SMART-SOFT
ГРУППА КОМПАНИЙ

TRAFFIC INSPECTOR NEXT GENERATION

Traffic Inspector Next Generation
для образовательных учреждений

Содержание

1. Компьютерные сети в школе

Компьютеры нашли широкое применение в образовательных учереждених начиная с 90-ых годов. В 2000-ых к этому добавился высокоскоростной доступ к Интернету. Компьютеры и сеть позволили поднять образование на новый уровень. Многочисленные образовательные программы позволяют лучше осваивать школьный материал. Веб-ресурсы Wikipedia и YouTube уже на равных соперничают с традиционными источниками знаний. Учащиеся могут использовать Интернет для удаленного обучения и общения со своими иностранными сверстниками. Система электронных дневников в большей степени вовлекает родителей учеников в школьную жизнь своих чад. Однако, использование компьютерных сетей сопряжено с рядом проблем, которые приходится решать школьным системным администраторам:

- Организация доступа сети образовательного учреждения в Интернет
- Защита от несанкционированного доступа к сети образовательного учреждения
- Запрет доступа к нежелательным ресурсам сети Интернет
- Отчетность по использованию Интернета
- Защита от вирусов

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

- Настройка сетевого экрана и NAT
- Настройка веб-прокси сервера
- Настройка веб-фильтрации
- Настройка Layer 7 фильтрации
- Настройка антивирусной проверки трафика

2. Организация доступа образовательного учреждения к сети Интернет

Большинство организаций, активно использующих в своей работе Интернет, сталкиваются с проблемой «раздачи» Интернета на все компьютеры во внутрненней 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 преробразования 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 значет, 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 предоставит 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 укажим 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 сети образовательного учреждения

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, настроеных 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 в 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 (подс***е***ти), 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**.

Устновите 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**.

Устновите 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**.

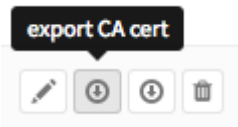
Для добавления новой записи, финализируйте ввод нажатием клавиши Enter. Для добавления всех поддоменов домена, укажите точку перед доменом. Например: для добавления всех поддоменов paypal.com введите .paypal.com, затем Enter.

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 следующющими настройками:

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

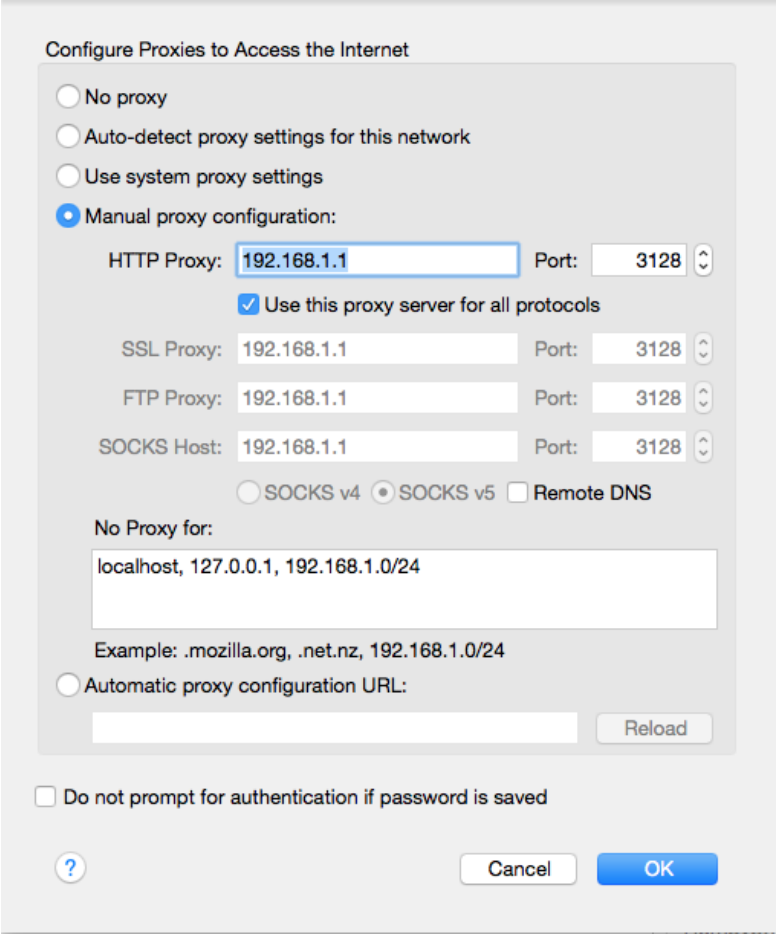
Далее, добавьте еще одно правило для блокировки HTTPS-доступа.

