ИНТЕРНЕТ РЕДАКЦИЯ материалов по ТИКСЕР БЕССТ v.4.x для технического специалиста

Введение

Настоящая ИНТЕРНЕТ РЕДАКЦИЯ материалов по ТИКСЕР БЕССТ v.4.x для технического специалиста описывает процесс установки и конфигурирования "типового коммуникационного сервера Белонина Сергея Станиславовича" и операционной системы CentOS, под управлением которой он должен функционировать

Настоящая ИНТЕРНЕТ РЕДАКЦИЯ материалов по ТИКСЕР БЕССТ v.4.x для технического специалиста предназначена для ознакомления посетителя сайта с возможностями, заложенными в «Типовом коммуникационном сервере Белонина Сергея Станиславовича, версия 4.x»

Условия распространения

Настоящая ИНТЕРНЕТ РЕДАКЦИЯ материалов по ТИКСЕР БЕССТ v.4.x для технического специалиста является собственностью автора и правообладателя Белонина Сергея Станиславовича и предоставляются посетителю сайта на условиях принятия посетителем сайта лицензионного договора, размещённого на сайте

До ознакомления с условиями лицензионного договора и полного принятия лицензионного договора посетителем сайта любое использование настоящей ИНТЕРНЕТ РЕДАКЦИИ материалов по ТИКСЕР БЕССТ v.4.x для технического специалиста ЗАПРЕЩЕНО

В случае, если экземпляр материалов по ТИКСЕР БЕССТ v.4.x для технического специалиста стал доступен кому либо не с официального сайта, использование такого экземпляра ЗАПРЕЩЕНО

Отказ от ответственности

Внимание !!! Ниже в настоящем разделе дублируются основные пункты отказа от ответственности из лицензионного договора

Правообладатель не берет на себя никаких обязательств (в том числе не берет на себя обязательства по обеспечению пригодности данных материалов для каких либо целей, по соответствию настоящих материалов пользовательским ожиданиям, по обеспечению правдивости и непротиворечивости настоящих материалов), также автор не несет никакой ответственности, связанной с настоящими материалами

Использующий настоящие материалы принимает на себя всю ответственность за использование или неиспользование настоящих материалов полностью или в любой их части, а также за результаты использования или неиспользования настоящих материалов полностью или в любой их части, включая любые непосредственные и любые опосредованные результаты, в том числе упущенную, недополученную прибыль, вред имиджу или деловой репутации

Использующий настоящие материалы соглашается, что не имеет и не будет иметь в будущем никаких претензий к автору настоящих материалов, связанных условиями распространения или содержимым настоящих материалов

ВНИМАНИЕ !!! В случае непринятия настоящих условий во всех деталях использовать настоящие материалы запрещается

Документация для технического специалиста

Задачи, стоящие перед техническим специалистом, сводится к первоначальной подготовке типового коммуникационного сервера и ввода его в эксплуатацию, а также (опционально) последующей технической поддержке. При этом в зависимости от конкретной подзадачи конфигурирование проводится либо на стороне типового коммуникационного сервера, либо на стороне клиентских рабочих станций. Соответственно объём технической документации в настоящей инструкции призван охватить типовые задачи, встающие перед техническим специалистом и обеспечить его информацией, достаточной для предусмотренных методов конфигурирования типового коммуникационного сервера

Общее устройство типового коммуникационного сервера и типовые методы конфигурирования

Текущая версия типового коммуникационного сервера ТИКСЕР БЕССТ v.4.0 основана на версии 4.2007.0.0 системы КоСиКУЛС БЕССТ (C) 2007, Sergey S. Belonin, и состоит из части оптимизированных компонент последней. Начальную подготовку типового коммуникационного сервера - установку и конфигурирование операционной системы, типовых UNIX сервисов и компонентов ТИКСЕР БЕССТ v.4.0 рекомендовано проводить по детально описываемой в соответствующих разделах «Установка ОС Linux CentOS 5.3» и «Установка ТИКСЕР БЕССТ v4» методике, причём большую часть операций проводит компонента «конфигуратор» на основании модифицированного техническим специалистом конфигурационного файла. Важно отметить, что для соблюдения требований безопасности важно изменить все типовые пароли в конфигурационном файле на новые - самостоятельно придуманные криптостойкие, а также сохранить эти пароли в надёжном месте

Ключевой особенностью ТИКСЕР БЕССТ v.4.0 является максимальное использование функционала, предоставляемого открытой операционной системой семейства UNIX и входящими в состав её дистрибутива типовыми открытыми сервисами UNIX. Коммерческие программные надстройки используются в основном для расширения типового функционала и повышения удобства управления в единообразном стиле. Следствием такого подхода является открытые для технического специалиста возможности как быстрого «вхождению» в мир UNIX решений, так и максимальная открытость и, при необходимости, доступность тонкой оптимизации ОС и типовых сервисов по мере приобретения опыта и роста квалификации в сфере администрирования по большей части ОС UNIX/Linux и типовых UNIX сервисов, и лишь в небольшой части - коммерческих надстроек

Таким образом ТИКСЕР БЕССТ v.4.0 может представлять интерес

для технического специалиста как:

