УТВЕРЖДЕНО

643.63024504.00001-04 90 01-ЛУ

Программный межсетевой экран

«Интернет Контроль Сервер»

Руководство администратора

643.63024504.00001-04 90 01

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

2016

АННОТАЦИЯ

В данном программном документе приведено руководство администратора по настройке и использованию программного межсетевого экрана «Интернет Контроль Сервер» (далее МЭ «ИКС», Изделие), предназначенного для обеспечения безопасности информации и управления сетевым трафиком при организации доступа между несколькими физическими сегментами сети с различными принятыми политиками безопасности.

В разделе «Общие сведения о программе» указаны назначение и функции программы и сведения о технических и программных средствах, обеспечивающих выполнение данной программы, а также требования к персоналу.

В разделе «Структура программы» приведены сведения о структуре программы, ее составных частях, о связях между составными частями и о связях с другими программами.

В разделе «Настройка программы» приведено описание действий по настройке программы на условия конкретного применения (настройка на состав технических и программных средств, выбор функций и др.).

В разделе «Описание старта Изделия и процедур проверки правильности старта» приведено описание запуска Изделия, в том числе и в ручном режиме, а также описана процедура проверки работоспособности программы.

В разделе «Резервное копирование и восстановление» приведено описание действий, требуемых для создания резервных копий и выполнения процедуры восстановления Изделия» после аппаратных и программных сбоев.

В разделе «Сообщения администратору Изделия» приведено описание сообщений, выдаваемых Изделием администратору.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Назначение программы

Изделие предназначено для обеспечения безопасности информации и управления сетевым трафиком при организации доступа между несколькими физическими сегментами сети с различными принятыми политиками безопасности.

1.2 Функции программы

Изделие реализует выполнение следующих функций:

1) разделения внутренних информационных потоков при решении задач информационной безопасности на объектах, обрабатывающих информацию различного уровня конфиденциальности;

2) аутентификации пользователей при доступе к различным информационным ресурсам;

3) аудита регистрируемых событий безопасности.

1.3 Минимальный состав технических средств

В состав используемых технических средств входит аппаратная платформа Изделия (сервер), конфигурация которых должна быть не хуже, чем указанные в Таблице 1. и Таблице 2. соответственно. Система поддерживает установку как на 32-битные, так и на 64-битные аппаратные средства.

Таблица 0 - Минимальные и рекомендуемые требования к аппаратному обеспечению

Характеристика	Минимально	Рекомендуемое
Частота центрального процессора	1.8 ГГц	2 ГГц и выше
Объем оперативной памяти	1024 Мб	1048 Мб и выше
Объем жесткого диска	160 Гб	320 Гб и выше

Следует учесть, что рекомендуемый объем устанавливаемых на сервера жестких дисков зависит от планируемого объема хранимых на этих серверах данных.

1.4 Минимальный состав программных средств

Изделие включает в себя операционную систему, поэтому не требует наличия дополнительного программного обеспечения.

1.5 Требования к персоналу (системному программисту)

Системный программист должен иметь как минимум среднее техническое образование.

В перечень задач, выполняемых системным программистом, должны входить:

1) задача поддержания работоспособности технических средств;

2) задача установки (инсталляции) и поддержания работоспособности Изделия.

2 СТРУКТУРА ПРОГРАММЫ

2.1 Сведения о структуре программы

1) компоненты:

- специальное программное обеспечение межсетевого экрана;

- графический интерфейс администратора;

- программное обеспечение клиента аутентификации.

2) специальное программное обеспечение устанавливается на аппаратную платформу межсетевого экрана и состоит из следующих функциональных модулей:

- модуль веб-интерфейса;

- модуль резервного копирования;

- модуль учёта статистики;

- модуль регистрации динамических адресов пользователей;

- модуль управления провайдерами;

- модуль фильтрации HTTP-трафика;

- модуль связи с windows-доменом;

- прокси-сервер;

- модуль управления сетевой подсистемой;

- модули поддержки VPN-протоколов;

- сетевые службы: DNS, DHCP, NTPD;

- модуль аудита;

- модуль мониторинга;

- службы файлового и веб-сервера;

- модуль управления жёсткими дисками;

- модуль межсетевого экрана;

- модуль IP-телефонии;

- модуль DLP и контент-фильтра;

- модуль антивируса;

- модуль антиспама;

- операционную систему;

- модуль кластер.

3) программное обеспечение клиента аутентификации.

Для режима аутентификации пользователей «xauth», изделие использует следующее пользовательское ПО:

- клиент аутентификации.

2.2 Сведения о связях между составными частями программы

Модули программы представляют собой отдельные программные комплексы, инсталлируемые в операционную систему при установке программы, связь между которыми осуществляется посредством выполнения команд графического интерфейса, которые интерпретируются в команды операционной системы.

2.3 Сведения о связях с другими программами

Доступ к графическому интерфейсу Изделия осуществляется посредством обозревателя сети Интернет (например, Mozilla Firefox версии 3.0 и выше, Internet Explorer версии 8 и выше, Opera версии 9 и выше или Google Chrome любой версии).

3 НАСТРОЙКА ПРОГРАММЫ

3.1 Настройка на состав технических средств

Специальной настройки на состав технических средств не требуется.

3.2 Настройка на состав программных средств

Установка программного обеспечения осуществляется администратором. Для установки программных модулей Изделия необходимо выполнить следующие действия:

Для установки Изделия необходимо:

1) вставить дистрибутивный CD-диск в привод компакт-дисков;

2) после окончания процесса загрузки, выбрать язык установки;

3) запустить процесс установки;

В процессе установки ПО Изделия необходимо выбрать жёсткий диск для установки, а также настройки для сетевых интерфейсов (имя устройства, сетевой адрес, маску подсети и шлюз).

По окончании процесса установки веб-интерфейс управления Изделием будет доступен по протоколу HTTP по ip-адресу, указанному на предыдущем этапе.

Настройка программы на работу

Первичная настройка сетевых интерфейсов и модуля «Межсетевой экран»

При первом входе в веб-интерфейс модуль «Межсетевой экран» имеет статус «не настроен». Первичная настройка считается завершенной, когда модуль «Межсетевой экран» приобретет статус «запущен».

Для этого необходимо, чтобы в модуле «Провайдеры и сети» был создан как минимум один сетевой интерфейс класса «Провайдер» и один класса «Локальная сеть».

Настройка сетевых интерфейсов может проводиться двумя способами:

1) запуском модуля «Мастер настройки сети» с пошаговым прохождением этапов настройки одновременно всех доступных интерфейсов с указанием необходимых параметров.

2) ручной настройкой каждого интерфейса в отдельности, используя меню «Добавить» в модуле «Провайдеры и сети».

В программе реализованы следующие типы сетевых интерфейсов. Они приведены в Таблице 2.

Таблица 2 - Типы сетевых интерфейсов

Тип	Описание
локальная сеть	внутренний интерфейс сервера. В этой сети будут находиться пользователи. Позволяет указать VLAN ID интерфейса
локальная сеть WIFI	беспроводной внутренний интерфейс сервера
внутренняя сеть	сеть предприятия, которая не подключена к ИКС напрямую и компьютеры которой выходят в интернет через ИКС
VPN-сеть	виртуальная частная сеть, позволяющая объединить в единую сеть пользователей, физически находящихся в различных местах. Кроме того, с помощью VPN можно организовать выход компьютеров локальной сети к интернету по логину/паролю. Объединяет подключения по протоколам PPTP, L2TP, L2TP+IPSec и PPPoE.
провайдер	внешний интерфейс сервера со статически или динамически (по протоколу DHCP) сконфигурированным ip-адресом.
провайдер PPPoE	внешний интерфейс сервера, подключающийся к провайдеру по протоколу PPPoE.
провайдер 3G	подключение к внешней сети с использованием CDMA/GPRS-устройства мобильного оператора
провайдер WIFI	беспроводной внешний интерфейс сервера

туннель IPIP, GRE, OpenVPN	механизм позволяющий объединить две (или более) удалённые и не связанные физически сети в единую логическую структуру.
Провайдер PPTP	внешний интерфейс сервера, подключающийся к провайдеру по протоколу PPTP со статически или динамически (выданным по протоколу DHCP) сконфигурированным ip-адресом в «серой» сети провайдера.
Провайдер L2TP	внешний интерфейс сервера, подключающийся к провайдеру по протоколу L2TP со статически или динамически (выданным по протоколу DHCP) сконфигурированным ip-адресом в «серой» сети провайдера.
DMZ сеть	внутренний интерфейс сервера. В этой сети могут находиться корпоративные сервера с внешними ip-адресами. Такая настройка сети проводится для повышения их безопасности и ограничения уровня доступа к ним посредством межсетевого экрана. Также позволяет указать VLAN ID.

После завершения первичной настройки можно переходить к добавлению пользователей программы.

Добавление пользователей программы

Пользователь – единица управления системой. Это наименьший объект применения политик программы и детализации статистики сетевого трафика. После того как пользователь добавлен, он получает доступ во внешнюю сеть (интернет) в соответствии со своим способом авторизации, а также индивидуальными и глобальными политиками доступа.

Добавление пользователя может быть осуществлено следующими способами:

1) использование модуля «Мастер создания пользователя» с пошаговым

прохождением этапов добавления параметров пользователя, таких как имя пользователя, имя входа (логин), пароль, один или несколько ip-адресов, а также почтовый ящик. Из всех параметров обязательным является только имя пользователя.

2) ручное создание пользователя с использованием меню «Добавить» - «Пользователь». Данным способом пользователю назначаются только имя, логин и пароль, остальные параметры редактируются непосредственно в индивидуальном модуле пользователя.

3) импорт пользователей возможен в четырех вариантах: из файла (источником служит файл формата TXT, в котором перечислены строки, содержащие параметры имя, логин, пароль, ip-адрес), из домена (импортирует пользователей Active Directory, для того, чтобы данный импорт был возможен, необходимо присоединить программу к домену через модуль «Сетевое окружение»), из сети (сканирует каждую локальную сеть на предмет доступных ip-адресов из адресного пространства сети), из LDAP/AD (аналогичен импорту из домена, однако не требует постоянного присоединения к нему).

4) авторизация по MAC. Применяется в том случае, когда в сети используются динамические адреса, но в качестве DHCP-сервера выступает не ИКС. Для того, чтобы добавить пользователю mac-адрес, перейдите во вкладку IP-адреса и нажмите Добавить - MAC-адрес. При этом пользователь получает доступ во внешнюю сеть по всем протоколам в соответствии с глобальными и индивидуальными политиками доступа

Способы авторизации пользователей

В Изделии применяются следующие способы авторизации пользователей:

1) авторизация по логину и паролю в модуле «Прокси-сервер» Изделия. Для того, чтобы пользователь мог подключиться к прокси-серверу, необходимо, чтобы в его веб-браузере был указан ip-адрес внутреннего интерфейса Изделия («Локальная сеть») и порт 3128 (по умолчанию, данный порт может быть изменен в настройках модуля «Прокси-сервер»). Сама авторизация может осуществляться двумя методами: по логину и паролю пользователя (пользователь, сделавший HTTP-запрос, получает первоначально приглашение на ввод своего логина и пароля доступа, а после успешной идентификации – результат запроса) и через домен (пользователь, зарегистрированный на сервере Active Directory, автоматически авторизуется на прокси-сервере). Второй метод возможен лишь в том случае, когда программа присоединена к домену Active Directory. Следует отметить, что в обоих случаях пользователю будет доступен выход во внешнюю сеть только по протоколу HTTP.