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

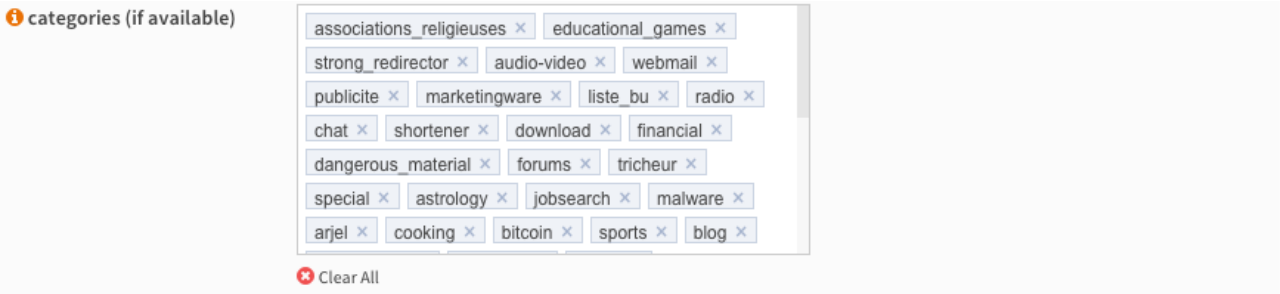
Нажмите **Сохранить изменения.**

Шаг 3 - Загрузка категорий

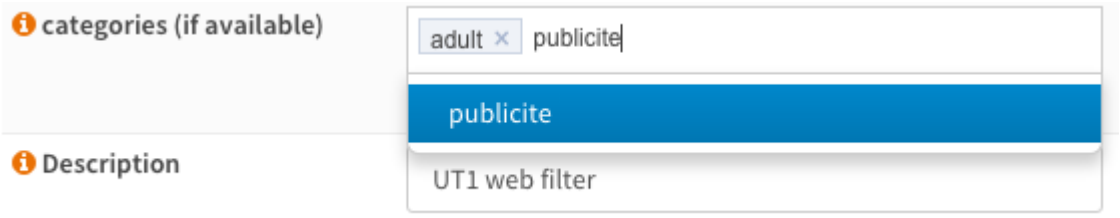
Нажмите **Загрузить списки доступа**. Учтите, что загрузка займет некоторое время (до нескольких минут), так как полный список (>19 МБ) конвертируется в списки контроля доступа Squid.

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 следующющими настройками:

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

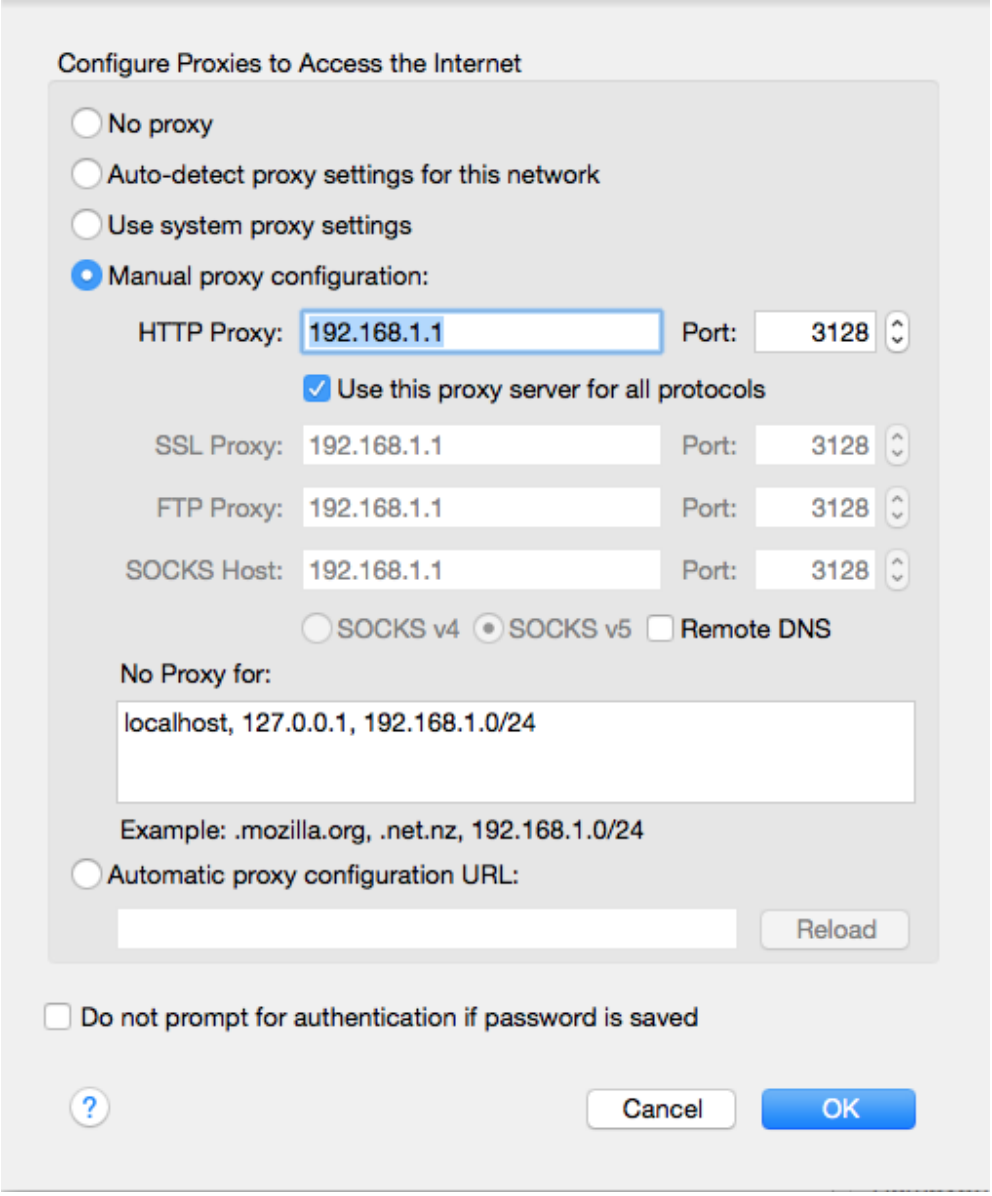
Далее, добавьте еще одно правило для блокировки HTTPS-доступа.

