SMART-SOFT
ГРУППА КОМПАНИЙ

TRAFFIC INSPECTOR NEXT GENERATION

Traffic Inspector Next Generation
для государственных учреждений

Содержание

1. Компьютерные сети в государственных учреждениях

Компьютерные сети играют важную роль в работе государственных учреждений. Рабочее место чиновника наверняка будет подключено к Интернету для более эффективного выполнения обязанностей последним. Госслужащие могут легко осуществлять коммуникацию с помощью электронной почты. Сеть обеспечивает доступ к критически важным приложениям и базам данных. В последнее время все большее количество социальных услуг оказывается через Интернет.

Вместе с тем, у всех достоинств Интернета есть и обратная сторона – возросшие риски в сфере информационной безопасности и сложность организации защищенного сетевого подключения. Проблемы, с которыми сталкиваются государственные учреждения, включают:

- Организация доступа к сети Интернет для корпоративной сети
- Защита от Интернет-угроз
- Борьба с нецелевым использованием Интернета
- Обеспечение отказоустойчивого доступа к Интернету
- Интеграция сетевого шлюза с доменной инфраструктурой Active Directory
- Сбор статистики по доступу 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 государственного учреждения и настройку наиболее актуального функционала:

- Настройка сетевого экрана и NAT
- Настройка веб-фильтрации
- Балансировка нагрузки и отказоустойчивость WAN-каналов
- Аппаратная отказоустойчивость (кластеризация)
- Настройка прозрачной аутентификации на прокси через Active Directory
- Работа с отчетами

2. Доступ государственного учреждения 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 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 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 сети государственного 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, 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-соединений 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**.

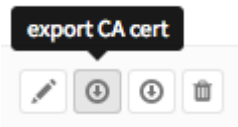
Для добавления новой записи, финализируйте ввод нажатием клавиши Enter. Для добавления всех поддоменов домена, укажите точку перед доменом. Например: для добавления всех поддоменов paypal.com введите .paypal.com, затем Enter.

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 применяться 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.

4.1.1. 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

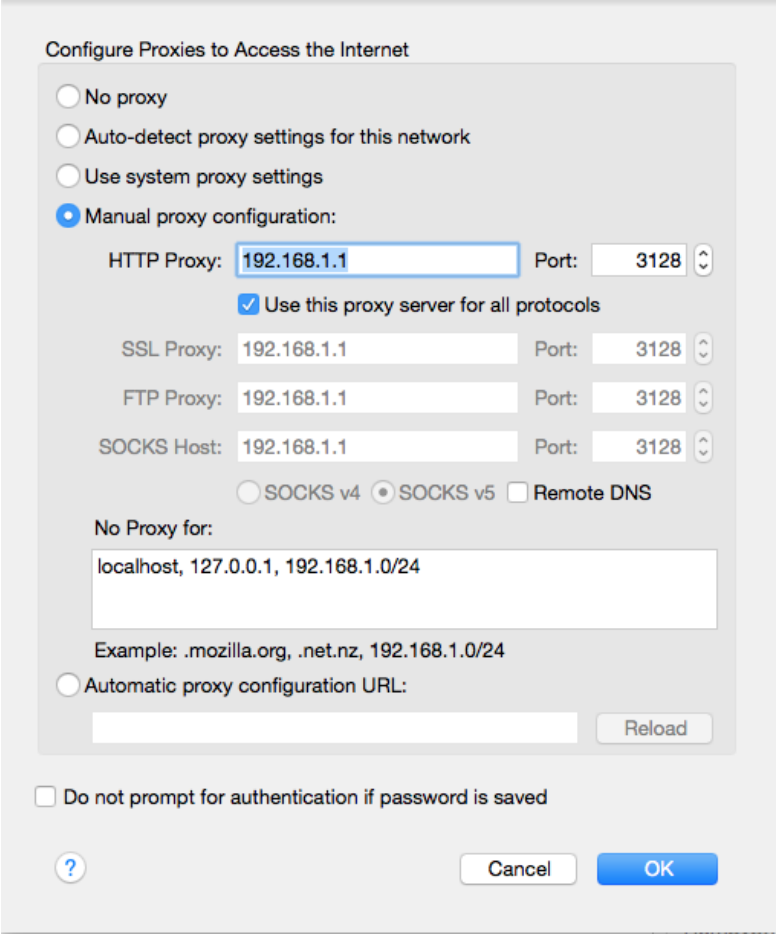
Далее, добавьте еще одно правило для блокировки HTTPS-доступа.

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

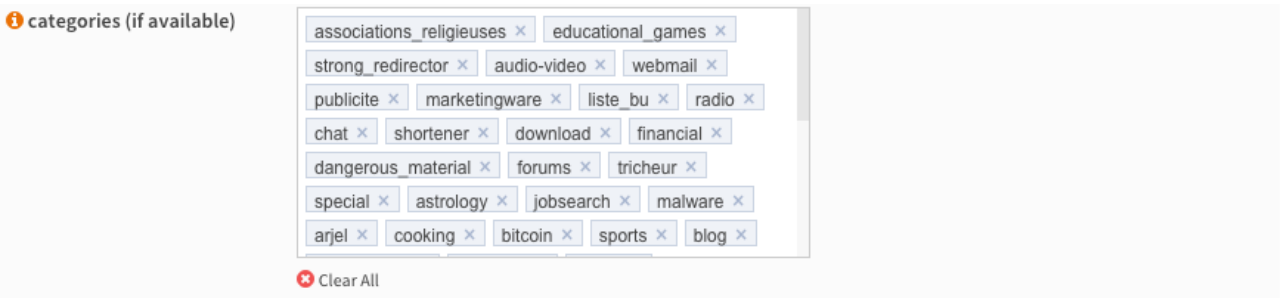
Нажмите **Сохранить изменения.**

Шаг 2 - Загрузка категорий

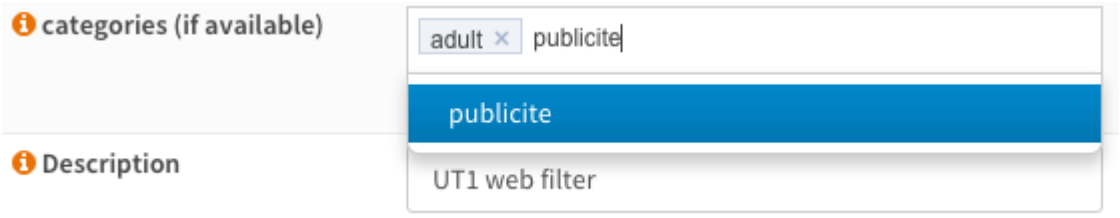
Нажмите **Загрузить списки доступа**. Учтите, что загрузка займет некоторое время (до нескольких минут), так как полный список (>19 МБ) конвертируется в списки контроля доступа Squid.

