SMART-SOFT
ГРУППА КОМПАНИЙ

TRAFFIC INSPECTOR NEXT GENERATION

Traffic Inspector Next Generation
для бизнес-организаций

Содержание

1. Компьютерные сети в бизнес-организации

Предприятия и компании по всему миру используют Интернет для электронной коммуникации, для быстрого доступа к информации, для связи географически удаленных филиалов, для организации работы удаленных сотрудников, наконец, для рекламы и продажи своей продукции. Вместе с тем, у всех достоинств Интернета есть и обратная сторона – возросшие риски в сфере информационной безопасности и сложности, связанные с контролем сетевого трафика. Проблемы, с которыми сталкиваются бизнес-предприятия, включают:

- Организация доступа к сети Интернет для корпоративной сети
- Защита от Интернет-угроз
- Борьба с нецелевым использованием Интернета
- Построение VPN-сети для подключения удаленных офисов
- Управление пропускной способностью Интернет-канала
- Обеспечение гостевого доступа в Интернет

Все обозначенные проблемы можно решить с помощью Traffic Inspector Next Generation – программно-аппаратного решения нового поколения от российской компании Смарт-Софт. Рассмотрим типичный сценарий применения Traffic Inspector Next Generation в сети бизнес-организации и настройку актуального функционала:

- Настройка сетевого экрана и NAT
- Настройка веб-фильтрации
- Настройка OpenVPN
- Настройка шейпера
- Настройка гостевой сети

2. Доступ бизнес-организации к сети Интернет

Большинство организаций, активно использующих в своей работе Интернет, сталкиваются с проблемой «раздачи» Интернета на все компьютеры во внутренней сети. То, что в простой речи называется «раздать Интернет», более технически верно обозначается термином «NAT». NAT расшифровывается как **network address translation** или **преобразование сетевых адресов**.

В наиболее общем сценарии, организации выделяется один «белый» IP-адрес, который присваивается WAN-адаптеру шлюза TI NG. Компьютеры внутренней сети настраиваются с использованием диапазона «серых» IP-адресов (RFC 1918). Для того чтобы работать в Интернете, компьютеры внутренней сети должны иметь «белые» адреса. Компьютеры внутренней сети таких адресов не имеют и, если нужно взаимодействовать с компьютерами в Интернете, отсылают свой трафик через шлюз TI NG. Шлюз не только маршрутизируют пакеты, но еще и переписывает адрес источника (и, если необходимо, порт источника) в этих пакетах. За счет этого, компьютеры внутренней сети, фактически, работают в Интернете под «белым» IP-адресом WAN-адаптера шлюза. Сам шлюз также сохраняет возможность работать с этого адреса. Шлюз TI NG отслеживает соединения и осуществляет прямые и обратные преобразования трафика.

Механизм NAT позволяет множеству компьютеров работать в Интернет под одним «белым» IP-адресов и дополнительно защищает внутреннюю сеть от несанкционированных обращений из Интернета. С другой стороны, возможность обращения к компьютерам внутренней сети из Интернета затруднена и требует дополнительной настройки, которая известна как «проброс портов».

Шаг 1 – Настройка NAT

В Traffic Inspector Next Generation настройки NAT доступны в разделе **Межсетевой экран-> NAT** на вкладке **Исходящий**. По умолчанию, здесь настроена опция **Автоматическое создание NAT правил для исходящего трафика (нельзя использовать созданные вручную правила)**. При данной настройке, к любому трафику из внутренней сети офиса автоматически применяется сначала прямое

преобразование адреса источника (и, если необходимо, порта источника), а для возвращающего трафика, принадлежащего данному соединению, и обратное преобразование.

Это означает, что Traffic Inspector NG готов «раздавать» Интернет на пользователей внутренней сети сразу после первоначальной настройки, и нет необходимости отдельно настраивать механизм NAT.

Шаг 2 – Проброс портов

Если необходимо предоставить доступ к серверу, расположенному во внутренней сети, с компьютеров, расположенных в Интернете, то нужно создать правило для проброса портов.

Например, настроим доступ к веб-сайту во внутренней сети со стороны Интернета. Веб-сайт работает на компьютере с IP-адресом 192.168.1.3 и слушает порт 80.

Создадим новое правило в разделе **Firewall -> NAT** на вкладке **Переадресация портов** и укажем следующие настройки:

Интерфейс	WAN
Версия TCP/IP	IPv4
Протокол	TCP
Источник	любой
Диапазон портов источника	любой – любой
Назначение	WAN адрес
Диапазон портов назначения	80 – 80 Порт (или диапазон портов), на который нужно подключатся из Интернета.
Адрес перенаправления	192.168.1.3 IP-адрес целевой машины во внутренней сети, на которую идет проброс
Целевой порт перенаправления	80

	Порт, который «слушает» веб-сервер
Описание	Публикация веб-сервера в Интернет
Зеркальный NAT	Включить (чистый NAT)
Ассоциированное правило сетевого экрана	Добавить ассоциированное правило

Примечание. Помимо создания правила для проброса (основного правила), необходимо создать правило для пропуска преобразованного трафика (дополнительное правило). Такое, дополнительное правило создается автоматически, если выбрана опция **Добавить ассоциированное правило** при создании основного правила.

Приводим пример создания дополнительного правила вручную для нашего сценария. Пройдите в раздел **Межсетевой экран -> Правила**, вкладка **WAN**. Кликните на значок + для создания нового правила. Создайте правило со следующими настройками:

Действие	Разрешение
Интерфейс	WAN
Версия TCP/IP	IPv4
Протокол	TCP
Источник	Любой
Диапазон портов источника	Любой – Любой
Назначение	192.168.1.3
Диапазон портов назначения	80 – 80
Описание	Правило для разрешения преобразованного трафика

3. Защита от несанкционированного доступа к корпоративной сети

Компьютеры, подключенные к Интернету, могут подвергнуться несанкционированному доступу со стороны хакеров и прочих недоброжелателей. В Traffic Inspector Next Generation проблема несанкционированного доступа решается с помощью сетевого экрана.

Настройки правил фильтрации доступны в разделе **Межсетевой экран -> Правила**.

Некоторые правила межсетевого экрана будут преднастроены.

- Правило **Anti-Lockout Rule** защищает администратора шлюза от потери доступа к web-интерфейсу. Данное правило разрешает доступ по протоколу HTTP (TCP/80), HTTPS (TCP/443) и SSH (TCP/22) на сам шлюз со стороны LAN-адаптера.
- Правило **Default allow LAN to any rule** разрешает неограниченный доступ со стороны LAN-адаптера для трафика, направленного в Интернет и на сам шлюз.

Учитывая преднастроенные правила, общая логика работы межсетевого экрана следующая. Правила межсетевого экрана задаются отдельно для каждого из адаптеров, настроенных в системе. Правила располагаются в виде списка. Если сетевой пакет удовлетворяет критериям правила, то к пакету применяется действие, заданное в правиле. Если к пакету применено правило, то пакет не будет сверяться с оставшимися правилами в списке. Если сетевой пакет не удовлетворяет критериям ни одного правила, то пакет блокируется (отбрасывается без индикации отправляющей стороне).

Порядок правил в списке, таким образом, имеет значение. В наиболее общем случае, запрещающие правила должны располагаться раньше (выше в списке) чем разрешающие.

По умолчанию, из внутренней сети разрешен любой доступ как на сам шлюз (LAN-адаптер шлюза), так и в Интернет. Любой трафик, являющийся ответным на тот, который был выпущен из внутренней сети, также свободно пропускается межсетевым

экраном. Любое (не санкционированное из внутренней сети) обращение к шлюзу со стороны WAN-адаптера (Интернета) запрещено.

Разрешения трафика со стороны WAN-адаптера

Для примера, разрешим подключение к шлюзу Traffic Inspector NG со стороны WAN-адаптера по протоколу SSH.

Пройдите в раздел **Межсетевой экран -> Правила**, вкладка **WAN**. Кликните на значок + для создания нового правила. Создайте правило со следующими настройками:

Действие	Разрешение
Интерфейс	WAN
Версия TCP/IP	IPv4
Протокол	TCP
Источник	Любой
Диапазон портов источника	Любой – Любой
Назначение	WAN адрес
Диапазон портов назначения	SSH
Описание	Правило для разрешения подключений по SSH со стороны Интернета

Нажмите **Сохранить** для применения настроек.

Помимо собственно защиты компьютера от несанкционированных подключений, многие другие механизмы реализуются отчасти или полностью за счет межсетевого экрана, например: NAT, проброс портов, перенаправление трафика на прокси, DNS-форвардинг, ограничение пропуска трафика из / в гостевую сеть и прочие.

Настройка межсетевого экрана для данных нужд рассматривается в соответствующих инструкциях.

4. Запрет доступа к нежелательным ресурсам сети Интернет

Борьба с нецелевым использованием Интернета в Traffic Inspector Next Generation осуществляется за счет фильтрации обращений к нежелательным ресурсам через прокси-сервер.

Рассмотрим этапы настройки прокси-сервера:

- Базовая настройка веб-прокси
- Настройка прозрачного проксирования
- Настройка перехвата и дешифровки защищенных HTTPS-соединений
- Настройка веб-фильтрации с помощью прокси

4.1. Базовая настройка веб-прокси

Шаг 1 - Включение / выключение прокси-сервера

Прокси-сервер поставляется с рекомендуемыми настройками по умолчанию. Для включения прокси пройдите в **Службы->Прокси-сервер->Администрирование**, установите флажок **Включить прокси** и нажмите **Применить**. Настройки по умолчанию запускают прокси на LAN-интерфейсе и порту 3128. Веб-прокси будет использовать локальную базу данных для аутентификации пользователей.

Шаг 2 - Изменение интерфейсов прокси

Для того чтобы поменять интерфейсы (подсети), на которых запускается прокси, кликните на вкладку **Forward прокси**. В поле **Интерфейсы прокси** добавьте / удалите нужные интерфейсы.

Внимание. Не забудьте нажать Enter или поставить запятую после ввода в поле тега, так как в противном случае ввод не происходит.

Шаг 3 - Изменение порта прокси

По умолчанию, прокси слушает порт 3128. Для того чтобы поменять данную настройку, кликните на вкладку **Forward прокси** и пропишите порт в поле **Порт прокси**. Сохраните изменения.

Шаг 4 - Включение кеша

Для включения кеша кликните на стрелку рядом с **Общими настройками прокси**, в выпадающем меню кликните на **Настройки локального кеша**.

Установите флажок **Включить локальный кеш** и нажмите **Применить**.

Примечание. Для правильного создания кеша нужно перезапустить службу в разделе **Службы->Диагностика**.

Шаг 5 - Расширенные настройки

Кликните на кнопку в левой верхней части формы. В расширенных настройках, можно изменить размер кеша, структуру папок, максимальный размер объекта в кеше.

Настройки по умолчанию подходят для обычной навигации по вебу и предполагают кеш размером 100 МБ и 4 МБ для максимального размера объекта.

Шаг 6 - Изменение метода аутентификации

Кликните на стрелку рядом со вкладкой **Forward прокси** для отображения выпадающего меню. Далее, **Настройки аутентификации,** выбираем нужные Аутентификаторы в поле **Метод аутентификации**. Кликните на **Убрать все**, если вы не хотите использовать аутентификацию.

В зависимости от настроек аутентификации, которые вы настроили в **Система->Доступ->Серверы**, можно выбрать один или насколько опций:

- Без аутентификации (оставить пустое поле)
- Локальная база пользователей
- LDAP
- RADIUS

Шаг 7 - Настройка FTP прокси

Кликните на стрелку рядом со вкладкой **Forward прокси** для отображения выпадающего меню. Далее, **Настройки FTP-прокси**, где выбираем один или несколько интерфейсов в поле **Интерфейсы FTP-прокси** и жмем **Применить**.

Примечание. FTP-прокси будет работать только если сам прокси-сервер включен. FTP-прокси обрабатывает только незашифрованный FTP-трафик.