2) авторизация по ip-адресу. Применяется в том случае, когда пользователи локальной сети имеют статические ip-адреса либо динамические ip-адреса, регистрируемые с привязкой к mac-адресу. Для того, чтобы пользователь мог получить доступ во внешнюю сеть, достаточно добавить его ip-адрес во вкладке «Ip-адреса» индивидуального модуля пользователя. Пользователь получает доступ во внешнюю сеть по всем протоколам в соответствии с глобальными и индивидуальными политиками доступа.

3) авторизация посредством клиентской части Изделия xauth.exe. Применяется в том случае, когда пользователи сети имеют динамические переменные ip-адреса. Как и при авторизации по ip-адресу, пользователь получает полный доступ во внешнюю сеть при данном типе авторизации. Для того, чтобы выполнить авторизацию, пользователю необходимо на своем компьютере запустить файл xauth.exe (применимо только для Windows-систем). Далее возможны два метода подключения: простая авторизация (пользователь получает приглашение на ввод своего логина и пароля) и авторизация через домен (пользователь, зарегистрированный на сервере Active Directory, автоматически авторизуется в программе). Второй метод возможен лишь в том случае, когда программа присоединена к домену Active Directory.

Настройка уровня доступа пользователей

Настройка доступа пользователей к веб-интерфейсу

В программе возможны следующие уровни доступа пользователя к веб-интерфейсу:

1) администратор – имеет полный доступ, может изменять любые параметры программы, реализованные через веб-интерфейс;

2) администратор группы – имеет ограниченный доступ к веб-интерфейсу, может контролировать уровень доступа пользователей группы, в которой он находится, не может изменять глобальные настройки системы;

3) пользователь – имеет ограниченный доступ только к своему индивидуальному модулю для просмотра статистики сетевого трафика.

Администратор также может создавать собственные роли в модуле «Роли». Роль нового пользователя задается при его создании и может быть в дальнейшем изменена редактированием пользователя.

Виды политик контроля доступа

В программе реализованы следующие функции контроля пользователей:

1) запрещающие, разрешающие правила и исключения – контролируют доступ пользователя к ip-адресам, протоколам, портам и mime-типам на уровне межсетевого экрана. Среди прочего, они позволяют заблокировать два протокола прикладного уровня при помощи layer7-фильтрации – это протоколы OSCAR (ICQ) и P2P (torrent).

2) запрещающие, разрешающие правила и исключения прокси – контролируют доступ пользователя к интернет-ресурсам по URL на уровне прокси-сервера;

3) ограничение скорости – изменяет скорость доступа к указанным ресурсам или к внешней или внутренней сети в целом;

4) выделение полосы пропускания – устанавливает минимальное значение скорости доступа к указанным ресурсам или к внешней или внутренней сети в целом;

5) квота – устанавливает максимальное значение полученного пользователем объема данных от указанного ресурса, по указанному протоколу (порту) или от внешней или внутренней сети в целом;

6) маршрут – устанавливает для пользователя индивидуальное направление потока передачи данных до указанного ресурса, по указанному протоколу (порту) или до внешней или внутренней сети в целом;

7) приоритет – присутствует только в глобальных правилах межсетевого экрана, позволяет установить очередность обработки потока передачи данных до указанного ресурса, по указанному протоколу (порту) или до внешней или внутренней сети в целом.

8) контроль DLP - добавляет правило, которое будет сканировать трафик пользователя в соответствии с настроенной базой отпечатков DLP.

9) правило контентной фильтрации - добавляет правило прокси, которое проверяет загружаемый html-код на совпадения с базой данных контент-фильтра.

10) ограничение количества соединений – создает правило межсетевого экрана, не позволяющее пользователю превышать указанное количество одновременных соединений с внешней сетью.

Кроме того, существуют специальные объекты, ускоряющие создание политик доступа:

1) категории – аналогичны разрешающим (запрещающим) правилам прокси, но позволяют включать в себя множество URL, а также добавляют фильтрацию по расширению загружаемого файла и ключевым словам; Они подразделяются на две группы – стандартные

категории – содержат статический список объектов и обновляются вместе с обновлением системы. Вторая группа – категории SkyDNS – это ссылки, обращающиеся к серверу сервиса SkyDNS и обновляющиеся динамически.

2) наборы правил – глобальные объекты, позволяющие сохранить любое количество пользовательских правил под указанным именем и применить без повторной настройки сразу к нескольким пользователям или группам. По умолчанию в модуле «Наборы правил» создаются глобальные объекты для каждой роли пользователя, при добавлении администратором новой роли, автоматически создается одноименный набор правил.

Также, каждому объекту может быть применен параметр «Время действия», ограничивающий время работы политики.

Очередность выполнения политик контроля пользователей

При применении различных политик контроля доступа пользователей следует учесть последовательность их применения:

1) Глобальные правила межсетевого экрана;

2) Глобальные профили ролей пользователей;

3) Политики корневой группы;

4) Политики вложенных групп;

5) Политики конкретного пользователя;

Детализация сетевого трафика пользователя

Модуль статистики представлен в программе в двух вариантах – собственно модуль и его элемент для каждого пользователя или группы.

Модуль «Отчеты» предоставляет сводный отчет всего потребленного из внешней сети трафика, выполненный в виде таблиц и графиков, список доступных типовых и пользовательских отчетов, а также форму фильтрации для формирования требуемого отчета.

Форма фильтрации разделена на две части: параметры и таблица статистики. Параметры представляют собой систему фильтров, которые можно применять к статистике пользователя в любых комбинациях.

Панель параметров предлагает следующие элементы фильтрации пользовательской статистики. Они представлены в Таблице 3.

Таблица 3 - Элементы фильтрации пользовательской статистики

Поле	Значение
группировка	группирует все элементы списка тарификации по указанному принципу
источник	позволяет отфильтровать сгруппированную статистику по указанному пользователю или группе
назначение	позволяет отфильтровать сгруппированную статистику по указанному направлению трафика
ip-адрес или домен	выделяет среди всей отфильтрованной статистике только относящуюся к указанному ip-адресу или домену
протокол/порт	выделяет среди всей отфильтрованной статистике только относящуюся к указанному протоколу/порту
mime-тип	выделяет среди всей отфильтрованной статистике только относящуюся к выбранному из списка mime-типу
дата (с … по)	выделяет среди всей отфильтрованной статистике только относящуюся к выбранному временному периоду
время	выделяет среди всей отфильтрованной статистике только относящуюся к указанному времени суток

При нажатии на кнопку […] справа от поля «Группировка» откроется список возможных группировок детализированной статистики.

Возможные группировки представлены в Таблице 4

Таблица 4 - Группировки детализированной статистики

Группировка	Значение
по назначениям	выводит детализацию статистики по источникам трафика

по источникам	выводит детализацию статистики по пользователям (группам)
по ip-адресам источников	выводит детализацию статистики по всем ip-адресам заведенных пользователей
по интерфейсам	выводит детализацию статистики по интерфейсам ИКС
по ip-адресам и доменам	выводит детализацию статистики по посещенным ip-адресам и доменным именам (сайтам)
по протоколам	выводит детализацию статистики по сетевым протоколам, используемым различными службами и программами
по портам	выводит детализацию статистики по портам транспортного уровня TCP/IP, используемым различными службами и программами
по времени (месяцам, дням, часам)	выводит детализацию статистики по временным периодам
детализация HTTP-трафика	выводит подробную детализацию HTTP-статистики, отсортированную по времени
детализация IP-трафика	выводит подробную детализацию IP-статистики, отсортированную по времени

После выбора всех необходимых фильтров нажмите кнопку «Показать» в нижней части панели. ИКС сформирует отчет и представит его в таблице 5. Поскольку построение отчета занимает какое-то время, в интерфейсе будет показан прогресс построения в виде заполняющейся шкалы с обозначением процента выполнения.

Кнопка «Параметры» позволяет скрыть или показать панель параметров.

Для того, чтобы запомнить выбранный набор фильтров, чтобы не настраивать его в дальнейшем заново, нажмите кнопку «Сохранить отчет» и введите имя нового отчета. Сохраненный отчет появится в списке доступных отчетов.

Таблица 5 - Форма отчета по статистике

Столбец	Значение
назначение	показывает элементы, по которым сгруппирована статистика
первое обращение	показывает время первого начисления данных по данному элементу
% от макс	показывает графически процентное соотношение статистики по данному объекту к общему объему статистики в пределах выбранных фильтров
трафик	показывает числовые значения трафика по каждому элементу (зеленым - входящий трафик, красным - исходящий)

Также, элементы модуля «Отчеты» представлены в каждом индивидуальном модуле пользователя или группы. Он содержит только два раздела – «Сводный отчет» и «Статистика», которые аналогичны таковым в модуле «Отчеты», но применяются для конкретного пользователя или группы.

Экспорт статистики в файл

В программе присутствует возможность переноса полученной в результате фильтрации статистики в файл выбранного формата для последующего сохранения либо распечатки.

Чтобы экспортировать данные, необходимо нажать кнопку «Экспортировать» в левом верхнем углу модуля и выбрать формат файла экспорта (*.csv, *.txt или *.xls). Программа предложит уточнить, выводить ли всю таблицу либо только указанные элементы. После нажатия кнопки ОК посредством стандартного загрузчика браузера необходимо указать путь сохранения файла.

Диапазоны адресов

Модуль «Диапазоны адресов» содержит список всех объектов тарификации, по которым программа ведет учет. По умолчанию источники на стороне локальных сетей считаются внутренними, на стороне провайдеров - внешними. ИКС - универсальный источник трафика, который показывает, сколько всего информации прошло через шлюз в обе стороны.

При необходимости администратор может создать собственный список адресов, подсетей или доменных имен, объединив их в пользовательский диапазона. Этот диапазон может быть внешним или внутренним (нетарифицируемым). По умолчанию создаваемый диапазон внутренний. Обычно создание такого диапазона необходимо, когда провайдер предоставляет доступ к внутренним ресурсам, которые не оплачиваются по тарифу. Чтобы отметить диапазон как внешний, необходимо установить флажок «Внешний диапазон адресов».

Настройка дополнительных служб

Каждая служба представляет собой модуль с обязательными разделами «Имя службы» и «Журнал».

В первом разделе находятся сведения о состоянии службы, а также кнопка «Включить» или «Выключить», если служба остановлена.

В закладке «Журнал» находится сводка всех системных сообщений. Журнал разделен на страницы, кнопками «вперед» и «назад» можно переходить со страницы на страницу, либо ввести номер страницы в поле и переключиться сразу на нее.

Записи в журнале выделяются цветом в зависимости от вида сообщения. Обычные сообщения системы отмечены белым цветом, сообщения о состоянии системы (включение/выключение) - зеленым, ошибки - красным.

В правом верхнем углу модуля находится строка поиска. С ее помощью можно искать в журнале нужные записи.