Шаг 3 - 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 4 - 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

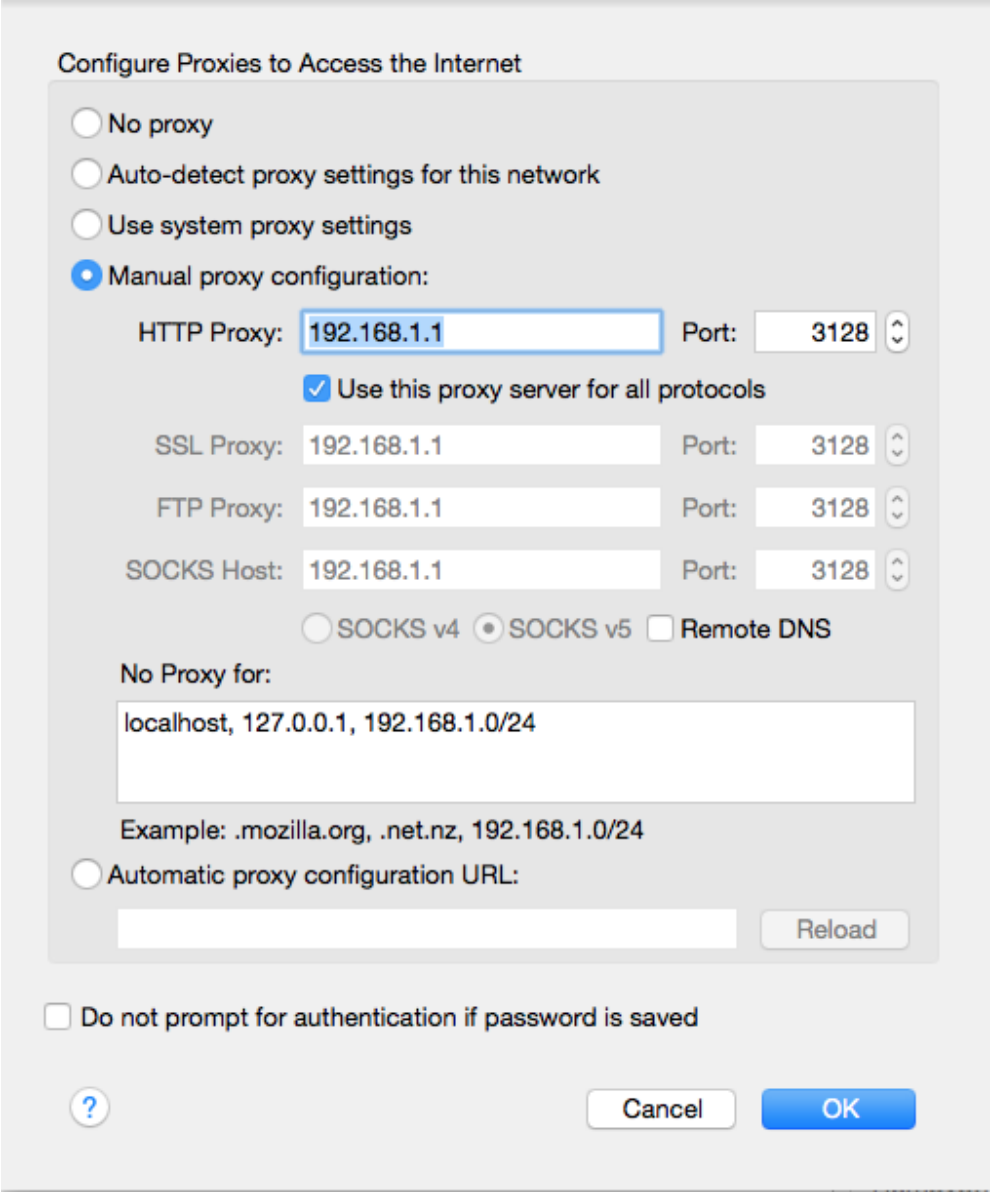
Далее, добавьте еще одно правило для блокировки HTTPS-доступа.

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 5 - 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. Переключение на запасные каналы при отказе основного и балансировка трафика между WAN-интерфейсами

В данной инструкций рассматривается:

- переключение на запасные каналы при отказе основного
- балансировка трафика между WAN-интерфейсами

6.1. Переключение на запасные каналы при отказе основного

Несколько WAN-каналов обычно используются в сценариях переключения при отказе и балансировки нагрузки, но в Traffic Inspector Next Generation эти два функционала можно сочетать.

Для настройки данного функционала нужно выполнить следующие шаги:

1. Добавить в настройки шлюзова мониторинговые IP-адреса
2. Добавить шлюзововую группу
3. Настроить DNS для каждого шлюза
4. Использовать маршрутизацию на основе политики для наших шлюзовых групп
5. Добавить правило для DNS-трафика, который направлен на само устройство TING

В нашем примере мы используем два ранее настроенных шлюза (раздел **Система -> Шлюзы -> Все**), в отношении которых мы убедились, что они являются рабочими. В качестве мониоринговых IP-адресов и IP-адресов DNS-серверов мы будем использовать адреса от публичного сервиса Google – 8.8.8.8 и 8.8.4.4. Конечно вы можете использовать собственные проверенные адреса.

Шаг 1 – Настройка мониторинговых IP-адресов

Данный шаг можно пропустить, если мониторинговые IP-адреса были настроены ранее и статус шлюзов указан как «Онлайн».

Для настройки мониторингового IP-адреса пройдите в раздел **Система -> Шлюзы -> Все**, выберите запись о шлюзе и кликните на символ «Карандаш» для редактирования его настроек. Убедитесь, что настроены следующие аспекты:

Отключить Мониторинг шлюзов	Флаг не установлен	Убедимся, что мониторинг включен
Монитор IP	8.8.8.8	Мы используем DNS от Google
Пометить шлюз как недоступный	Флаг не установлен	

Далее, кликаем на следующем символе «Карандаш» для редактирования настроек второго шлюза. Убедитесь, что настроены следующие аспекты:

Отключить Мониторинг шлюзов	Флаг не установлен	Убедимся, что мониторинг включен
Монитор IP	8.8.4.4	Мы используем альтернативный DNS-сервер от Google
Пометить шлюз как недоступный	Флаг не установлен	

Шаг 2 – Добавление шлюзовой группы

Пройдите в раздел **Система -> Шлюзы -> Группа** и нажмите на + Добавить группу в верхнем правом углу.

Используйте следующие настройки:

Имя группы	WANGWGROUP	Имя группы, по которому не нее можно ссылаться

Приоритет шлюза	WANGW / Tier 1	Выберите первый шлюз и Ранг 1
..	WAN2GW / Tier 2	Выберите второй шлюз и Ранг 2
Уровень срабатывания	Потеря пакетов	Выберите необходимый уровень срабатывания
Описание	Failover Group	Произвольное описание

Пояснение по настройке «Уровень срабатывания»

- Участник недоступен

Срабатывает при 100% потере пакетов.

- Потеря пакетов

Срабатывает, когда потеря пакетов превышает установленное пороговое значение.

- Большая задержка

Срабатывает, когда задержка превышает установленное пороговое значение.

- Потеря пакетов и высокая задержка

Срабатывает, когда потеря пакетов превышает установленное пороговое значение или когда задержка превышает установленное пороговое значение.

Шаг 3 – Настройка DNS для каждого шлюза

Пройдите в раздел **Система -> Настройки -> Общие** и убедитесь, что каждый шлюз использует свой собственный DNS-сервер:

8.8.8.8	WANGW
8.8.4.4	WAN2GW

Шаг 4 – Настройка маршрутизации по политикам

Пройдите в раздел **Сетевой экран -> Правила**.

В нашем примере, мы модифицируем уже существующее правило для пропуска всего трафика из LAN-сети. Кликните на символ «Карандаш» рядом с этим правилом (Default allow LAN to any rule).

В поле Шлюз пропишите имя шлюзовой группы *WANGWGROUP*.

Сохраните настройки, чтобы они применились.

Примечание.

Из-за данного правила, весь трафик из LAN-сети будет направляться на выбранную шлюзовую группу. Это означает, что трафик, направленный самому устройству TING, также будет маршрутизироваться в этом (в данном случае, неправильном) направлении. Именно этим объясняется необходимость создания правила для DNS-трафика, которое описано на шаге 5.

Шаг 5 – Создание разрешающего правила для DNS-трафика

Над правилом для пропуска трафика из LAN, поместите правило, которое позволит маршрутизации DNS-трафика / 53 порт на шлюзовую группу в случае когда этот трафик направлен самому устройству или генерируется самим устройством.

Действие	Разрешение	Разрешить прохождение трафика
Интерфейс	LAN	
TCP/IP версии	IPv4	В нашм примере используем IPv4
Протокол	TCP/UDP	Выбираем нужный протокол
Источник	any	
Назначение	Единственный хост или сеть	
Назначение	192.168.1.1/32	IP сетевого экрана, поэтому

		маска /32
Диапазон портов назначения	DNS – DNS	Только DNS
Категория	DNS	
Описание	Local Route DNS	Произвольное описание
Шлюз	default	Выбираем default

Расширенные опции

Для каждого шлюза могут быть настроены несколько расширенных опций, которые меняют дефолтное поведение / пороги значений. Данные опции можно поменять в разделе **Система -> Шлюзы -> Все**; кликните на символ «Карандаш» рядом со шлюзом, настройки которого нужно модифицировать.