- инструмент быстрого вхождения в мир UNIX с мало затратным получением работающего комплексного решения и перспективой углубления своих знаний и квалификации в сфере администрирования по большей части повсеместно используемых UNIX решений
- инструмент экономии времени и трудозатрат квалифицированного специалиста на выполнении большого объёма типовых операций по конфигурированию операционных систем UNIX/Linux и типовых коммуникационных сервисов
- инструмент, существенно расширяющий функциональность типовых коммуникационных сервисов (по сравнению с предоставляемой типовыми дистрибутивами UNIX/Linux). Все расширения выполнены однотипно и предоставляют возможности, востребованные специалистами по системному администрированию и компьютерной безопасности

примечание: *настоящая инструкция не является учебником по системному администрированию UNIX и администрированию типовых коммуникационных сервисов UNIX, такой информации много в сети Интернет и различных печатных источниках. В связи с большим объёмом охватываемых тем настоящая инструкция описывает общую архитектуру работы каждой компоненты, указывает использованный в качестве базового типовой сервис UNIX и акцентируется на аспектах конфигурирования расширяющих типовой функционал компонент*

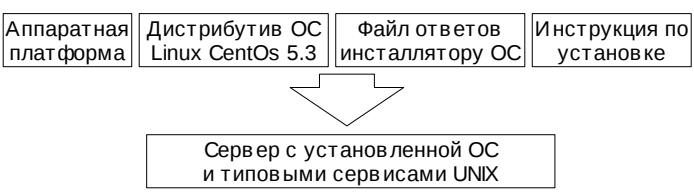
Обзор архитектуры и особенности конфигурирования компоненты «Базовая установка ОС»

ТИКСЕР БЕССТ v.4.0 является надстройкой над операционной системой (ОС) Linux CentOS 5.3. Поэтому при подготовке типового коммуникационного сервера изначально устанавливается операционная система и ряд сервисов UNIX из состава дистрибутива CentOS 5.3

Установка операционной системы вместе с типовыми сервисами является задачей, требующей привлечения квалифицированного технического специалиста, однако дистрибутив CentOS 5.3 реализует режим автоматизированной установки на основе заранее подготовленного файла ответов

Задачей компоненты «Базовая установка ОС» является организация первоначальной установки ОС и типовых сервисов в режиме, требующем минимальных затрат труда и минимальных требований к квалификации

Программных модулей расширения эта компонента не содержит. Она содержит несколько заранее подготовленных файлов ответов для инсталлятора дистрибутива CentOS 5.3 и документацию, пошагово описывающую процесс установки ОС и типовых UNIX сервисов



Файлы ответа выполнены универсальными и предназначены для различных вариантов аппаратной платформы и процедуры установки. Поддерживаются автоматизированная установка на SATA и PATA диски с отдачей файла ответов как через дискету, так и

через подключаемый USB накопитель (USB Flush)

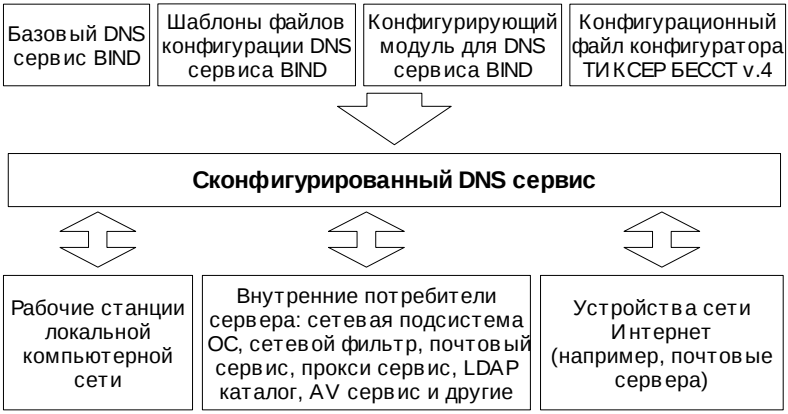
Начальное конфигурирование операционной системы и типовых сервисов UNIX выполняется другими компонентами ТИКСЕР БЕССТ v.4.0 и будет рассмотрено в обзоре соответствующих компонент

Обзор архитектуры и особенности конфигурирования компоненты «Сервер DNS»

DNS сервер является важным сервисом, востребованным как сетевой подсистемой ОС, так и практически всеми типовыми сервисами UNIX и компонентами ТИКСЕР БЕССТ v.4.0

Конфигурирование DNS сервера производится конфигуратором ТИКСЕР БЕССТ v.4.0 методом модификации входящих в поставку ТИКСЕР БЕССТ v.4.0 шаблонов значениями, рассчитываемыми на основе данных конфигурационного файла конфигуратора (конфигурации внутренней и внешней IP подсетей, а также имени обслуживаемого домена)

После проведения начального конфигурирования какого либо интерактивного управления компонентой не предусмотрено, она функционирует в автоматическом режиме



Программных модулей расширения эта компонента не содержит. В качестве базового используется распространённый DNS сервер Bind, входящий в дистрибутив CentOS 5.3. В процессе конфигурирования сформированные конфигурационные файлы размещаются в каталоге /var/named/chroot/..., и, при наличии должной квалификации, могут модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется

примечание: *типовой коммуникационный сервер самостоятельно обрабатывает DNS запросы к обслуживаемому им домену, что требует возможности обращения к внешнему IP адресу сервера из сети Интернет по портам tcp:53 и udp:53, равно как и возможности обращений с сервера к ресурсам Интернет по этим портам. Т.к. иногда провайдеры блокируют эти порты для своих клиентов, необходимо отдельно оговаривать этот момент с провайдером*