Журнал всегда отображает события за текущую дату. Чтобы посмотреть события в другой день, необходимо выбрать нужную дату, используя календарь в левом верхнем углу модуля.

В модуле каждой службы добавлена кнопка очистки журнала

Настройка DNS-сервера

DNS-сервер служит для преобразования ip-адресов в доменные имена узлов. Основной внешний параметр DNS-сервера - список разрешений для трансфера зон. Сюда добавляются адреса других DNS-серверов, которые имеют право получать записи зон от программы.

Основной внешний параметр DNS-сервера - список разрешений для трансфера зон. Сюда добавляются адреса других DNS-серверов, которые имеют право получать записи зон от ИКС.

Если в системе не создано ни одного провайдера, то в данной вкладке можно вписать DNS-сервера, которые будет использовать ИКС.

Также, вы можете определить, устанавливать ли первичным DNS-сервером контроллер домена в том случае, если ИКС является его членом.

Зоны DNS-сервера

Зона — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен, а чаще — одновременно на нескольких серверах. Целью выделения части дерева в отдельную зону является передача ответственности за соответствующий домен другому лицу или организации, так называемое делегирование. Как связная часть дерева, зона внутри тоже представляет собой дерево.

Вкладка «Зоны» позволяет создавать DNS-зоны для работы различных служб ИКС, таких как веб-сервер, почтовый сервер и джаббер-сервер.

Различаются следующие типы DNS-зон:

DNS-зона

Для создания первичной DNS-зоны, нажмите кнопку «Добавить» → «DNS-зона». ИКС запросит ввести параметры приведенные в таблице 6.

Таблица 6 - Параметры DNS зон

Параметр	Значение
Имя зоны	Имя домена, за который отвечает данная зона DNS-сервера
DNS-сервер	Имя сервера, отвечающего за эту зону (соответствующая NS-запись появится в списке записей зоны автоматически)
E-mail администратора	Почтовый адрес администратора, отвечающего за данную зону

TTL (Time To Live)	Допустимое время хранения данной ресурсной записи в кэше неответственного DNS-сервера в секундах
Обновление	Временной интервал в секундах, через который вторичный сервер будет проверять необходимость обновления информации.
Повторение попытки	Временной интервал в секундах, через который вторичный сервер будет повторять обращения при неудаче.
Устаревание	Временной интервал в секундах, через который вторичный сервер будет считать имеющуюся у него информацию устаревшей.
Отрицательное TTL	Значение времени жизни информации на кэширующих серверах ((ttl) в последующих записях ресурсов).

Вкладка «Доступ» позволяет определить внешние адреса, имеющие право доступа к информации данной зоны. По умолчанию разрешено чтение из всех сетей.

Вторичная DNS-зона

Вторичный сервер имен поддерживает локальную копию файла зоны. Для обработки запросов за пределами зоны сервер использует адреса корневых серверов или переадресующий сервер.

Если ИКС выступает в качестве вторичного сервера зоны, необходимо нажать кнопку «Добавить» → «Вторичная DNS-зона».

Сервер запросит параметры приведенные в таблице 7.

Таблица 7 - Параметры вторичной DNS-зоны

Параметр	Значение
Имя зоны	Имя домена, который обслуживает данная зона
Ip-адрес первичного	Ip-адрес сервера, хранящего файл зоны, откуда вторичный сервер

сервера	получает данные

Обратная DNS-зона

Обратная (in-addr.arpa) зона — специальная доменная зона, предназначенная для определения имени хоста по его IPv4-адресу, используя PTR-запись. Адрес хоста AAA.BBB.CCC.DDD транслируется в обратной нотации и превращается в DDD.CCC.BBB.AAA.in-addr.arpa. Благодаря иерархической модели управления именами появляется возможность делегировать управление зоной владельцу диапазона IP-адресов. Для этого в записях авторитативного DNS-сервера указывают, что за зону CCC.BBB.AAA.in-addr.arpa (то есть за сеть AAA.BBB.CCC.DDD/24) отвечает отдельный сервер.

Для создания обратной DNS-зоны необходимо нажать кнопку «Добавить» → «Обратная DNS-зона». Программа предложит ввести необходимые параметры.

Все параметры аналогичны параметрам первичной DNS-зоны. Адрес зоны вводится в формате CCC.BBB.AAA - первые три октета подсети AAA.BBB.CCC.DDD/24 (в обратном порядке), в которой располагается домен.

После создания зоны можно переходить к добавлению записей.

Запись NS (name server) указывает на DNS-сервер для данного домена.

Параметры записи NS приведены в таблице 8.

Таблица 8 - Параметры записи NS

Параметр	Значение
DNS-зона	Определяет домен, за который отвечает данный сервер. Имена доменов пишутся без точки, таким образом к ним прибавляется имя зоны. Чтобы обозначить всю зону целиком, указывается символ «@».
DNS-сервер	Имя DNS-сервера, отвечающего за домен.

Запись A (address record) или запись адреса связывает имя хоста с адресом IP.

Параметры записи A приведены в таблице 9.

Таблица 9 - Параметры записи A

Параметр	Значение
имя хоста	Определяет имя хоста в домене. Имена хостов пишутся без точки, таким образом к ним прибавляется имя зоны. Чтобы обозначить домен целиком, указывается символ »@».
Ip-адрес	Ip-адрес сервера, на котором расположен данный хост.

Запись MX (mail exchange) или почтовый обменник указывает сервер(ы) обмена почтой для данного домена.

Параметры записи приведены в таблице 10.

Таблица 10 - Параметры записи MX

Параметр	Значение
почтовый сервер	Определяет имя почтового сервера в домене. Имена серверов пишутся без точки, таким образом к ним прибавляется имя зоны. Чтобы обозначить домен целиком, указывается символ »@».
приоритет	Используется для равномерного распределения нагрузки в случае нескольких почтовых серверов в домене. Более низкое значение показывает более высокий приоритет.
имя хоста	Указывает имя хоста, на котором расположен почтовый сервер.

Запись CNAME (canonical name record) или каноническая запись имени (псевдоним) используется для перенаправления запроса на другое имя.

Параметры записи приведены в таблице 11.

Таблица 11 - Параметры записи CNAME

Параметр	Значение
псевдоним	Определяет псевдоним хоста.

имя хоста	Указывает официальное имя хоста в домене.

Запись SRV (server selection) указывает на серверы для сервисов, используется, в частности, для Jabber и Active Directory.

Параметры записи приведены в таблице 12.

Таблица 12 - Параметры записи SRV

Параметр	Значение
сервис	Имя сервиса согласно RFC-3232 (IANA Assigned Port Numbers).
протокол	Указывает протокол, по которому предоставляется сервис (TCP, UDP).
имя хоста	Указывает имя хоста, на котором расположен данный сервис.
приоритет	Используется для равномерного распределения нагрузки в случае нескольких серверов одного вида сервиса в домене. Более низкое значение показывает более высокий приоритет.
вес	Число в диапазоне от 0 до 65535. Учитывается в случае наличия нескольких SRV-записей с одинаковым приоритетом. Посредством этого значения осуществляется балансировка: значение определяет, какая доля запросов направляется на хост.
сервер	Доменное имя, услуги по которому предоставляет сервис; точка в конце обязательна, иначе к имени будет автоматически добавлен домен используемой зоны.
порт	Порт работы сервиса.

Запись TXT - Текст, содержит текстовые данные любого вида. Применяется редко и специфичным образом.

Параметры записи приведены в таблице 13.

Таблица 13 - Параметры записи TXT

Параметр	Значение
Имя хоста	Определяет имя хоста, для которого добавляется запись.
Текст	Многострочное поле, позволяющее вводить произвольный текст.

Запись PTR (pointer) или запись указателя связывает IP хоста с его каноническим именем. Запрос в домене in-addr.arpa на IP хоста в reverse форме вернёт имя (FQDN) данного хоста. В целях уменьшения объёма нежелательной корреспонденции (спама) многие серверы-получатели электронной почты могут проверять наличие PTR записи для хоста, с которого происходит отправка. В этом случае PTR запись для IP адреса должна соответствовать имени отправляющего почтового сервера, которым он представляется в процессе SMTPсессии. Данная запись применяется при создании обратной DNS-зоны

Параметры записи приведены в таблице 14.

Таблица 14 - Параметры записи PTR

Параметр	Значение
Ip-адрес	Определяет оставшиеся октеты ip-адреса хоста в зоне in-addr-arpa.
Имя хоста	Имя хоста, расположенного на данном ip-адресе.

Настройка FTP-сервера

FTP—сервер позволяет размещать на сервере файлы и предоставлять им доступ по сети. Поддерживается анонимный вход и авторизация по логину и паролю. Для пользователей можно задавать различные права доступа.

Вкладка «Настройки» позволяет определить следующие параметры:

Порт - определяет порт передачи данных протокола (по умолчанию стандартный порт 21)

Порты для пассивного FTP. Изначально протокол предполагал встречное TCP-соединение от сервера к клиенту для передачи файла или содержимого каталога. Это делало невозможным общение с сервером, если клиент находится за NAT, кроме того, часто запрос

соединения к клиенту блокируется межсетевым экраном. Чтобы этого избежать, было разработано расширение протокола FTP passive mode, когда соединение для передачи данных тоже происходит от клиента к серверу. Для этих целей выделяется диапазон портов, к которым могут подключаться клиенты. Чем большее число одновременных соединений устанавливают клиенты, тем шире должен быть этот диапазон.

Максимальное количество соединений - максимальное количество одновременно подключенных клиентов.

Максимальное количество подключений с одного логина - ограничивает пользователя числом одновременно создаваемый FTP-сессий с его логина (по умолчанию не ограничено).

Максимальное количество подключений с одного хоста - ограничивает пользователя числом подключений с одного ip-адреса (по умолчанию не ограничено).

Сертификат для FTPS. Сервер может работать как по стандартному протоколу, в котором при передаче файлов данные не шифруются (что небезопасно), так и по протоколу FTPS (File Transfer Protocol + SSL, или FTP/SSL) — защищённому протоколу для передачи файлов. Для этих целей используются SSL-сертификаты. Нажав на кнопку […], вы можете назначить службе заранее созданный в соответствующем модуле сертификат.

Чтобы добавить новый ресурс необходимо перейти на вкладку «FTP-ресурсы» и нажать на кнопку «Добавить» - «FTP-ресурс».

После ввода имени и описание ресурса необходимо добавить директорию из структуры хранилища файлов. Для этого нужно нажать кнопку […] в графе «источник» и указать папку, в которой будет располагаться содержимое FTP-ресурса. При необходимости можно создать новую папку в каталоге.

В окне «Права доступа» администратору необходимо выбрать пользователей или группы и отметить для них права доступа к ресурсу. Разрешить гостевой доступ - отметив этот пункт администратор предоставляет возможность просмотра файлов FTP ресурса любому подключившемуся к серверу.

Чтобы более точно определить права пользователей, необходимо нажать на кнопку […] в строке соответствующего пользователя или группы. В появившемся окне нужно отметить флажками необходимые права доступа.

Настройка Jabber-сервера

Jabber-сервер позволяет пользователям программы общаться между собой по протоколу XMPP.