В настоящее время поддерживаются опции:

- Пороговое значение задержки

Наименьшее и наибольшее пороговые значения для задержки в миллисекундах.

- Пороговые значения потери пакетов

Наименьшее и наибольшее пороговые значения для потери пакетов в процентах.

- Интервал опроса

Как часто посылается мониторинговый ICMP-пакет в секундах.

- Недоступен

Количество секунд после неудачного ICMP-запроса, после которого сработает сигнализация о недоступности.

- Средняя задержка ответов

Количество ответов используемых для вычисления среднего значения задержки перед срабатыванием сигнализация о недоступности.

- Среднее количество потерянных пакетов опроса

Количество тестовых пакетов для вычисления среднего количества потерянных пакетов.

- Задержка утраченного опроса

Задержка после которой вычисляется потеря пакетов.

6.2. Балансировка трафика между WAN-интерфейсами

Для настройки балансировки нагрузки следуйте той же инструкции, что и при настройке переключения при отказе, то на шаге 2 выберите одинаковый ранг для обоих шлюзов.

В результате поведение изменится с переключения при отказе на равное распределение трафика между выбранными шлюзами.

«Залипающие» соединения

Некоторые веб-сайты не будут работать, если IP-клиента измениться в процессе существования соединения. Для решения данной проблемы можно использовать настройку **Залипающие соединения**, которая обеспечивает маршрутизации всех пакетов соединения через один и тот же шлюз.

Для включения данной опции, пройдите в **Система -> Настройки -> Разное.**

Неравномерная балансировка

Если у вас имеет ассиметричное подключение где один провайдерский канал имеет большую пропускную способность чем другой, то можно установить настройки «веса» для каждого шлюза и изменить тем самым баланс нагрузки. Например, если у вас один канал – 10 Мбит/с, а второй – 20 Мбит/с, то настройте вес первого шлюза как «1» и второго – как «2». Как результат, второй шлюз получит вдвое больше трафика чем первый.

Данные опции можно поменять в разделе **Система -> Шлюзы -> Все**; кликните на символ «Карандаш» рядом со шлюзом, настройки которого нужно модифицировать.

Совместное использование балансировки и переключения при отказе

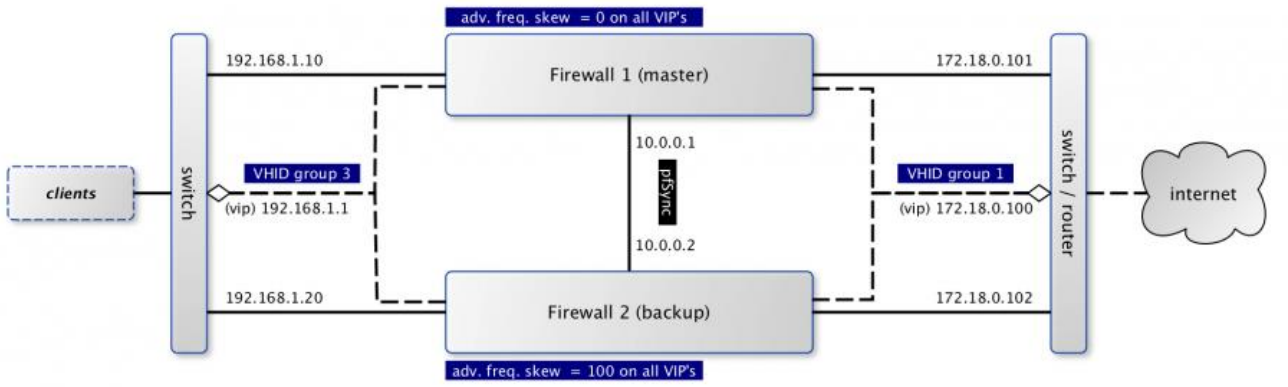
Для совместного использования балансировки и Failover у вас будет 2 или более соединений для нужд балансировки и 1 и более подключений для переключения при отказе. Traffic Inspector Next Generation поддерживает 5 рангов (групп избыточности), и в каждой группе может быть несколько WAN-каналов.

Настройка завершена!

7. Настройка аппаратной отказоустойчивости

Одна из наиболее интересных функциональных черт Traffic Inspector Next Generation – это возможность настройки кластера из нескольких сетевых экранов с автоматическим переключением на запасное устройства в случае возникновения проблем с основным.

В нашем примере, IP-сеть 192.168.1.0/24 будет – это внутренняя сеть организации, и сеть 172.8.0.0/24 используется для маршрутизации трафика пользователей в Интернет.



При использовании CARP, все интерфейсы, участвующие в работе протокола, должны иметь по собственному IP-адресу в сочетании с одним общим виртуальным IP-адресом, который и будет использоваться для общения с внутренней и внешней сетями. На изображении пунктирные линии обозначают виртуальные IP-адреса.

Терминология

Кратко поясним терминологию, с которой столкнемся в процессе настройки CARP-кластера:

CARP

Common Address Redundancy Protocol имеет IP-идентификатор 112, происходит из среды операционных систем OpenBSD, и использует мульти вещательные пакеты для того, чтобы сигнализировать соседним машинами о состоянии данной машины. Обязательно убедитесь, что ничего не будет препятствовать прием CARP-пакетов на интерфейсах. Каждый виртуальный интерфейс должен иметь уникальный Virtual Host ID (vhid), который находится в совместном использовании сразу несколькими машинами. Для определения, какая из запасных машин подменит основную в случае выхода её из строя, машины имеют настроенный параметр «смещение» (skew), который публикуют посредством рассылки сообщений. Меньшее значение смещения означает больший приоритет (основная машина в группе имеет смещение равное «0»).

pfSync

Совместно с CARP для синхнонизации состояния сетевых экранов используется протокол pfSync. При переключении на запасной сетевой экран нужно обеспечить, что он «знал» о всех соединениях – так переключение пройдет фактически незаметно. Настоятельно рекомендуем использовать выделенный интерфейс для обмена pfSync-пакетами между шлюзами – и по причинам безопасности, и по причинам производительности.

XMLRPC sync

Traffic Inspector Next Generation имеет механизм для синхронизации настроек запасных сетевых экранов с основным. Данный механизм называется XMLRPC sync и настраивается в разделе **Система -> Высокий уровень доступности**.

Шаг 1- Настройка интерфейсов и базовые правила сетевого экрана

В нашем примере используется три интерфейса, для которых используем достаточно базовые настройки.

Основной сетевой экран

Убедитесь, что все три интерфейса настроены и имеют следующие IP-адреса и сети:

LAN	192.168.1.10/24
WAN	172.18.0.101/24
PFSYNC	10.0.0.1

Далее, нужно убедиться, что нужные протоколы могут использоваться на наших интерфейсах – для этого пройдите в раздел **Межсетевой экран -> Правила** и проверьте, что интерфейсы LAN и WAN позволяют пропускать по меньшей мере CARP-пакеты. Поскольку мы соединяем два шлюза прямым кабельным соединением через интерфейс PFSYNC, то для него можно создать одно правило, которое будет пропускать весь трафик по всем протоколам. Как альтернатива, можно разрешить только трафик для GUI (HTTP или HTTPS) и pfSync-трафик.

Запасной сетевой экран

Для интерфейсов запасного сетевого экрана мы используем следующие адреса:

LAN	192.168.1.20/24
WAN	172.18.0.102/24
PFSYNC	10.0.0.2

Поскольку от запасного сетевого экрана требуется лишь возможность синхронизировать состояние с основным сетевым экраном, нам нужно всего лишь разрешить прием pfSync-трафик по интерфейсу PFSYNC.

