EcoNATDPI

CG-NAT, BRAS, URL-фильтрация

3 в 1U

ДЛЯ ОПЕРАТОРОВ СВЯЗИ И ПРЕДПРИЯТИЙ

Оглавление

1. Общие положения

1.1. Назначение и область применения

Решение сертифицировано (ССС) и предназначено для применения на сетях операторов связи и предприятий.
Производительность — от 24 Гбит/с (12G Full Duplex) до 120 Гбит/с (60G Full Duplex) в зависимости от модификации.
Оборудование обеспечивает следующую функциональность:

- **CG-NAT** – с **COPM** логированием через Syslog и Netflow v9
- **BRAS** – Services Gateway для ограничения абонентам скорости доступа, отключения неплательщиков с переадресацией на портал (страницу «пора платить»).
- **URL Filtering** - фильтрация абонентов по списку Zapret-info, предоставление услуг «детский интернет»

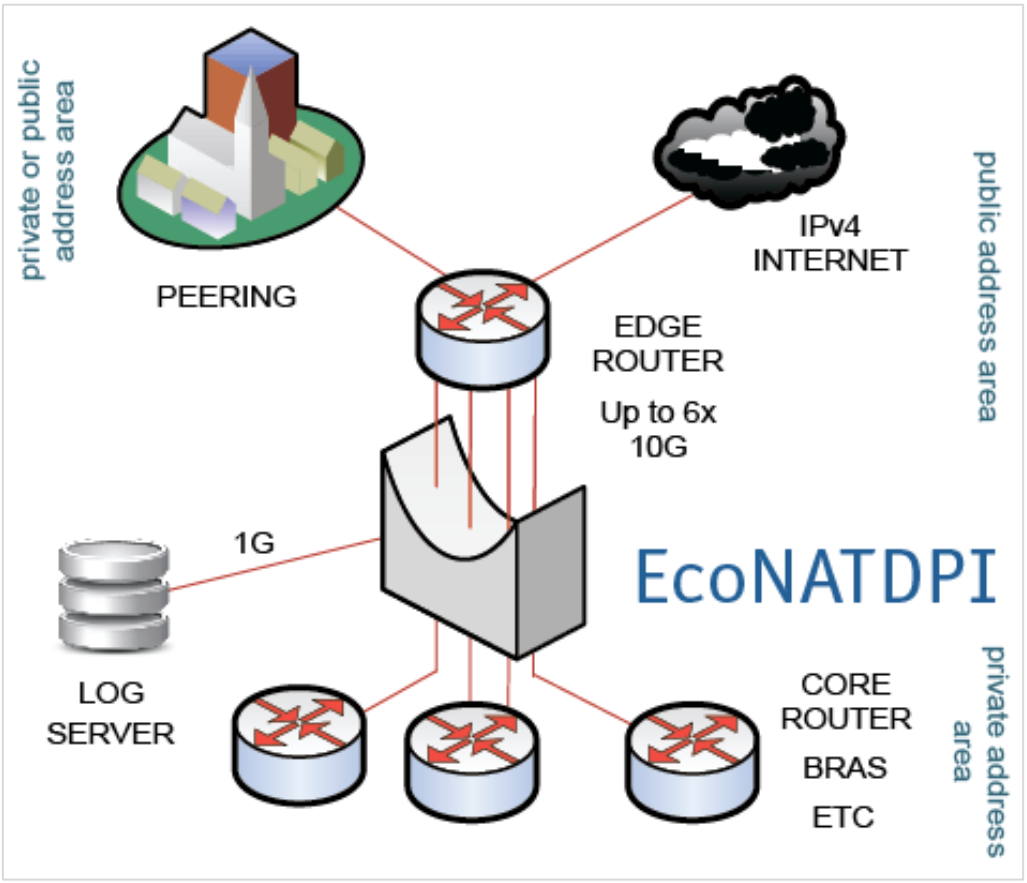
Приобретается любой набор функционала, например, CG-NAT + BRAS, или только BRAS.

1.2. Разновидности платформ

- Все платформы имеют выделенный 1GE порт MNG (out-of-band management).
- 1 порт 1GE для скоростного логирования соединений Syslog и Netflow v9
- 2, 6 или 12 портов 10G для абонентского трафика

Все платформы работают на скорости проводов – для пакетов со средней длиной 480 байт и более.