4.2. Настройка прозрачного проксирования

Прокси-сервер TING поддерживает работу в прозрачном режиме. Суть "прозрачного проксирования" - пользователи не имеют явных настроек на веб-прокси, тем не менее их трафик все равно попадет на веб-прокси.

Шаг 1 - Прозрачный HTTP-прокси

Пройдите в **Сервисы->Прокси сервер->Администрирование**.

Затем, на вкладке **Forward прокси,** выберите **Общие настройки**.

Установите флажок **Включить прозрачный HTTP-прокси** и нажмите **Применить**.

Примечание. Перенаправление на веб-прокси достигается за счет использования правил межсетевого экрана, и далее мы описываем как создать такое правило.

Шаг 2 - Правило NAT / Firewall для перенаправления HTTP-трафика

Самый простой способ добавить правило NAT / Firewall – это кликнуть на иконку (i), находящуюся слева от настройки **Включить прозрачный HTTP-прокси,** и затем на ссылку **добавить новое правило сетевого экрана**.

Правило должно иметь следующие настройки:

Интерфейс	LAN
Протокол	TCP
Источник	LAN сеть
Диапазон портов источника	Любой - любой

Назначение	Любой
Диапазон портов назначения	HTTP - HTTP
Адрес перенаправления	127.0.0.1
Порт перенаправления	3128
Описание	Перенаправление трафика на прокси
Зеркальный NAT	Включить (чистый NAT)
Ассоцированное правило сетевого экрана	Добавить ассоциированное правило

Используем данные настройки и жмем **Применить**.

4.3. Настройка перехвата и дешифровки защищенных HTTPS-соединений

Все больше и больше веб-сайтов используют HTTPS – криптографическое расширение протокола HTTP. В случае с HTTPS, трафик, которым обменивается браузер и веб-сервер, шифруется с помощью криптографического протокола SSL / TLS. Для пользователя, данный факт означает конфиденциальность и безопасность, для системного администратора – дополнительную головную боль и невозможность контролировать данные передаваемые в рамках зашифрованных соединений.

Для решения данной проблемы, Traffic Inspector Next Generation оснащен функционалом для перехвата и дешифровки HTTPS-трафика. Это значит, что TI NG может применять URL-фильтрацию даже для защищенного трафика.

Перехват HTTPS-соединениний основывается на атаке типа man-in-the-middle, поэтому используйте этот функционал только если вы действительно понимаете, что делаете, и если политики вашей организации позволяют доступ к конфиденциальным данным пользователей. Может оказаться полезным отключить механизм перехвата и дешифрования HTTPS-соединений для некоторых сервисов (например, сервисов электронного банкинга).

Шаг 1 - Создание центра сертификации для нужд перехвата HTTPS

Прежде всего нужно создать центр сертификации. Пройдите в **Система -> Доверенные сертификаты -> Полномочия.**

Кликните на ссылку Добавить или импортировать ЦС в верхнем правом углу экрана для создания нового ЦС.

В нашем примере мы используем следующие настройки:

Описание	TING-SSL
Метод	Создать внутренний ЦС
Длина ключа (биты)	2048
Digest алгоритм	SHA256
Срок жизни (дней)	356
Код страны	RU (Россия)
Область	MO
Город	Коломна
Организация	TING
Email адрес	spam@smart-soft.ru
Простое имя	ting-ssl-ca

Сохраните настройки.

Шаг 2 - Включение перехвата HTTPS

Пройдите в **Сервисы->Прокси сервер->Администрирование**.

Затем, на вкладке **Forward прокси,** выберите **Общие настройки**.

Установите флажок **Включить SSL-режим**, и в качестве ЦС выберите ранее созданный ЦС.

Нажмите **Применить**.

Шаг 3 - Правило NAT / Firewall для перенаправления HTTPS-трафика

Самый простой способ добавить правило NAT / Firewall – это кликнуть на иконку (i), находящуюся слева от настройки **Включить прозрачный HTTP-прокси,** и затем на ссылку **добавить новое правило сетевого экрана**.

Правило должно иметь следующие настройки:

Интерфейс	LAN
Протокол	TCP
Источник	LAN net
Диапазон портов источника	Любой - любой
Назначение	Любой
Диапазон портов назначения	HTTPS - HTTPS
Адрес перенаправления	127.0.0.1
Порт перенаправления	3129
Описание	Перенаправление трафика на прокси
Зеркальный NAT	Включить (чистый NAT)
Ассоцированное правило сетевого экрана	Добавить ассоциированное правило

Используем данные настройки и жмем **Применить**.

Шаг 4 - Настройка исключений

Данный шаг важен и требует ответственного подхода! Для того, чтобы дешифрование HTTPS не проводилось в отношении доверенных сайтов и чтобы не затрагивать их алгоритмы безопасности, нужно добавить доменные имена и все поддомены таких сайтов в поле **Отключить перехват SSL для сайтов**.

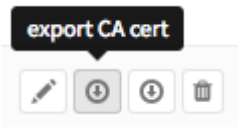
Для добавления новой записи, финализируйте ввод нажатием клавиши Enter. Для добавления всех поддоменов домена, укажите точку перед доменом. Например: для добавления всех поддоменов paypal.com введите .paypal.com, затем Enter.

Примечание

Проследите, что бы сайты электронного банкинга и сайты, на которых пользователи указывают личную информацию, логины / пароли, были добавлены в данное поле.

Шаг 5 - Настройка ОС/Браузера

Поскольку браузеры по умолчанию не доверяют нашему ЦС, пользователю постоянно выдается предупреждение при обращении к HTTPS-сайтам. Для решения данной проблемы, вам нужно импортировать ранее созданный в Traffic Inspector Next Generation издательский сертификат в клиентскую операционную систему. Для экспортирования сертификата, пройдите в **Система -> Доверенные сертификаты -> Полномочия** и кликните на соответствующую иконку.



Далее, на клиентской машине импортируйте сертификат издательства.

4.4. Настройка веб-фильтрации с помощью прокси

Для настройки фильтрации с помощью прокси пройдите в раздел **Службы->Прокси-сервер->Администрирование**, вкладка **Forward прокси,** пункт меню **Список контроля доступа**.

Здесь можно:

- Настроить **Разрешенные подсети** (По умолчанию будут разрешены подсети, подключенные к интерфейсам прокси)
- Добавить **Неограниченные IP-адреса** («Неограниченные» значит, что для клиентов с данных IP-адресов не будут применятся аутентификация и черные списки).
- Добавить **IP-адреса запрещенных хостов** (Запрещенный хост не сможет пользоваться услугами данного прокси)
- **Белый список** (Кликните на иконку (i) для ознакомления с примерами, белые списки являются более приоритетными чем черные списки)

- **Черный список** (Если ресурс не разрешен в белом списке, то его указание в черном списке, запретит доступ к нему. Здесь можно использовать регулярные выражения).

Внимание. Не забудьте нажать Enter или поставить запятую после ввода в поле тега, так как в противном случае ввод не происходит. Тег должен выглядеть так:

Рассмотрим два примера веб-фильтрации: фильтрация рекламы и фильтрация нежелательных категорий сайтов.

4.4.1.Фильтрация рекламы

Шаг 1 - Загрузка списка для фильтрации

Для данного примера мы используем список, доступный по адресу:

http://pgl.yoyo.org/adservers/serverlist.php?hostformat=nohtml

Это простой текстовый файл, который выглядит следующим образом:

101com.com

101order.com

123found.com

180hits.de

180searchassistant.com

1x1rank.com

207.net

247media.com

Пройдите в **Службы->Прокси-сервер->Администрирование** и кликните на вкладку **Загружаемые списки контроля доступа**. Далее, кликните на **+** в нижнем правом углу формы для создания нового списка.

Укажите следующие значения:

Включено	Флажок установлен
Имя файла	yoyoads
URL	http://pgl.yoyo.org/adservers/serverlist.php?hostformat=nohtml
Категории	(оставить пустым)
Описание	Yoyo Ads Blacklist

Сохраните изменения.

Далее, кликните на **Загрузить списки доступа** и **Применить** для того, чтобы включить черный список / блокировщик рекламы.

Шаг 2 - Правило фаервола для запрета обхода прокси

Для того, чтобы никто не смог обойти прокси, нам нужно создать запрещающее правило фаервола. Пройдите в **Межсетевой экран->Правила** на вкладку **LAN** и создайте правило со следующими настройками:

Действие	Блокировка
Интерфейс	LAN
Протокол	TCP/UDP
Источник	LAN net
Диапазон портов назначения	HTTP
Категория	Блокировать трафик мимо прокси
Описание	Блокировать HTTP-трафик

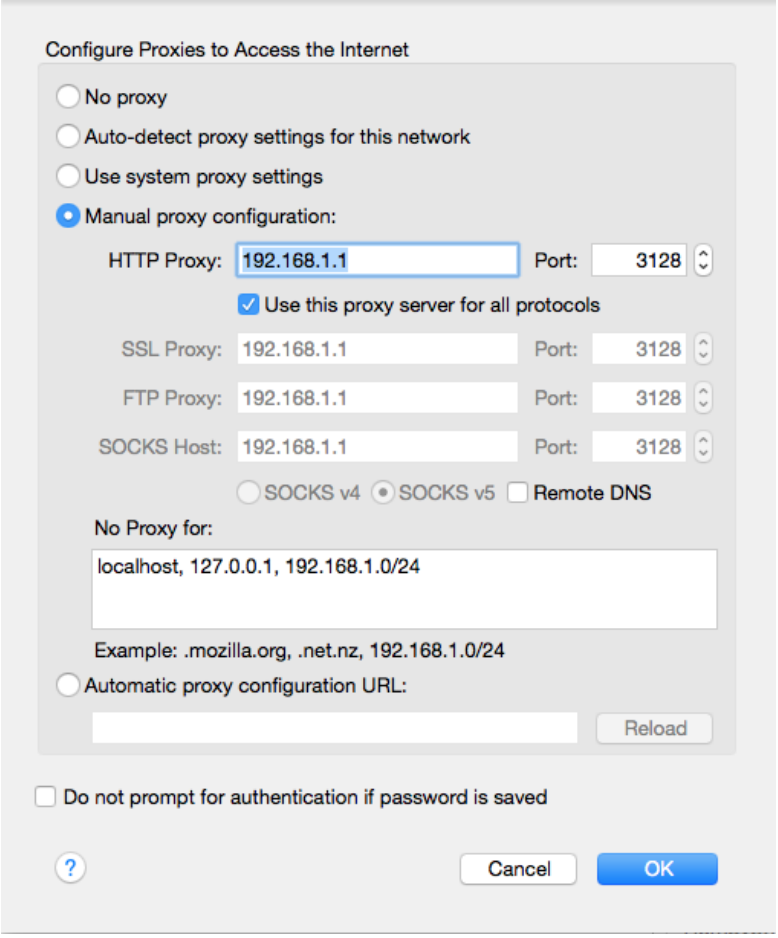
Далее, добавьте еще одно правило для блокировки HTTPS-доступа.

Действие	Блокировка
Интерфейс	LAN
Протокол	TCP/UDP
Источник	LAN net
Диапазон портов назначения	HTTPS
Категория	Блокировать трафик мимо прокси
Описание	Блокировать HTTPS-трафик

Сохраните и примените изменения

Шаг 3 - Настройка браузера

Для настройки браузера, зайдите в сетевые настройки и укажите адрес и порт прокси-сервера аналогично тому, как показано в примере для Firefox:



4.4.2. Фильтрация нежелательных категорий сайтов

Шаг 1 - Загрузка списка для фильтрации

Для данной инструкции мы используем **Список для веб-категоризации UT1**, поддерживаемый Фабрисом Прижаном из Тулузского Университета. Данный список распространяется под лицензией Creative Commons.

Другие популярные списки, которые хорошо работают в Traffic Inspector NG, включают:

- **Shallalist.de <http://www.shallalist.de/>**

Бесплатный для личного использования и частично-платный для коммерческого использования.

- **URLBlacklist.com <http://urlblacklist.com/>**

Платный коммерческий список.

