Эшелон
комплексная безопасность

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

УТВЕРЖДЕН
НПЕШ.465614.002 РА-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «КОМПЛЕКС ПРОТИВОДЕЙСТВИЯ ПРОГРАММНО-АППАРАТНЫМ ВОЗДЕЙСТВИЯМ (КП ПАВ) «РУБИКОН» С ПОДДЕРЖКОЙ ВИРТУАЛЬНЫХ СЕТЕЙ
НПЕШ.465614.002

Руководство администратора

НПЕШ.465614.002 РА

Версия документа 1.2

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Идентификация документа

Название документа	Программно-аппаратный комплекс «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с поддержкой виртуальных сетей. Руководство администратора
Версия документа	Версия 1.2
Обозначение документа	НПЕШ.465614.002 РА
Идентификация КП ПАВ «Рубикон»	Программно-аппаратный комплекс «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с поддержкой виртуальных сетей. НПЕШ.465614.002
Идентификация разработчика	АО «НПО «Эшелон»
Уровень доверия	Оценочный уровень доверия 5 (ОУД5), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ALC_FLR.3 «Систематическое устранение недостатков», ALC_CMC.5 «Расширенная поддержка», ALC_DVS.2 «Достаточность мер безопасности», AVA_VAN.5 «Усиленный методический анализ», расширенный компонентами ADV_IMP_EXT.3 «Реализация КП ПАВ «Рубикон»», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения КП ПАВ «Рубикон»», AMA_SIA_EXT.3(1) «Анализ влияния обновлений на безопасность КП ПАВ «Рубикон»», ALC_UPI_EXT.1 Процедуры обновления базы решающих правил, AMA_SIA_EXT.3(2) Экспертиза анализа влияния обновлений базы решающих правил на безопасность системы обнаружения вторжений.
Идентификация ПЗ	Методический документ ФСТЭК России «Профиль защиты межсетевого экрана типа «А» второго класса защиты, ИТ.МЭ.А2.ПЗ» Методический документ ФСТЭК России «Профиль защиты межсетевого экрана типа «Б» второго класса защиты, ИТ.МЭ.Б2.ПЗ» Методический документ ФСТЭК России «Профиль защиты систем обнаружения вторжений уровня сети второго класса защиты, ИТ.СОВ.С2.ПЗ»

Идентификация ОК	Требования к межсетевым экранам, утвержденные приказом ФСТЭК России от 09 февраля 2016 г. № 9. Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
Ключевые слова	Межсетевой экран, система обнаружения вторжений, ОУД5

1.2 Аннотация документа

Документ предназначен для ознакомления потребителей с технической информацией об изделии «Программно-аппаратный комплекс «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с поддержкой виртуальных сетей» НПЕШ.465614.002 (далее по тексту – «КП ПАВ «Рубикон») и содержит общие сведения об КП ПАВ «РУБИКОН», организационно-распорядительные меры, сведения о структуре КП ПАВ «РУБИКОН», описание настроек и тексты сообщений, выдаваемых в ходе выполнения настройки, проверки, а также о процессе функционирования КП ПАВ «РУБИКОН».

Настоящий документ соответствует ТДБ «AGD_OPE.1 Руководство пользователя по эксплуатации», «AGD_PRE.1 Подготовительные процедуры» о чем свидетельствует следующая таблица.

Идентификатор требования	Содержание требования	Раздел документа
AGD_OPE.1 Руководство пользователя по эксплуатации		
AGD_OPE.1.1C	В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений.	2, 5.3
AGD_OPE.1.2C	В руководстве пользователя по эксплуатации в рамках каждой пользовательской роли должно быть представлено описание принципов безопасной работы с предоставленными в КП ПАВ «Рубикон» интерфейсами	5.3, 6, 7, 8, 9, 10, 11, 12
AGD_OPE.1.3C	В руководстве пользователя по эксплуатации должно быть представлено описание доступных для каждой пользовательской роли функций и интерфейсов, особенно всех параметров безопасности под управлением пользователя, с указанием безопасных значений, если это уместно	5.3
AGD_OPE.1.4C	В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено четкое представление каждого типа имеющих значение для безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением ФБО	10.1
AGD_OPE.1.5C	В руководстве пользователя по эксплуатации должны быть идентифицированы все возможные режимы работы КП ПАВ «Рубикон» (включая операции после сбоев и ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования	4, 13
AGD_OPE.1.6C	В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть приведено описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ, имеющих отношение к пользователю	3.2, 5.3
AGD_OPE.1.7C	Руководство пользователя по эксплуатации должно быть четким и обоснованным	-

AGD_PRE1.1C	В подготовительных процедурах должны описываться все шаги, необходимые для безопасной приемки поставленного КП ПАВ «Рубикон» в соответствии с процедурами поставки заявителя (разработчика, производителя)	3.1
AGD_PRE1.2C	В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки КП ПАВ «Рубикон» , реализации и оценки реализации всех функций безопасности среды функционирования КП ПАВ «Рубикон» в соответствии с целями безопасности для среды функционирования, описанными в ЗБ	3.1, 5

1.3 Термины и определения

В настоящем документе используются термины и определения согласно ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» и ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств».