1.3. Схема включения устройства и расположение в сети провайдера



Устройство EcoNATDPI представляет собой прозрачный L2 мост.
Все порты 10G для абонентского трафика делятся пары: Inside (LAN) и Outside (WAN). Каждая пара портов LAN+WAN – это псевдо-провод: пакеты, пришедшие на LAN-1 передаются на WAN-1, пришедшие на WAN-3 – передаются на LAN-3 и так далее. Передача пакетов между разными парами не происходит. При этом все структуры данных – таблица трансляций, сессий и пр. – общие для всего устройства.
Поскольку устройство является мостом, оно включается между двумя маршрутизаторами (PE и Core) или между двумя VRF одного маршрутизатора.
Все или несколько LAN портов могут быть объединены в LAG (на базе LACP) на маршрутизаторе, аналогично – для WAN портов. EcoNATDPI прозрачно пропускает кадры ARP, IP-Multicast, сервисный трафик LACP и другие кадры Ethernet, в которые не инкапсулированы IP –пакеты.
Для связи между PE и Core маршрутизаторами настраивается IP - сеть точка – точка. На маршрутизаторе Core настраиваете default маршрут через IP на PE. На маршрутизаторе PE настраивается маршрут к абонентской сети через IP на CORE. Если используется CG-NAT, то необходимо настроить маршрут к сетям своих глобальных адресов (в которые транслируется трафик абонентов) через IP на CORE. Также PE может получать маршруты к абонентским сетям через протоколы динамической маршрутизации – если не используется CG-NAT.

2. Функциональность CG-NAT

2.1. Общее описание возможностей

2.1.1. Высочайшая производительность

Устройство EcoNATDPI спроектировано с учетом растущих требований операторов и обеспечивает защиту инвестиций на длительную перспективу.

- Скорость создания новых соединений — **8 млн/сек** с блочным логированием**,** 2.5 млн/сек с логированием каждой сессии для СОРМ
- Общее число трансляций/сессий — до **256 млн, достаточно для 1 млн одновременно работающих абонентов**
- Пакетная производительность достаточна для работы «на скорости проводов» при среднем размере пакетов 480 байт

Колоссальный запас производительности позволяет избежать проблем в случае проведения по провайдеру потенциальных сетевых атак, штормов и пр., а также избежать исчерпания ресурса так, как это происходит с другими вендорами. Высочайшая скорость создания соединений позволяет за доли секунды пересоздать соединения в случае переключения трафика на резервное устройство – практически незаметно для абонентов.

2.1.2. Поддержка множества типов трансляции

EcoNAT поддерживает до 32 одновременно работающих NAT пулов, которые могут отличаться типом трансляции, диапазонами публичных IPv4 адресов, лимитами числа соединений для абонентов и диапазонами выделяемых при трансляции портов UDP и TCP.

2.1.3. ACLs

Критерием для выбора пула являются ACL (Access Control Lists), связанные с каждым пулом. ACL анализируются в порядке приоритетов пулов и могут включать в себя как Source адрес, так и Destination адрес IP пакета. Таким образом, наряду с основной задачей, операторы могут применять данное решение для участия в пиринговых сетях с пересекающимися диапазонами IP адресов.

2.1.4. EcoNAT поддерживает различные типы трансляции одновременно: CGNмAT/PAT, Basic NAT, статическую трансляцию 1:1

CGNAT

CGNAT / PAT (Port Address Translation) – основный режим работы EcoNAT, позволяющий разделять использование публичного IPv4 адреса между несколькими абонентами. В этом режиме транслируется не только адреса, но и порты. Количество портов TCP и UDP, одновременно используемых абонентом, можно лимитировать.

BNAT

BNAT (Basic NAT) – классический NAT режим, при котором абоненту на время работы выделяется временный публичный IPv4 адрес, транслируются только адреса (порты остаются неизменными). У этого режима есть два варианта: прозрачный, разрешающий входящие внешние соединения по любым портам и закрытый, допускающий соединения извне лишь по портам, инициированным изнутри абонентом.

1:1

В статическом режиме (он же еще именуется трансляцией 1:1) за каждым абонентским IP адресом статически административно закреплен публичный IP адрес. Посредством данного метода оператор связи может оперативно выдавать абонентам статические публичные IP без изменения настроек CPE абонента.