Вкладка «Настройки» позволяет определить следующие параметры:

Настройки ICQ-транспорта

Полезной особенностью XMPP систем являются транспорты, или шлюзы, позволяющие пользователям получать доступ к сетям, использующим другие протоколы, такие, как OSCAR (ICQ).

Для настройки ICQ-транспорта нужно указать сервер соединения и порт передачи даных.

Настройки Jabber-конференций

Конференция - место общения нескольких пользователей jabber. Имеет неповторяющееся в пределах одного сервера имя.

Параметр «Аккаунт администратора» определяет пользователя, который всегда будет администратором в любой создаваемой комнате.

Сертификат SSL - необходим для создания защищенного соединения «клиент-сервер». По умолчанию данные по протоколу передаются в открытом виде. Чтобы избежать этого, необходимо нажать кнопку […] в поле и выбрать заранее сгенерированный SSL-сертификат.

Прежде чем добавлять пользовательские аккаунты, необходимо создать jabber-домен. Для этого во вкладке «Домены и аккаунты» нужно нажать кнопку «Добавить» → «Jabber-домен».

После этого, выделив созданный домен, можно добавлять в него пользовательские аккаунты. Программа попросит ввести имя аккаунта, пароль и выбрать пользователя, за которым данный аккаунт будет закреплен в общем ростере.

При создании jabber-доменов и аккаунтов соответствующие домены и аккаунты появляются в модуле «Почта». Верно и обратное.

Во вкладке «Ростер» администратор может видеть список контактов всех созданных на ИКС jabber-доменов так, как они будут отображаться в контакт-листе пользователя, подключившегося к ИКС по своему jabber-аккаунту.

Настройка сетевого окружения

«Сетевое окружение» - модуль для подключения ИКС к ресурсам локальной сети предприятия, а также к Active Directory.

Вкладка «Идентификация» определяет роль ИКС в локальной сети предприятия. После назначения сетевого NetBIOS-имени для сервера, вы можете выбрать одну из следующих ролей, приведенных в таблице 15.

Таблица 15 - Примеры ролей во вкладке «Идентификация»

Роль	Значение
Рабочая группа	В сети предприятия не используется контроллер домена (AD), компьютеры находятся в одной рабочей группе, WINS-сервер отсутствует. По умолчанию ИКС находится в рабочей группе WORKGROUP, при необходимости вы можете ее переименовать
Домен	В сети предприятия используется контроллер домена (AD). ИКС может быть присоединен к домену.
Контроллер домена	ИКС сам выступает в роли контроллера домена.

Флажок «Использовать WINS-сервер» включит сервер WINS на сервере. Чтобы корректно использовать эту опцию, на всех рабочих мащинах также должен быть указан ИКС в качестве WINS-сервера.

Флажок «Мастер-браузер» назначит сервер мастер-браузером сети. При запуске компьютеров в сети начинают происходить выборы главного компьютера, который будет отвечать за списки компьютеров в сетевом окружении и которого и называют главным обозревателем или мастер-браузером (master browse server).

После нажатия кнопки «Сохранить» программа применит выбранную вами роль в сетевом окружении. Если вы выбрали роль «Домен», то сервер запросит параметры присоединения к домену.

Сначала ИКС попробует обнаружить адрес контроллера домена самостоятельно. Если ему это по какой-то причине не удастся, введите адрес вручную, затем введите логин и пароль предварительно заведенного на контроллере домена пользователя.

Чтобы программа могла импортировать пользователей из домена и синхронизировать их через LDAP, доменный пользователь, заведенный для ИКС, должен обладать привилегиями администратора домена.

Для того, чтобы сервер мог присоединиться к домену и обмениваться данными с контроллером, необходимо, чтобы сервер-контроллер домена был занесен в список пользователей ИКС, и его авторизация проходила по ip-адресу.

Если подключение к домену прошло успешно, справа от поля с именем домена появится зеленый кружок.

Добавить новый ресурс в сетевое окружение администратор может, перейдя на вкладку «Общие ресурсы» и нажав на кнопку «Добавить» - «Общий ресурс». Создание ресурса и назначение прав пользователей аналогично созданию FTP-ресурса.

Настройка антивируса

В программе присутствуют три модуля, отвечающие за файловую безопасность системы – «Антивирус», «Антивирус Dr. Web» и «Антивирус Касперского». «Антивирус» представляет собой комбинацию свободно распространяемых программных модулей ClamAV и Havp. «Антивирус Dr. Web» представляет проприоритарное программное обеспечение Dr. Web, право на использование которого приобретается отдельно в виде лицензионного ключа, который необходимо загрузить кнопкой «Загрузить ключ лицензии» во вкладке «Информация». Других настроек данных модулей не требуется. «Антивирус Kaspersky» представляет проприоритарное программное обеспечение Лаборатории Касперского, право на использование которого приобретается отдельно в виде лицензионного ключа, который необходимо загрузить кнопкой «Загрузить ключ лицензии» во вкладке «Информация». Других настроек данных модулей не требуется.

Настройка антиспама

В программе присутствуют модуль антиспама, отвечающие за безопасность почты. «Антиспам Kaspersky» представляет проприоритарное программное обеспечение Лаборатории Касперского, право на использование которого приобретается отдельно в виде лицензионного ключа, который необходимо загрузить кнопкой «Загрузить ключ лицензии» во вкладке «Информация». По умолчанию в настройках модуля включены следующие функции, которые можно отключить:

1) Фильтры

- распознование изображений

- UDS

- DNS-запросы

- пользовательские списки DNS (по умолчанию исползуются базы Касперского)

- SURBL (по умолчанию исползуются базы Касперского)

- SPF

2) Проверка

- обычного текста

- HTML

- PDF

- MS Office

- RTF

Также можно настроить чёрные/белые списки ip-адресов, email-адресов, ключевых фраз.

Настройка веб-сервера

Веб-сервер используется для развертывания в программе HTTP-ресурсов, доступных ограниченно из внутренней сети предприятия или из внешней сети полностью.

Во вкладке «Настройки» модуля «Веб» настраиваются следующие параметры:

Имя хоста - определяет внешнее доменное имя хоста. Необходимо для корректной работы веб-ресурса по доменному имени.

E-mail администратора - позволяет указать e-mail ответственного за веб-сервера системного администратора на тот случай, если в работе сервера возникнут перебои.

Порт HTTP - позволяет переназначить порт, по которому веб-сервер принимает HTTP-запросы (по умолчанию 80).

При обращении к корневой папке, открывать веб-интерфейс ИКС - по умолчанию директория веб-сервера -находится в корневой папке primary. При обращении на ИКС без указания пути или имени домена, пользователь обращается к корневой папке. Если в ней нет

индексных файлов (index.html, index.php), то ИКС перенаправляет запрос с 80 порта на 81 и открывает веб-интерфейс.

Тип авторизации. Если веб-ресурс или виртуальный хост не предназначены для гостевого входа, то данная опция позволяет определить, каким образом пользователи будут авторизоваться на ресурсе при входе.

Порт HTTPS - позволяет переназначить порт, по которому веб-сервер принимает HTTPS-запросы (по умолчанию 443).

Сертификат для HTTPS. Сервер может работать как по стандартному протоколу, в котором при передаче файлов данные не шифруются (что небезопасно), так и по защищённому протоколу HTTPS с использованием SSL . Для этих целей используются SSL-сертификаты. Нажав на кнопку […], вы можете назначить службе заранее созданный в соответствующем модуле сертификат.

Перенаправлять с HTTP на HTTPS - укажите этот флажок, если вы хотите, чтобы веб-сервер всегда работал по защищенному соединению.

Для того, чтобы создать веб-ресурс, который позволит разместить на сервере интернет-сайт, необходимо перейти во вкладку «Веб-ресурсы» и нажать кнопку «Добавить».

Доступные типы веб-ресурсов указаны в таблице 16.

Таблица 16 - Типы веб-ресурсов

Название	Значение
Веб-ресурс	Отвечает на http-запросы по ip-адресам интерфейсов ИКС, создается в единственном экземпляре.
Виртуальный хост	Позволяет создать неограниченное количество веб-ресурсов, отвечающих каждый за свой веб-сайт по имени сайта.
Виртуальный хост с перенаправлением	Позволяет ИКС перенаправлять запросы на указанное имя сайта в случае, когда сам сервер с сайтом находится к примеру в локальной сети предприятия (аналог перенаправления портов)

При создании веб-ресурса администратор может указать его название и описание и настроить следующие параметры:

Источник - указание папки, в которой лежат файлы данного ресурса. После ввода имени и описания для ресурса необходимо добавить директорию из структуры хранилища файлов. Для этого также, как и в других модулях, нужно нажать кнопку […] и указать папку, в которой будет располагаться содержимое сайта. При необходимости, можно создать новую папку в каталоге.

Разрешить листинг директории - позволяет серверу отобразить список всех файлов и папок ресурса, в случае если в корневой папке не обнаружены индексные файлы index.html или index.php.

Разрешить выполнение PHP скриптов - разрешает серверу выполнять на html-страницах php-скрипты.

Кодировка по умолчанию - определяет значение кодировки отображаемых html-страниц ресурса по умолчанию.

Права доступа - определяет список пользователей, имеющих доступ к просмотру сайта. Установка флажка «Гостевой вход» позволяет просмотр сайта любым хостом.

Основной ресурс при создании сайта - виртуальный хост. Параметр «Виртуальный хост» аналогичен имени веб-ресурса, но должен содержать доменное имя сайта, на которое он будет отвечать по http-запросу. Для корректной работы виртуального хоста в большинстве случаев требуется настройка dns-зон доменного имени. К настройкам, присутствующим в веб-ресурсе, добавляются следующие:

Создать ссылку для www.%domainname% - позволяет принимать http-запросы как на имя сайта, указанное в названии, так и на него же с добавлением домена WWW.

Сертификат для HTTPS - нажав на кнопку […], администратор может назначить данному сайту заранее созданный в соответствующем модуле сертификат.

Перенаправлять с HTTP на HTTPS - указание этого флажка назначает данному сайту всегда работать по защищенному соединению.

Также, как и веб-ресурс, виртуальный хост позволяет настроить уровень доступа пользователей.

Последний вариант использования модуля – виртуальный хост с перенаправлением. Поскольку все параметры самого веб-ресурса в данном случае отвечает сервер, на котором этот ресурс расположен, доступны для редактирования только следующие опции:

Адрес перенаправления - ip-адрес хоста, на котором работает веб-сервер с

указанным ресурсом.

HTTP - включение этого флажка позволяет изменить порт передачи http-запросов со стандартного 80 на указанный пользователем.

HTTPS - включение этого флажка позволяет изменить порт передачи https-запросов со стандартного 443 на указанный пользователем.

Каждый раз, когда создается веб-ресурс или виртуальный хост, в сервере баз данных MariaDB 10 за ним закрепляется база данных, с которой может взаимодействовать сайт, расположенный на ресурсе, посредством php-запросов.

Для того, чтобы вызвать параметры базы данных ресурса, необходимо выделить его в общем списке и нажать кнопку «База данных».

В появившемся окне отобразятся параметры подключения к базе данных: имя базы, логин и пароль для подключения. Эти параметры необходимо использовать для php-скриптов ресурса.