- **Squidblacklist.org <http://www.squidblacklist.org/>**

Платный коммерческий список.

Кликните на вкладку **Загружаемые списки контроля доступа**. Далее, кликните на **+** в нижнем правом углу формы для создания нового списка.

Появится окно, в котором нужно указать следующие значения:

Включено	Флажок установлен
Имя файла	UT1
URL	(копировать / вставить URL)
Категории	(оставить пустым)
Описание	UT1 web филтр
URL	ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz

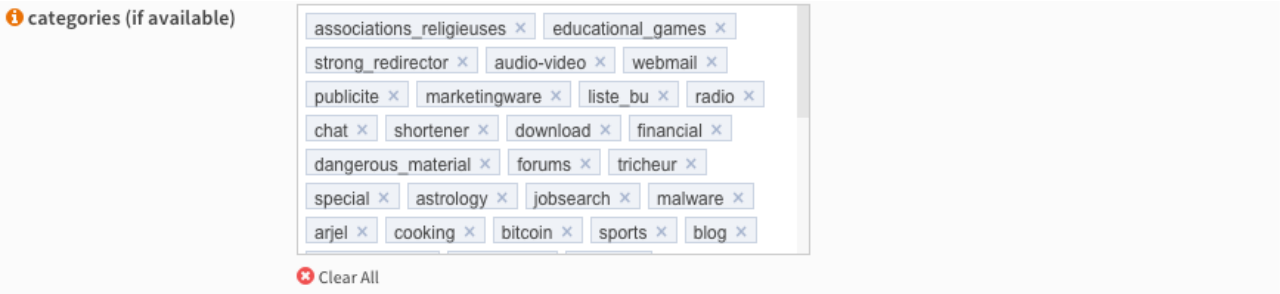
Нажмите **Сохранить изменения.**

Шаг 3 - Загрузка категорий

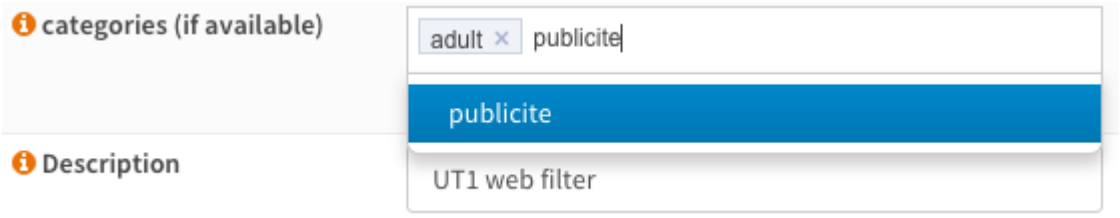
Нажмите **Загрузить списки доступа**. Учтите, что загрузка займет некоторое время (до нескольких минут), так как полный список (>19 МБ) конвертируется в списки контроля доступа Squid.

Шаг 4 - Настройка категорий

Выберите нужные категории – кликните на иконку с изображением карандаша рядом с описанием списка. Будет открыто окно редактирования, в котором - все доступные категории, извлеченные из списка.



Например, мы будем фильтровать рекламу и контент для взрослых. Самый простой способ добиться этого – очистить список и выбрать следующие записи из выпадающего списка:



Далее **Сохраните изменения** и нажмите **Загрузить списки доступа** для того, чтобы загрузить и перестроить список на основе выбранных категорий. Это займет примерно столько же времени как и загрузка первого списка, так как одна лишь секция категорий для взрослых занимает порядка 15 МБ.

Шаг 5 - Правило фаервола для запрета обхода прокси

Для того, чтобы никто не смог обойти прокси, нам нужно создать запрещающее правило фаервола. Пройдите в **Межсетевой экран->Правила** на вкладку **LAN** и создайте правило со следующими настройками:

Действие	Блокировка
Интерфейс	LAN
Протокол	TCP/UDP
Источник	LAN net
Диапазон портов назначения	HTTP
Категория	Блокировать трафик мимо прокси
Описание	Блокировать HTTP-трафик

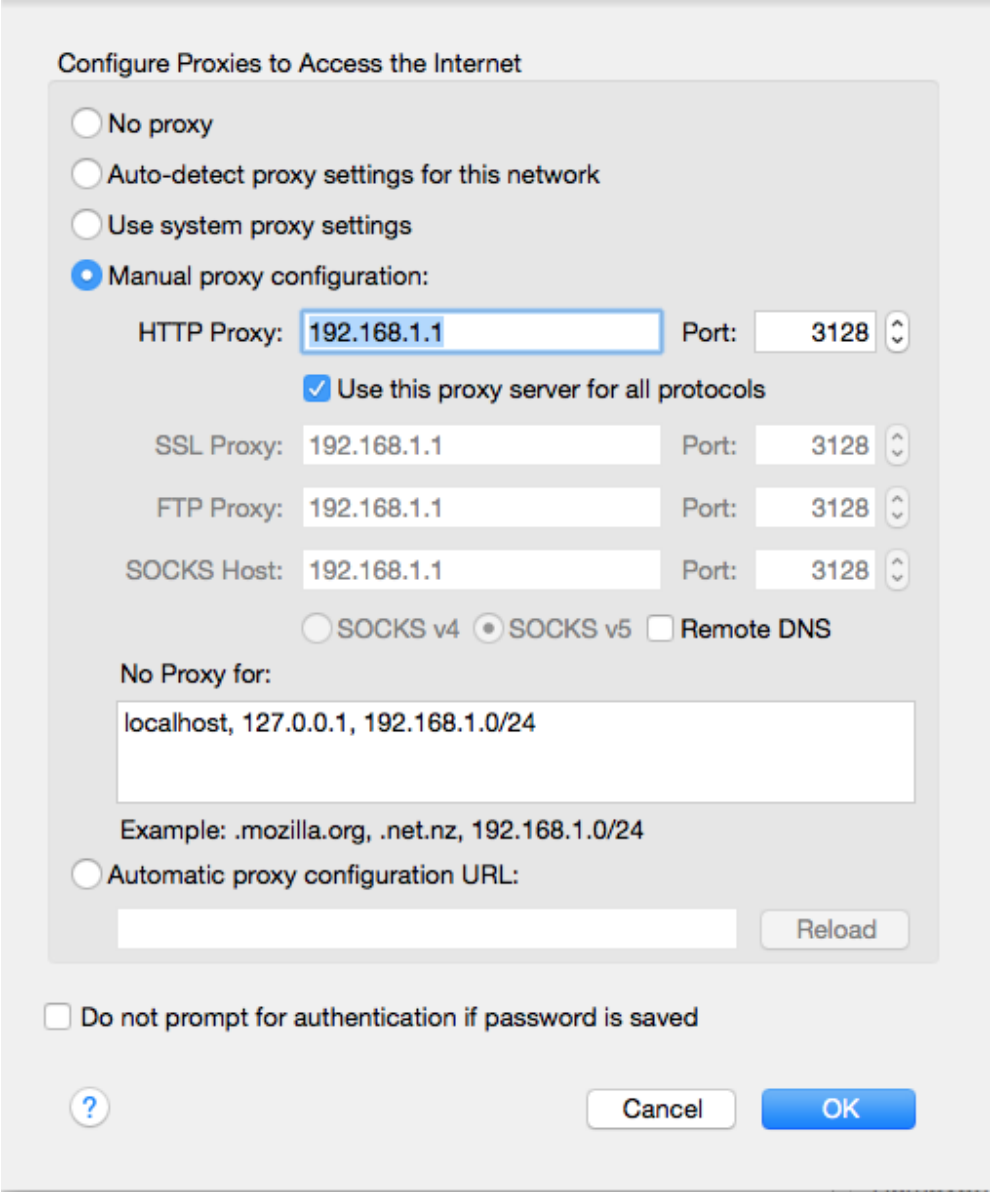
Далее, добавьте еще одно правило для блокировки HTTPS-доступа.

Действие	Блокировка
Интерфейс	LAN
Протокол	TCP/UDP
Источник	LAN net
Диапазон портов назначения	HTTPS
Категория	Блокировать трафик мимо прокси
Описание	Блокировать HTTPS-трафик

Сохраните и примените изменения

Шаг 6 - Настройка браузера

Для настройки браузера, зайдите в сетевые настройки и укажите адрес и порт прокси-сервера аналогично тому, как показано в примере для Firefox:



5. Ограничения P2P-трафика

Функционал L7-фильтрации позволяет распознавать и фильтровать трафик приложений в независимости от используемых ими сетевых портов.

Например, запретим пользователям внутренней сети использовать BitTorrent.

Шаг 1 – Включение функционала L7-фильтрации

Настройка функционала осуществляется в разделе **Службы -> Анализатор трафика**. Установите флаг **Включить анализатор трафика**.

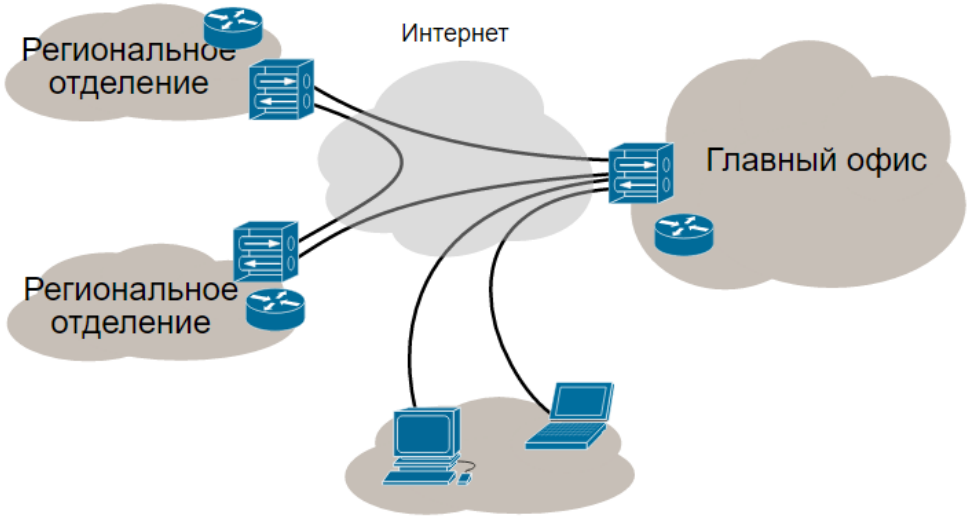
Шаг 2 – Создание правила для запрета BitTorrent

Кликните на иконку «+» и создайте правило со следующими настройками:

Включен	Флаг установлен
Порядковый номер	Оставить по умолчанию
Отправитель	IP-адрес отправителя или IP-сеть отправителей (в нашем примере, 10.0.0.0/24)
Службы	Блокируемое приложения (в нашем примере, BitTorrent)
Разрешить	Флаг снят

Настройка завершена!

6. Использование технологии VPN



Для минимизации затрат при объединений 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 филиальный 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»).