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

Фунционал 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 фунционала 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. Антивирусная защита

О плагине HTTP Antivirus Proxy

Плагин HAVP представляет собой специализированный прокси-сервер, которому в виде библиотеки подключается антивирусный движок ClamAV. Плагин HAVP обеспечивает централизованную проверку трафика на уровне шлюза.

Поддерживается проверка:

- HTTP-трафика
- FTP over HTTP-трафика (обращение к FTP-серверу через HTTP-прокси)
- HTTPS-трафика, при настроенном функционале перехвата HTTPS-соединений, а также трафик

Механизм антивирусной проверки устроен следующим образом. Пользовательский веб-трафик попадает к демону Squid (по причине наличия у пользователя явных настроек на HTTP-прокси или из-за механизма прозрачного проксирования). В настройках Squid прописан каскад на вышестоящий прокси (HAVP), который, в действительности, выполняется на этой же машине и использует сокет 127.0.0.1:8080. HAVP прокси и интегрированный в него антивирусный движок ClamAV обеспечивают антивирусную проверку трафика.

Настройка плагина HAVP включает в себя следующие шаги.

Шаг 1 – Установка плагина HAVP

Пройдите в раздел **Система -> Прошивка -> Обновления**, вкладка Плагины и нажмите Проверить наличие обновлений.

Примечание. Для успешной проверки обновлений в вашем устройстве TING должен быть установлен лицензионный сертификат. Для получения информации по установке сертификата, обратитесь к инструкции **Начало работы с TING**.

В случае успешной проверки обновлений, вы увидите список доступных плагинов. Выберите плагин **os-havp** и нажмите на значок +, чтобы установить его.

Шаг 2 – Настройка веб-прокси Squid

Для работы HAVP плагина, требуется включенный и настроенный веб-прокси. Для получения информации по настройке веб-прокси, обратитесь к инструкции **Настройка веб-прокси**.

Дополнительно, можно настроить прозрачное проксирование. Суть "прозрачного проксирования" - пользователи не имеют явных настроек на веб-прокси, тем не менее их трафик все равно попадет на прокси. Для получения информации по настройке прозрачного проксирования, обратитесь к инструкции **Настройка прозрачного проксирования**.

Шаг 3 – Настройка плагина HAVP

Пройдите в раздел **Службы -> HTTP Antivirus Proxy -> Администрирование**.

Для включения HAVP плагина, установите флаг **Включить HAVP**.

Примечание. Запуск и перезапуск HAVP-плагина требует времени, так как сопровождается загрузкой антивирусной базы (размером в среднем 100 МБ) в оперативную память.

Для сканирования изображений, установите флаг **Включить сканирование изображений**.

Определите пороговое значение размера файла в поле **Maximum size of scaned file (MB)**. Файлы большего размера проверяться не будут.

После включения плагина HAVP перезагрузите шлюз – **Maintenance -> Перезагрузка**.

