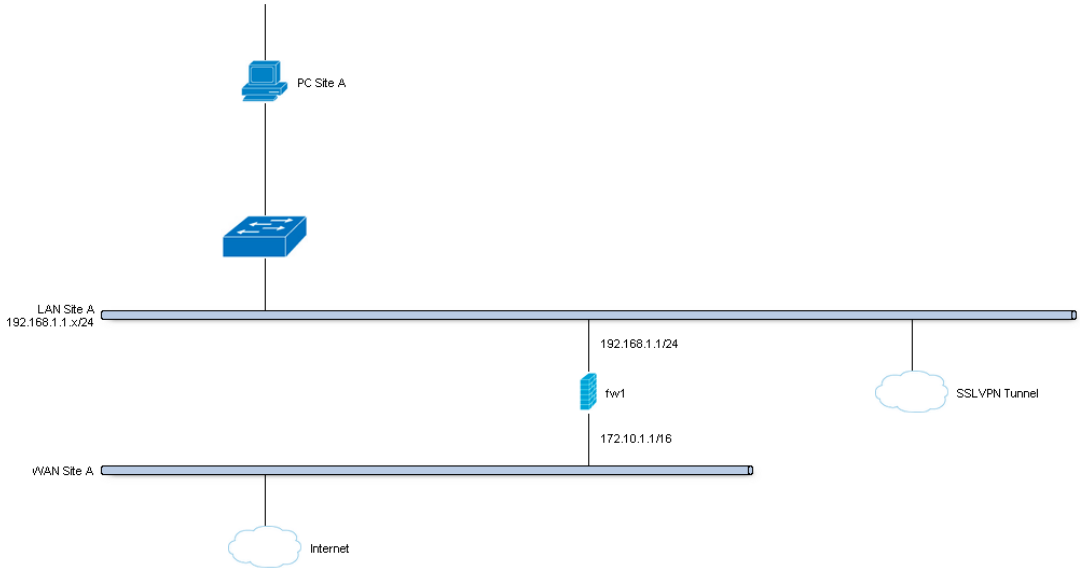
Для минимизации затрат при объединении географически удаленных филиалов используют технологию VPN (расшифровывается как Virtual Private Network или виртуальная частная сеть). В каждом филиале есть своя сеть, и устанавливается свой пограничный маршрутизатор (устройство Traffic Inspector Next Generation), через который осуществляется подключение к сети Интернет. Между пограничными маршрутизаторами также, настраиваются шифрованные туннели для взаимодействия между компьютерами филиалов. Пакет, генерируемый компьютером в одном из филиалов и предназначенный компьютеру в другом филиале, достигает пограничный маршрутизатор и, согласно таблице маршрутизации, высылается с туннельного интерфейса, что подразумевает его шифровку и инкапсуляцию в другой (инкапсулирующий) пакет. Инкапсулирующий пакет доставляется декапсулятору (т.е. пограничному маршрутизатору удаленного филиала) по публичному Интернету. Декапсулятор извлекает инкапсулированный пакет, осуществляет его дешифровку и маршрутизирует по направлению к компьютеру, которому адресован пакет. Таким образом, технология VPN использует публичный Интернет в качестве средства доставки IP-трафика разнесенных филиальных сетей. Конфиденциальность данных при их передаче через публичный Интернет обеспечивается за счет шифрации / дешифрации, осуществляемой пограничными маршрутизаторами. Помимо подключения типа «сайт - сайт» описанного выше, технология может также использоваться для подключения удаленных сотрудников к корпоративной сети (подключения типа «узел - сайт»).

В данной инструкции мы рассмотрим настройку популярной, кроссплатформенной технологии OpenVPN для объединения двух офисов в режиме «сайт - сайт». Перед тем как начинать настройку OpenVPN SSL туннеля убедитесь, что маршрутизаторы Traffic Inspector Next Generation имеют адекватные сетевые настройки. Также, за каждым из маршрутизаторов располагается уникальная IP-подсеть - между этими сетями будет настроена маршрутизация через VPN-туннель.
Обычно, в режиме «сайт-сайт» две географически разнесенные сети взаимодействуют через «белые» IP-адреса. В нашем примере мы используем «серые» IP-адреса на WAN-адаптерах. Traffic Inspector Next Generation, по умолчанию, запрещает прием пакетов с «серыми» адресами со стороны WAN-интерфейсов, и этот функционал нужно выключить для нашего примера. Для этого, пройдите в Интерфейсы -> [WAN] и уберите флаг «Блокировать частные сети» (Не забудьте сохранить и применить настройки).

Сетевые настройки маршрутизаторов в локации А и Б приведены ниже.