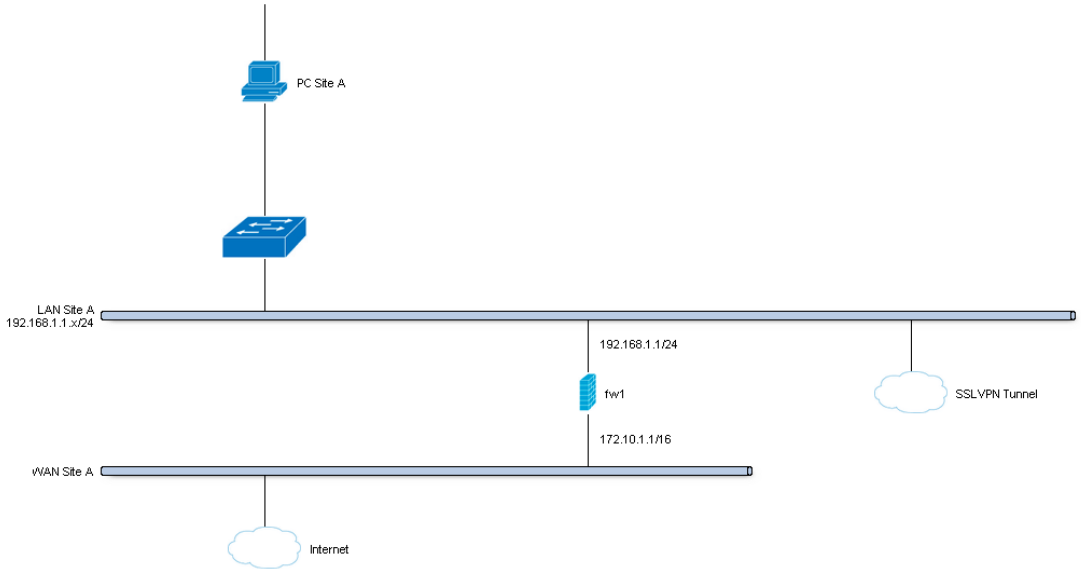
В данной инструкции мы рассмотрим настройку популярной, кроссплатформенной технологии OpenVPN для объединения двух офисов в режиме «сайт - сайт». Перед тем как начинать настройку OpenVPN SSL туннеля убедитесь, что маршрутизаторы Traffic Inspector Next Generation имеют адекватные сетевые настройки. Также, 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.

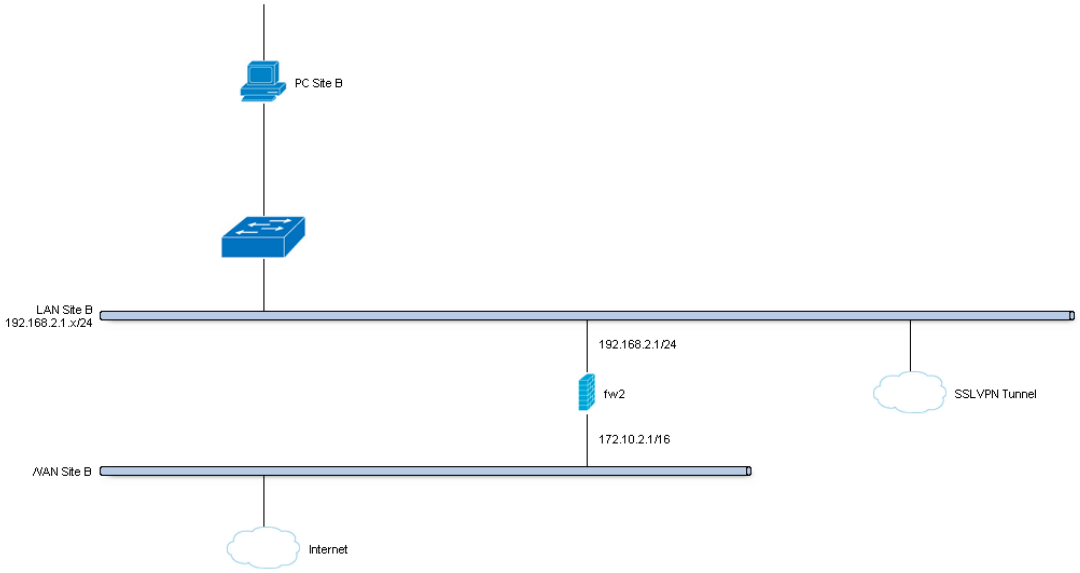
Маршрутизатор в локации A

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

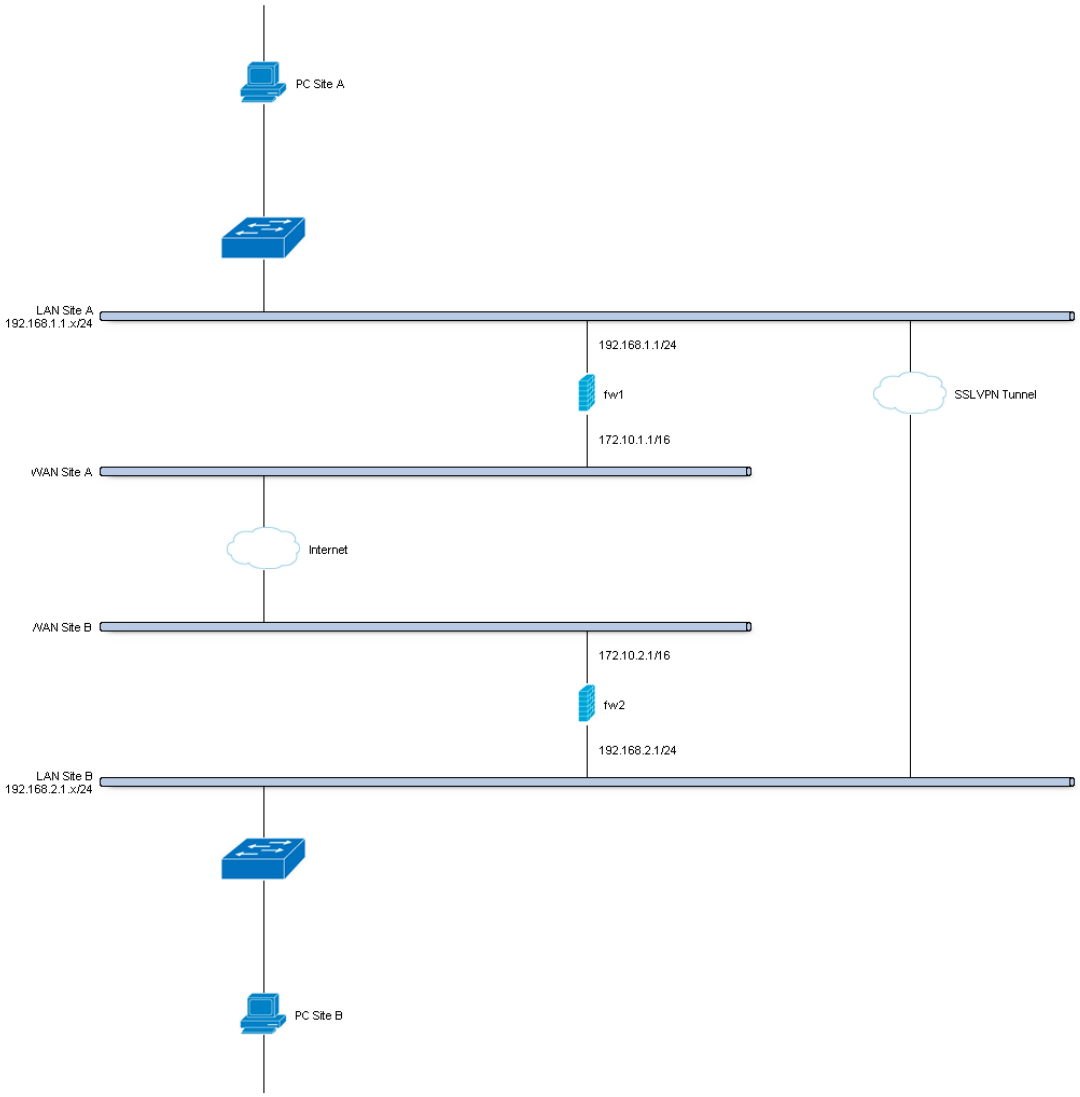


Маршрутизатор в локации Б

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



Шаг 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.

Шаг 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:

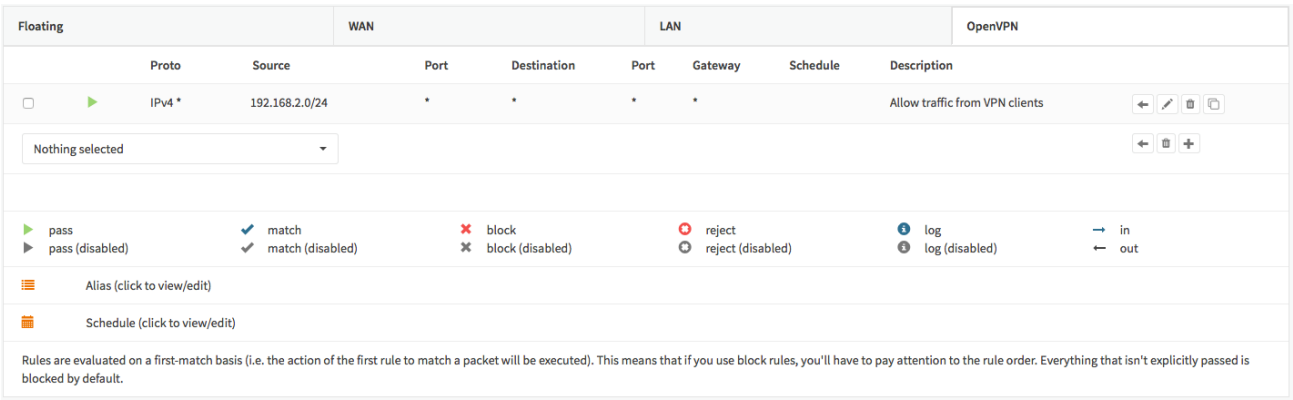
```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
0960c87c3aafa8f306fe270c1564380b
7922543563a17b5d2636b4ef9412dd09
9ad44974ca1b293963e0f8ac9cbdd97c
2c31bf35f0df45c9e928ccb033e6d51d
2caaec02d649ad081c68d7bc7d28030e
9182c9597a83024097bea860e52d9c66
1b9e0048fbf951ce8659bc56edb7f9a1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

Шаг 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.

Шаг 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.

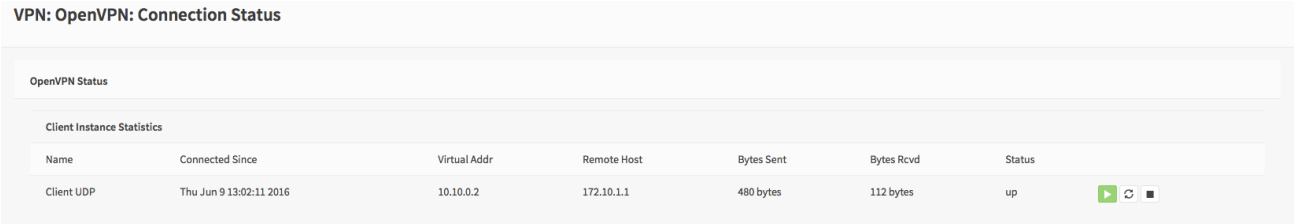
Примечание. Несмотря на то, что мы настраиваем подключение типа «сайт - сайт», только маршрутизатор в центральном офисе настраивается как «VPN-сервер», маршрутизаторы в остальных филиалах настраиваются как «VPN-клиенты».

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

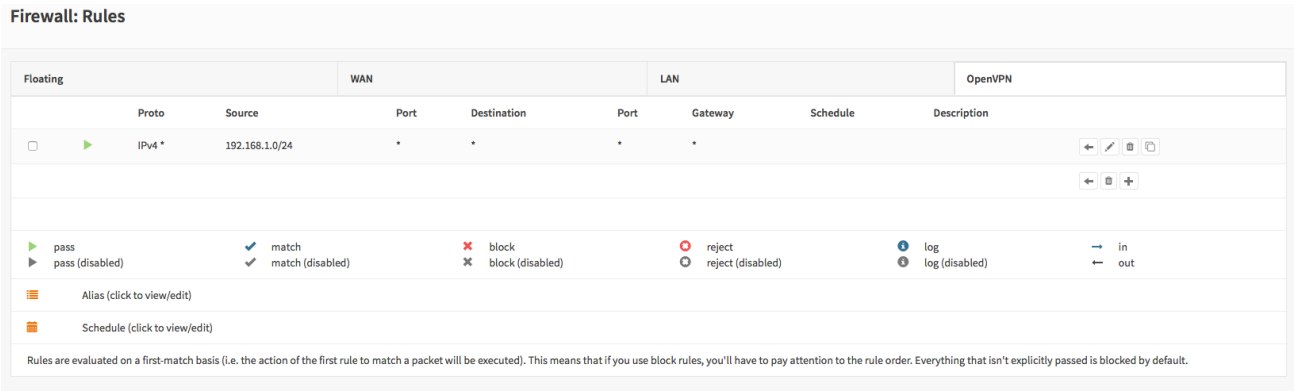
Кликните **Сохранить** для применения настроек.

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



Шаг 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).



Настройка VPN завершена.

7. Управление трафиком (traffic shaping)

Traffic Inspector Next Generation позволяет разграничивать пропускную способность Интернет-канала между пользователями и приоритезировать обработку критичного к задержкам трафика (VoIP, видео-связь). Рассмотрим наиболее распространенные сценарии использования шейпера, встроенного в Traffic Inspector Next Generation.

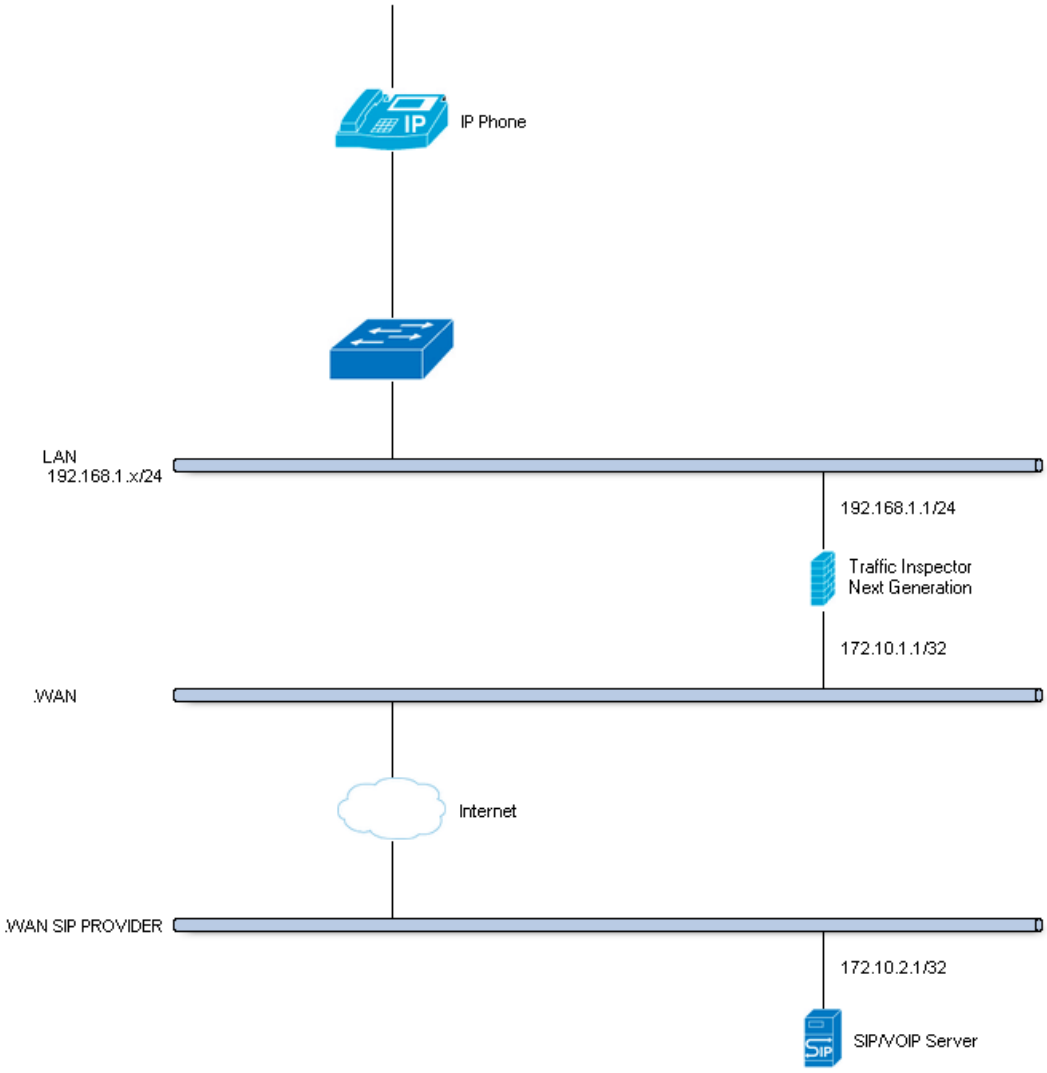
В данной инструкции описывается следующие сценарии:

- Резервирование полосы для трафика критичного к задержкам
- Распределение пропускной способности Интернет-канала поровну между пользователями внутренней сети
- Ограничение максимальной скорости работы пользователя
- Приоритезация трафика приложения с помощью очередей
- Шейпирование для гостевой сети

7.1. Резервирование полосы для трафика критичного к задержкам

В данном сценарии мы создадим логический канал для трафика, направленного на, и идущего с нашего Voice Over IP-сервера.

Необходимо обеспечить 4 канала по 64 Кбит/с для передачи несжатых голосовых данных, что в общей сложности дает цифру 256 Кбит/с. В данном примере, пропускная способность интернет-канала равна 10 Мбит/с на скачивание и 1 Мбит/с на upload.



Шейпирование для VOIP / SIP-транка

Для того, чтобы начать настройку, пройдите в раздел **Сетевой экран -> Ограничитель -> Настройки**.

Шаг 1 – Создание Upload and Download каналов

На вкладе **Каналы**, кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования канала.

Создаем Upload-канал (для трафика, направленного на наш VOIP-сервер).

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	256	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Kbit/s	Единица измерения пропускной способности
mask	(Пусто)	Используется для автоматического создания очередей, Оставьте пустым для данного примера
description	PipeUp-256Kbps	Произвольное описание

Создаем Upload-канал для остального трафика (1024Kbps - 256Kbps = 768Kbps).

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	768	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Kbit/s	Единица измерения пропускной способности
mask	(Пусто)	Используется для автоматического создания очередей, Оставьте пустым для данного

		примера
description	PipeUp-768Kbps	Произвольное описание

Создаем Download-канал (для трафика, идущего с нашего VOIP-сервера).

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	256	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Kbit/s	Единица измерения пропускной способности
mask	(Пусто)	Используется для автоматического создания очередей, Оставьте пустым для данного примера
description	PipeDown-256Kbps	Произвольное описание

Создаем Download-канал для остального трафика (10240Kbps - 256Kbps = 9984Kbps).

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	9984	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Kbit/s	Единица измерения пропускной способности
mask	(Пусто)	Используется для автоматического создания очередей, Оставьте пустым для данного примера
description	PipeDown-9984Kbps	Произвольное описание

Шаг 2 – Создание правил

На вкладе **Правила** кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования правила.

Создаем правило для трафика, направленного на наш VOIP-сервер (Upload).

sequence	11	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	any	IP-адрес источника, оставляем Любой
src-port	any	Порт источника, оставляем Любой
destination	172.10.2.1	IP-адрес назначения, указываем адрес VOIP-сервера
dst-port	any	Порт назначения, оставляем Любой
target	PipeUP-256Kbps	Выбираем Upload-канал, PipeUp-256Kbps
description	ShapeVOIPUpload	Произвольное описание

Создаем правило для трафика, идущего от нашего VOIP-сервера (Download).

sequence	21	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	172.10.2.1	IP-адрес источника, указываем адрес VOIP-сервера
src-port	any	Порт источника, оставляем Любой
destination	any	IP-адрес назначения, оставляем Любой
dst-port	any	Порт назначения, оставляем Любой
target	PipeDown256Kbps	Выбираем Download-канал, PipeDown-256Kbps
description	ShapeVOIPDown	Произвольное описание

Создаем правило для остального Upload-трафика, направленного в Интернет

sequence	31	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	192.168.1.0/24	IP-адрес источника, указываем диапазон внутренней сети
src-port	any	Порт источника, оставляем Любой
destination	any	IP-адрес назначения, оставляем Любой
dst-port	any	Порт назначения, оставляем Любой
target	PipeUp-768Kbps	Выбираем Upload-канал, PipeUp-768Kbps
description	ShapeUpload	Произвольное описание

Создаем правило для остального Download-трафика, идущего с Интернета

sequence	41	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	any	IP-адрес источника, оставляем Любой
src-port	any	Порт источника, оставляем Любой
destination	192.168.1.0/24	IP-адрес назначения, указываем диапазон внутренней сети
dst-port	any	Порт назначения, оставляем Любой
target	PipeDown-9984Kbps	Выбираем Download-канал, PipeDown-9984Kbps
description	ShapeDown	Произвольное описание

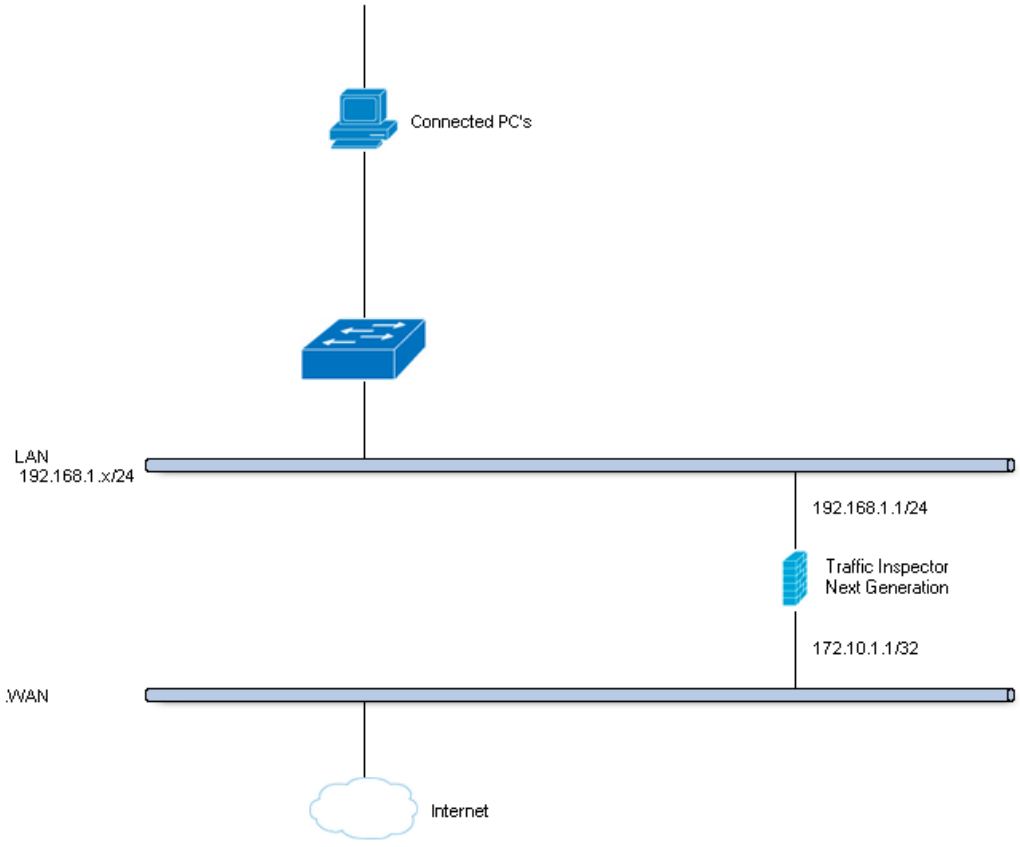
Примечание.

Обязательно соблюдайте указанную последовательность действий. Важно убедится, что нужный трафик проходит через нужный канал.

Нажмите **Применить** для того, чтобы активировать правила шейпирования.

7.2. Распределение пропускной способности Интернет-канала поровну между пользователями внутренней сети

В данном примере, мы поровну разделим пропускную способность интернет-канала - 10 Мбит/с на скачивание и 1 Мбит/с на upload - между пользователями внутренней сети.



Для того, чтобы начать настройку, пройдите в раздел **Сетевой экран -> Ограничитель -> Настройки**.

Шаг 1 – Создание Upload and Download каналов

На вкладе **Каналы**, кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования канала.

Создание Upload-канала

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	1	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Mbit/s	Единица измерения пропускной способности
Mask	destination	Выберите «Destination» для разделения пропускной способности
description	PipeUp-1Mbps	Произвольное описание

Создание Download-канала

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	10	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Mbit/s	Единица измерения пропускной способности
mask	destination	Выберите «Destination» для того, чтобы разделить пропускную способность между пользователями
description	PipeDown-10Mbps	Произвольное описание

Шаг 2 – Создание правил

На вкладе **Правила** кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования правила.

Создаем правило для трафика, направленного в Интернет (Upload)

sequence	11	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	192.168.1.0/24	IP-адрес источника, указываем диапазон внутренней сети
src-port	any	Порт источника, оставляем Любой
destination	any	IP-адрес назначения, оставляем Любой
dst-port	any	Порт назначения, оставляем Любой
target	PipeUP-1Mbps	Выбираем Upload-канал, PipeUp-1Mbps
description	ShapeUpload	Произвольное описание

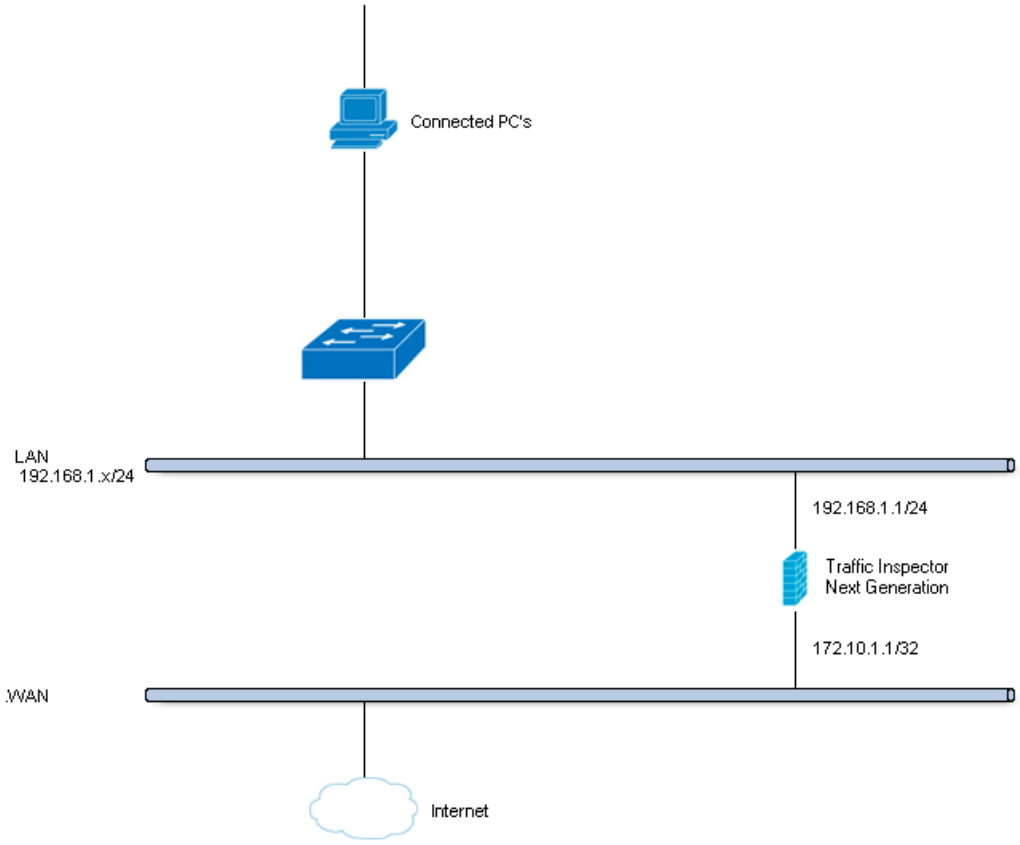
Создаем правило для трафика, идущего с Интернета (Download)

sequence	21	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	any	IP-адрес источника, оставляем Любой
src-port	any	Порт источника, оставляем Любой