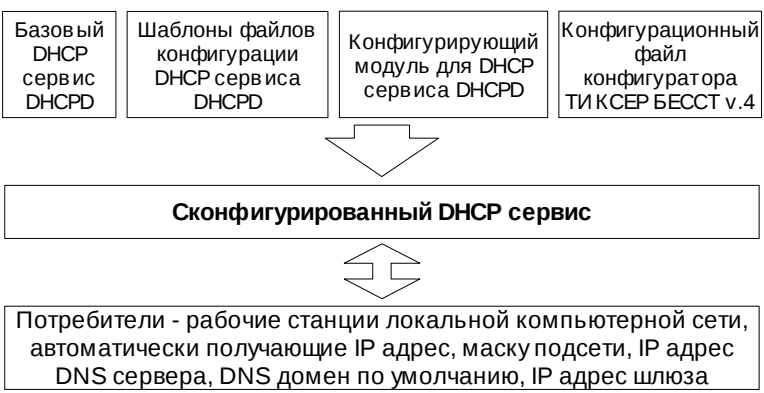
Обзор архитектуры и особенности конфигурирования компоненты «Сервер DHCP»

В текущей редакции ТИКСЕР БЕССТ v.4.0 компонента сервера DHCP представлена как указанием установки сам типовой сервис UNIX,

так и модифицируемым шаблоном конфигурации, входящим в поставку ТИКСЕР БЕССТ v.4.0. Модификации рассчитываются на основе данных конфигурационного файла конфигуратора (конфигурации внутренней подсети и имени домена), однако по умолчанию сервис DHCP не запускается, т.к. возможно перекрытие выдаваемых диапазонов адресов с адресом внутреннего сетевого интерфейса типового коммуникационного сервера

В общем случае в процессе промышленного функционирования запущенный DHCP сервер сильно облегчает жизнь администратору, так как автоматически отдаёт клиентским рабочим станциям уникальный IP адрес и настройки компьютерной сети (имя домена по умолчанию, имя DNS сервера, IP шлюза по умолчанию), однако это не всегда является тем, что нужно в каждом конкретном случае

Программных модулей расширения эта компонента не содержит. В качестве базового используется распространённый DHCP сервер dhcpd, входящий в дистрибутив CentOS 5.3. Сформированный конфигурационный файл размещается по пути /etc/dhcpd.conf и, при наличии должной квалификации, могут модифицироваться техническим специалистам под конкретные нужды



ВНИМАНИЕ !!! Для типового функционирования ТРЕБУЕТСЯ ручная

модификация конфигурационного файла квалифицированным техническим специалистом, которому необходимо указать начало и конец диапазона IP адресов для отдачи их по запросам от клиентских рабочих станций. Прочие модификации конфигурационного файла базового сервиса проводятся автоматически в процессе конфигурирования

При отсутствии противопоказаний рекомендуется активировать запуск сервиса DHCP при загрузке командой «chkconfig --level 35 dhcpd on»

примечание: *в случае, если сервис DHCP не запущен, при настройке клиентских рабочих станций необходимо конфигурировать все сетевые параметры на рабочих станциях вручную*

Обзор архитектуры и особенности конфигурирования компоненты «Сервер SSH»

Сервер SSH востребован при удалённом администрировании типового коммуникационного сервера, обеспечивая возможность удалённого входа технического специалиста на сервер по защищённому шифрованному каналу

Однако, как показывает практика, конфигурация из коробки требует некоторой оптимизации. В частности крайне желательно изменять порт сервера, т.к. распространённым методом атаки является автоматический подбор пароля пользователя роботами, расположенными в Интернет и производящими автоматизированный поиск ресурсов с отвечающим типовым портом SSH tcp:22. По умолчанию порт tcp:22 замещается на tcp:65157. Также проводится рад других модификаций

Новый конфигурационный файл формируется выделенным модулем конфигуратора ТИКСЕР БЕССТ v.4.0 на основе шаблона конфигурации, входящего в поставку ТИКСЕР БЕССТ v.4.0

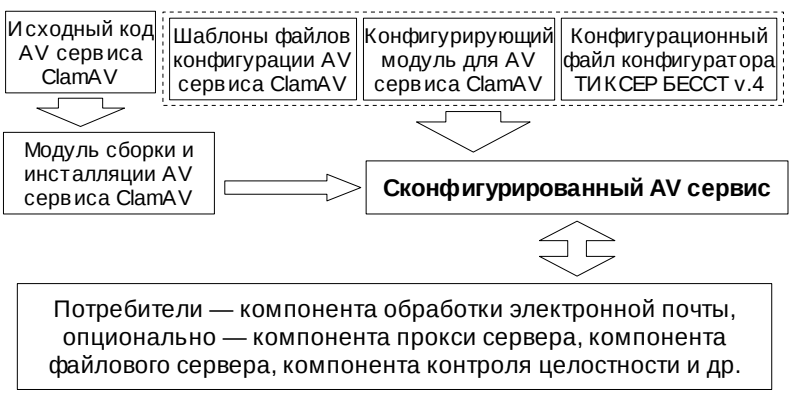
Программных модулей расширения эта компонента не содержит. В качестве базового используется распространённый SSH сервер

OpenSSH, входящий в дистрибутив CentOS 5.3. Сформированный конфигурационный файл размещается по пути /etc/.ssh/sshd.conf и, при наличии должной квалификации, может модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется

примечание: *для защиты от сканирования 22 порта сервис SSH ожидает соединений на изменённом порту 65157, что может быть дополнительно изменено техническим специалистом путём редактирования конфигурационного файла базового сервиса*

Обзор архитектуры и особенности конфигурирования компоненты «Антивирусная служба»

В качестве основы антивирусного сервиса используется продукт ClamAV, пакет которого _не_входит_ в дистрибутив операционной системы CentOS 5.3. Несмотря на то, что он есть в сторонних репозитариях пакетов, ТИКСЕР БЕССТ v.4.0 предполагает компилирование и установку ClamAV из исходных кодов, копия которых поставляется вместе с дистрибутивом ТИКСЕР БЕССТ v.4.0 по лицензии GNU GPL v.2 без каких либо модификаций



В дальнейшем антивирусный сервис используется компонентой обработки электронной почты для защиты почтового оборота от вирусов, а также может использоваться в ряде не типовых для версии 4.0 ТИКСЕР БЕССТ решений

Отдельный модуль конфигуратора ТИКСЕР БЕССТ v.4.0 проводит сборку и установку ClamAV из исходных кодов, а также формирует конфигурационные файлы на основе шаблонов конфигурации, входящих в поставку ТИКСЕР БЕССТ v.4.0

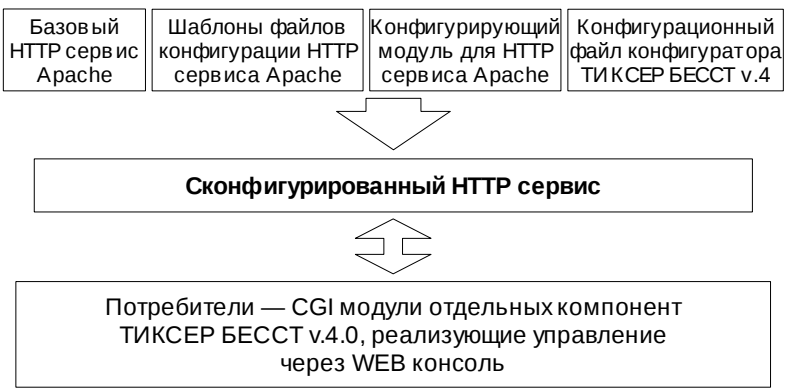
Сформированные конфигурационные файлы размещается по путям /usr/local/etc/clamd.conf и /usr/local/etc/freshclam.conf и, при наличии должной квалификации, может модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется

Базовый сервис может создавать записи в соответствующих ему журналах каталога /var/log/clamav

Кроме того, через WEB консоль управления конечному пользователю доступны программные модули расширения, предоставляющие доступ к журналам функционирования как основного сервиса clamd, так и механизма обновления антивирусных баз freshclam

Обзор архитектуры и особенности конфигурирования компоненты «WEB консоль управления»

Компонента «WEB консоль управления» состоит из базового сервиса, в качестве которого используется типовой UNIX сервис Apache, входящий в дистрибутив CentOS 5.3, и ряда модулей интерактивного взаимодействия с пользователями. Такие модули, в силу большего подчинения другим, узкоспециализированным компонентам, рассматриваются в описании каждой отдельной компоненты



Конфигурационный файл базового сервиса Apache формируется на основе шаблонов конфигурации, входящих в поставку ТИКСЕР БЕССТ v.4.0 отдельным модулем конфигуратора ТИКСЕР БЕССТ v.4.0. Сформированный конфигурационный файл размещается по пути /etc/httpd/httpd.conf и, при наличии должной квалификации, может модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется

Базовый сервис Apache может создавать записи в соответствующих ему журналах каталога /var/log/http

Обзор архитектуры и особенности конфигурирования компоненты «конфигурирования сетевого фильтра и сбора статистики о проходящем IP трафике»

Компонента реализует конфигурирование сетевого фильтра и механизма SNAT на типовом коммуникационном сервере, производит сбор статистики о проходящем трафике и его агрегацию, обеспечивает построение типовых отчётов по утилизации трафика (через соответствующие модули WEB консоли), а также реализует интерактивный механизм построения произвольных запросов к базе статистики (через соответствующие модули WEB консоли)

В процессе первоначальной подготовки типового коммуникационного сервера специальный модуль конфигуратора формирует конфигурационный файл компоненты методом модификации шаблонов конфигурации, входящих в поставку ТИКСЕР БЕССТ v.4.0, значениями, рассчитываемыми на основе данных конфигурационного файла конфигуратора (конфигурации внутренней и внешней IP подсетей, а также имени обслуживаемого домена)

Сформированный конфигурационный файл доступен по пути /usr/local/cosiculs/etc/iprules.conf и, при наличии должной квалификации, могут модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется.