Шаг 2- Настройка виртуальных IP-адресов

На основном сетевом экране мы настроим виртуальные IP-адреса, которые также попадут на запасной сетевой экран в результате синхронизации. Пройдите в раздел **Сетевой экран -> Виртуальные IP-адреса** и добавьте два виртуальных IP-адреса как показано ниже:

Тип	Carp
Интерфейс	WAN
IP-адрес	172.18.0.100/24
Пароль	ting
VHID группа	1
Частота публикации	Base 1 / Skew 0
Описание	VIP WAN

Тип	Carp
Интерфейс	LAN
IP-адрес	192.168.1.1/24
Пароль	ting
VHID группа	3
Частота публикации	Base 1 / Skew 0
Описание	VIP LAN

Шаг 3 - Настройка NAT

Настройка CARP-кластера требует перенастройки NAT, так как теперь именно виртуальный IP-адрес должен прописываться в пакетах при их преобразовании.

Пройдите в раздел **Сетевой экран -> NAT** и выберите раздел «Исходящий». Далее, на странице выберите **Ручное создание правил исходящего NAT** и в правилах,

которые в качестве источника имеют 192.168.1.0/24, пропишите использование CARP-интерфейса (172.18.0.100) в поле **Транслируемый IP-адрес / целевой IP-адрес**.

Шаг 4 - Настройка DHCP-сервера

В ситуации, когда используется DHCP-сервер для раздачи адресов в локальной сети, нужно учесть некоторые моменты. Все пользователи должны использовать в качестве адреса шлюза по умолчанию виртуальный IP-адрес группы, а не реальный IP-адрес шлюза, распространяемый DHCP-сервером.

Пройдите в раздел **Службы -> Сервер** и пропишите виртуальный IP-адрес в следующих настройках:

- Шлюз
- DNS-серверы
- IP-адрес участника для аварийного переключения

Шаг 5 - Настройка XMLRPC и pfSync

Пройдите в раздел **Система -> Высокий уровень доступности** и установите флажок «Синхронизировать состояния» для того, чтобы включить pfSync. Также, настройте адрес хоста, с которым будет идти синхронизация (10.0.0.2). Данная настройка осуществляется на всех машинах-членах кластера.

Далее, на основной машине группе избыточности включите синхронизацию с помощью XMLRPC. Для этого в поле **Synchronize Config to IP** укажите запасного члена кластера, с которым будет происходить синхронизация, а также выберите синхронизируемые настройки:

Правила межсетевого экрана
NAT
DHCPD
Виртуальные IP-адреса

Шаг 6 - Финальные настройки и проверка

Для того, чтобы все настройки были применены, перезагрузите оба сетевых экрана.

Для проверки работы кластера, мы установим SSH-подключение с клиентского компьютера в локальной сети к некоторому хосту в Интернете. После этого, вы должны видеть информацию по этому соединению в таблице состояния на обоих сетевых экранах. Далее, попытайтесь выключить сетевой кабель из главного сетевого экрана, и обработка соединения должна быть перехвачена запасным сетевым экраном.

Настройка завершена!

8. Настройка аутентификации в Active Directory через Kerberos на прокси

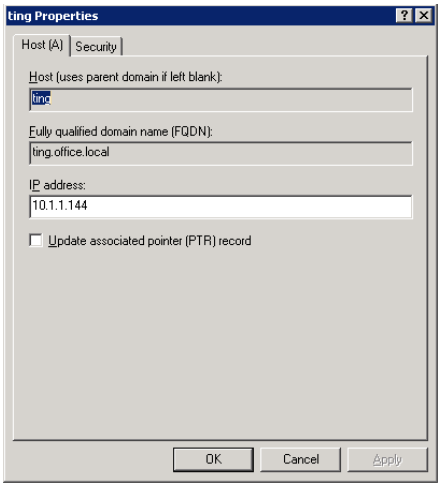
Шаг 1 – Настройка доменного DNS-сервера

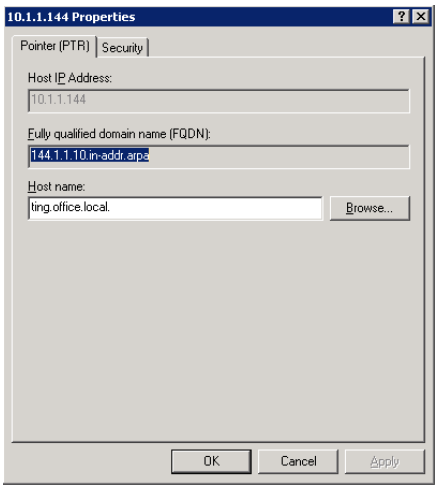
В нашем примере, используются следующие сетевые идентификаторы:

Устройство	IP-адрес	DNS-имя
контроллер домена	10.1.1.15	adm2.office.local
TING	10.1.1.144	ting.office.local

На доменном DNS-сервере:

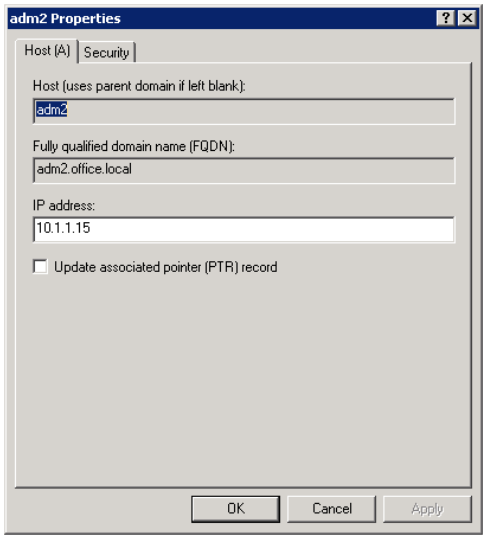
- добавьте в прямую доменную зону запись типа A, позволяющую осуществлять прямое преобразование DNS-имени устройства TING в его IP-адрес
- добавьте в обратную доменную зону запись типа PTR, позволяющую осуществлять обратное преобразование IP-адреса устройства TING в его DNS-имя



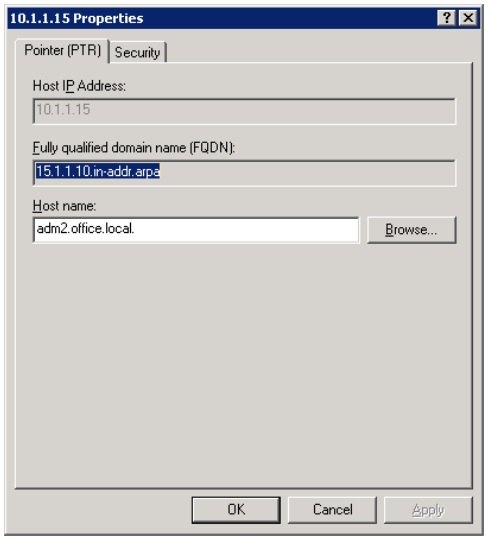


Проверьте существование на DNS-сервере:

- в прямой доменную зону запись типа A, позволяющую осуществлять прямое преобразование DNS-имени контроллера домена в его IP-адрес



- в обратной доменной зоне запись типа PTR, позволяющую осуществлять обратное преобразование IP-адреса контроллера домена в его DNS-имя



Шаг 2 – Настройка DNS-параметров устройства TI NG

Пройдите в раздел **Система -> Настройки -> Общие настройки**.

