Модули, входящие в комплекс NetUP UTM, и их назначение.

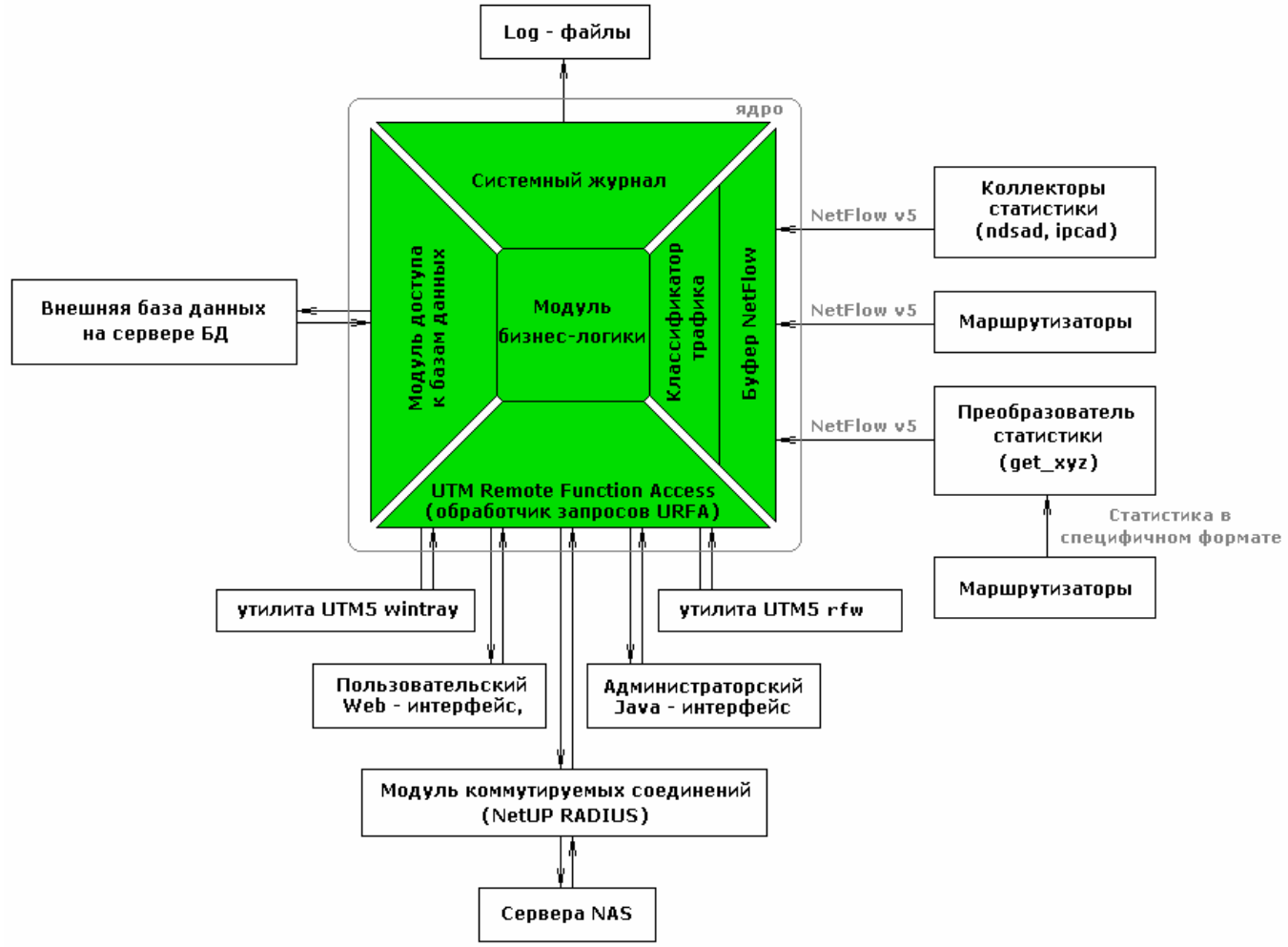


Схема объединения модулей NetUP UTM 5.0 в биллинговую систему.

Ядро.

Ядро биллинговой системы NetUP UTM – это основной модуль, отвечающий за работу с базой данных, обеспечение доступа к ней и обработку входящей информации согласно внутренним правилам (таких как тарификация, периодические списания). Ядро – это отдельный многопоточный процесс, работающий в пользовательском режиме. При запуске ядро, как правило, работает в режиме администраторских привилегий. Структура ядра такова, что оно органично вписывается в многопроцессорные архитектуры и при высоких нагрузках равномерно использует все предоставленные ресурсы.