Журналы работы программных надстроек компоненты находятся в каталоге /var/log/cosiculs, базовый сервис netfilter может создавать записи в соответствующих ему журнале каталога /var/log/messages

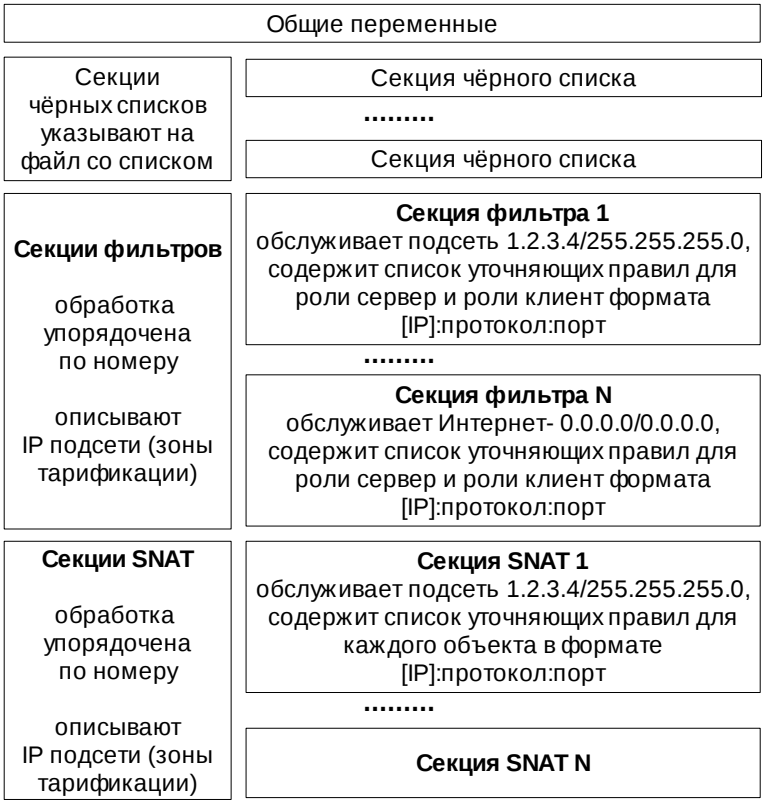
Однако в процессе дальнейшей технической поддержки может возникнуть необходимость в модификации конфигурации компоненты, для чего необходимо представлять себе архитектуру конфигирирующего сетевой фильтр модуля компоненты

Непосредственно опции конфигурационного файла описаны в комментариях к каждой опции, однако кроме этого необходимо учитывать следующую информацию

Сетевой фильтр и механизм SNAT конфигурируются модулем конфигурирования сетевого фильтра текущей компоненты на основании данных конфигурационного файла

В общем случае конфигурационный файл содержит описание отдельных конфигурационных зон нескольких типов. Каждая конфигурационная зона в пределах одного типа должна иметь уникальный номер, на основании которых производится упорядочивание обработки конфигурационных зон одного типа. При запуске модуля конфигуратора сетевого фильтра происходит

чтение данных конфигурационного файла и сетевой фильтр последовательно конфигурируется данными упорядоченных конфигурационных зон для типов - чёрный список IP, далее - упорядоченные конфигурационные зоны сетевого фильтра, далее - упорядоченные конфигурационные зоны SNAT



Конфигурационные зоны типа «чёрный список IP адресов» содержат ссылку на файл со списком IP адресов, которые нужно блокировать сразу

Конфигурационные зоны типа «сетевой фильтр» описывают отдельные подсети (тарификационные зоны), определяемые в общем случае адресом и маской подсети и IP адресом интерфейса коммуникационного сервера, через который производится взаимодействие с подсетью

Далее для каждой тарификационной зоны описываются уточняющие записи, которые содержат разрешающие фильтры для трафика, в котором типовой коммуникационный сервер выступает в роли клиента или сервера, для протоколов tcp и udp. Т.е. всего два набора (asClient и asServer) уточняющих записей для каждой тарификационной зоны типа «сетевой фильтр»

Каждое уточняющее условие имеет формат ip_адрес:протокол:порт, причём ip_адрес может быть опущен, а может указываться для сужения разрешающих правил

В случае, если IP трафик соответствует условиям описания подсети (тарификационной зоне), он пропускается только при соответствии правилам в данной тарификационной зоне. Если трафик, соответствующий общему описанию тарификационной зоны, не соответствует ни одному соответствующему зоне уточняющему правилу, он отбрасывается. Статистика при этом собирается как по пропущенному далее, так и по отброшенному трафику

примечание: *важно присваивать номера тарификационных зон в правильном порядке, в частности тарификационная зона, обслуживающая обращение к Интернет должна иметь самый большой номер среди тарификационных зон типа «сетевой фильтр». В противном случае трафик будет причисляться к Интернет зоне раньше имеющих больший номер, и не дойдет до правильной тарификационной зоны. Это произойдет потому, что адрес подсети (0.0.0.0) и маска подсети (0.0.0.0) для зоны Интернет подразумевают весь трафик*

Конфигурационные зоны типа «SNAT трансляция» также описывают отдельные подсети (тарификационные зоны), определяемые в общем случае адресом и маской подсети и IP адресом интерфейса коммуникационного сервера, через который производится взаимодействие с подсетью

Для каждой такой зоны существует только один список уточняющих правил в формате удалённый_IP:протокол:порт. Каждое такое правило отражает отдельного локального клиента, которому требуется получить прямой доступ в Интернет. В целях безопасности рекомендуется максимально сужать разрешаемый пользователю коридор (Одним из наиболее ярких примеров поля применения данной возможности является разрешение проброса разнообразного бухгалтерского софта, клиент - банков, систем отчётности и т.п., использующих нестандартные порты)