- В поле **Имя хоста** укажите полное имя устройства TING.
- В поле **Домен** укажите полное DNS-имя домена.
- В поле **DNS-серверы**, укажите IP-адрес доменного DNS-сервера.
- В поле Настройки DNS-сервера, уберите флаг напротив опции **Не используйте DNS-форвардер как DNS-сервер для межсетевого экрана**

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

```
cat /etc/resolv.conf
```

В выводе вы должны увидеть указанный ранее IP-адрес (в нашем примере – 10.1.1.15), например:

```
nameserver 10.1.1.15
```

Проверьте прямое и обратное разрешение DNS-записей с устройства TING. Выполните команды:

```
dig ting.office.local
```

Пример успешного результата:

```
; <<>> DiG 9.10.4-P2 <<>> ting.office.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3919
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;ting.office.local.             IN      A

;; ANSWER SECTION:
ting.office.local.      3600    IN      A       10.1.1.144

;; Query time: 2 msec
```

```
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 27 16:39:46 MSK 2016
;; MSG SIZE  rcvd: 62
```

dig –x 10.1.1.144

Пример успешного результата:

```
; <<>> DiG 9.10.4-P2 <<>> -x 10.1.1.144
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5615
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;144.1.1.10.in-addr.arpa.       IN      PTR

;; ANSWER SECTION:
144.1.1.10.in-addr.arpa. 3600   IN      PTR     ting.office.local.

;; Query time: 7 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 27 16:42:55 MSK 2016
;; MSG SIZE  rcvd: 83
```

dig adm2.office.local

Пример успешного результата:

```
; <<>> DiG 9.10.4-P2 <<>> adm2.office.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60218
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;adm2.office.local.             IN      A

;; ANSWER SECTION:
```

```
adm2.office.local.      3600    IN      A       10.1.1.15

;; Query time: 18 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 27 16:44:17 MSK 2016
;; MSG SIZE  rcvd: 62
```

dig –x 10.1.1.15

Пример успешного результата:

```
; <<>> DiG 9.10.4-P2 <<>> -x 10.1.1.15
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57694
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;15.1.1.10.in-addr.arpa.                IN      PTR

;; ANSWER SECTION:
15.1.1.10.in-addr.arpa. 1200    IN      PTR     adm2.office.local.

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Sep 27 16:41:54 MSK 2016
;; MSG SIZE  rcvd: 82
```

Шаг 3 – Настройка сетевого времени

Настройка времени на устройстве производится в рамках работы мастера первоначальной настройки – **Система -> Мастер**. Также, настройки времени доступны в разделе **Службы -> Сетевое время -> Общие настройки**. В поле **Серверы времени** укажите ваш предпочитаемый сервер времени, например: time.bakulev.ru.

Шаг 4 – Настройка LDAP-коннектора

Для успешного подключения к базе пользователей Active Directory нужно настроить параметры подключения.

Пройдите в раздел **Система -> Доступ -> Серверы,** в правом верхнем углу нажмите на кнопку **Добавить сервер** и задайте следующие настройки:

Описательное имя	AD connector
Тип	LDAP
Имя хоста или IP-адрес	10.1.1.15
Значение порта	389
Транспортный протокол	TCP
Версия протокола	3
Привязать параметры доступа	Уникальное имя пользователя: имя доменной учетной записи с правами чтения из домена Пароль: пароль для учетной записи
Область поиска	Уровень: единичный База поиска: DC = office, DC = local (наш домен имеет DNS-имя office.local)
Контейнеры для аутентификации	Выберите контейнеры, в которых располагаются доменные учетные записи (например, CN=Users,DC=office,DC=local)
Начальный шаблон	Microsoft AD
Атрибут присвоения имени пользователю	samAccountName

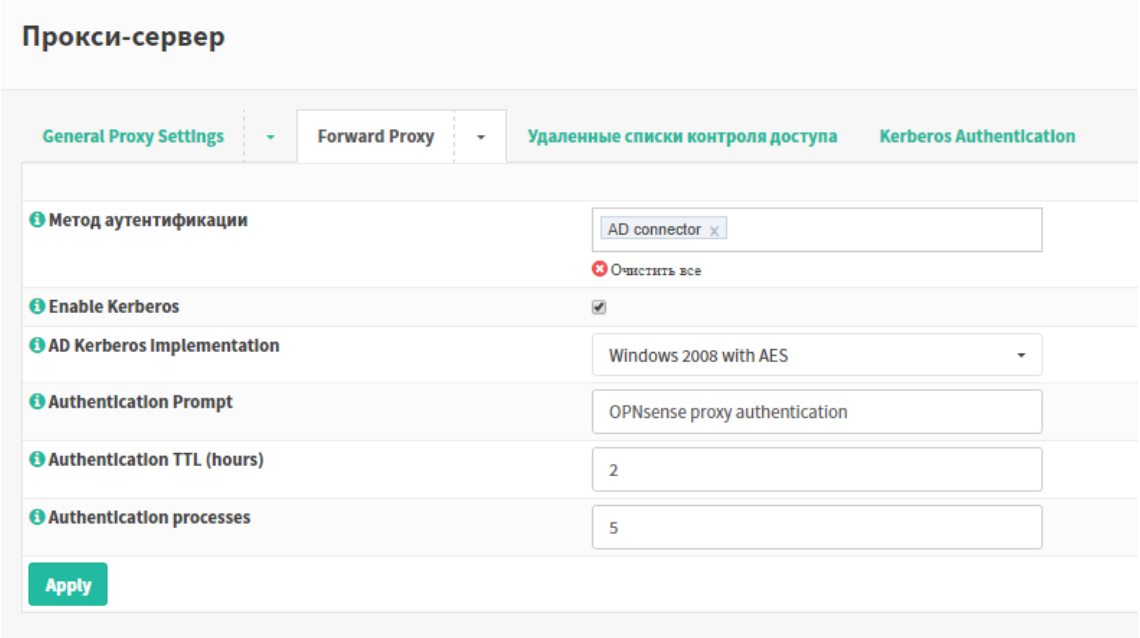
Шаг 5 – Настройка Kerberos

Пройдите в раздел **Службы -> Прокси-сервер -> Администрирование**.

Исходим из того, что начальная настройка прокси-сервера произведена и он слушает порт TCP / 3128.

В меню **Forward Proxy** выберите пункт **Authentication Settings**. В поле **Метод аутентификации**, выберите ранее созданный LDAP-коннектор – AD connector.

Установите флаг **Enable Kerberos**.



Проверка. Подключитесь к шлюзу по SSH. Выполните команду:

```
cat /etc/krb5.conf
```

В выводе вы должны увидеть настройки аналогичные приведенным ниже:

```
 # Autogenerated config. Do not edit manualy.

[libdefaults]

          default_realm = OFFICE.LOCAL

          dns_lookup_kdc = no

          dns_lookup_realm = no

          ticket_lifetime = 24h
```

```
        default_keytab_name = /usr/local/etc/squid/squid.keytab
        default_tgs_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
        default_tkt_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
        permitted_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
[realms]
        OFFICE.LOCAL = {
                kdc = 10.1.1.15
                admin_server = 10.1.1.15
                default_domain = office.local
        }
[domain_realm]
        .office.local = OFFICE.LOCAL
        office.local = OFFICE.LOCAL
```

Пройдите на вкладку **Kerberos Authentication**.

В поле **AD admin login**, укажите учетную запись администратора домена.

В поле **AD admin password**, укажите пароль для учетной записи администратора домена.