Обработчик запросов URFA (UTM Remote Function Access) является сервером вызовов удалённых процедур. Он принимает соединения от клиентов системы и осуществляет выполнение запрошенных команд внутри ядра. Эта компонента служит в большей степени для организации пользовательских и администраторских интерфейсов.

URFA – это модуль доступа к ядру системы из внешних приложений. Он проводит авторизацию пользователей по схеме CHAP и обеспечивает работу удалённого пользователя. Протокол поддерживает передачу данных и вызов функций. URFA проверяет, разрешён ли данному пользователю доступ к вызываемой функции и, если разрешён, пользователю позволяется начать обмен данными. В противном случае система дает отказ в доступе.

Каждой сессии выделяется 128-битный случайный идентификатор (SID), повторение которого исключается. Этот SID может быть использован повторно для открытия доступа. В случае сбоя при восстановлении сессии SID будет удален, и пользователь вновь будет вынужден ввести логин и пароль. SID привязывается к IP-адресу клиента и автоматически удаляется после некоторого времени простоя (см.

переменную web_session_timeout). Восстановление сессии возможно лишь в случае, когда получен доступ с правами системного пользователя.

При открытии сессии создается таблица разрешенных вызовов, состоящая из списка символов, имевшихся на момент генерации в системе, и прав доступа к ним. Если после открытия сессии будет подгружен дополнительный модуль, то эти вызовы будут в числе запрещённых для пользователя. В таком случае, пользователю необходимо подключиться заново.

В случае, если в момент выгрузки модуля, кто-то работает с ним, операция выгрузки завершится неудачей. Однако все символы этого модуля будут помечены как удаленные и в дальнейшем все вызовы к ним не будут успешными. В тот момент, когда последняя ссылка на символы будет удалена (сессия закрыта), модуль можно окончательно выгрузить. Постоянные модули выгружать нельзя, при попытке их выгрузить будет возвращена ошибка и на работе модуля это никак не скажется.

В случае сбоя при проверке лицензий модуль не будет подгружен. Лицензии привязываются к двоичному коду модуля, что гарантирует пользователю то, что загруженный модуль действительно собран в компании NetUP и полностью отвечает требованиям безопасности и корректности работы. Однако это требует, чтобы при обновлении модуля была получена обновленная лицензия.

Буфер NetFlow принимает данные о трафике в формате NetFlow версии 5. Для устройств, не поддерживающих выдачу статистики по этому протоколу, необходимо воспользоваться преобразователем статистики из любого протокола в NetFlow версии 5 – утилитой get_xyz.

Классификатор трафика – модуль ядра, осуществляющий сортировку всего трафика на категории (классы трафика) по признакам, обозначенным в настройках системы. Признаки классификации задаются в центре управления UTM.

Модуль бизнес-логики отвечает за тарификацию всех услуг, в том числе и передачу IP-трафика. Он осуществляет перевод количества оказанных оператором услуг в денежный эквивалент, принимая во внимание все зависимости, указанные администратором системы.

Системный журнал сообщений ведёт все записи о функционировании UTM. Он позволяет администраторам проводить диагностику системы и получать информацию о сбоях в работе системы.

Модуль доступа к базам данных представляет собой унифицированный интерфейс БД и осуществляет перевод внутрисистемных запросов к данным в запросы к внешней базе данных. Это позволяет добиться независимости UTM от какой-либо конкретной системы управления БД.

Прием данных происходит посредством буфера NetFlow и URFA. Исходные данные считываются из базы данных при запуске. Изменения, сделанные впоследствии напрямую в базу, могут привести к неконтролируемому поведению системы.

NetFlow данные поступают на обработку в бизнес-модуль, где рассчитываются все необходимые списания. В случае высокой пиковой загрузки NetFlow поток может быть буферизован, что несколько снизит возможные потери. «Сырые» данные NetFlow сохраняются посредством объектно-ориентированной базы данных GigaBase (http://www.garret.ru/~knizhnik/gigabase.html). При старте модуль этой БД создаётся в отдельной нити и, по возможности, с высоким приоритетом.

URFA поддерживает динамическую загрузку модулей (liburfa). Они могут быть как выгружаемыми, так и постоянными. Последние – это модули, содержащие критичные для управления системой вызовы или выгрузка которых может привести к сбоям. Первые - это, обычно, просто библиотеки вызовов. Загруженные в данный момент модули можно просмотреть в интерфейсе администратора во вкладке (Дополнительно | Плагины).

Модуль коммутируемых соединений (NetUP RADIUS).