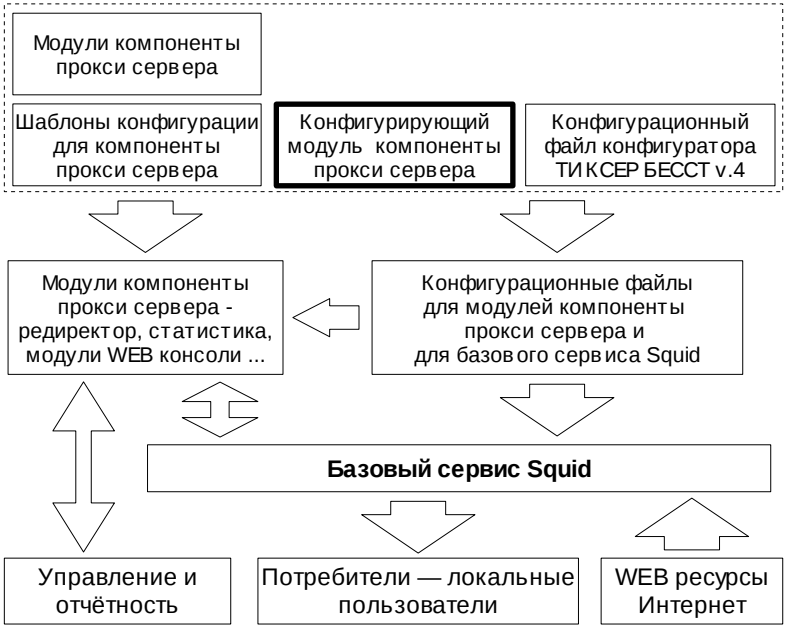
Для всех тарификационных зон важно выставить уникальный в пределах конфигурационного файла статистический префикс из нескольких латинских символов, уникальное наименование зоны и флаги учёта статистики зоны как статистики внешнего или внутреннего трафика. Если для зон сетевого фильтра обычно выставляется либо флаг внешнего, либо флаг внутреннего трафика, то зоны трансляции SNAT должны иметь выставленными оба флага
Модули сбора и агрегации статистики о проходящем IP трафике, равно как и модули отображения типовых отчётов и построителя запросов к базе статистики не подлежат какому либо конфигурированию

Нужно понимать, что любое ручное переконфигурирование требует тщательной увязки конфигурации сетевых компонентов ОС, модуля конфигуратора сетевого фильтра и настроек DNS сервера как минимум, и должно проводиться только при чётком понимании целей, ожидаемых результатов и методов достижения

Обзор архитектуры и особенности конфигурирования компоненты «полицейско биллинговая система прокси сервера»

Компонента реализует единую точку подключения к WEB ресурсам, что позволяет организовать кэширование загружаемых данных (что несколько экономит трафик), сбор статистики и лимитирование доступа. Конечному пользователю доступны через WEB консоль как возможности управлять лимитирующими записями, так и получение типовых отчётов и формирование детализированных отчётов через интерактивный построитель запросов к базе статистики

Дополнительно реализована отключаемая фильтрация баннеров по предустановленному списку сайтов баннерных сетей



Доступ к WEB ресурсам может предоставляться как без авторизации на основе разрешающего правила для всей локальной подсети (в этом случае лимитирующие записи не учитываются), так и по лимитирующим записям, которые могут учитывать имя пользователя (в этом случае требуется предварительная авторизация пользователя) и/или IP адрес локального клиентского компьютера

Авторизацию и учёт лимитирующих записей для каждого запроса осуществляет модуль биллингового агента, подключаемый к базовому сервису предусмотренным для базового сервиса методом подключения редиректоров. Функционирование модуля биллингового агента определяет конфигурационный файл, все опции которого снабжены наглядными комментариями

В качестве базового используется распространённый proxy сервер Squid, входящий в дистрибутив CentOS 5.3. Конфигурационные файлы базового сервиса и надстроек формируются отдельным конфигурационным модулем методом модификации входящих в поставку ТИКСЕР БЕССТ v.4.0 конфигурационных шаблонов

Сформированный конфигурационный файл базового сервиса размещается по пути /etc/squid/squid.conf, а конфигурационный файл надстроек компоненты располагается по пути /usr/local/cosiculs/etc/squidbilling.conf. При наличии должной квалификации эти файлы могут модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется

Журналы работы модулей программных надстроек компоненты находятся в каталоге /var/log/cosiculs, журнал базового сервиса расположен в каталоге /var/log/squid

примечание: *при активации лимитирования (по умолчанию) важно не забывать добавлять лимитирующие записи, которые вступят в действие не сразу, но после очередного запуска модуля агрегации данных (по умолчанию запускается раз в пять минут)*

Обзор архитектуры и особенности конфигурирования компоненты «обработки электронной почты»

Компонента обработки электронной почты существенно расширяет типовой функционал постовых серверов, что достигается путём внедрения в процесс обработки электронной корреспонденции модуля контроля обработки. Модуль контроля обработки реализует архивирование всей проходящей электронной корреспонденции, а также экспериментальный функционал принятия решений об обработке каждого письма на основе задаваемых конечным пользователем правил

Дополнительно реализуется сбор статистики об обработке электронной корреспонденции, а также антивирусная защита и защита от нежелательных почтовых рассылок (СПАМа)

Управление архивом, правилами обработки и доступ к типовым статистическим отчётам доступен конечному пользователю через WEB консоль