Нажмите на кнопку **Create keytab**. В поле **Output**, вы должны увидеть вывод аналогичный тому, который приведен ниже:

```
-- init_password: Wiping the computer password structure
 -- generate_new_password: Generating a new, random password for the computer account
 -- generate_new_password:  Characters read from /dev/udandom = 77
 -- get_dc_host: Attempting to find a Domain Controller to use (DNS SRV RR TCP)
 -- get_dc_host: Attempting to find a Domain Controller to use (DNS SRV RR UDP)
 -- get_dc_host: Attempting to find a Domain Controller to use (DNS domain)
```

```
 -- get_dc_host: Found DC:

 -- get_dc_host: Canonicalizing DC through forward/reverse lookup...

 -- get_dc_host: Found Domain Controller: prim3.office.local

 -- create_fake_krb5_conf: Created a fake krb5.conf file: /tmp/.msktkrb5.conf-h7CCuz

 -- reload: Reloading Kerberos Context

 -- finalize_exec: SAM Account Name is: TING-K$

 -- try_machine_keytab_princ: Trying to authenticate for TING-K$ from local keytab...

 -- switch_default_ccache: Using the local credential cache: FILE:/tmp/.mskt_krb5_ccache-bdixiS

 -- finalize_exec: Authenticated using method 1


 -- ldap_connect: Connecting to LDAP server: prim3.office.local try_tls=YES

 -- ldap_connect: Connecting to LDAP server: prim3.office.local try_tls=NO

 -- ldap_connect: LDAP_OPT_X_SASL_SSF=56


 -- ldap_get_base_dn: Determining default LDAP base: dc=OFFICE,dc=LOCAL

 -- ldap_check_account: Checking that a computer account for TING-K$ exists

 -- ldap_check_account: Checking computer account - found

 -- ldap_check_account: Found userAccountControl = 0x1000


 -- ldap_check_account: Found supportedEncryptionTypes = 28


 -- ldap_check_account: Found dNSHostName = ting.office.local


 -- ldap_check_account:   Found Principal: host/ting.office.local

 -- ldap_check_account:   Found Principal: HTTP/TING.office.local

 -- ldap_check_account:   Found User Principal: HTTP/TING.office.local

 -- ldap_check_account_strings: Inspecting (and updating) computer account attributes

 --    ldap_simple_set_attr:    Calling    ldap_modify_ext_s    to    set    userPrincipalName    to
HTTP/TING.office.local@OFFICE.LOCAL
```

```
 -- ldap_simple_set_attr: ldap_modify_ext_s failed (Insufficient access)

 -- ldap_set_supportedEncryptionTypes: No need to change msDs-supportedEncryptionTypes they are
28


 -- ldap_set_userAccountControl_flag: Setting userAccountControl bit at 0x200000 to 0x0

 -- ldap_set_userAccountControl_flag:  userAccountControl not changed 0x1000


 -- set_password: Attempting to reset computer's password

 -- set_password: Try using keytab for TING-K$ to change password


 -- ldap_get_pwdLastSet: pwdLastSet is 131190263156887998

 -- set_password: Successfully set password, waiting for it to be reflected in LDAP.

 -- ldap_get_pwdLastSet: pwdLastSet is 131194477372469996

 -- set_password: Successfully reset computer's password

 --    execute:    Updating    all    entries    for    ting.office.local    in    the    keytab
WRFILE:/usr/local/etc/squid/squid.keytab


 -- update_keytab: Updating all entires for TING-K$

 -- ldap_get_kvno: KVNO is 3

 -- add_principal_keytab: Adding principal to keytab: TING-K$

 -- add_principal_keytab: Removing entries with kvno < 0

 -- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local

 -- add_principal_keytab:   Adding entry of enctype 0x17

 -- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local

 -- add_principal_keytab:   Adding entry of enctype 0x11

 -- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local

 -- add_principal_keytab:   Adding entry of enctype 0x12

 -- add_principal_keytab: Adding principal to keytab: host/ting.office.local

 -- add_principal_keytab: Removing entries with kvno < 0
```

```
-- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local
-- add_principal_keytab:   Adding entry of enctype 0x17
-- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local
-- add_principal_keytab:   Adding entry of enctype 0x11
-- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local
-- add_principal_keytab:   Adding entry of enctype 0x12
-- add_principal_keytab: Adding principal to keytab: HTTP/TING.office.local
-- add_principal_keytab: Removing entries with kvno < 0
-- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local
-- add_principal_keytab:   Adding entry of enctype 0x17
-- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local
-- add_principal_keytab:   Adding entry of enctype 0x11
-- add_principal_keytab:     Using salt of OFFICE.LOCALhostting-k.office.local
-- add_principal_keytab:   Adding entry of enctype 0x12
-- ~msktutil_exec: Destroying msktutil_exec
-- ldap_cleanup: Disconnecting from LDAP server
-- init_password: Wiping the computer password structure
-- ~KRB5Context: Destroying Kerberos Context
```

Примечание. После генерации keytab, перезагрузите службу squid.

Проверка.

Нажмите на кнопку **Show keytab**. В поле **Output**, вы должны увидеть вывод аналогичный тому, который приведен ниже:

```
/usr/local/etc/squid/squid.keytab:


Vno  Type                    Principal                           Aliases
  2  arcfour-hmac-md5         TING-K$@OFFICE.LOCAL
  2  aes128-cts-hmac-sha1-96  TING-K$@OFFICE.LOCAL
  2  aes256-cts-hmac-sha1-96  TING-K$@OFFICE.LOCAL
  2  arcfour-hmac-md5         HTTP/TING.office.local@OFFICE.LOCAL
  2  aes128-cts-hmac-sha1-96  HTTP/TING.office.local@OFFICE.LOCAL
  2  aes256-cts-hmac-sha1-96  HTTP/TING.office.local@OFFICE.LOCAL
  2  arcfour-hmac-md5         host/ting.office.local@OFFICE.LOCAL
  2  aes128-cts-hmac-sha1-96  host/ting.office.local@OFFICE.LOCAL
  2  aes256-cts-hmac-sha1-96  host/ting.office.local@OFFICE.LOCAL
  3  arcfour-hmac-md5         TING-K$@OFFICE.LOCAL
  3  aes128-cts-hmac-sha1-96  TING-K$@OFFICE.LOCAL
  3  aes256-cts-hmac-sha1-96  TING-K$@OFFICE.LOCAL
  3  arcfour-hmac-md5         host/ting.office.local@OFFICE.LOCAL
  3  aes128-cts-hmac-sha1-96  host/ting.office.local@OFFICE.LOCAL
  3  aes256-cts-hmac-sha1-96  host/ting.office.local@OFFICE.LOCAL
  3  arcfour-hmac-md5         HTTP/TING.office.local@OFFICE.LOCAL
  3  aes128-cts-hmac-sha1-96  HTTP/TING.office.local@OFFICE.LOCAL
  3  aes256-cts-hmac-sha1-96  HTTP/TING.office.local@OFFICE.LOCAL
```

Нажмите на кнопку **Test Kerberos login** и проведите тестовую аутенитификацию по доменной учетной записи. В поле **Output**, вы должны увидеть вывод аналогичный тому, который приведен ниже:

AF oRQwEqADCgEAoQsGCSqGSIb3EgECAg== khilchenko@OFFICE.LOCAL

BH quit command

Настройка завершена!

9. Отчеты по использованию Интернета

Отчетность по использованию сети Интернет реализована за счет технологии Netflow и Netflow-анализатора (Insight).

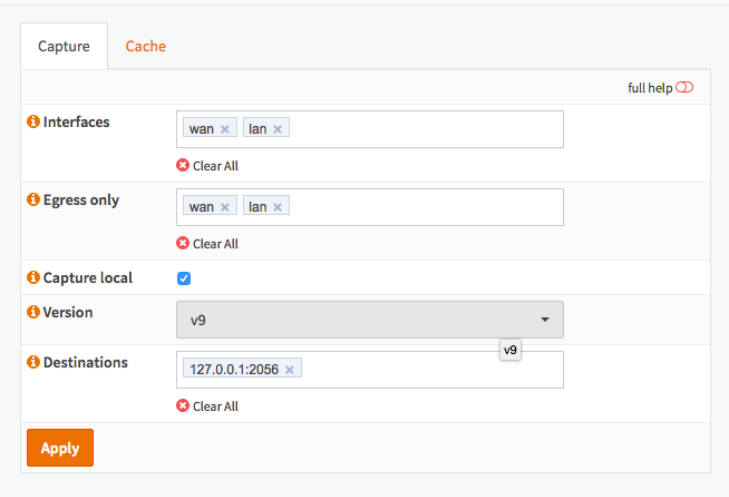
Netflow – технология мониторинга от Cisco. Во FreeBSD она реализована за счет модуля ядра ng_netflow (Netgraph). Поскольку Netgraph находится в ядре, он работает быстро и с минимальными затратами по сравнению с softflowd или pfflowd.

В то время как многие решения для мониторинга (Nagios, Cacti и vnstat) способны собирать только простую статистику по трафику, NetFlow учитывает информацию по потокам (сетевым соединениям), включая IP-адрес и порт источника и назначения.

TING поддерживает возможность экспортирования Netflow данных во внешние коллекторы, а также имеет встроенным Netflow-анализатором (Insight).