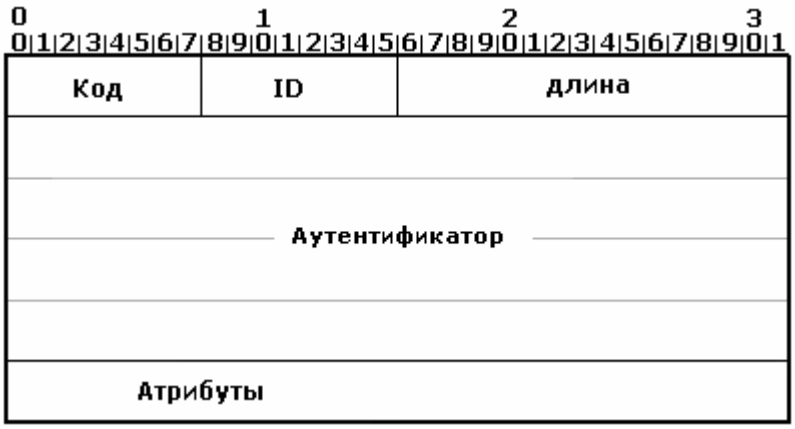
Модуль коммутируемых соединений представляет собой сервер NetUP RADIUS и предназначен для обработки запросов на авторизацию и учёт потребленных услуг.

Сервер NetUP RADIUS представляет собой приложение, которое в реальном времени обрабатывает поступающие к нему запросы по протоколу Remote Authentication Dial In User Service (RADIUS) – RFC 2138 и RFC 2139. При обработке запросов сервер NetUP RADIUS обращается к ядру системы по протоколу URFA.

Протокол Remote Authentication Dial In User Service (RADIUS) описан в документах RFC 2138 и RFC 2139 и предназначен для обеспечения авторизации, аутентификации и аккаунтинга между сервером доступа и сервером авторизации. Протоколу RADIUS официально присвоен порт UDP 1812.

Данный протокол был разработан для облегчения управления большим количеством модемных пулов. Например, когда в сети имеются несколько устройств, к которым должны иметь доступ пользователи, и на каждом устройстве содержится информация обо всех пользователях, то администрирование такой системы значительно усложняется, превращаясь в головную боль администратора. Проблема может быть решена установкой одного центрального сервера авторизации, а все сетевые устройства производили бы запросы к нему по стандартному протоколу RADIUS. При этом в качестве серверов доступа могут выступать устройства любых производителей, поддерживающие протокол RADIUS.

В общем виде формат RADIUS-пакета выглядит, как показано на рисунке.



Поле «Код» размером один байт и может принимать следующие значения: 1 – запрос на проверку доступа (Access-Request), 2 – доступ разрешён (Access-Accept), 3 – в доступе отказано (Access-Reject), 4 – запрос на учёт (Accounting-Request), 5 – ответ на запрос на учёт (Accounting-Response), 255 – зарезервированное значение (Reserved).

Поле «Длина» размером два байта указывает на полный размер всего пакета RADIUS.

Поле «Аутентификатор» размером 16 байт содержит информацию для проверки подлинности пересылаемых пакетов.

Поле «Атрибуты» RADIUS переменной длины содержит полезные данные. Данное поле состоит из последовательности атрибутов и соответствующих присвоенных значений. Каждый атрибут имеет своё числовое обозначение (идентификатор). Например, атрибут User-Name имеет числовое значение 1 и содержит в себе имя пользователя, а атрибут User-Password имеет значение 2 и содержит в себе пароль пользователя в открытом виде.

При подключении пользователя сначала происходит его аутентификация, т. е. проверка подлинности. Для этого сервер доступа предлагает пользователю ввести логин (имя учётной записи) и пароль. После ввода этих данных сервер доступа формирует пакет Access-request и отсылает его серверу RADIUS.

В данном пакете содержатся введённые пользователем данные. Следует учесть, что есть несколько методов аутентификации и содержимое пакета с запросом на аутентификацию будет содержать разные данные в зависимости от того, какой метод используется. Наиболее распространенные методы – PAP и CHAP.

PAP (Password Authentication Protocol) – простейший протокол аутентификации. Он не предусматривает использования шифрования паролей. При аутентификации по этому методу сервер доступа заполняет атрибуты «Имя пользователя» (User-Name) и «Пароль пользователя» (User-Password) и отсылает запрос серверу RADIUS.