destination	192.168.1.0/24	IP-адрес назначения, указываем диапазон внутренней сети
dst-port	any	Порт назначения, оставляем Любой
target	PipeDown-10Mbps	Выбираем Download-канал, PipeDown-10Mbps
description	ShapeDownload	Произвольное описание

Нажмите **Применить** для того, чтобы активировать правила шейпирования.

7.3. Ограничение максимальной скорости работы пользователя

В данном примере, мы разделим download-скорость таким образом, что каждый пользователь получит не более 1 Мбит/с.



Для того, чтобы начать настройку, пройдите в раздел **Сетевой экран -> Ограничитель -> Настройки**.

Шаг 1 – Создание каналов

На вкладе **Каналы**, кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования канала.

Создание Download-канала

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	1	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Mbit/s	Единица измерения пропускной способности
mask	source	Выберите «Source» для того, чтобы ограничит скорость пользователя
description	PipeDown-1Mbps	Произвольное описание

Шаг 2 – Создание правил

На вкладе **Правила** кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования правила.

Создаем правило для трафика, идущего с Интернета (Download)

sequence	21	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP

source	any	IP-адрес источника, оставляем Любой
src-port	any	Порт источника, оставляем Любой
destination	192.168.1.0/24	IP-адрес назначения, указываем диапазон внутренней сети
dst-port	any	Порт назначения, оставляем Любой
target	PipeDown-1Mbps	Выбираем Download-канал, PipeDown-10Mbps
description	ShapeDownload	Произвольное описание

Примечание.

Если вы хотите ограничить скорость только для одного IP-адреса, тогда введите этот адрес в поле Назначение вместо диапазона IP-адресов внутренней сети.

Нажмите **Применить** для того, чтобы активировать правила шейпирования.

7.4. Приоритезация трафика приложения с помощью очередей

С помощью очередей мы можем управлять пропускной способностью в логическом канале и давать некоторым приложениям больше пропускной способности чем другим.

Идея проста: предположим, у нас есть логический канал на 10 Мбит/с и 2 приложения, например SMTP (электронная почта) и HTTPS (веб-браузер). HTTPS получает вес «1» и SMTP-трафик получает вес «9». Когда пропускная способность логического канала будет занята полностью, почтовый трафик получит в 9 раз большую пропускную способность чем веб-трафик, т.е. в результате будем иметь 1 Мбит/с для веб-трафика и 9 Мбит/с для почты.

В нашем примере, мы регулируем только download-трафик, но совершенно такую же регулировку можно сделать и для upload-трафика.

Приложение	Вес	Минимальная пропускная способность
SMTP (порт 25)	9	9 Мбит/с
HTTP (порт 80)	1	1 Мбит/с
HTTPS (порт 443)		

Для того, чтобы начать настройку, пройдите в раздел **Сетевой экран -> Ограничитель -> Настройки**.

Шаг 1 – Создание каналов

На вкладе **Каналы**, кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования канала.

Создание Download-канала (10 Мбит/с)

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	10	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Mbit/s	Единица измерения пропускной способности
mask	(Пусто)	Используется для автоматического создания очередей, Оставьте пустым для данного примера
description	PipeDown-10Mbps	Произвольное описание

Шаг 2 – Создание очередей

На вкладе **Очереди**, кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования очереди.

Создание очереди для SMTP

enabled	Флаг установлен	Установить флажок для включения канала
pipe	PipeDown-10Mbps	Выбираем канал
weight	9	Цифровое значение веса
mask	(empty)	Оставьте пустым
description	Queue-SMTP	Произвольное описание

Создание очереди для HTTP

enabled	Флаг установлен	Установить флажок для включения канала
pipe	PipeDown-10Mbps	Выбираем канал
weight	1	Цифровое значение веса
mask	(empty)	Оставьте пустым
description	Queue-HTTP	Произвольное описание

Шаг 3 – Создание правил

На вкладе **Правила** кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования правила.

Создаем правило для SMTP-трафика (Download)

sequence	11	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	any	IP-адрес источника, оставляем Любой
src-port	smtp	Порт источника, выбираем smtp или 25
destination	any	IP-адрес назначения, оставляем Любой
dst-port	any	Порт назначения, оставляем Любой

target	Queue-SMTP	Выбираем SMTP-очередь
description	ShapeSMTPDownload	Произвольное описание

Создаем правило для HTTP-трафика (Download)

sequence	21	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	any	IP-адрес источника, оставляем Любой
src-port	http	Порт источника, выбираем http или 80
destination	any	IP-адрес назначения, оставляем Любой
dst-port	any	Порт назначения, оставляем Любой
target	Queue-HTTP	Выбираем HTTP-очередь
description	ShapeHTTPDownload	Произвольное описание

Создаем правило для HTTPS-трафика (Download)

sequence	31	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
proto	ip	Выберите протокол, в нашем случае IP
source	any	IP-адрес источника, оставляем Любой
src-port	https	Порт источника, выбираем https или 443
destination	any	IP-адрес назначения, оставляем Любой
dst-port	any	Порт назначения, оставляем Любой

target	Queue-HTTP	Выбираем HTTP-очередь
description	ShapeHTTPSDownload	Произвольное описание

Примечание.

Как видно, HTTP- и HTTPS-трафик попадают в одну и ту же очередь и будут обрабатываться одинаково (с максимальной скоростью в 1 Мбит/с).

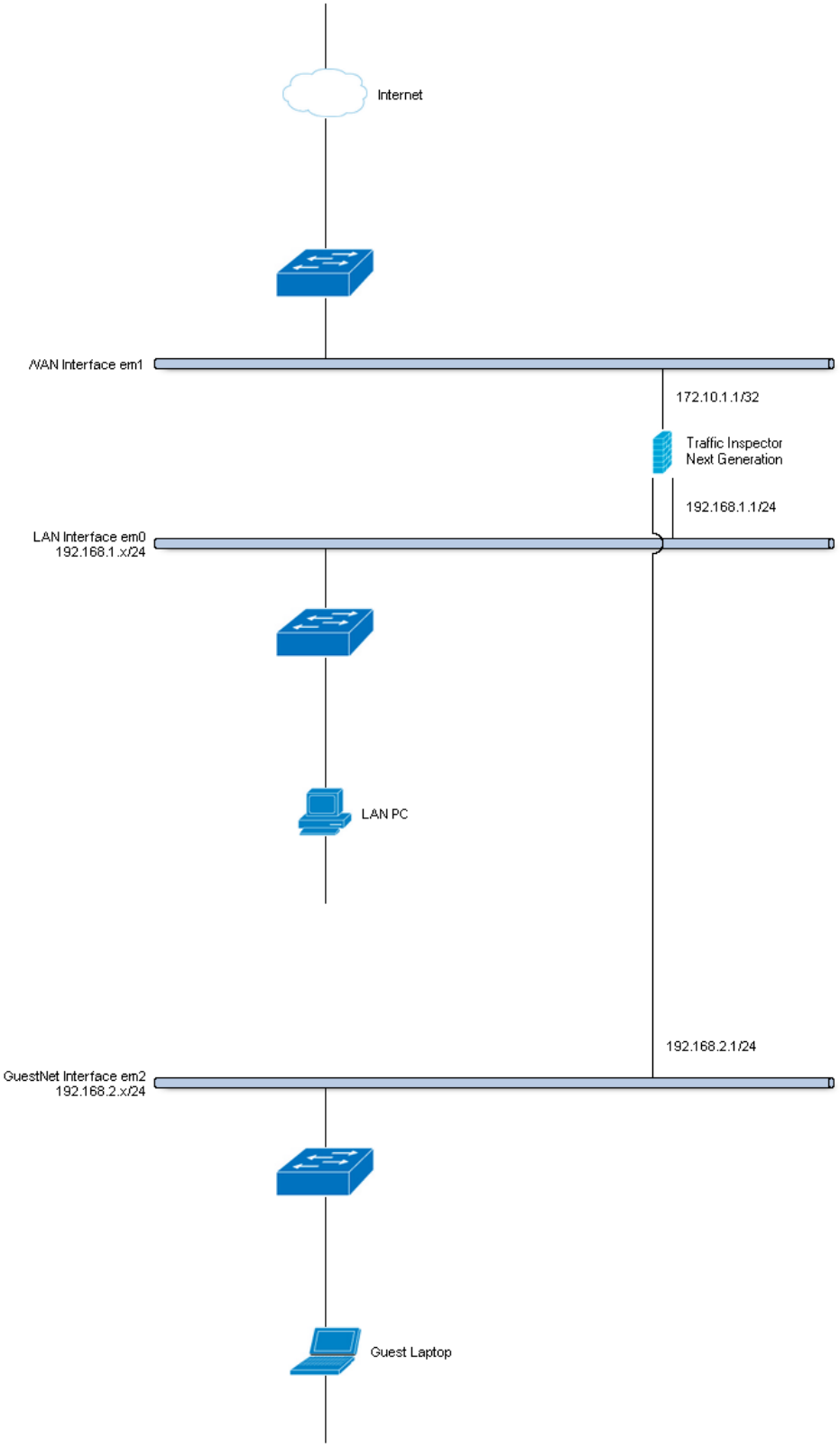
Нажмите **Применить** для того, чтобы активировать правила шейпирования.

7.5. Шейпирование для гостевой сети

Одна из особенностей шейпера Traffic Inspector Next Generation – это возможность добавлять правила с использованием двух интерфейсов. Данная опция позволяет шейпировать трафик по-разному в зависимости от направления движения от одного интерфейса к другому интерфейсу.

В этом примере, мы задействуем данный функционал для совместного пользования симметричного 10 Мбит/с Интернет-канала двумя сетями – внутренней LAN-сетью и гостевой сетью.

Внутренняя LAN-сеть не будет ограничена. Гостевая сеть будет иметь следующие ограничения – 1 Мбит/с на загрузку и 1 Мбит/с на upload.


Internet
WAN Interface em1
172.10.1.1/32
Traffic Inspector
Next Generation
192.168.1.1/24
LAN Interface em0
192.168.1.x/24
LAN PC
192.168.2.1/24
GuestNet Interface em2
192.168.2.x/24
Guest Laptop

Для того, чтобы начать настройку, пройдите в раздел **Сетевой экран -> Ограничитель -> Настройки**.

Шаг 1 – Создание Upload and Download каналов

На вкладе **Каналы**, кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования канала.

Создание Upload-канала (GuestNet – em2)

enabled	Флаг установлен	Установить флажок для включения канала
bandwidth	1	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Mbit/s	Единица измерения пропускной способности
Mask	(Пусто)	Используется для автоматического создания очередей, Оставьте пустым для данного примера
description	PipeUp-1Mbps	Произвольное описание

Создание Download-канала (GuestNet – em2)

enabled	Установлен	Установить флажок для включения канала
bandwidth	2	Цифровое обозначение желаемой пропускной способности
Единица измерения bandwidth	Mbit/s	Единица измерения пропускной способности
mask	(Пусто)	Используется для автоматического создания очередей, Оставьте пустым для данного примера
description	PipeDown-2Mbps	Произвольное описание

Шаг 2 – Создание правил

На вкладе **Правила** кликните на значок «+» в нижнем правом углу. Появится пустое окно редактирования правила.

Примечание. Сначала измените режим на «расширенный» - кликните по переключателю в левом верхнем углу диалогового окна. Клик переведет его из состояния «выключен» (красный) и «включен» (зеленый).

Создаем правило для трафика, направленного в Интернет (Upload)

sequence	21	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
interface2	GuestNet	Выберите интерфейс, подключенный к гостевой сети
proto	ip	Выберите протокол, в нашем случае IP
source	any	IP-адрес источника, любой
src-port	any	Порт источника, оставляем Любой
destination	any	IP-адрес назначения, оставляем Любой
dst-port	any	Порт назначения, оставляем Любой
direction	out	Входящие пакеты (download)
target	PipeUp-1Mbps	Выбираем Upload-канал, PipeUp-1Mbps
description	GuestNetUpload	Произвольное описание

Создаем правило для трафика, идущего с Интернета (Download)