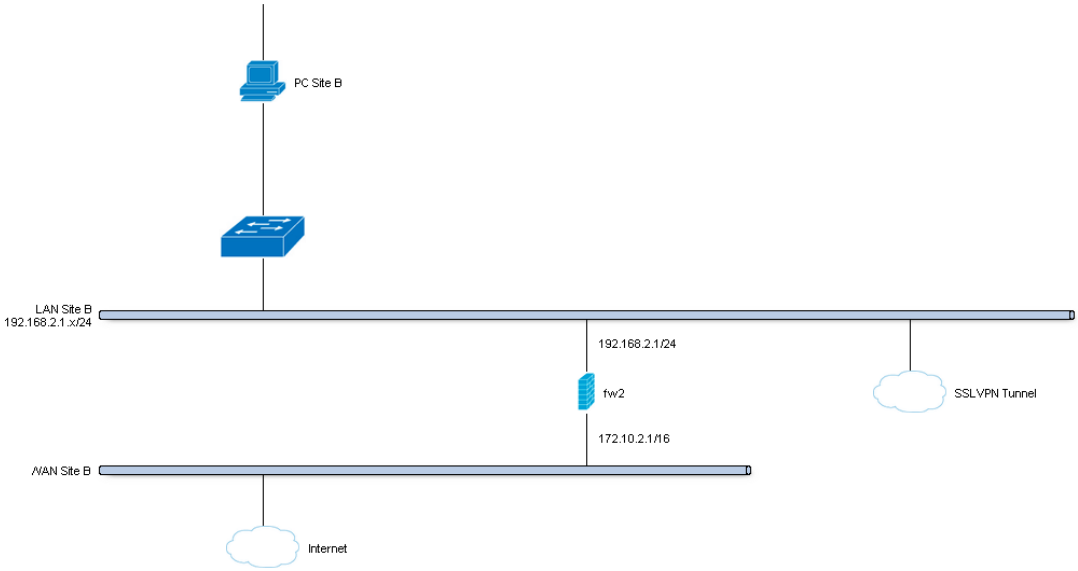
Маршрутизатор в локации A

Имя хоста	fw1
WAN IP	172.10.1.1/16
LAN IP	192.168.1.1/24
DHCP-диапазон для LAN	192.168.1.100-192.168.1.200
Туннельная сеть	10.10.0.0/24