CHAP (Challenge Handshake Authentication Protocol) – более сложный и защищённый протокол, описанных в документе RFC 1994. Он использует зашифрованные пароли. При аутентификации по этому протоколу сервер доступа генерирует случайное 16-байтное значение (CHAP challenge) и отсылает его на компьютер пользователя. После этого компьютер пользователя отсылает обратно в незашифрованном виде логин пользователя, и зашифрованное значение (hash), полученное из строки вызова, идентификатора сеанса и пароля пользователя с применением алгоритма MD5. Протокол MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) очень похож на CHAP.

После получения данных аутентификации сервер RADIUS проводит их проверку и, если они корректны, то отсылает обратно пакет «Доступ разрешен» (Access-Accept). В противном случае посылается пакет «В доступе отказано» (Access-Reject).

В пакете «Доступ разрешен» (Access-Accept) также в поле атрибутов могут передаваться параметры для установки сеанса, например, IP-адрес пользователя (Framed-IP-Address), тип протокола (Framed-Protocol), максимальное количество времени, отведённое на сессию (Session-Timeout).
Сервер доступа, получив пакет «Доступ разрешен» (Access-Accept), устанавливает соединение с пользователем. Если данный пакет не получен либо получен пакет «В доступе отказано» (Access-Reject), то соединение разрывается.

После успешного установления соединения сервер доступа отсылает на сервер RADIUS пакет «Запрос на учёт» (Accounting-Request), в котором содержится информация о начале предоставления услуги и параметрах сеанса: порт на который подключился пользователь (NAS-Port), идентификатор сессии (Acct-Session-Id). Это так называемая стартовая запись.

При окончании сеанса отсылается пакет со стоп-записью. В этом пакете содержится информация об окончании предоставления услуги. Также в этом пакете содержится информация о том, сколько времени предоставлялась услуга (Acct-Session-Time), сколько принято или передано байт в ходе работы.

База данных.

Все сведения о пользователях, их лицевых счетах и услугах хранятся в базе данных Gigabase на сервере баз данных (поддерживаются MySQL 3.x, 4.x и PostgreSQL 7.x). Причем настоятельно рекомендуется использовать MySQL с поддержкой InnoDB, так как данное решение позволяет существенно повысить надежность хранения данных.

База данных биллинговой системы является критическим узлом, вследствие того, что она хранит очень важную и ценную информацию, поэтому рекомендуется регулярно сохранять резервную копию БД при помощи утилиты utm5_backup.sh.

Для осуществления переноса данных об учетных записях пользователей, тарифах, списаниях служит утилита to_utm.pl. Утилита написана на языке Perl и поставляется в исходном коде. Благодаря этому имеется возможность перенести данные практически из любой системы, исправив код скрипта согласно структуре базы данных, из которой осуществляется перенос.

Администраторский Java-интерфейс.

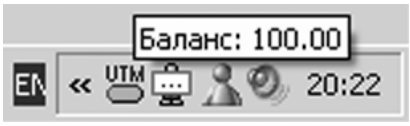
Управление учётными записями и настройками биллинговой системы производится с помощью центра управления UTM (администраторский Java-интерфейс). Интерфейс администратора представляет собой Java-приложение, хранящееся на компьютере администратора и подключающееся удаленно к ядру при запуске. Для функционирования программы необходимо наличие операционной системы с поддержкой графической оболочки и виртуальной машины Java версии 2.

Пользовательский Web - интерфейс.

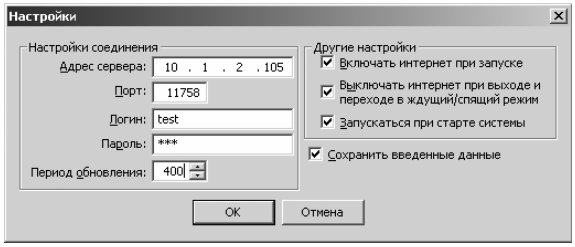
Пользователь, которому предоставляются услуги, тарифицируемые биллинговой системой NetUP UTM, имеет возможность контролировать состояние своего счета, а так же формировать отчеты по услугам за желаемый период в своем личном виртуальном кабинете.

Для входа в виртуальный кабинет пользователя необходимо запустить Интернет-браузер (Internet Explorer, Opera, Netscape Navigator, Konqueror) и набрать в адресной строке URL https://your.server/cgi-bin/utm5/aaa5.

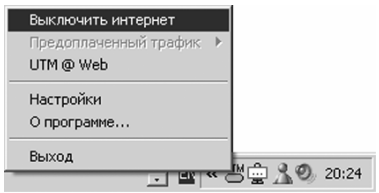
Утилита utm5 wintray. Для оперативного и удобного доступа к балансу лицевого счета рекомендуется использовать утилиту utm5_wintray.