9.1. Настройка NetFlow

Для настройки NetFlow Exporter зайдите в **Reporting->NetFlow**.



В поле **Интерфейсы** выберите все интерфейсы, с которых хотите собирать данные; обычно выбирают все доступные интерфейсы.

В поле **Только исходящий** выберите WAN-интерфейсы, чтобы избежать повторного подсчета натированного трафика.

Для возможности локального анализа с использованием Insight, включите **Локальный захват пакетов**.

В зависимости от ситуации вы можете использовать версию NetFlow 5 или 9. Версия 5 не поддерживает IPv6.

Добавьте точку сохранения (IP-адрес: порт, затем нажать Enter). Локальный IP-адрес будет добавлен автоматически, если выбран **Локальный захват пакетов**.

9.2. Работа с Insight

TING имеет в своем составе гибкий и производительный Netflow-анализатор Insight. Для того, чтобы использовать Insight, необходимо настроить Netflow для захвата Netflow-данных на локальном хосте. Информация по настройке Netflow приведена выше.

Пользовательский интерфейс

Insight полностью интегрирован в TING. Графический интерфейс Insight прост, но вместе с тем функционален.

Insight предлагает широкий набор инструментов для анализа, начиная от Обзорных графиков и заканчивая средством выгрузки данных в CSV-файлы для дальнейшего анализа в вашем любимом spreadsheet-приложении.

Графики и суммарные данные

Режим отображения по умолчанию – Топ по пользователям и Обзорные графики. Данный режим отображения позволяет быстро ознакомится с текущими и ранее

существовавшими потоками и представляет собой график для входящего и исходящего трафика для каждого используемого интерфейса.

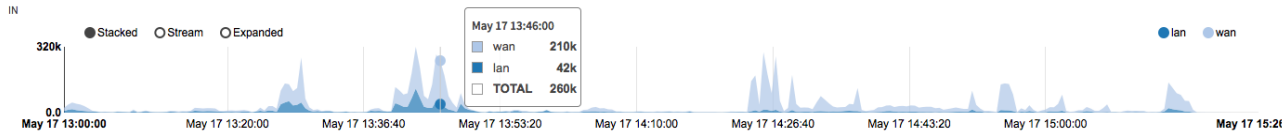
Выбор диапазона и разрешающая точность

В верхнем правом углу можно выбрать диапазон дат и разрешающую точность отчетов по учтенным потокам трафика.

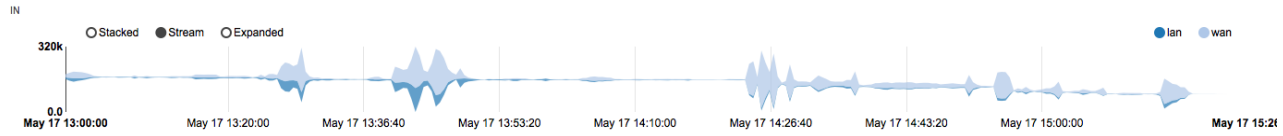
Тип отображения

Можно отображать информацию по потокам трафика в виде многослойного графика (используется по умолчанию), потокового графика или расширенного графика для сравнения данных по разным интерфейсам.

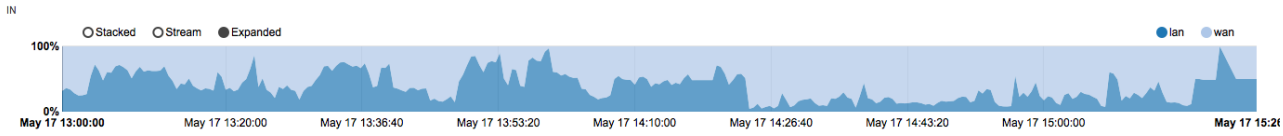
Многослойный



Потоковый



Расширенный



Топ по пользователям

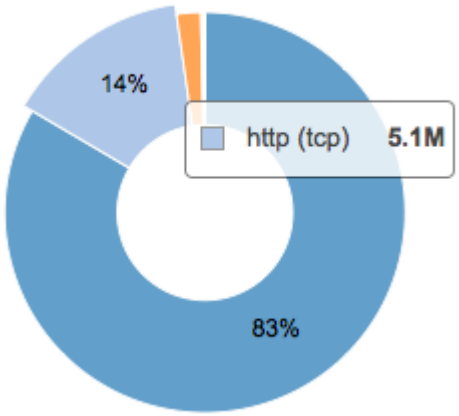
Для выбранного интерфейса отображаются 25 наиболее активных пользователей (по портам и IP-адресам), в пределах выбранного диапазона дат.

Топ по интерфейсам

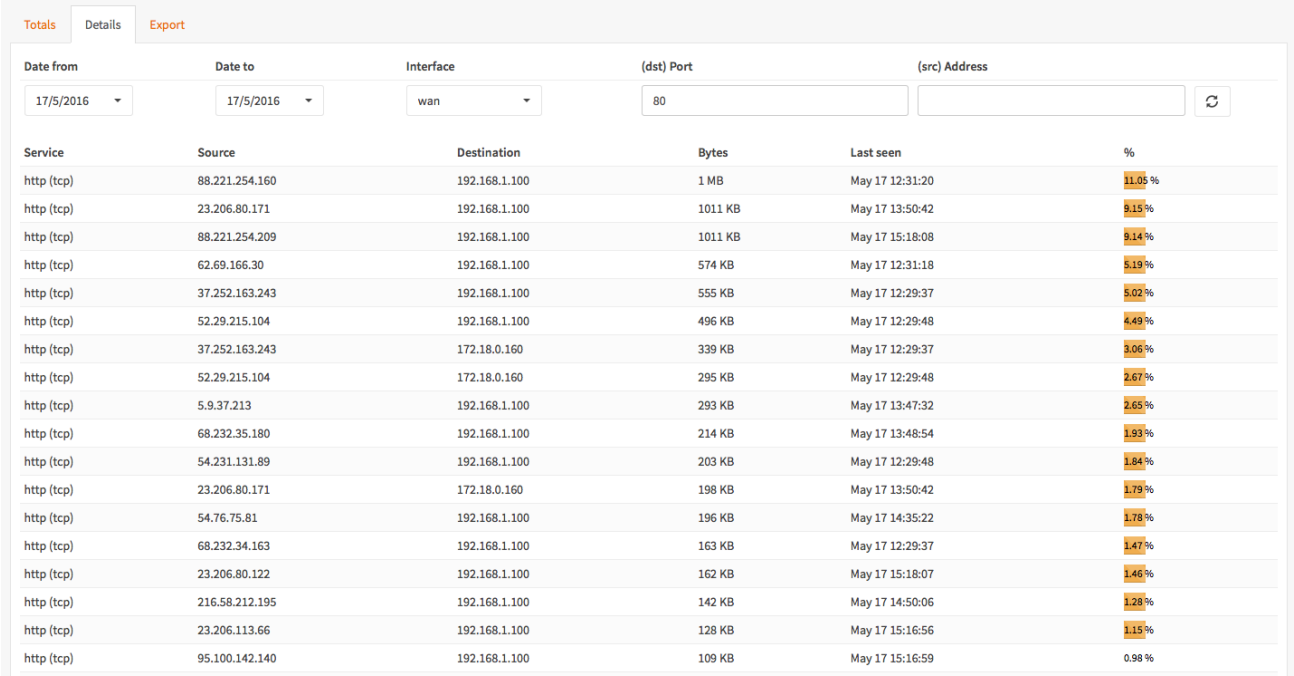
При выборе интерфейса отображаются 25 наиболее активных пользователей.

Кольцевая диаграмма по портам

Кольцевая диаграмма показывает трафик по портам / приложениям в процентном отношении. Можно изменить режим отображения одинарным или двойным щелчком по одному из отображаемых портов.



Щелчек по сектору кольцевой диаграммы открывает страницу с более детализированной информацией.