Если у администратора уже есть дамп рабочей базы данных, он может загрузить его, используя кнопку «Загрузить базу». В появившемся окне будет предложено выбрать имя файла дампа для загрузки, кодировку дампа, а также флажок, определяющий сохранность предыдущих данных в базе после загрузки.

Приложения

Для того, чтобы быстро разместить сайт на ИКС, в систему интегрированы несколько популярных пакетов, которые можно установить на виртуальный хост.

Для того, чтобы добавить приложение, нужно нажать на имя виртуального хоста для перехода в его настройки, либо на кнопку «Приложения», чтобы перейти непосредственно в список приложений ресурса.

Чтобы добавить приложение, нужно нажать кнопку «Добавить» и выбрать из выпадающего списка нужное веб-приложение.

ИКС поддерживает установку следующих приложений:

Gallery DokuWiki Drupal Harmony Joomla LiveStreet Made Simple Faanui MaxSite MediaWiki MyBB Phorum phpBB phpMyAdmin SMF OwnCloud

После выбора нужного приложения, можно задать папку для его установки, пароль и e-mail администратора.

Начнется установка приложения. Ее можно отменить кнопкой «Отмена». Когда индикатор готовности достигнет 100%, приложение будет установлено.

Настройка службы Fail2Ban

Системный администратор можете использовать данный модуль для блокировки IP-адреса, с которых предпринимается слишком много попыток авторизации в почте.

Модуль может быть использован для IP-телефонии.

Настройка модуля «Журнал ICQ»

Системный администратор можете использовать модуль отслеживания icq-сообщений для некоторых методов контроля сотрудников организации, таких как, к примеру, утечка конфиденциальной информации. Однако использование данного модуля является вмешательством в частную жизнь сотрудников. Перед его включением рекомендуется ознакомить работников предприятия с положением правил предприятия или трудового договора о том, что их icq-переговоры документируются.

Вкладка «Настройки» позволяет изменить единственный параметр «Порт» - определяет порт перехвата данных протокола OSCAR (по умолчанию стандартный порт 5190).

Во вкладке «Журнал сообщений» отображаются все перехваченные сообщения с разделением по пользователям, от которых и которым эти сообщения пришли.

Журнал ICQ работает не со всеми сторонними клиентами службы ICQ и не перехватывает зашифрованные сообщения.

Настройка почтового сервера

Почтовый сервер программы предназначен для получения и отправки сообщений по e-mail, а также обладает множеством других функций

Вкладка «Настройки» позволяет определить следующие параметры почтового сервера:

Порт SMTP/POP3/IMAP - позволяет изменить стандартные порты приема и отправки почтовых сообщений.

Интерфейсы для SMTP/POP3/IMAP - позволяет выбрать интерфейсы сервера, по

которым осуществляется прием и отправка почтовых сообщений. По умолчанию задействованы все интерфейсы.

Следующие два поля позволяют установить максимальный размер письма (в мегабайтах) и максимальное количество писем с одного Ip-адреса в минуту.

Релей по умолчанию. Релей — узел, занимающийся получением/пересылкой сообщений (электронной почты), в данном случае в его роли по умолчанию выступает ИКС. В некоторых случаях может потребоваться прописать другой сервер, через который программа будет отправлять почту (например, в случае мультидропного почтового ящика, настроенного на почтовом сервере провайдера).

Адреса, с которых разрешена пересылка - это список адресов и доменных имен, с которых программа будет всегда принимать почту без проверки серыми списками и проверки соответствия прямой и обратной записей.

Адреса, с которых запрещена пересылка - это список адресов и доменных имен, почтовые сообщения с которых программа всегда будет отклонять.

Черные списки RBL. RBL, Real-time Blackhole List (или DNSBL — DNS blacklist или DNS blocklist) — списки хостов, хранимые с использованием системы архитектуры DNS. Обычно используются для борьбы со спамом. Почтовый сервер обращается к DNSBL, и проверяет в нём наличие IP-адреса клиента, с которого он принимает сообщение. При положительном ответе считается, что происходит попытка приёма спам-сообщения. Серверу отправителя сообщается ошибка 5xx (неустранимая ошибка) и сообщение не принимается. В большинстве случаев изменять этот список не требуется.

Домен по умолчанию для авторизации определяет почтовый домен, который будет автоматически подставляться при авторизации пользователя. При указании домена по умолчанию пользователи этого домена смогут авторизоваться по имени почтового ящика без указания домена.

При создании ящика автоматически создавать папки - содержит список стандартных папок, создаваемых в почтовом ящике. При необходимости можно изменить их состав.

Проверять почту антивирусом Clamav/Dr.Web - установка этих флажков дает сигнал почтовому серверу проверять входящие и исходящие письма на наличие в них вирусов. При положительном результате вместо самого письма получателю придет сообщение о результатах проверки.

Использовать серые списки. Серые списки (Greylisting) — способ автоматической блокировки спама, основанный на том, что «поведение» программного обеспечения, предназначенного для рассылки спама, отличается от поведения обычных серверов электронной почты. Если почтовый сервер получателя отказывается принять письмо и сообщает о «временной ошибке», сервер отправителя обязан позже повторить попытку. Администратор может включить данный режим для усиленной проверки почты на спам. После включения данной опции станут доступными для редактирования параметры серых списков - время игнорирования повторной отправки (в секундах), время ожидания повторной отправки (в часах), время хранения отправителя в белом списке (в днях).

Имя сервера для SMTP определяет параметр SMTP Banner Postfix.

Разрешить SSL разрешает SSL/TLS-авторизацию пользователей. После включения данной опции становятся доступны параметры, определяющие порты работы служб SMTP SSL,POP3 SSL и IMAP SSL.

Сертификат для SMTP/POP3/IMAP - как и другие службы программы почтовый сервер может работать как по стандартному протоколу, в котором при передаче файлов данные не шифруются (что небезопасно), так и по защищённому. Для этих целей используются SSL-сертификаты. Нажав на кнопку […], администратор может назначить для каждого протокола заранее созданный в соответствующем модуле сертификат.

Использовать DLP - запускает службу проверки почтовых сообщений по отпечаткам конфиденциальной информации.

Жесткий диск для хранения почты позволяет переместить хранилище почты на отдельный жесткий диск. По умолчанию почта хранится на системном разделе.

Подпись для веб-интерфейса включается в настройках почтового сервера, для этого необходимо установить флажок «использовать подпись» и ввести подпись в окне, которое открывается по кнопке «редактировать html», после чего сохранить настройки.

Подпись можно вводить как в режиме wysiwyg так и в режиме html.

В подписи можно использовать переменные в виде [имя переменной], их возможные значения указаны ниже:

cn - Имя пользователя

ou - Группа в которой он находится

mail - Почтовый адрес

description - Поле "описание" пользователя

notes - Поле "комментарий" пользователя

telephonenumber - Поле "телефон" пользователя

title - Поле "должность" пользователя

url - Поле "Веб-сайт" пользователя

postaladdress - Поле "Адрес" пользователя

pager - Поле "ICQ" пользователя

ounotes - Поле "описание" группы в которой он находится

Для вставки изображений используется кодирование изображения в data:url. Это делается следующим образом: используя сервис http://dataurl.net/#dataurlmaker (или подобный) изображение конвертируется в формат <img src=«data:image/png;…» …>, затем полученный текст вставляется в html-код подписи.

Загрузить логотип для Roundcube - эта кнопка позволяет выбрать изображение, которое будет находиться в левом верхнем углу почтового веб-интерфейса. Например, логотип организации.

Прежде чем добавлять пользовательские почтовые ящики, необходимо создать почтовый домен. Для этого во вкладке «Домены и ящики» нужно нажать кнопку «Добавить» → «почтовый домен». После этого, выделив созданный домен, можно добавлять в него пользовательские почтовые ящики. Сервер попросит ввести имя ящика, пароль и выбрать пользователя, за которым данный ящик будет закреплен. При необходимости можно указать квоту - максимально зарезервированное место на жестком диске ИКС для хранения писем данного пользователя. После превышения этой квоты письма для пользователя приниматься не будут. По умолчанию квота отсутствует.

Не обязательно создавать отдельный почтовый ящик для каждого необходимого вам почтового имени. Вместо этого можно создать ссылку на указанный ящик. Тогда все письма, приходящие на имя ссылки, будут перенаправляться на реально существующий ящик.

Администратор может настроить управление перепиской пользователей ИКС,

используя различные рассылки и перенаправления писем во вкладке «Фильтры».

Для того чтобы создать новый фильтр, сперва необходимо выбрать условия срабатывания - при совпадении всех условий, любого из условий или применить ко всем сообщениям независимо от условий.

Фильтровать входящие и исходящие письма можно по теме письма, отправителю, получателю и размеру (в килобайтах). Проверка на совпадение условия может быть строгая («совпадает с») или не строгая («содержит», «начинается с», «заканчивается на»), а также обратная («не содержит»). Можно назначить любое количество условий для одного фильтра.

Последний шаг - выбор действия, происходящего после срабатывания фильтра. Можно переместить письмо, скопировать его на другой адрес либо удалить. Первые два условия позволяют вписать имя почтового ящика либо выбрать его из списка созданных на ИКС.

В фильтры также была добавлена поддержка папок внутри почтового ящика, а также система распознавания регулярных выражений.

%s = sender

%r = recipient

%Y(M) = date

%u = recipient user

%d = recipient domain

%Su = sender user

%Sd = sender domain

Рассылки - это те же фильтры, но с упрощенным интерфейсом, в котором достаточно указать те ящики, на которые будет распространена рассылка. Ящик, на который приходит письмо-оригинал в системе не должен быть заведен, поскольку он представляет собой ссылку.

Во вкладке «Антиспам» системный администратор может включить или выключить работу антиспам-фильтра, установив соответствующий флажок, а также настроить уровень строгости проверки. В антиспаме применяется балловая система оценки строгости. 0 - минимальный уровень проверки, 100 - максимальный.

Для управления почтовыми аккаунтами, расположенными на других серверах,

можете применяется функция «сборщик почты». С его помощью программа подключается к указанному почтовому серверу под выбранным логином и паролем и перемещает либо копирует содержащуюся почту на почтовые ящики пользователей.

Администратор может указать, что делать с письмами на сервере - собирать все, собирать только новые, оставлять письма на сервере или удалять их. Также настраивается интервал работы сборщика и число загружаемых писем за сессию.

Во вкладке «Почтовая очередь» показаны письма, ожидающие отправки, или которые по каким-то причинам не были отправлены (к примеру, отклонены серым списком вышестоящего почтового сервера). При выборе любого объекта из списка можно увидеть код ошибки, по которой он не был доставлен. Управлять почтовой очередью можно посредством кнопок «Очистить очередь» и «Отправить все». Также, каждое письмо можно попытаться отправить индивидуально или удалить его из очереди.

Для контроля входящего и исходящего почтового трафика, а также спама и нежелательных писем присутствует раздел «Статистика».

Также как и в пользовательской статистике, администратор может применять различные фильтры на панели управления к общим сведениям о почтовом трафике сервера и выводить их в виде таблицы. Столбцы таблицы варьируются в зависимости от применяемого фильтра.

Настройка сертификатов

В разделе «Сертификаты» хранится список всех SSL-сертификатов, применяющихся в службах программы.