2.2. Особенности реализации CG-NAT

Full Cone NAT (EIM/EIF)

Full Cone NAT является особенностью, отличающей CGNAT от традиционных видов NAT/PAT и обеспечивает максимальную прозрачность CGNAT для различных приложений, в т.ч. мобильных, P2P, игр и др. EIM/EIF позволяет любым внешним хостам устанавливать соединения с абонентом извне по тем портам, для которых трансляция была ранее инициирована самим абонентом.

Port Block Allocation (PBA)

Для уменьшения количества данных, которые требуется логировать, EcoNAT реализует PBA (Port Block Allocation). Порты для трансляции абонентам выдаются не по одному, а непрерывными блоками с диапазоном 64–512 портов. Таким образом, выполняется лишь две записи в лог для всего блока портов: при выделении блока портов абоненту и при высвобождении всего блока.

IP pairing

С целью обеспечения наилучшей прозрачности CGNAT все соединения абонента, относящиеся к одному пулу, привязаны к одному и тому же IP адресу.

Hairpinning

Hairpinning позволяет двум абонентам внутри NAT взаимодействовать друг с другом через NAT, не посылая пакеты вовне.

Aging

При длительной неактивности (период зависит он настроек пула и состояния соединения) неиспользуемые соединения закрываются, высвобождая порты. Блок портов считается свободным в случае, когда высвободились все порты из диапазона данного блока и истек таймаут ожидания.

ALG – Application Layer Gateway

EcoNAT поддерживает 4 типа ALG для максимально прозрачного пропуска трафика следующих протоколов прикладного уровня в режиме CG-NAT: **FTP, SIP, RTSP, PPTP**

Логирование трансляций – Syslog (для СОРМ)

EcoNAT поддерживает возможность логировать сетевые трансляции абонентов, используя стандартный **Syslog** интерфейс (Local_IP, Global_IP, Global_Port_Range, Protocol). За счет PBA (выделения портов блоками по 64 -512 шт.) в десятки раз снижается объем логируемой информации.

Логирование соединений - Syslog и Netflow v9 (для СОРМ)

Поддерживается логирование всех соединений: (Local_IP, Local_Port, Global_IP, Global_Port, Destination_IP, Destination_Port, Protocol) – Syslog и Netflow v9.

3. Функциональность BRAS

3.1. Назначение и область применения

Функциональность BRAS позволяет оператору связи реализовать сервисный шлюз для ограничения скорости доступа абонентов к IP сервисам и услугам передачи данных в обоих направлениях, отключать абонентов с переадресацией абонентов на портал или страницу «пора платить», а также для демонстрации абонентам информационных сообщений путем переадресации на портал.

Предполагается следующая сервисная модель **IPoE**:

- отсутствие инкапсуляции PPTP, PPPoE и др., чистый IPoE;
- абонент однозначно идентифицируется своим IPv4 адресом внутри сети провайдера;
- шлюзом для абонентов служит не BRAS, а коммутатор агрегации, или ядра (L3 – connected абоненты).

IP – адрес абоненту может выдаваться либо статически, либо динамически – при помощи DHCP сервера, связанного с системой биллинга;

3.2. Описание возможностей BRAS

3.2.1. Высочайшая производительность

Устройство поддерживает работу на скорости проводов, **до 1 млн** активных одновременно работающих абонентов, имеющих правила Policing в обоих направлениях.

3.2.2. Особенности реализации BRAS

Open Garden

Предусмотрена возможность задать ACL «Open Garden» с перечнем сетей, доступных отключенным абонентам – DNS серверы, сайт компании, платежных систем, банков и т.д.

Policing RX/TX

Ограничение скорости трафика абоненту возможно в обоих направлениях независимо, в диапазоне от 64 Кбит/с до 100 Гбит/с.

Burst

С целью увеличения комфорта абонентов последним дается возможность передать на максимально возможной скорости т.н. Burst – всплеск трафика в объеме, соответствующем 1 секунде трафика с законтрактованной скоростью, что способствует быстрой загрузке WEB страниц, комфортной для абонента.

Режим PUSH - предзагрузка правил на основе проприетарного протокола

Данный протокол взаимодействия с биллингом предполагает заблаговременную загрузку правил в систему и последующую синхронизацию, что выгодно отличает протокол от систем на базе RADIUS.
Системы на базе RADIUS в случае внезапной подачи трафика и массовой авторизации десятков тысяч абонентов подвержены перегрузкам с потенциальными отказами в обслуживании для абонентов.