Шаг 4 – Проверка настроек плагина HAVP

Подключитесь к шлюзу по SSH. Для этого можно использовать популярный SSH-клиент Putty. Выполните команду:

cat /usr/local/etc/squid/squid.cong

Конфигурационный файл Squid должен заканчиваться строками:

cache_peer 127.0.0.1 parent 8080 0 no-query no-digest

never_direct allow all

Шаг 5 – Настройка исключений

В раздел **Службы -> HTTP Antivirus Proxy -> Администрирование**, щелкните на значок + в нижнем правом углу экрана. Задайте URL, в отношении которого сканирование выполняться не будет, например:

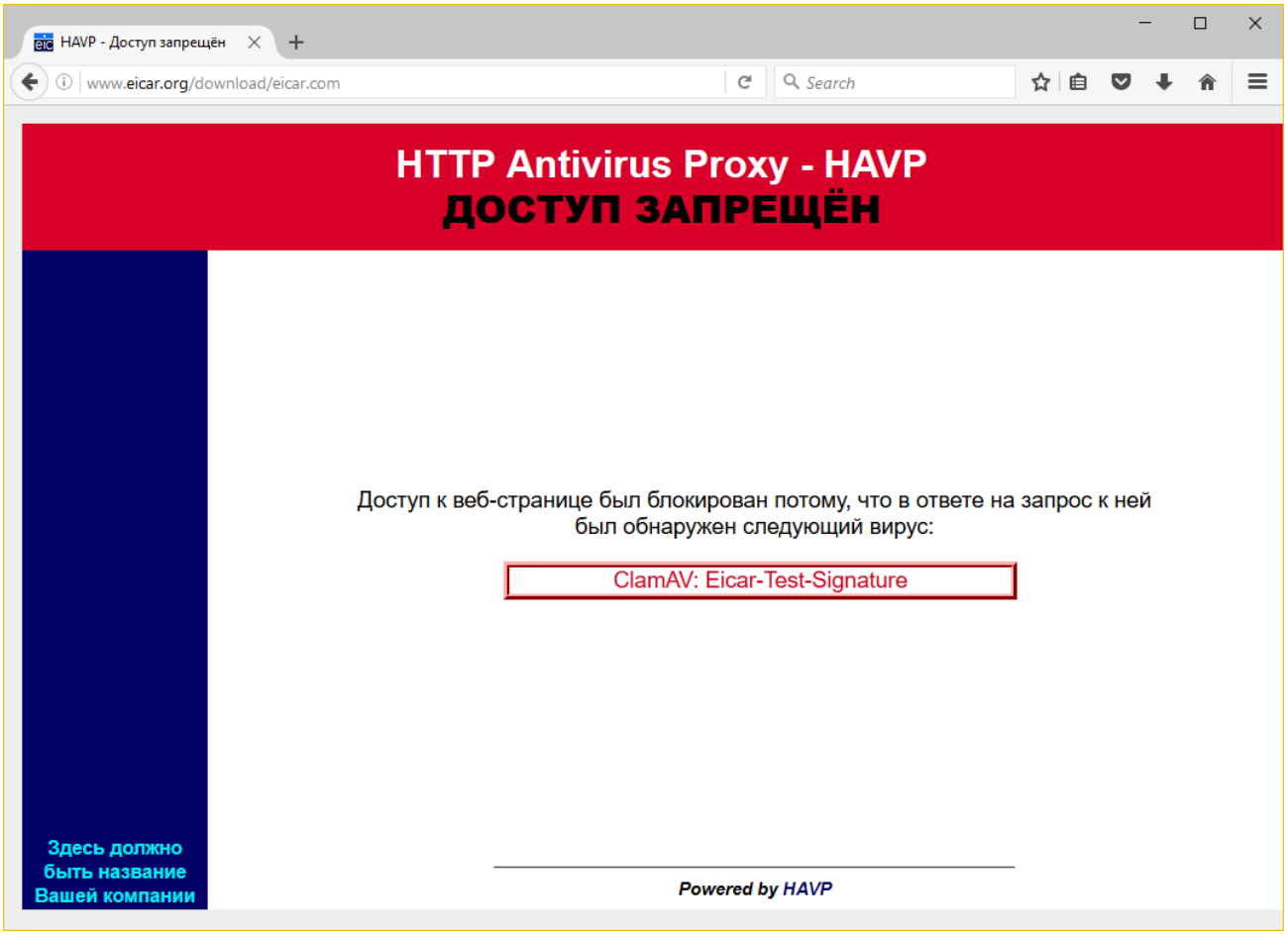
Примечания.

URL задается в формате без схемы (т.е. без части **http://**).

Исключение применимо только для указанного URL. Например, если мы исключаем сканирование URL <example.org>, то URL <example.org/example.exe> сканироваться будет.

Шаг 6 – Антивирусная проверка

При обнаружении потенциально опасного содержимого, HAVP плагин отображает страницу блокировки в браузере пользователя:



Настройка завершена!