Список представлен в виде дерева, а поле модуля поделено на столбцы, в которых показана основная информация о сертификатах: тип ключа родительского сертификата, дата начала действия и окончания, а также имя хоста (или ip-адрес), который представляет данный сертификат. Администратор также может экспортировать созданные сертификаты или импортировать сторонние при помощи кнопок «Экспорт» и «Импорт», а также просматривать информацию о выбранном сертификате при помощи кнопки «Просмотр сертификата».

Чтобы создать новый SSL-сертификат, необходимо нажать кнопку «Добавить» → «Сертификат».

Сначала заполняются данные сертификата - наименование, код страны,

местоположение, сведения об организации, имя хоста или ip-адрес. Затем во вкладке «Настройки» определяется роль сертификата - CA (корневой) или конечный, устанавливается метод шифрования, время действия и длина ключа в битах.

Первоначально всегда должен создаваться корневой сертификат, затем - дочерние конечные сертификаты! К службам ИКС, применяются только конечные сертификаты.

После этого во вкладке «Использование ключа» и необходимо выбрать в списке необходимый шаблон использования. Выбор шаблона автоматически установит флажки параметров сертификата применительно к выбранной роли. Опытный системный администратор может установить флажки вручную. Вкладка «Netscape» позволяет установить дополнительные netscape-расширения для сертификата.

После нажатия кнопки «Добавить» ИКС предложит зашифровать ключ паролем.

Настройка хранилища файлов

Хранилище файлов представляет собой список всех пользовательских ресурсов, расположенных на ИКС. Модуль состоит из двух частей: в левой части общее дерево папок, в правой - список файлов и папок выделенной папки в дереве. Также в левой части содержится информация об объеме папки или файла, типе, а также дате последнего изменения.

Посредством кнопок на верхней панели вы можете создавать, удалять и переименовывать все папки за исключением primary - эта папка является корневой и не подлежит редактированию. Для того, чтобы последовательно не разворачивать дерево, а сразу переместиться в нужное место, можно вручную ввести путь до нужного ресурса в адресной строке.

Поскольку хранилище файлов является универсальным центром контроля пользовательских ресурсов, администратор может создавать различные ресурсы непосредственно из модуля. Для этого нужно выделить нужную папку в правой части модуля, нажать на появившуюся кнопку «Открыть доступ» и выбрать тип создаваемого ресурса: Общий доступ, Веб-доступ или FTP-доступ.

В некоторых случаях веб-серверу требуются дополнительные права для работы с файлами. Для таких ситуаций используются расширенные настройки ресурса. Для того, чтобы разрешить веб-серверу запись в папку, необходимо выделить ресурс в правой части модуля и нажать на кнопку «Права». Появится окно, в котором необходимо установить

флажок «Разрешить веб-серверу-запись», после чего нажать ОК.

Модуль «Все службы»

В модуле «все службы» отображается список всех запущенных служб программы.

Здесь можно выбрать, какие службы будут использоваться, а какие можно отключить. Статус службы сохраняется между перезагрузками, отключенная служба не будет запущена при следующем включении питания сервера.

Настройка DHCP

Использование DHCP настраивается индивидуально для каждой локальной сети и выполняется в модуле "Провайдеры и сети".

Для того, чтобы разрешить работу DHCP в какой-то локальной сети, необходимо отредактировать её, включить опцию «разрешить DHCP в этой сети» и задать диапазон адресов, которые будут раздаваться DHCP-сервером (в виде 192.168.1.1-192.168.1.100 или 192.168.1.1\16).

Если DHCP не включен ни для одной локальной сети, то сервис будет находится в состоянии «не настроен».

На вкладке «Настройки» администратор может указать адреса сервера времени, DNS- и WINS-сервера, которые будут установлены на компьютере клиента. Кроме того, здесь можно указать путь до TFTP-сервера, необходимого для некоторых конфигураций (к примеру, для настройки тонких клиентов), а также срок, на который за клиентом резервируется IP-адрес (срок аренды).

На вкладке «Адреса» можно увидеть всех пользователей, которые в данный момент получили адреса по DHCP.

Для того, чтобы одному и тому же компьютеру каждый раз выдавался один и тот же IP-адрес, необходимо задать соответствие между MAC-адресом сетевой карты и IP-адресом. Чтобы закрепить за пользователем текущий IP адрес можно воспользоваться кнопкой «Связать IP с MAC». Связи из модуля «ARP-таблица» также будут использоваться DHCP-сервером для выдачи адресов.

Для того чтобы задать пользователю другой IP необходимо скопировать MAC и нажать кнопку «Добавить» - «DHCP адрес». Затем вставить MAC и ввести новый IP - изменение произойдет по истечению срока аренды, или при повторном подключении пользователя.

Для IP-адресов, присвоенных пользователям, будут отображаться имена владельцев. Клик по имени пользователя переместит в его персональный модуль.

DHCP-сервер использует общий список сопоставлений IP- и MAC-адресов с модулем «ARP-таблица»

Настройка VPN-сервера

Для контроля пользователей, подключающихся по технологии VPN на ИКС выделен модуль «VPN».

Во вкладке «Настройки» администратор может выбрать тип авторизации пользователей на сервере - по логину/паролю ИКС или через домен (при условии, что ИКС интегрирован в домен и пользователи импортированы из AD).

Вкладка «Пользователи» отображает список пользователей ИКС и позволяет определить, кому из них разрешено VPN-подключение. По умолчанию разрешающие флажки установлены для всех пользователей, которым присвоены адреса из VPN-сети. При необходимости администратор может запретить пользователю подключение, сняв флажок.

Во вкладке «Текущие сеансы» системный администратор может просмотреть кто из пользователей в настоящее время подключен, увидеть время подключения, а также при необходимости отключить пользователя.

Настройка прокси-сервера

Прокси-сервер программы настраивается по умолчанию при настройке сетевого подключения и заведении пользователей. Однако, при необходимости, его настройки могут быть изменены.

Прокси-сервер выполняет кеширование веб-страниц и объектов, которые пользователи скачивают из интернета. Таким образом экономится интернет-трафик и увеличивается скорость доступа к веб-страницам.

Эффективность работы кеша зависит от его размера. Для организации с большим количеством пользователей, рекомендуется установить размер кеша в соответсвующем поле в несколько гигабайт. Также, вы можете ограничить размер загружаемого файла в поле «Ограничивать размер ответа» (В мегабайтах).

Содержимое кеша прокси-сервера можно посмотреть на вкладке «Содержимое кеша».

Для того, чтобы включить антивирусное сканирование веб-трафика каким-либо антивирусным модулем, необходимо включить соответствующую опцию в настройках прокси. Параметр «Максимальный объем для сканирования» определяет максимальный размер файла, единовременно проходящего обработку антивирусом. Файлы, размер которых превышает указанный, сканироваться не будут, что может повысить производительность.

Список разрешённых портов для SSL определяет, к каким портам разрешён доступ с использованием метода CONNECT.

ICAP (Internet Content Adaptation Protocol) - протокол расширения для прокси-сервера. В большинстве случаев он используется для сканирования на вирусы проходящего трафика и применения к нему различных контент-фильтров. Системный администратор может подключить к прокси-серверу ИКС сторонний ICAP-сервер, отметив соответствующий флажок в настройках и указав его адрес.

Если в организации несколько проксирующих серверов, расположенных иерархично, то вышестоящий для сервера прокси-сервер будет являться его родительским прокси. Кроме того, в качестве родительского прокси может выступать любой узел сети.

Чтобы ИКС перенаправлял запросы, приходящие на его прокси-сервер, на родительский прокси, необходимо указать его ip-адрес и порт назначения во вкладке «Родительский прокси».

Прокси-сервера могут обмениваться данными своих кэшей по протоколу ICP. В случае работы сети через несколько прокси это может значительно ускорить работу. Если родительский прокси поддерживает работу протокола, нужно отметить соответствующий флажок и указать порт работы службы (по умолчанию 3130).

Если родительский прокси работает с авторизацией, то в нижеследующих полях необходимо указать логин и пароль для подключения.

Автоконфигурация прокси

Для того, чтобы не прописывать вручную прокси-сервер на каждой клиентской машине, вы можете воспользоваться автоконфигуратором. В браузере клиента должна быть выставлена опция «Автоматическая конфигурация прокси», все остальные настройки определит ИКС.

Он включается установкой флажка в соответствующей вкладке. Вы можете отметить один или несколько протоколов из доступных (HTTP, HTTPS, FTP).

Опция публикации скрипта автонастройки определяет, будет ли он доступен по ip-адресу сервера либо по созданному виртуальному хосту с доменным именем. При выборе виртуального хоста, он автоматически создастся в системе. Флажок «Создать запись на ДНС-сервере» автоматически добавит зону с нужными записями для этого виртуального хоста.

Публиковать скрипт автоконфигурации по DHCP - данный параметр передает настройки прокси всем DHCP-клиентам сервера.

Настройка HTTPS-фильтрации

Для того, чтобы получить возможность фильтровать HTTPS-трафик пользователей, необходимо сделать следующее:

1. Добавить корневой сертификат (CA) со стандартными настройками в модуле Сертификаты. Сертификат должен быть нешифрованным

2. Выбрать данный сертификат в поле «Сертификат для ssl-фильтрации» модуля Прокси. После этого правила фильтрации начнут работать, однако в связи с подменой сертификата при запросе браузер пользователя будет сообщать о некорректном сертификате. Чтобы исключить данную ошибку, необходимо сделать следующее:

3. В модуле Сертификаты экспортировать данный сертификат на машину конечного пользователя.

4. В настройках браузера пользователя добавить сертификат в доверенные корневые центры сертификации

Для прокси сервера имеется возможность аноннимизации для внешних ресурсов. Позволяет скрыть ip-адрес пользователя, находящегося за прокси-сервером, а также скрыть признаки наличия прокси-сервера.

Настройка DLP и контент-фильтра.

При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Настройки

Модуль DLP проверяет отпечатки в почтовых сообщениях ИКС и в HTTP-трафике. Чтобы начать активную проверку, отметьте флажками одну или обе из возможностей работы.

Дальнейшие параметры позволяют определить, по каким критериям определять конфиденциальность информации, а также порог срабатывания. При необходимости, вы можете определить максимальный размер обрабатываемого файла, что позволит снизить нагрузку модуля на систему. Также, настройки позволяют задействовать контент-фильтр для работы с пользователями и определить данные, используемые для проверки. Отключение одного из видов данных (шаблоны и ключевые слова) позволяет снизить нагрузку на систему.

База DLP

В следующей вкладке можно создать список отпечатков по файлам и ключевым словам, согласно которому будет происходить проверка. В список ключевых слов также входят шаблоны, которые состоят из регулярных выражений аналогично правилам прокси.

База контент-фильтра

Контент-фильтр позволяет настроить правила пользователей на блокировку интернет-страниц, если в их HTML-коде содержатся заданные ключевые слова или регулярные выражения.

После добавления объектов DLP и контент-фильтрации, их можно назначить нужным пользователям или группам через правила и ограничения.

Настройка телефонии.