Комфортный старт

При подаче трафика после перезагрузки устройства последнее прозрачно пропускает трафик всех абонентов на максимальной скорости – до момента окончания синхронизации с биллинговой системой, что занимает доли секунды.

Режим PULL - управление по стандарту RADIUS

Стандартный протокол взаимодействия с биллингом предполагает авторизацию абонентов на основе протокола RADIUS. При появлении пакетов трафика от ранее не авторизованного SRC IP абонента, последний авторизуется посредством RADIUS, где username=SRC_IP. Поддерживается RADIUS CoA для PUSH - деавторизации абонента и смены скорости доступа или ACL в режиме реального времени.

Пропуск протоколов маршрутизации

В конфигурации BRAS имеется возможность явно указать необходимость прозрачно пропускать трафик протоколов динамической маршрутизации (OSPF, BGP) которым обмениваются коммутаторы и маршрутизаторы, окружающие EcoNATDPI.

Назначение сервисов отдельным абонентам

Для ограничения скорости приема и передачи данных или перенаправления на портал для пополнения счета абонента в EcoBRAS используется система конфигурируемых политик и сервисов. Которые представляют собой набор действий, выполняемых в случае попадания адреса источника или назначения сессии в указанный ACL. Благодаря данной реализации, параметры доступа для каждого абонента могут задаваться статически конфигурируемыми сервисами и динамически, с помощью протокола RADIUS.

Отдельная консоль

Для упрощения работы службы технической поддержки предусмотрена отдельная консоль CLI-BRAS, отличная от основной управляющей консоли устройства и позволяющая выполнять ограниченный набор команд, связанных с функциональностью BRAS: просмотр данных по контракту и IP – адресу, таких как скорость Policy RX/TX, количество переданных пакетов и объем переданных данных в обоих

направлениях (акаунтинг), деавторизация контракта, IP – адреса.

3.2.3. Интеграция с биллинговой системой

Устройство поддерживает оригинальный протокол взаимодействия с биллинговой системой (описание протокола доступно по запросу).

Протокол основан на методе PUSH: биллинг периодически соединяется с BRAS по TCP и дает серию текстовых команд. Периодически биллинг опрашивает, какие контракты заведены на устройстве и добавляет/удаляет недостающие или лишние. При этом возможно управление абонентским трафиком в режиме реального времени (как в случае с CoA RADIUS), в т.ч. при помощи нескольких биллинговых систем одновременно.

Акаунтинг

Система допускает возможность съема информации об объеме переданных данных в байтах - по каждому IP в каждом из направлений.
Производитель обеспечивает услуги по интеграции любой биллинговой системы с BRAS, при этом биллинг может не иметь открытого API, а только поддерживать RADIUS протокол.

4. Функциональность URL Filtering

4.1. Назначение и область применения

Функциональность URL Filtering позволяет провайдерам выполнять требования законодательства в отношении фильтрации нежелательных и запрещенных ресурсов в сети Интернет, оказывать услуги типа «детский интернет» с фильтрацией по большим спискам и реализовывать сценарии, направленные на снижение оттока абонентской базы. Кроме того, возможна реализация сценариев показа таргетированной контекстной рекламы. Поддерживается фильтрация HTTP и HTTPS по всем TCP - портам.

4.2. Описание возможностей

4.2.1. Высочайшая производительность

Устройство способно обрабатывать весь WEB – трафик провайдера, независимо от TCP порта и осуществлять фильтрацию по спискам black-list совокупной емкостью до 30 Млн записей.

4.2.2. Фильтрация HTTP и HTTPS

Для HTTP/1.X поддерживается фильтрация по IP, Hostname, URL – с переадресацией на заранее заданную страницу «ресурс запрещен» - индивидуальную для сработавшего списка.

Для HTTPS поддерживается фильтрация по Hostname – с разрывом соединения с запрещенным ресурсом.

Для HTTPS экстракция Hostname осуществляется как из запроса, так из передаваемого с сервера сертификата.

4.2.3. Поддержка множества списков фильтрации

Система поддерживает одновременную работу до 16 списков для фильтрации трафика абонентов. Абонент может фильтроваться как по одному, так и по нескольким спискам одновременно, что определяется ACL. Список с наименьшим номером, в котором произошло срабатывание, будет причиной блокировки.