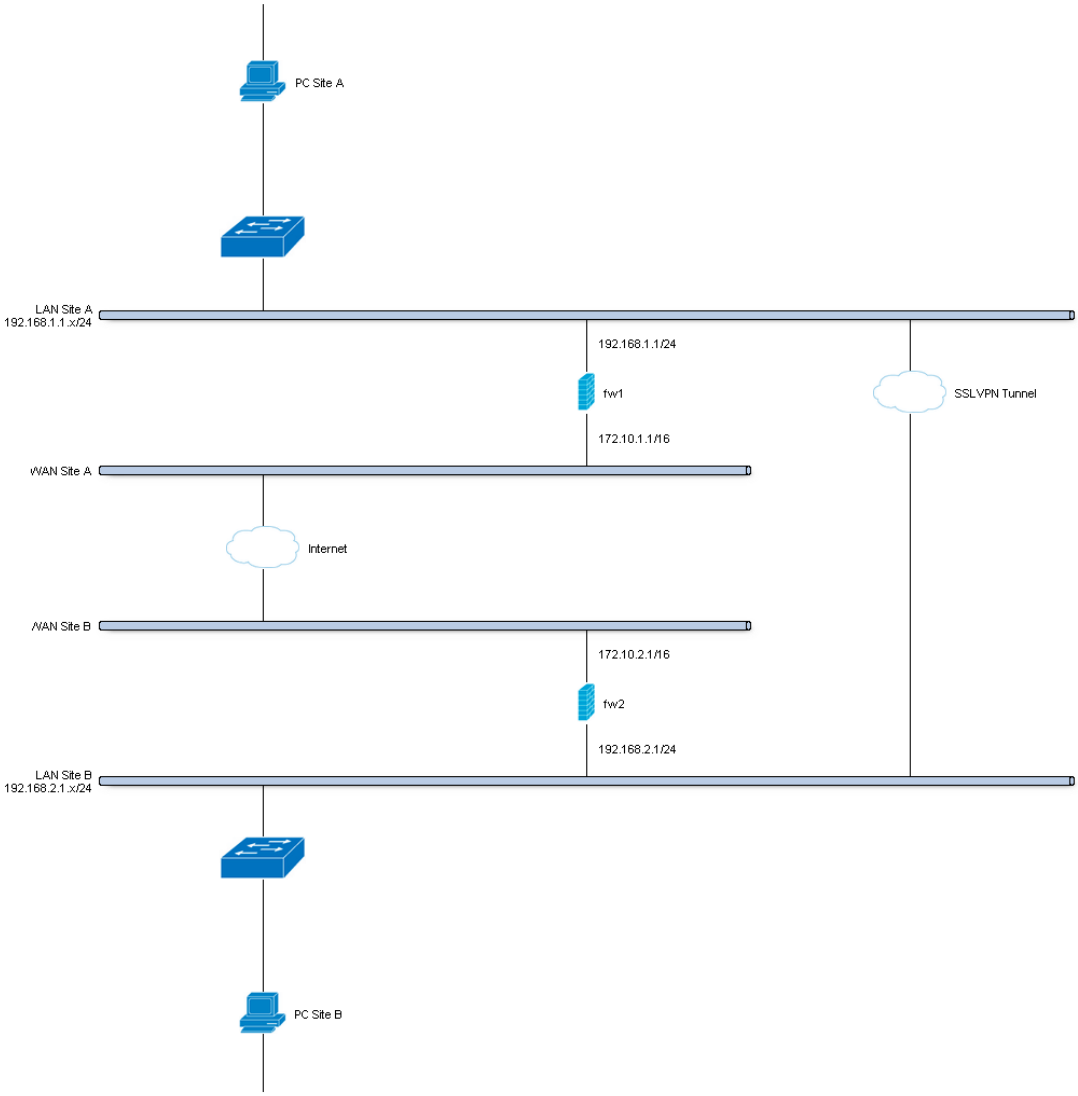


Маршрутизатор в локации Б

Имя хоста	fw2
WAN IP	172.10.2.1/16
LAN IP	192.168.2.0/24
DHCP-диапазон для LAN	192.168.2.100-192.168.2.200
Туннельная сеть	10.10.0.0/24



Полная схема VPN-сети



2. Настройка

2.1 Настройка VPN-сервера

Пройдите в VPN -> OpenVPN -> Серверы и кликните на Добавить сервер в верхнем правом углу формы. Используйте следующие настройки (настройки, которые мы опускаем, должны остаться по умолчанию):

Режим сервера	Пиринговая сеть (общий ключ)
Протокол	UDP
Режим работы устройства	tun
Интерфейс	WAN
Локальный порт	1194
Описание	SSL VPN Server
Совместно используемый ключ	Установите флажок для генерации нового ключа
Алгоритм шифрования	AES-256-CBC (256-bit)
Дайджест-алгоритм аутентификации	SHA512 (512-bit)
Hardware Crypto	Без аппаратного ускорения криптоалгоритмов
Туннельная сеть IPv4	10.10.0.0/24
Локальная сеть/сети IPv4	192.168.1.0/24
Удаленная сеть/сети IPv4	192.168.2.0/24
Сжатие	Включено с использованием адаптивного сжатия

Нажмите Сохранить для добавления нового сервера.

2.2 Копирование совместно используемого ключа

После создания нового сервера, в его настройках генерируется ключ, который также нужно прописать на противоположной стороне туннеля.

Для копирования ключа, щелкните на иконку «карандаш» напротив ранее созданного VPN-сервера.

Сохраните данный ключ и никому его не рассказывайте!

Пример того, как выглядит ключ:

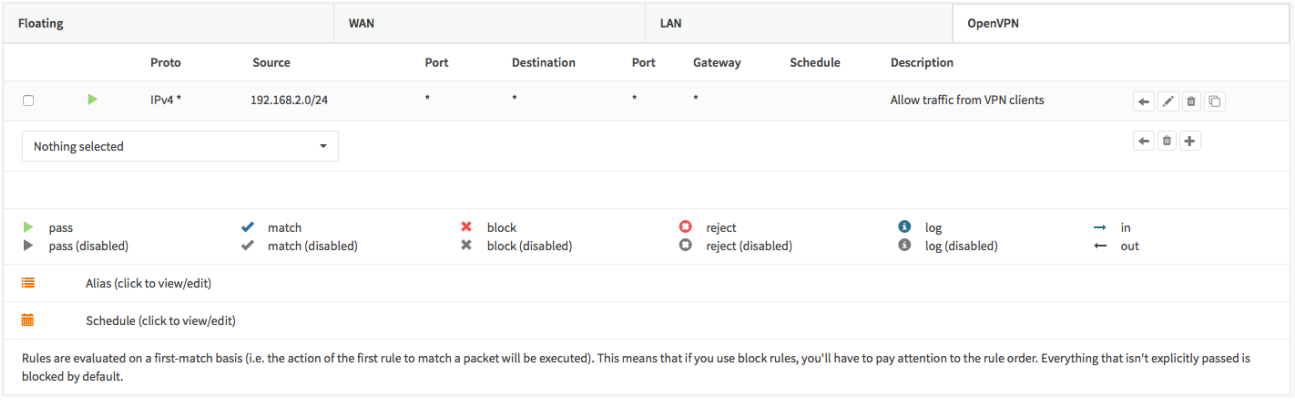
```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
0960c87c3aafa8f306fe270c1564380b
7922543563a17b5d2636b4ef9412dd09
9ad44974ca1b293963e0f8ac9cbdd97c
2c31bf35f0df45c9e928ccb033e6d51d
2caaec02d649ad081c68d7bc7d28030e
9182c9597a83024097bea860e52d9c66
1b9e0048fbf951ce8659bc56edb7f9a1
14f7740fc9231a3750557e02eb112712
ac4b9980d4c740ec96a4357f3940ed90
d1bbf8eed3de135c886fe2eff8e8b943
ab1f52b59def4c9ebeacc5eb48425189
c43887a6237c29e0724f5f45a0f70635
10680bec8bfb67c21bf2b4866268594c
9ba093668064f9a898e6a6ad103b401d
b2047132f0dc8db2230db38444d689fa
ddba46bf6f892ae90c59415f94b82750
-----END OpenVPN Static key V1-----
```