В качестве базового используется распространённый email сервер Exim, входящий в дистрибутив CentOS 5.3. Функционирование модулей надстройки и базовых сервисов компоненты определяется конфигурационными файлами, формируемыми отдельным конфигурационным модулем методом модификации входящих в поставку ТИКСЕР БЕССТ v.4.0 конфигурационных шаблонов. Опции конфигурационных файлов модулей надстройки снабжены комментариями

Сформированные конфигурационные файлы базового сервиса размещается по пути /etc/exim/..., а конфигурационный файл надстроек компоненты располагается по пути /usr/local/cosiculs/etc/email.conf. При наличии должной квалификации эти файлы могут модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется

Журналы работы модулей программных надстроек компоненты находятся в каталоге /var/log/cosiculs, журнал базового сервиса расположен в каталоге /var/log/exim

примечание1: *по умолчанию экспериментальный функционал учёта правил обработки электронной корреспонденции выключен, при необходимости он должен быть включён в конфигурационном файле модулей надстройки текущей компоненты*

примечание2: *в связи с невозможностью предварительного определения среды функционирования компоненты в стандартную поставку включено минимальное количество антиСПАМ опций, при необходимости построения более серьёзной защиты требуется доконфигурирование техническим специалистом*

Обзор архитектуры и особенности конфигурирования компоненты «управления учётными записями пользователей UNIX»

Компонента выполнена максимально простой и обеспечивает управление учётными записями пользователей UNIX из WEB консоли

Для того, чтобы учётные записи не пересекались с учётными записями каталога LDAP и с системными учётными записями, компонента конфигурирует диапазон идентификаторов (ID), отдельный от системных учётных записей, а, при использовании каталога LDAP компонента управления каталогом также работает с отдельным диапазоном идентификаторов

В качестве базового используются штатные утилиты UNIX (useradd, groupadd и т.п.), входящие в дистрибутив CentOS 5.3. Конфигурационные файлы базового сервиса и надстроек формируются отдельным конфигурационным модулем методом модификации входящих в поставку ТИКСЕР БЕССТ v.4.0 конфигурационных шаблонов

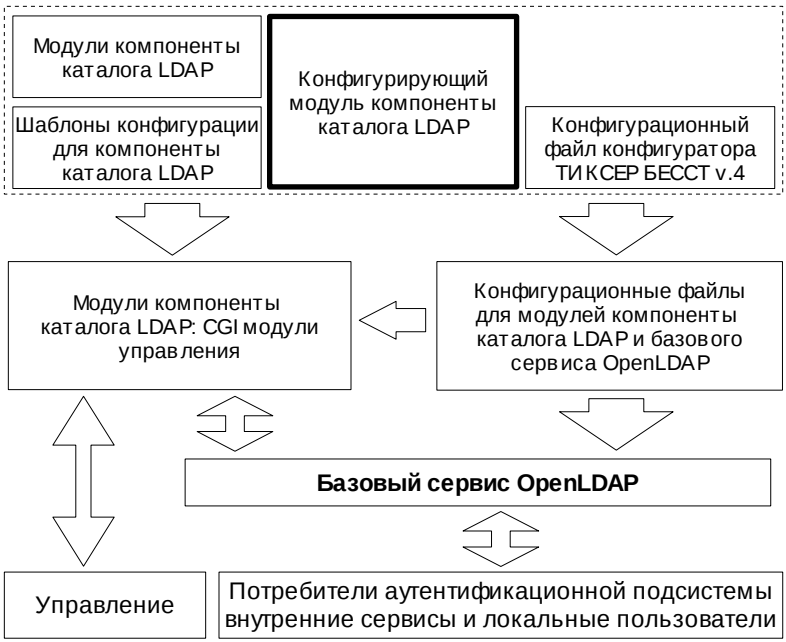
Сформированный конфигурационный файл базового сервиса размещается по пути /etc/login.defs и другие, а конфигурационный файл надстроек компоненты располагается по пути /usr/local/cosiculs/etc/uumanage.conf. При наличии должной квалификации эти файлы могут модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется

Журналы работы модулей программных надстроек компоненты находятся в каталоге /var/log/cosiculs, журналы базового сервиса расположены в каталоге /var/log

Обзор архитектуры и особенности конфигурирования компоненты «управления каталогом LDAP»

Компонента управления каталогом LDAP в ТИКСЕР БЕССТ v.4.0 имеет статус экспериментальной. По большей части это вызвано более сложным, по сравнению с компонентой управления учётными записями пользователей UNIX, управлением

Функционал каталога LDAP местами незаменим средствами других компонент, и для типового коммуникационного сервера компонента отлажена. Компонента может использоваться в качестве основы для развёртывания сервиса каталога масштаба предприятия, но это не типовое решение, выходящее далеко за рамки настоящей инструкции



В качестве базового используется распространённый LDAP сервер OpenLDAP и клиентские модули pam_ldap и nss_ldap, входящие в дистрибутив CentOS 5.3. Конфигурационные файлы базового сервиса и модулей программных надстроек компоненты формируются отдельным конфигурационным модулем методом модификации входящих в поставку ТИКСЕР БЕССТ v.4.0 конфигурационных шаблонов