Данная программа запускается на компьютере пользователя и с настраиваемым периодом обновляет информацию о текущем состоянии баланса и количестве оставшегося предоплаченного трафика. При запуске необходимо указать, где находится ядро биллинговой системы и логин/пароль для доступа.



Так же при помощи этой утилиты можно производить включение и выключение Интернета.



Сервера доступа (NAS).

Сервер доступа NAS (Network Access Server) – является связующим звеном между компьютером пользователя и интернетом. В его роли может выступать компьютер, а так же любое оборудование, поддерживающее авторизацию клиентов по протоколу RADIUS или сбор статистики по протоколу NetFlow v5. Дополнительная утилита get_xyz позволяет преобразовать в NetFlow 5 (или сохранить в файл) статистику по трафику с маршрутизаторов MikroTik, NSG, Revolution или в формате Cisco IP-accounting.

Универсальные сборщики статистики.

Коллектор статистики (ndsad) - NetUP Data Stream Accounting Daemon. В общем случае возможны два способа включения в сеть:

- ndsad запускается на роутере, а биллинговая система – на удаленном сервере, находящемся либо внутри локальной сети, либо вне её;
- ndsad и биллинговая система UTM работают на одном сервере, служащим маршрутизатором между локальной и глобальной сетями.

Для обмена данными между демоном ndsad и ядром системы используется протокол UDP, данные передаются в формате NetFlow версии 5. Для правильной работы системы в рассмотренной конфигурации необходимо направить поток UDP-пакетов, содержащих информацию о трафике, на локальную машину на порт, «прослушиваемый» ядром системы. Порт UDP и хост для принятия данных о трафике задаются в

конфигурационном файле /netup/utm5/utm5.cfg. Если статистика собирается с локальной машины, то хостом для принятия данных следует указать 127.0.0.1.

Список поддерживаемых семейств сетевых устройств

Для ОС семейства BSD: vlan, bfe, tun, ng, nv, lo, dc, fxp, pcn, rl, sf, sis, ste, tl, tx, vr, wb, xl, de, txp, vx, bge, em, gx, lge, nge, sk, ti, wx, cx, ed, el, ep, ie, is, le, ex, lnc, my, wi, an.

Для ОС семейства Linux: lo, eth, ppp.

На платформе Win32 в стандартной поставке поддерживаются только устройства Ethernet, которые объединены в семейство eth.

Преобразователь статистики (get_xyz). Ядро биллинговой системы NetUP UTM 5 рассчитано на сбор статистики по протоколу NetFlow v. 5. Для приведения статистики в формат NetFlow предназначен универсальный сборщик статистики NetUP get_xyz. Сборщик написан на языке C++ и поставляется в исходных кодах. Благодаря этому возможен сбор статистики и преобразование в NetFlow v.5 практически с любых устройств или файлов. При этом также имеется возможность запускать неограниченное число сборщиков get_xyz и отправлять статистику в одно ядро биллинговой системы.

Утилита get_xyz в стандартной поставке имеет возможность собирать статистику по трафику с маршрутизаторов Cisco IP-Accounting, MikroTik, NSG, Revolution и передачи ее по протоколу Cisco NetFlow v5 либо сохранения в файл.

Универсальный сборщик статистики (utm5_unif). Если в импортируемом файле с данными по трафику не присутствуют IP-адреса, но присутствуют логины пользователей, то обработку таких данных можно осуществить при помощи программы utm5_unif.

Вспомогательные утилиты.

Генератор статистики по протоколу NetFlow (utm5_flowgen) служит для тестового эмулирования работы пользователей и экспорта статистики по протоколу NetFlow v.5.

Генератор статистики по протоколу RADIUS (utm5_radgen) используется для тестового эмулирования работы пользователей и экспорта статистики по протоколу RADIUS.

Утилита для резервного копирования базы данных (utm5_backup). Для обеспечения сохранности данных рекомендуется периодически делать резервное архивирование SQL-базы данных. Для этого необходимо выполнить скрипт из поставки UTM: /netup/utm5/bin/utm5_backup.sh. При этом будет создан файл /netup/utm5/backup/UTM5.YY_MM_DD.gz, где YY – год создания архива, MM – месяц, DD – день.

Утилита для загрузки IP-сетей (utm5_load_tc.pl) представляет собой скрипт на языке Perl для загрузки списка IP-сетей из файла в классы трафика.

г.Москва, Лужнецкая набережная, д.2/4, строение 1, 5 этаж, офис 1
Почтовый адрес: 119311, Москва, а/я 87
Телефоны: +7 (095) 543-9220 (многоканальный)
+7 (095) 540-9652
+7 (095) 540-9653