2.3 Создание правил сетевого экрана

Для прохождения VPN-трафика от удаленной стороны, нам нужно разрешить доступ к порту OpenVPN-сервера на WAN-интерфейсе. В случае, когда удаленных офисов будет много, нужно будет открывать порты для каждого из них.

Создадим разрешающее правило в разделе Сетевой экран -> Правила на вкладке WAN для протокола UDP и порта 1194 (именно его использует первый экземпляр OpdenVPN-сервера).

Далее, создадим разрешающее правило в разделе Сетевой экран -> Правила на вкладке OPENVPN для прохождения трафика из удаленной филиальной сети (192.168.2.0/24). В нашем примере, мы разрешаем удаленным клиентам доступ к любому компьютеру в нашей локальной сети, однако, вы можете разрешить доступ только к одному или нескольким локальным IP-адресам.



Настройка в локации А завершена.

2.4 Настройка сервера в локации Б

На втором устройстве Traffic Inspector Next Generation пройдите в раздел VPN-> OpenVPN-> Клиенты и кликните по Добавить клиента в верхнем правом углу формы.

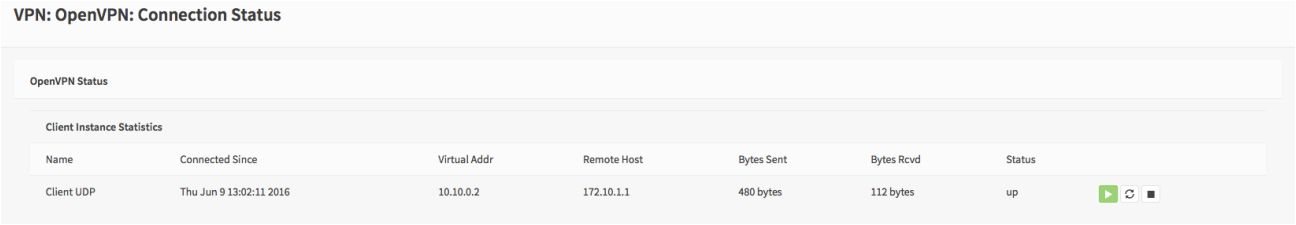
Примечание. Несмотря на то, что мы настраиваем подключение типа «сайт - сайт», только маршрутизатор в центральном офисе настраивается как «VPN-сервер», маршрутизаторы в остальных филиалах настраиваются как «VPN-клиенты».

Используйте следующие настройки (настройки, которые мы опускаем, должны остаться по умолчанию):

Режим сервера	Пиринговая сеть (общий ключ)
Протокол	UDP
Режим работы устройства	tun
Интерфейс	WAN
Адрес сервера	172.10.1.1
Порт сервера	1194
Описание	SSL VPN Client
Совместно используемый ключ	Уберите флажок и вставьте ключ, скопированный с маршрутизатора, настроенного как «VPN-сервер»
Encryption algorithm	AES-256-CBC (256-bit)
Auth Digest Algorithm	SHA512 (512-bit)
Hardware Crypto	Без аппаратного ускорения криптоалгоритмов
IPv4 Tunnel Network	10.10.0.0/24
IPv4 Remote Network/s	192.168.1.0/24
Сжатие	Включено с использованием адаптивного сжатия

Кликните Сохранить для применения настроек.

Статус соединения можно посмотреть в разделе VPN-> OpenVPN-> Статус соединения.



2.5 Настройка правил сетевого экрана на сервере в локации Б

Далее, создадим разрешающее правило в разделе Сетевой экран -> Правила на вкладке OPENVPN для прохождения трафика из удаленной филиальной сети (192.168.1.0/24).