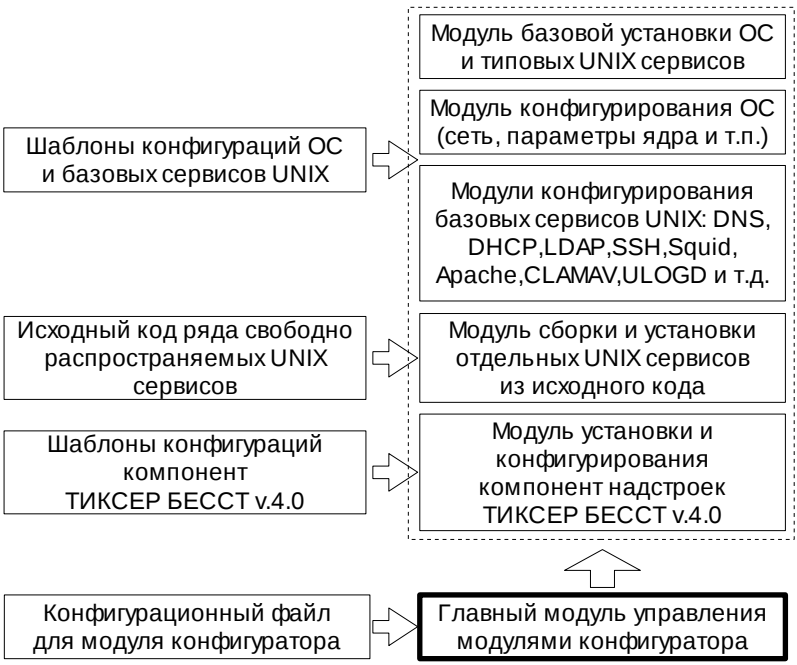
Сформированные конфигурационные файлы базового сервиса размещаются в каталогах /etc/openldap/ и /etc/, а конфигурационный файл надстроек компоненты располагается по пути /usr/local/cosiculs/etc/ldap.conf. Кроме конфигурационных файлов базового сервиса и программных надстроек компоненты соответствующий модуль конфигуратора ТИКСЕР БЕССТ v.4.0 перенастраивает в операционной системе механизмы аутентификации и получения данных учётной записи

При наличии должной квалификации и чётком понимании организации работы каталога LDAP эти файлы могут модифицироваться техническим специалистам под конкретные нужды. Для типового функционирования никакой ручной модификации не требуется

Журналы работы модулей программных надстроек компоненты находятся в каталоге /var/log/cosiculs, журнал базового сервиса расположены в по пути /var/log/messages

Обзор архитектуры и особенности конфигурирования компоненты «Конфигуратор ТИКСЕР БЕССТ»

Основной задачей компоненты является первоначальная подготовка типового коммуникационного сервера, включающая начальное конфигурирование операционной системы и типовых сервисов UNIX, сборку и установку ряда свободных программных пакетов, не входящих в дистрибутив операционной системы, а также установку и конфигурирование непосредственно компонент ТИКСЕР БЕССТ v.4.0



Компонента состоит из ряда программных модулей, выполняющих узко специализированные задачи по конфигурированию отдельной

компоненты и настройке базовых сервисов для такой компоненты, базовой конфигурации ОС или сборке и установке отдельных программных пакетов

Все эти модули управляются общим модулем управления, реализующим предварительные проверки и запуск модулей в нужной последовательности, т.к. отдельные компоненты находятся в зависимости друг от друга

Компонента функционирует на основе конфигурационного файла, параметры которого должны быть модифицированы техническим специалистом до запуска процесса конфигурирования в соответствии со своей рабочей средой

Параметры конфигурационного файла снабжены комментариями и подразделяются на пароли, параметры сетевой конфигурации и параметры выбора вариантов работы отдельных компонент

Все пароли настоятельно рекомендуется изменить на сложные криптостойкие перед запуском конфигуратора, и сохранить эти новые пароли в надёжном месте. Вводить в эксплуатацию сервер, сконфигурированный с паролями по умолчанию, недопустимо

Поддерживаются следующие отдельные пароли:

- пароль администратора СУБД PostgreSQL
- пароль администратора каталога LDAP
- пароль администратора на вход в WEB консоль и формирование отчётов
- пароль администратора на модифицирующие действия в WEB консоли
- пароль root (администратора) операционной системы

Пароли администратора на вход в WEB консоль и формирование отчётов реализованы как стандартный механизм ограничения

доступа WEB сервера Apache через записи в .htaccess. Сам список пользователей с хэшами паролей расположен в каталоге /usr/local/cosiculs/etc и может модифицироваться техническим специалистом. При этом корректные строки с именами и хэшами могут быть получены командой htpasswd, входящей в поставку WEB сервера Apache

Пароли администратора на модифицирующие действия в WEB консоли поддерживаются отдельным списком, расположенным по адресу /usr/local/cosiculs/etc/Admin.list и может модифицироваться техническим специалистом. При этом корректные строки с именами и хэшами могут быть получены командой /usr/local/cosiculs/sbin/createPasswd

Параметры настройки сетевой подсистемы должны быть собраны перед началом работ инсталляции типового коммуникационного сервера, как это описано в разделе «подготовительные мероприятия» инструкции по установке ТИКСЕР БЕССТ v.4.0 и аккуратно перенесены в конфигурационный файл конфигуратора

Выбор конкретных значений для **параметров выбора режимов работы отдельных компонент** диктуется ситуацией в каждом конкретном случае, изменение значения параметров, установленных по умолчанию, проводится техническим специалистом при наличии обоснованной необходимости