4.2.4. ACLs

Критерием для выбора списка фильтрации являются ACL (Access Control Lists), связанные в конфигурации с каждым списком фильтрации. ACL анализируются в порядке приоритетов списка и включают в себя Source_IP адрес или сеть, идентифицирующий индивидуального, корпоративного абонента, или их группу.

4.2.5. Автоматическая загрузка фильтра Zapret-Info

Устройство обеспечивает автоматическую загрузку списка фильтрации с сайта Роскомнадзора – не реже одного раза в сутки. Для этого необходимо заранее по TFTP загрузить на устройство надлежащим образом криптографический сертификат подписи sig и запрос xml, после чего настроить через CLI загрузку по расписанию.

4.2.6. Особенности реализации

Индивидуальный URL переадресации

В зависимости от того, какой список «сработал» в конкретном случае, абоненту может демонстрироваться различная страница с описанием причин блокировки (Redirect-URL для каждого списка задается в его конфигурации).

Механизм загрузки списков

Списки загружаются по протоколам TFTP, FTP, HTTP и Zapret-info путем выдачи специальных команд через основную управляющую консоль CLI, либо по расписанию.

Загрузка списков по расписанию

Настройками конфигурации можно предусмотреть загрузку списка с заданного URL с требуемой периодичностью.

4.2.7. Интеграция с биллинговой системой

Для организации услуги «детский интернет» предусмотрена возможность выдачи биллингом управляющих команд, активирующих / деактивирующих в режиме реального времени фильтрацию заданного IP – адреса абонента по определенному набору списков фильтрации (перечень списков определяется командой с биллинга).
Опция доступна только совместно с модулем BRAS.

4.3. Сценарий удержания абонентской базы (информирование об акциях)

Устройство поддерживает возможность переадресации абонента на заранее сконфигурированный URL – адрес портала в случае посещения любого из сайтов, входящих в специальный список, загруженный на устройство.

Для удержания абонентской базы провайдер, эксплуатирующий систему, может составить и загрузить на устройство список URL сайтом конкурирующих провайдеров, в т.ч., содержащих тарифные планы. В случае, если абонент пытается зайти на одну из таких страниц, он будет переадресован на специально подготовленную страницу портала, где сможет ознакомиться со специальными условиями своего провайдера и далее уже перейти на сайт конкурента, который хотел посетить. Страница портала может быть динамической и демонстрировать различные условия в зависимости от IP абонента и страницы конкурента, которую он намеревался посетить.

4.3.1. Особенности реализации

Передача на портал сведений об абоненте и посещаемом сайте

В URL портала могут быть добавлены переменные: локальный IP абонента, URL сайта, вызвавший срабатывание, HASH атрибутов браузера (позволяет идентифицировать компьютер в домохозяйстве, скрытый за NAT с общим IP для квартиры). Переданные на портал параметры позволят реализовать переадресацию абонента с портала на ту страницу конкурента, которую он хотел посетить - как сразу же (при этом текст спец. предложения откроется в отдельном окне), так и после ознакомления с текстом спец. предложения на портале.

Ограничение на число переадресаций

Система позволяет задать «мораторий» на срабатывание переадресации, чтобы не раздражать абонентов. Например, администратор может задать таймаут в 1 месяц. В этом случае, если абонент был переадресован по срабатыванию фильтра, то в следующий раз срабатывание сможет произойти не ранее чем через 1 месяц с момента прошлой переадресации. Компьютер абонента может идентифицироваться

как по IP абонента, так и по сочетанию IP и подписи браузера – для различения отдельных компьютеров в домохозяйстве.

Динамическая загрузка списка

Список ресурсов, при посещении которых может происходить переадресация может автоматически подгружаться на устройство согласно заданному расписанию.

4.4. Интеграция с ЦАИР

Функциональность URL Filtering EcoNAT может использоваться совместно со средствами контентной фильтрации ЦАИР. В этом случае база классифицированных ресурсов ЦАИР загружается автоматически и EcoNAT использует ее в списках фильтрации.

4.5. Гибкость конфигурирования

В сочетании с функциональностью BRAS для каждого клиента могут быть настроены свои критерии выбора списков фильтрации. При этом также сохраняется возможность динамически назначать сервисы с помощью протокола RADIUS.