За обработку VoIP-данных в ИКС отвечает модуль «Телефония», разработанный на базе сервера ip-телефонии Asterisk. Это свободное решение компьютерной телефонии с открытым исходным кодом, оно достаточно надежное и давно зарекомендовавшее себя с положительной стороны. В настоящее время модуль поддерживает передачу данных по протоколам SIP и IAX.

При входе в модуль отображается его состояние, кнопка «Выключить» (или «Включить» если модуль выключен) и последние сообщения в журнале.

Телефонные номера

Следующая вкладка отображает список телефонных номеров, зарегистрированных на АТС. В ней можно создать следующие объекты:

Телефонный номер. Имеет следующие параметры: собственно номер, краткое описание, пароль, задаваемый при необходимости и пользователь, к которому данный номер

привязан в общей книге. Флажок «Разрешать подключаться извне» позволяет определить, будет ли доступен номер для подключения из внешних сетей.

Факс позволяет принимать факсы на указанный номер и сохранять их в формате TIFF в папке Хранилища файлов.

Группа номеров - предназначена для объединения телефонных номеров. Не несет функциональной нагрузки, предназначена для удобства навигации по списку.

Настройки

Следующая вкладка позволяет задать некоторые настройки модуля.

Флажок Записывать звонки сохраняет звонки в виде файлов в формате MP3. Прослушать звонки можно из вкладки «Журнал звонков».

Порт SIP, порт IAX определяют порт сигнализации соответствующего протокола.

Порты для входящих задают диапазон портов, по которым идет обмен данными установленного соединения.

Время ожидания ответа определяет таймаут, по которому сервер отключает звонящего или переключает его согласно настроенным правилам и перенаправлениям.

Следующие параметры позволяют использовать голосовую почту и определить ее настройки.

Номер для голосовой почты указывает номер обращения пользователя для прослушивания своей голосовой почты.

Номер для безусловной переадресации определяет добавочный набор для переадресации звонка на нужный номер. Переадресация начнется сразу же.

Номер для переадресации определяет добавочный набор для переадресации звонка на нужный номер, предварительно организовав связь с указанным номером. Переадресация начнется после того, как абонент, набравший переадесацию закончит разговор с номером, на который организована переадресация, и отключится.

Последние два параметра определяют настройки определителя номера, в случае, если установлен соответствующий флажок. Это порт определителя и сети, для которых он работает.

Внешние каналы

Система позволяет обмениваться звонками между сотрудниками организации внутри сети без каких-либо дополнительных настроек. Для того, чтобы настроить входящие и исходящие звонки во внешнюю сеть, необходимо добавить хотя бы один внешний канал связи.

В текущей версии поддерживаются два вида каналов - SIP и IAX. Чтобы настроить новый канал, нужно нажать кнопку «Добавить».

Провайдер SIP позволяет настроить сервер подключения, телефонный номер, при необходимости указать логин и пароль. Флажок Автоматически создавать правило, используя префикс служит для указания префикса внешнего звонка по умолчанию. Данный префикс представляет собой цифру, по которой модуль ориентируется, направлять ли звонок во внешнюю сеть. Например, звонок на номер 555-3333 при указанном префиксе 9 будет набираться клиентом как 9-555-3333. Последняя опция режим DTMF позволяет выбрать один из режимов тонального набора.

IAX2 Аналогично провайдеру SIP, провайдер IAX в качестве параметров запрашивает сервер подключения, телефонный номер, при необходимости логин и пароль и внешний префикс. Опция, отличная от настроек провайдера SIP - режим работы. Если вы используете канал связи для подключения к внешнему серверу провайдера, то необходимо использовать опцию «клиент». В случае, когда к ИКС подключаются другие клиенты по внешнему каналу, используйте опцию «сервер».

Туннель SIP или IAX объединяет несколько серверов с телефонией для обмена и перенаправления звонков.

Правила

Для управлением входящими и исходящими звонками предназначена вкладка «Правила звонков». Все звонки по умолчанию разделены на внешние и внутренние. При необходимости вы можете добавить новый набор правил и добавить к нему необходимые правила.

Правила подразделяются на следующие элементы:

Принять вызов - автоматически принимает звонки на все известные номера.

Повесить трубку отключает звонящего абонента, если он совпадает с указанными условиями.

Ждать набора номера включает ожидание в течение указанного промежутка времени, пока абонент не наберет номер полностью. Это делается для предотвращения быстрого звонка на внутренний номер, который совпадает с началом внешнего номера.

Время действия – указывает время действия для каждого правила.

Перенаправить вызов. Если входящий или исходящий абонент совпадает с указанными условиями, то он перенаправляется на номер или набор правил, в соответствии с которым обрабатывается звонок.

Преобразовать номер изменяет номер звонящего или набранный номер при совпадении с условиями набора.

Звонок через внешний канал отправляет звонок, подходящий под заданные условия, через выбранного внешнего провайдера связи.

Перенаправления

Перенаправления служат для организации вызова на указанный внешний номер, если абонент не отвечает или занят.

Очереди

Используются для равномерной нагрузки на абонентов и удержания звонка до первого освободившегося номера

Журнал звонков

В журнале звонков перечислены все входящие и исходящие звонки в систему, в том числе перенаправленные и неотвеченные. Также, можно прослушать и скачать в виде аудиофайла записанный звонок, если включена опция записи в настройках модуля.

Настройка перенаправления портов

Иногда возникает необходимость снаружи организовать доступ к компьютеру, находящемуся в локальной сети: для подключения к windows-серверу по RDP, для подключения к локальному веб-серверу и т.д. В этом случае обычно используется функция перенаправления портов.

При создании перенаправления, необходимо ввести протокол, порт перенаправления (порт который будет открыт на сервере и на который будут подключаться компьютеры из внешней сети), а также порт и хост назначения (порт и адрес компьютера, к которому

необходимо организовать доступ). При необходимости можно указать интерфейс или группу интерфейсов, на которых будет реализовано перенаправление портов.

Также можно перенаправлять диапазоны портов, введя номера портов через дефис: например «10000-10100».

Если необходимо, чтобы машины локальной сети при обращении на перенаправленный порт попадали на хост назначения, можно включить опцию «разрешить подключаться из локальной сети». При этом локальные соединения будут проходить через NAT и хост назначения увидит эти подключения как инициированные ИКС.

Для того, чтобы в межсетевом экране автоматически создалось правило, разрешающее подключение на данное перенаправление, необходимо включить соответствующий флажок.

Опция «Использовать NAT» позволяет подключаться через перенаправление портов к хостам, для которых ИКС не указан в качестве шлюза.

Настройка сервера времени

Модуль «Время и дата» позволяет установить системное время, выбрать временную зону, а также синхронизировать системное время с серверами точного времени в Интернете.

Для синхронизации системных часов с временем интернета, необходимо нажать кнопку «Синхронизировать сейчас».

В случае использования NTP-сервера, адреса указанные в блоке «Синхронизация», будут использоваться встроенным NTP-сервером ИКС в качестве адресов эталонных серверов.

Вкладка «Сервер времени» отображает текущее состояние модуля, общую информацию о сервере времени программы, а также кнопку «Выключить» (или «Включить если модуль выключен) для управления модулем.

Настройка IP-TV

За трансляцию multicast-пакетов цифрового телевидения в ИКС отвечает служба Multicast-прокси. Чтобы запустить ее, необходимо перейти в модуль «Все службы» и найти в списке данную службу. При нажатии на имя службы, вы попадете в одноименный модуль, где можно указать настройки приема и передачи.

Вкладка «Настройки» содержит три параметра:

Порт - указывает внутренний порт, на который будет происходит подключение приемника IP-TV, по умолчанию 4022

Адрес - в данном поле необходимо указать интерфейс, на который поступает multicast-поток от провайдера.

Автоматически создавать разрешающее правило - данный флажок разрешает транслировать поток от провайдера к приемнику и создает соответствующее правило в межсетевом экране.

Для того, чтобы настроить подключение приемника, необходимо изменить параметры плейлиста следующим образом:

http://{address}:{port}/{protocol}/{channel_addr}:{channel_port}

То есть, если в плейлисте указано

rtp://@111.22.33.44:1234

то после редактирования должно получиться:

http://192.168.1.1:4022/udp/111.22.33.44:1234

где 192.168.1.1 - адрес ИКС в локальной сети.

Настройка кластера

Кластер предназначен для распределения нагрузки исходящих пакетов из локальной сети. Является системой из нескольких серверов ИКС, которые имеют общую синхронизированную базу настроек. Изменение настроек может производиться с любого сервера, входящего в состав кластера.

Внимание: настройки провайдеров и локальных сетей локальны для каждого сервера, но при этом они сохраняются на всех узлах кластера, поэтому для настройки сетей и провайдеров следует использовать разные имена.

Перед настройкой все сервера нужно объединить в одну сеть. Рекомендуется использовать отдельный интерфейс сетевой карты, т.к. в этой сети будут передаваться служебные данные кластера.

Активация кластеризации производится в консоли восстановления ИКС: Управление сервером –Кластер.

На каждом сервере сперва необходимо включить модуль кластеризации (Включить кластеризацию).

Далее выбираем один из серверов как главный, к которому будем подключать все остальные. В данном случае “главный сервер” не означает, что он имеет больший приоритет, все сервера в кластере равнозначны, это делается для удобства первоначальной настройки.

На всех серверах (кроме “главного”) подключаемся к кластеру (Подключиться к кластеру). Создаем резервную копию текущих настроек. Указываем адрес “главного” сервера. После подключения сервер получит текущий список узлов кластера и синхронизирует базу данных.

Внимание: когда сервер подключается к кластеру, все его настройки стираются и заменяются на общие настройки кластера. Поэтому рекомендуется сначала произвести настройки кластера, а после производить прочие настройки.

Внимание: после создания кластера при настройке сети нельзя изменять адрес интерфейса, который используется для связи улов кластера.

После настройки кластера рекомендуется на интерфейсе провайдера закрыть порты 49495 и 49496 по протоколу TCP (служебные порты кластера).

В web интерфейсе можно посмотреть текущий статус кластера: Обслуживание - Сервера – Кластер. Версия базы данных всех узлов должна совпадать.

Для распределения нагрузки между серверами устанавливается балансировщик. На балансировщике указываются ip адреса серверов кластера. Также балансировщик мониторит состояние серверов и исключает из списка балансировки проблемные сервера.

Настройки веб-интерфейса программы

В этом разделе можно настроить некоторые параметры веб-интерфейса ИКС: язык интерфейса, тему оформления и т.д. Тема иконок определяет внешний вид логотипа и текст сообщения, которые выводятся при входе в веб-интерфейс.

Также администратор может изменить порт веб-интерфейса на случай, если порт 81 используется в других целях (например, для перенаправления порта или привязки виртуального хоста). Порт для доступа по протоколу HTTPS по умолчанию 444, его также можно изменить.

Таймаут сессии определяет время бездействия пользователя, по окончании которого будет произведен автоматический выход из веб-интерфейса.

Для входа в веб-интерфейс может быть назначен заранее созданный сертификат.

Для того, чтобы постоянно не обращаться к сайту документации ИКС, в веб-интерфейс встроена документация, открывающаяся по щелчку на стрелке в правой части интерфейса.