Service	Source	Destination	Bytes	Last seen	%
http (tcp)	88.221.254.160	192.168.1.100	1 MB	May 17 12:31:20	11.05 %
http (tcp)	23.206.80.171	192.168.1.100	1011 KB	May 17 13:50:42	9.15 %
http (tcp)	88.221.254.209	192.168.1.100	1011 KB	May 17 15:18:08	9.14 %
http (tcp)	62.69.166.30	192.168.1.100	574 KB	May 17 12:31:18	5.19 %
http (tcp)	37.252.163.243	192.168.1.100	555 KB	May 17 12:29:37	5.02 %
http (tcp)	52.29.215.104	192.168.1.100	496 KB	May 17 12:29:48	4.49 %
http (tcp)	37.252.163.243	172.18.0.160	339 KB	May 17 12:29:37	3.06 %
http (tcp)	52.29.215.104	172.18.0.160	295 KB	May 17 12:29:48	2.67 %
http (tcp)	5.9.37.213	192.168.1.100	293 KB	May 17 13:47:32	2.65 %
http (tcp)	68.232.35.180	192.168.1.100	214 KB	May 17 13:48:54	1.93 %
http (tcp)	54.231.131.89	192.168.1.100	203 KB	May 17 12:29:48	1.84 %
http (tcp)	23.206.80.171	172.18.0.160	198 KB	May 17 13:50:42	1.79 %
http (tcp)	54.76.75.81	192.168.1.100	196 KB	May 17 14:35:22	1.78 %
http (tcp)	68.232.34.163	192.168.1.100	163 KB	May 17 12:29:37	1.47 %
http (tcp)	23.206.80.122	192.168.1.100	162 KB	May 17 15:18:07	1.46 %
http (tcp)	216.58.212.195	192.168.1.100	142 KB	May 17 14:50:06	1.28 %
http (tcp)	23.206.113.66	192.168.1.100	128 KB	May 17 15:16:56	1.15 %
http (tcp)	95.100.142.140	192.168.1.100	109 KB	May 17 15:16:59	0.98 %

Кольцевая диаграмма по IP-адресам

Кольцевая диаграмма по IP-адресам работает аналогично кольцевой диаграмме по портам и показывает процент трафика для IP-адреса пользователя. Можно изменить режим отображения одинарным или двойным щелчком по одному из отображаемых IP-адресов.

Щелчок по сектору кольцевой диаграммы открывает страницу с более детализированной информацией.

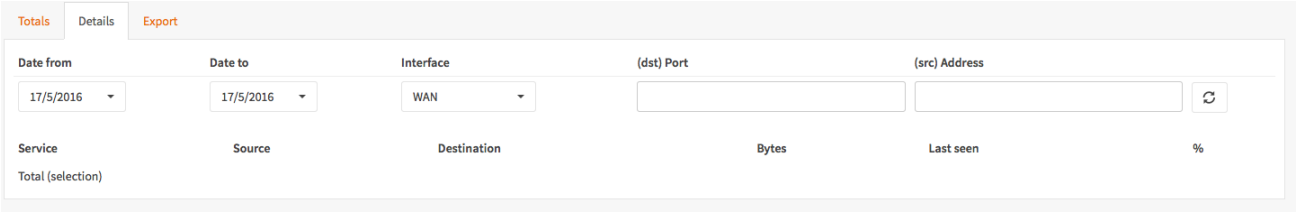
Суммарные данные по интерфейсу

Последняя версия TING включает отчет по **Суммарным данным по интерфейсу.** В отчете есть данные по пакетам (Входящие, Исходящие, Сумма Вход./Исход.) и байтам (Входящие, Исходящие, Сумма Вход./Исход.).

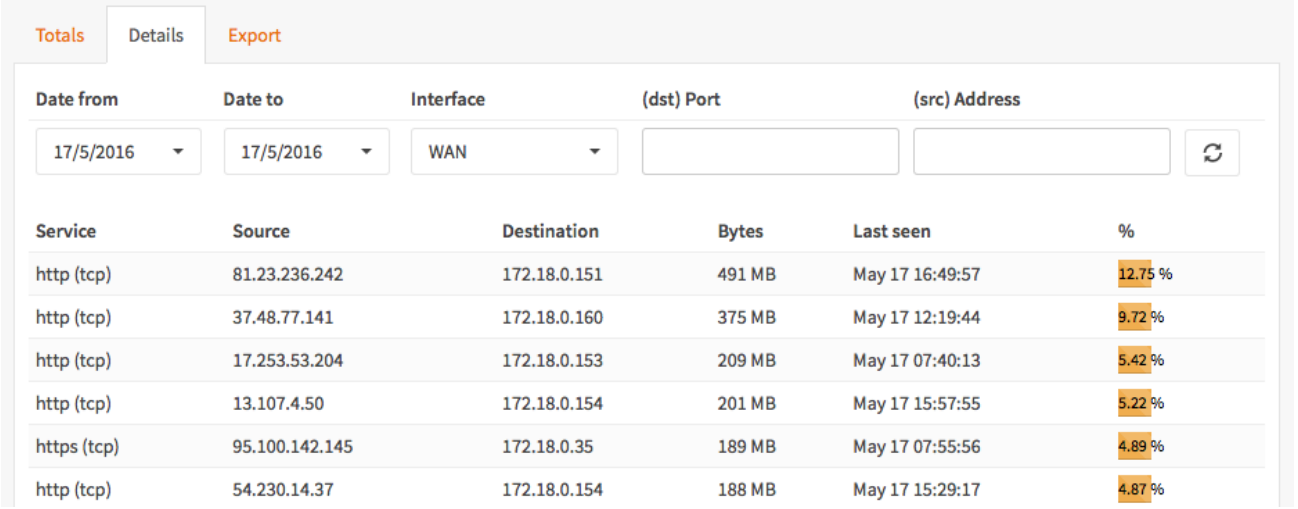
Вкладка Подробности

Пользователь может попасть на страницу с детализированной информацией, щелкнув по сектору кольцевой диаграммы и вкладке **Подробности**.

При открытии детализованной информации через вкладку, пользователь получает возможность составить новый запрос.

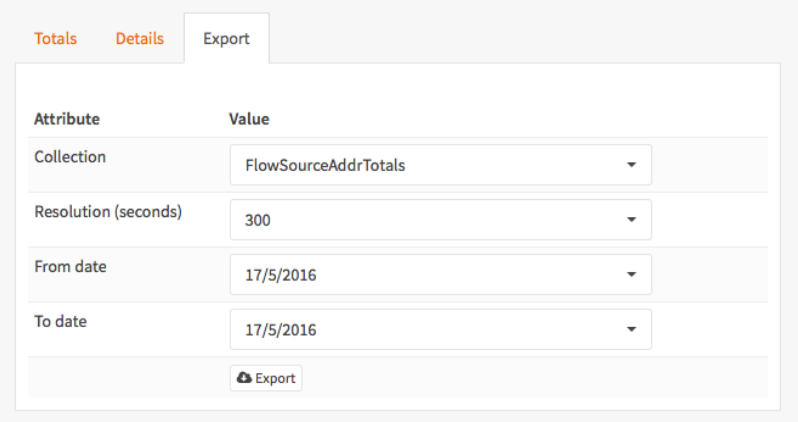


После выбора диапазона дат и интерфейса, можно ограничить вывод данных с помощью фильтров по порту и IP-адресу. Поле, в котором указывается порт и адрес, можно оставить пустым для отображения наиболее полной статистики.



Вкладка Экспорт

На вкладке **Экспорт** можно экспортировать данные для последующего анализа в других spreadsheet-приложениях.



Для экспортирования, выберите набор:

FlowSourceAddrTotals – Суммарные данные по IP-адресу источника

FlowInterfaceTotals - Суммарные данные по интерфейсу

FlowDstPortTotals - Суммарные данные по порту назначения

FlowSourceAddrDetails – Полные данные по IP-адресу источника

Выберите разрешающую точность в секундах (300,3600,86400)

Выберите диапазон дат и кликните клавишу **Экспортировать**.