sequence	11	Номер генерируется автоматически, менять не нужно
interface	WAN	Выберите интерфейс, подключенный к интернету
interface2	GuestNet	Выберите интерфейс, подключенный к гостевой сети
proto	ip	Выберите протокол, в нашем случае IP
source	any	IP-адрес источника, любой
src-port	any	Порт источника, оставляем Любой
destination	any	IP-адрес назначения, оставляем Любой
dst-port	any	Порт назначения, оставляем Любой

direction	in	Входящие пакеты (download)
target	PipeDown-2Mbps	Выбираем Download-канал, PipeDown-2Mbps
description	GuestNetDownload	Произвольное описание

Нажмите **Применить** для того, чтобы активировать правила шейпирования.

8. Настройка гостевой сети

Функционал гостевой сети может использоваться в ресторанах, отелях или на предприятиях, где предоставляется гостевой доступа в Интернет. Общая схема работы пользователей гостевой сети следующая. Пользователь регистрируется на ресепшен в организации и получает карту (простой бумажный носитель с логином/паролем, который нужно использовать при доступе в Интернет). Устройство пользователя (например, смартфон) автоматически подключается к общедоступной Wi-Fi точке доступа заведения. Аналогично, клиентское устройство (например, ноутбук) может подключаться в проводную Ethernet-сеть организации. Пользователь Для того, чтобы воспользоваться Интернетом, пользователь обращается на нужный ему веб-сайт. Вместо запрошенного сайта, пользователь сначала попадет на внутренний портал (Captive Portal), где увидит информацию, подготовленную системным администратором (например, информация об организации, о правилах использования Интернет-доступа в организации). После ввода логина / пароля, указанного в карте, пользователь получает доступ в Интернет. Пользователи смогут работать в Интернет в течении предусмотренного администратором времени и не будут иметь доступ в остальные части сети организации.

В данной инструкции мы опишем настройку Captive Portal и генерацию серии карт для пользователей, а также сопутствующие настройки межсетевого экрана и DHCP-сервера.

Шаг 1 – Настройка интерфейсов

В данном примере, помимо LAN и WAN интерфейса будет использоваться GUESTNET интерфейс, который должен быть подключен к коммутатору или Wi-Fi точке в гостевой сети. Настройка коммутатора или точки доступа в данном документе не рассматривается.

Пройдите в раздел **Интерфейсы -> Назначения портов** и кликните на значок + для назначения нового интерфейса. Нажмите **Сохранить**. Выберите **Включить интерфейс** и введите следующие данные:

Описание	GUESTNET	Описательное имя для интерфейса
Блокировать частные сети	Не выбран	
Блокировать bogon сети	Не выбран	
Тип конфигурации IPv4	Статический IPv4	Статичный IPv4 адрес
Тип конфигурации IPv6	Отсутствует	
MAC-адрес	(Оставить пустым)	
Максимальный размер кадра	(Оставить пустым)	
Максимальный размер сегмента	(Оставить пустым)	
Скорость и двусторонний режим передачи данных	По умолчанию	
IPv4-адрес	192.168.200.1/24	Используем IP-адрес из диапазона гостевой сети, например 192.168.200.1
Публичный IPv4-адрес шлюза	Отсутствует	

Нажмите **Сохранить** для применения настроек.

Шаг 2 – Настройка DHCP-сервер

Пройдите в раздел **Службы -> DHCP -> Сервер** и кликните на вкладку **GUESTNET**.

Введите следующие настройки DHCP-сервера для гостевой сети (поля, которые явно не указаны остаются по умолчанию):

Включен	Флаг установлен	Включение DHCP-сервера на интерфейсе GUESTNET
Доступный диапазон	192.168.200.100 по 192.168.200.200	Выдавать IP-адреса из этого диапазона
DNS-серверы	192.168.200.1	Помещать в аренду информацию о DNS-серверах
Шлюз	192.168.200.1	Помещать в аренду информацию о шлюзе

Нажмите **Сохранить** для применения настроек.

Шаг 3 – Создание правил межсетевого экрана

Пройдите в раздел **Межсетевой экран -> Правила** для добавления нового правила. Далее, добавьте правила в указанном порядке.

Разрешение DNS

Данным правилом мы разрешаем гостевым пользователям доступ к DNS-форвардеру на устройстве TING. Введите следующие настройки правила (поля, которые явно не указаны остаются по умолчанию):

Действие	Разрешение
Интерфейс	GUESTNET
Протокол	TCP/UDP
Источник	GUESTNET net
Назначение	GUESTNET address
Диапазон портов назначения	DNS/DNS
Категория	Базовые правила для гостевой сети
Описание	Разрешение для DNS-трафика

Нажмите **Сохранить**.

Разрешение доступа на внутренний портал

Данным правилом мы разрешаем гостевым пользователям доступ ко внутреннему порталу на устройстве TING. Введите следующие настройки правила (поля, которые явно не указаны остаются по умолчанию):

Действие	Разрешение
Интерфейс	GUESTNET
Протокол	TCP
Источник	GUESTNET net
Назначение	GUESTNET address
Диапазон портов назначения	8000/10000
Категория	Базовые правила для гостевой сети
Описание	Разрешение доступа на внутреннний портал

Нажмите **Сохранить**.

Запрет доступа к локальным сетям

Данным правилом мы запрещаем доступ из гостевой сети в LAN-сеть организации. Введите следующие настройки правила (поля, которые явно не указаны остаются по умолчанию):

Действие	Блокирование
Интерфейс	GUESTNET
Протокол	ANY
Источник	GUESTNET net
Назначение	LAN net
Категория	Базовые правила для гостевой сети
Описание	Запрет доступа к локальным сетям

Нажмите **Сохранить**.

Запрет всего остального трафика, адресованного на устройство TING

Данным правилом мы запрещаем любой остальной трафик на устройство TING. Введите следующие настройки правила (поля, которые явно не указаны остаются по умолчанию):

Действие	Блокирование
Интерфейс	GUESTNET
Протокол	ANY
Источник	GUESTNET net

Назначение	GUESTNET address
Категория	Базовые правила для гостевой сети
Описание	Запрет всего остального трафика, адресованного на устройство TING

Нажмите **Сохранить**.

Разрешение всего трафика от гостевой сети

Данным правилом мы запрещаем любой остальной трафик на устройство TING. Введите следующие настройки правила (поля, которые явно не указаны остаются по умолчанию):

Действие	Разрешение
Интерфейс	GUESTNET
Протокол	ANY
Источник	GUESTNET net
Назначение	ANY
Категория	Базовые правила для гостевой сети
Описание	Разрешение всего трафика от гостевой сети

Нажмите **Сохранить**.

Шаг 4 – Настройка внутреннего портала

Пройдите в раздел **Службы -> Captive Portal -> Администрирование**. Кликните на значок + для добавления новой зоны. Для нашего сценария мы будем использовать следующие настройки:

Enabled	Флаг установлен	
Interfaces	GUESTNET	Уберите значение по умолчанию и поставьте GUESTNET
Authenticate using	(пусто)	***В дальнейшем, мы изменим настройку в этом поле***
Idle timeout	0	Выключите таймаут при простое
Hard timeout	0	Не задаем жестого значения таймаута
Concurrent user logins	Флаг не	Пользователь сможет залогинится

	установлен	только однажды
SSL certificate	Отсутствует	Использовать нешифрованый HTTP
Hostname	(оставить пустым)	
Allowed addresses	(оставить пустым)	
Custom template	Отсутствует	Использовать шаблон по умолчанию ***В дальнейшем, мы изменим настройку в этом поле***
Description	Гостевая сеть	smart_soft_zone

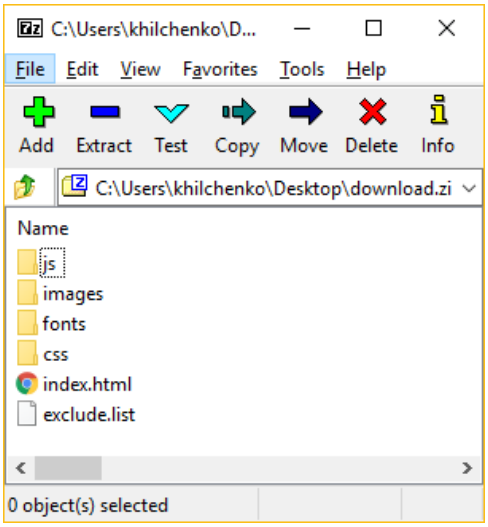
Примечание. При подключение гостевых сетей по нескольким интерфейсам, эти интерфейсы могут относится к одной зоне, или каждый интерфейс может находиться в своей собственной зоне.

Шаг 5 – Создание шаблона

Редактирование шаблона Captive Portal – одна из сильных сторон Traffic Inspector Next Generation, и сам процесс редактирования достаточно прост.

Пройдите в раздел **Службы -> Captive Portal,** вкладка **Шаблоны**, и кликните на значок загрузки для того, чтобы загрузить шаблон.

Мы модифицируем стандартный шаблон. Распакуйте скачанный zip-архив на своей машине. Содержимое архива должно быть примерно следующим:



Большинство файлов шаблона можно модифицировать, другие нельзя. При загрузке обратно на шлюз любые изменения файлов, указанные в exclude.list, будут игнорироваться. В настоящее время, к таким игнорируемым изменениям относятся Java-скрипты и некоторые шрифты.

Поменяем стандартную страницу на что-нибудь вроде этого:

Для этого, откройте файл **index.htlm** в вашем любимом текстовом редакторе и сделайте следующие изменения:

- Измените логотип на логотип компании
- Удалите навигационную строку в верхней части страницы
- Удалите высоту и ширину из <img> тега
- Добавьте нужный текст-приветствие
- Добавьте гиперссылку на веб-сайт организации

Найдите следующий блок в файле index.htlm:

```
<header class="page-head">
<nav class="navbar navbar-default" >
    <div class="container-fluid">
        <div class="navbar-header">
            <a class="navbar-brand" href="#">
                <img class="brand-logo" src="images/default-logo.png" height="30" width="150">
            </a>
        </div>
    </div>
</nav>
</header>
```

И поменяйте на блок:

```
<header class="page-head">
    <div align="center">
      <a href="#">
          <img class="brand-logo" src="images/company-logo.png">
      </a>
      <h1>Добро пожаловать в гостевую сеть компании Smart-Soft.</h1>
      <h2>Вы можете свободно пользоваться нашей сетью в профессиональных целях.<h2>
      <h3>Для получения дополнительной информации, пожалуйста, обратитесь на наш сайт: <a
href="https://smart-soft.ru">smart-soft.ru</a></h3>
    </div>
</header>
```

Скопируйте новую картинку с логотипом компании в папку **images**. Далее, запакуйте папку шаблона в zip-архив и закачайте его на устройство TING (к примеру, наш zip-архив называется **smart_soft.zip**). Начните закачку кликнув на значок + на вкладе **Шаблоны**. Введите имя для закачиваемого шаблона (например, **smart_soft**). По этому имени мы будем ссылаться на шаблон в интерфейсе TING. Нажмите кнопку **Загрузка**.

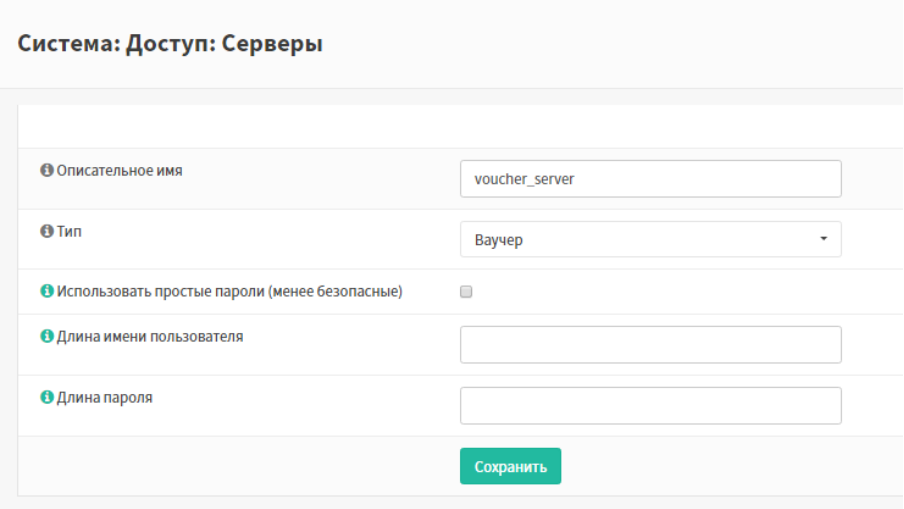
Вернитесь к ранее созданной зоне – раздел **Службы -> Captive Portal -> Администрирование**, редактирование зоны **Зона для гостевой сети**.

В поле **Custom template** выберите ранее закачанный шаблон **smart_soft**.

Шаг 6 – Создание сервера ваучеров

Пройдите в раздел **Система -> Доступ -> Серверы** и кликните на кнопку **Добавить сервер** в верхнем правом углу.

Описательное имя	voucher_server
Тип	Ваучер



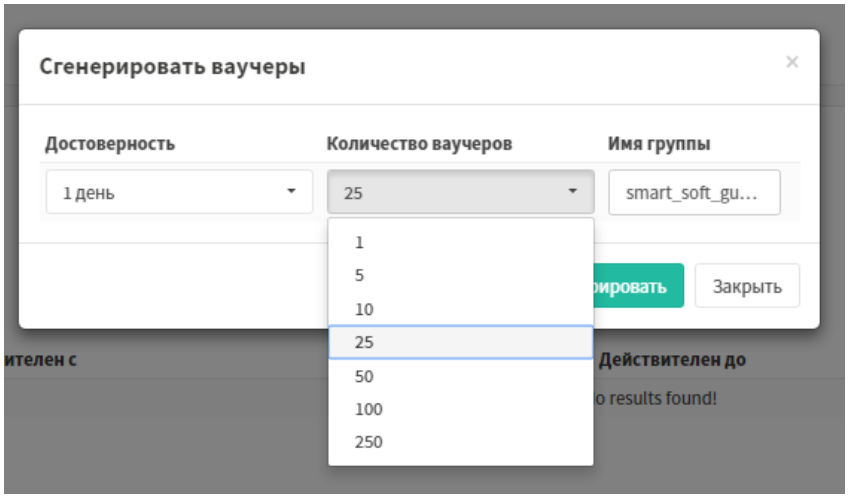
Остальные поля остаются по умолчанию.

Вернитесь к ранее созданной зоне – раздел **Службы -> Captive Portal -> Администрирование**, редактирование зоны **smart_soft_zone**. В поле **Authenticate using (Аутентифицироваться с помощью)** выберите ранее созданный сервер ваучеров.

Шаг 7 – Создание ваучеров

Пройдите в раздел **Службы -> Captive Portal -> Ваучеры**. Кликните на кнопку **Создать ваучеры**.

Создадим для наших гостей ваучеры сроком на один день.



Введите срок действия – 1 день, количество – 25 ваучеров, и имя группы Wi-Fi доступ.

Будет сгенерирован файл **wi-fi pass.csv**. Ниже приводится пример содержания данного файла:

username	password	vouchergroup	validity
DK.DM7R(	aS_@Mu)p81	Wi-Fi pass	86400
kvV+V=2q	T-8KIR=h2)	Wi-Fi pass	86400
9*m/*)PK	9INp3[TyeK	Wi-Fi pass	86400
4N?THK$:	JSNvi@Tm*n	Wi-Fi pass	86400
p)=Kmh7M	a4:W!(;)pI	Wi-Fi pass	86400
G)IAbw=y	4-21m]pAyp	Wi-Fi pass	86400
#NAME?	y0-+2qmUa\	Wi-Fi pass	86400
AuydiRS#	RpK[3KHv?Z	Wi-Fi pass	86400
Th\aaAo@	R@9/9T\@mA	Wi-Fi pass	86400
_+K0ya[2	Jp21RCK7$*	Wi-Fi pass	86400
\::NRmn!	:gRNGiNvhx	Wi-Fi pass	86400
:RJp2DWy	X2MH=iTeHU	Wi-Fi pass	86400
_MBVFXr3	TwTb.Jp58$	Wi-Fi pass	86400
bL9RrrFX	?]omD7IU+?	Wi-Fi pass	86400
h1yAN0S5	dHPkSo)MRz	Wi-Fi pass	86400
*xJrHu$I	$oTppt)97=	Wi-Fi pass	86400
UA09*vDr	;)0N1iapbD	Wi-Fi pass	86400
U7?)eZ4P	R#S_rZ[ChE	Wi-Fi pass	86400
4S)ZR!1@	80X:q(HVXm	Wi-Fi pass	86400
aKkq3!7T	x:m]k8_42F	Wi-Fi pass	86400
T/e%eu2H	KXTW8g;J:N	Wi-Fi pass	86400
\XzaG-KH	94a4Xon0m*	Wi-Fi pass	86400
t;2/wvIa	(#2[vFW,Ii	Wi-Fi pass	86400
_NAT9xgn	]2AS+5;gCM	Wi-Fi pass	86400
V,:$gq;B	2Mo4?d]?@P	Wi-Fi pass	86400

username	Имя пользователя, под которым будет логиниться гостевой пользователь
password	Пароль, который будет указывать гостевой пользователь

vouchergroup	Имя группы ваучеров
validity	Время жизни ваучера в секундах

Далее, мы можете создать карточки на бумажном носителе и вписать в них информацию из ранее сгенерированного файла с паролями.

Примечание. Из соображений безопасности пароли для ваучеров не хранятся на устройстве TING.

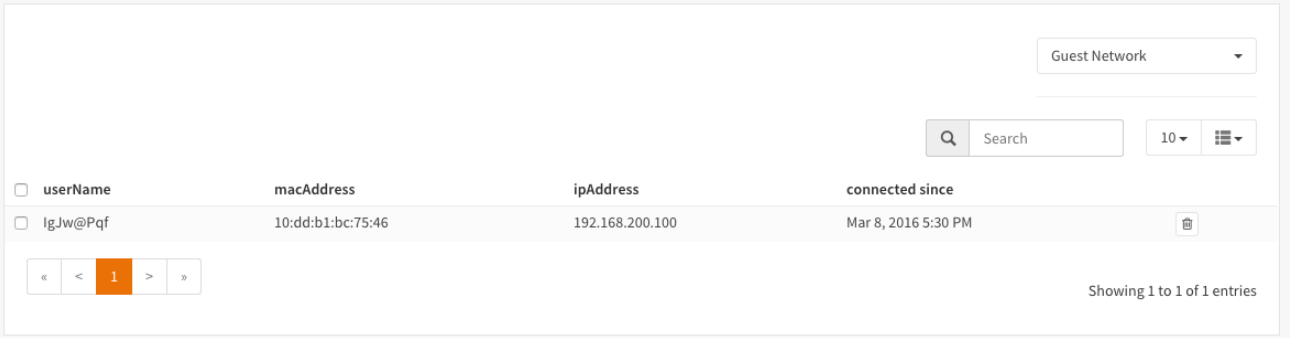
Шаг 8 – Аутентификация по ваучерам

Теперь, когда пользователи попадут на портал, они увидят поле ввода логина и пароля. Логин и пароль предоставляется пользователю на карте.

После активации пользователя по карте запускается таймер времени, который будет идти безотносительно того аутентифицирован пользователь в конкретный момент или нет.

Шаг 9 – Проверка сессий гостевых пользователей

Для того, чтобы увидеть активные сессий гостевых пользователей, пройдите в **Службы -> Captive Portal -> Сессии**. Сессия выглядит так:



Шаг 10 – Проверка состояния ваучеров

Вы можете посмотреть срок действия и статус ваучеров пройдя в раздел **Службы -> Captive Portal -> Ваучеры**.

Настройка завершена!