Настройка физических носителей

В модуле «Жесткие диски» содержится список всех жестких дисков, физически подключенных к компьютеру, на котором установлена программа.

Список представлен в виде дерева, в котором есть два главных раздела - неиспользуемые диски и основной системный раздел (зеркало). В основном разделе перечислены диски, входящие в зеркальный массив, на котором установлена система.

Для того, чтобы добавить жесткий диск в систему, необходимо создать пользовательский раздел Stripe или Mirror. Нажмите «Добавить» и выберите тип создаваемого раздела. Затем при помощи мыши перетащите по очереди неиспользуемые жесткие диски, которые необходимо добавить в раздел. После добавления в модуле Хранилище файлов появится дополнительная корневая папка, в которой можно создавать файловые ресурсы.

4 ПРОВЕРКА ПРОГРАММЫ

4.1 Описание старта и остановки Изделия

Изделие стартует автоматически после включения питания аппаратной части. Для управления вручную остановкой или перезагрузкой необходимо воспользоваться модулем «Управление питанием» веб-интерфейса или меню «Настройка сервера» консоли восстановления.

4.2 Описание процедуры проверки правильности старта Изделия

После загрузки операционной системы программа последовательно загружает рабочие модули. Этот процесс отображается на экране монитора в виде вывода строки с именем модуля или службы и его статусом. Признаком успешной загрузки модуля или службы является статус «ОК», признаком неисправности – статус «ОШИБКА».

Некоторые службы, такие как «Антивирус», «Jabber-сервер», «ARP-таблица», имеют длительное время загрузки, в то время как ожидание отклика службы ограничено. Такие службы могут выдавать статус «ОШИБКА» при старте Изделия, в данном случае это не является неисправностью. В целях контроля правильности загрузки Изделия следует загрузить веб-интерфейс и в модуле «Все службы» проверить, что статус соответствующих модулей и служб – «запущен».

Для проверки работоспособности веб-интерфейса администратор должен обратиться к внутреннему или внешнему сетевому адресу программы с помощью веб-браузера.

5 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

5.1 Процедура резервного копирования и восстановления

В случае программных или аппаратных сбоев, когда загрузка штатным образом Изделия или ОС невозможна, необходимо заново установить программу и провести процедуру восстановления:

Процедуры аварийного восстановления выполняются при помощи модуля «Резервные копии» с использованием ранее созданных резервных копий ПО Изделия или образа системы.

5.2 Выключение аппаратной платформы

Для корректного выключения аппаратной платформы необходимо нажать кнопку «Выключение» или «Перезагрузка» в модуле «Управление питанием» или аналогичные пункты в меню «Настройка сервера» консоли восстановления.

5.3 Создание резервных копий

Процедура резервного копирования Изделия.

Для создания резервной копии ПО Изделия в веб-интерфейсе выберите модуль «Резервные копии» раздела «Обслуживание».

В данном разделе необходимо выполнить следующие действия:

1) Нажать копку «Добавить» и выбрать пункт «Резервная копия»;

2) В открывшемся коне выбора данных для резервирования отметить флажками нужное;

3) Нажать кнопку «Добавить». Начнется резервное копирование данных. Когда полоса прогресса копирования остановится на значении 100%, резервная копия будет создана.

4) Во избежание потери резервных копий в случае аппаратного сбоя Изделия, рекомендуется сохранить резервную копию системы на отдельном носителе. Для этого следует выделить требуемую резервную копию, нажать кнопку «Скачать» и указать место, куда будет сохранена копия.

Автоматизация резервного копирования.

В программе реализована возможность автоматического создания резервных копий с

указанной частотой и на указанные носители информации.

В меню «Настройки» модуля «Резервные копии» можно указать следующие параметры автоматического резервного копирования:

периодичность создания копии настроек системы, она включает в себя только конфигурацию всех модулей

периодичность создания полной резервной копии

копирование создаваемой резервной копии на flash-накопитель, в том числе на файловую систему NTFS.

копирование создаваемой резервной копии на физически удаленный носитель по протоколу FTP.

Вкладка «Шаблоны» позволяет гибко настроить автоматическое резервное копирование выбранных данных в указанное время.

Для того, чтобы хранить резервные копии большого размера можно использовать дополнительный жесткий диск. В настройках резервного копирования укажите раздел, содержащий этот диск, и резервирование будет происходить на него.

5.4 Восстановление настроек системы

При установке программы на другую аппаратную часть или восстановления системы после сбоя, необходимо произвести развертывание резервной копии системы:

1) В модуле «Резервные копии» нажать кнопку «Закачать» и указать место хранения резервной копии.

2) После того, как резервная копия появится в списке доступных резервных копий программы, нажмите кнопку «Восстановить», на запрос системы о целесообразности выполняемого действия ответьте «Да».

3) Второй метод восстановления системы – из консоли восстановления. В ней нужно выбрать меню Управление сервером – Резервные копии. Появится список доступных резервных копий.

5.5 Восстановление свойств МЭ после сбоев и отказов оборудования

Процедура восстановления свойств МЭ после сбоев и отказов оборудования:

1) осуществить отключение ПЭВМ 5 от электропитания;

2) осуществить подключение ПЭВМ 5 к сети электропитания;

3) осуществить включение ПЭВМ 5;

4) дождаться загрузки ПО Изделия;

5) в случае выявления ошибок во время загрузки ПО Изделия необходимо переустановить ПО Изделия.

5.6 Использование консоли восстановления

Консоль восстановления - это служебный интерфейс Изделия, работающий в текстовом режиме. Для того, чтобы воспользоваться средствами консоли существуют два способа:

1) подключить к Изделию монитор и клавиатуру;

2) воспользоваться любым ssh-клиентом (например Putty) и подключиться на 22 порт Изделия (в этом случае в модуле «Межсетевой экран» → «Настройки» должен быть разрешен доступ по протоколу SSH с хоста, с которого производится подключение), по умолчанию логин - recshell, пароль - recovery.

Консоль восстановления позволяет произвести следующие операции:

1) Проверка и корректировка таблицы маршрутизации ИКС (пункт меню Настройка сети - маршрутизация). Здесь администратор может просмотреть текущую таблицу маршрутизации, удалить какой-либо из маршрутов либо добавить новый.

2) Проверка и корректировка сетевых интерфейсов ИКС (пункт меню Настройка сети - сетевые интерфейсы). Системный администратор может вывести информацию по состоянию каждого из интерфейсов, проверить, подключен ли сетевой кабель (у подключенного интерфейса status: active), верно ли назначены ip-адреса, при необходимости удалить ip-адрес с интерфейса а также назначить новый.

3) Выключение межсетевого экрана (пункт меню Настройка сети - межсетевой экран). В случае, если ИКС по каким-либо причинам блокирует доступ к веб-интерфейсу, можно временно отключить межсетевой экран до устранения причины блокировки.

Утилиты Ping и Trace (Настройка сети - утилиты). Позволяют проверить доступность локального или удаленного хоста.

Смена пароля на аккаунт администратора и на вход в консоль восстановления (Управление сервером - пароли).

Добавление диска в зеркальный массив (Управление сервером - RAID).

Обновление конфигурации ИКС (Управление сервером - обновление всех настроек).

Перезагрузка (Управление сервером - перезагрузка).

Выключение (Управление сервером - выключение).

Консоль восстановления является вспомогательным инструментом для диагностики неисправностей ИКС. Все изменения, произведенные в ней, за исключением смены паролей и установки дисков в массив, будут сброшены при любом изменении в веб-интерфейсе ИКС или после перезагрузки.

5.7 Инструменты виртуализации.

ИКС может быть установлен на виртуальную машину. Если в качестве основной системы используется VmWare, то для более тесной интеграции систем в ИКС установлены Vmware Tools версии 5.

6 СООБЩЕНИЯ СИСТЕМНОМУ АДМИНИТРАТОРУ

В зависимости от ситуации программа может выдавать следующие сообщения, которые могут требовать вмешательства системного администратора или являться информационными.

«К сожалению, ваш браузер не поддерживается» - сообщение, выдаваемое администратору в том случае, если он пользуется для доступа к веб-интерфейсу браузером, не указанным в системных требования к программе.

«Неверный логин или пароль» - администратор или пользователь указал неверное имя входа (логин) или пароль для входа в систему.

«До окончания срока активации осталось … дней» - сообщение, напоминающее об оставшемся сроке эксплуатации незарегистрированного Изделия.

«Тестовый срок истек» - сообщение, информирующее о том, что срок эксплуатации незарегистрированного Изделия истек, и дальнейшая эксплуатация возможна только после регистрации программы.

«Вы действительно хотите выключить сервис?» - система запрашивает администратора подтверждение выключения выбранной службы.

«Вы действительно хотите удалить эти элементы?» - система запрашивает администратора подтверждение удаления выбранных данных.

«Вы действительно хотите удалить файл лицензии?» - запрос на подтверждение удаления лицензионного регистрационного файла программы.

«Не удалось зарегистрироваться на сервере активации» - нет интернет-доступа к серверу активации компании «А-Реал Консалтинг».

«Вы действительно хотите добавить диск в раздел?» - запрос на подтверждение перемещения неиспользуемого диска в созданный раздел.

«Данная операция необратима. Удалить диск из раздела можно будет только удалив сам раздел!» - сообщение о невозможности обратного процесса при перемещения дополнительного жесткого диска в раздел.

«Не удалось получить список пользователей домена. Возможно ИКС не является членом домена» - сообщение появляется при импорте пользователей из домена в случае, если программа не подключена к контроллеру домена.

«Вы действительно хотите выключить (перезагрузить) сервер?» - система запрашивает администратора подтверждение выключения (перезагрузки) аппаратной части Изделия.

«Конфликт со следующими сетевыми интерфейсами:» - в программе назначены ip-адреса одного сетевого диапазона на разных сетевых интерфейсах.

«Вы действительно хотите восстановить резервную копию?» - запрос на подтверждение восстановления системы из сохраненной резервной копии.

«Не удалось загрузить статистику» - сообщение появляется в модуле «Пользователи» во время динамической загрузки статистики в том случае, если связь с сервером утеряна.

«Не удалось сохранить» - при нормальной работе программы сообщение возникает в двух случаях: если утеряна связь с сервером в момент сохранения какого-либо параметра либо в случае слишком долгого выполнения запроса за время, превышающее допустимое. В ином случае данное сообщение свидетельствует о неверной работе программы.

«Не удалось обнаружить контроллер домена» - сообщение, возникающее при указании настроек контроллера домена. Программа первоначально пытается автоматически обнаружить контроллер домена в сети, если это невозможно, то показывается данное сообщение.

«Сохранение настроек…» - модуль сохраняет настройки и недоступен для редактирования и просмотра.

«Загрузка…» - модуль загружает данные и недоступен для редактирования и просмотра.

«Выполняется активация» - идет процесс активации программы.

«Восстановление резервной копии...» - идет процесс развертывания сохраненной резервной копии.

«Синхронизация…» - идет процесс синхронизация сервера времени с выбранным внешним сервером.

«Удаление…» - идет процесс удаления элемента программы.

«Перемещение…» - идет процесс перемещения пользователя или группы на другой уровень.

7 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Основание (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись ответственного лица за проведение изменения	Подпись лица, ответственного за эксплуатацию программного изделия