Squid	Программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP.
Администратор КП ПАВ «Рубикон»	Уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию КП ПАВ «Рубикон»
Задание по безопасности	Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного КП ПАВ «Рубикон»
Объект оценки	Подлежащий сертификации (оценке) КП ПАВ «Рубикон»
Политика безопасности КП ПАВ «Рубикон»	Совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых КП ПАВ «Рубикон»
Профиль защиты	Совокупность требований безопасности для КП ПАВ «Рубикон»
Разработчик	АО «НПО «Эшелон»
Угроза безопасности информации	Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.
Функции безопасности КП ПАВ «Рубикон»	Совокупность всех функций безопасности КП ПАВ «Рубикон» , направленных на осуществление политики безопасности объекта оценки (ПБО).

1.4 Перечень сокращений

DHCP - Dynamic Host Configuration Protocol;

DNS - Domain Name System;

ICMP - Internet Control Message Protocol;

IP - Internet Protocol;

SID - Security Identifier;

VPN - Virtual Private Network;

БРП - база решающих правил;

ЗБ - задание по безопасности;

ИС - информационная система;

ИТ - информационная технология;

МЭ - межсетевой экран;

ОС - операционная система;

ОУД - оценочный уровень доверия;

ПБО - политика безопасности объекта оценки;

ПЗ - профиль защиты;

ПО - программное обеспечение;

САВЗ - средства антивирусной защиты;

СВТ - средство вычислительной техники;

СЗИ - средство защиты информации;

СОВ - система обнаружения вторжений;

ТДБ - требования доверия к безопасности;

УЦ - удостоверяющий центр;

ФБО - функции безопасности объекта оценки;

ФТБ - функциональные требования безопасности.

Оглавление

1.5 Общие сведения

КП ПАВ «Рубикон» предназначен для выполнения следующих функций:

- контроль и фильтрация сетевого трафика;
- идентификация и аутентификация;
- регистрация событий безопасности;
- обеспечение бесперебойного функционирования и восстановления;
- тестирование и контроль целостности;
- преобразование сетевых адресов;
- маскирование;
- приоритизация информационных потоков;
- управление;
- взаимодействие с другими средствами защиты информации;
- обнаружение вторжений.

Функции контроля и фильтрации сетевого трафика реализуются в соответствии с заданными правилами проходящих через него информационных потоков. КП ПАВ «Рубикон» используется в целях обеспечения защиты информации (некриптографическими методами), содержащей сведения, составляющие государственную тайну, и иной информации ограниченного доступа.

2 ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ МЕРЫ

2.1 Процедуры поставки

2.1.1 Общий порядок поставки

КП ПАВ «Рубикон» поставляется в составе изделия Программно-аппаратный комплекс «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с поддержкой виртуальных сетей. НПЕШ.465614.002.

При поставке КП ПАВ «Рубикон» заказчику от среды производства до среды установки АО «НПО «Эшелон» (далее Разработчик) выполняет следующие действия:

1) расчет контрольных сумм файлов программного обеспечения КП ПАВ «Рубикон», установленного на аппаратную платформу;

2) упаковка комплекта поставки;

3) передача упакованного комплекта поставки на склад готовой продукции;

4) выдача упакованного комплекта поставки уполномоченному представителю заказчика.

2.1.2 Комплект поставки

Базовый комплект поставки КП ПАВ «Рубикон» содержит следующие комплектующие:

1) аппаратная платформа с установленным программными и аппаратными компонентами КП ПАВ «Рубикон» НПЕШ.465614.002;

2) программное изделие (ПО) «Рубикон» НПЕШ.00501-01, поставляемое на оптических носителях и включающее в себя:

a) установочный дистрибутив ПО «Рубикон»,

b) патч «update-0.7-12»,

c) патч «update-tls-0.2-1»;

3) формуляр на КП ПАВ «Рубикон» НПЕШ.465614.002-ХХФО, где ХХ-номер реализации;

4) руководство администратора НПЕШ.465614.002РА;

5) гарантийный талон и сертификат на техническую поддержку;

6) необходимые кабели, розетки, монтажные комплектующие согласно варианту реализации КП ПАВ «Рубикон» и ТУ на КП ПАВ «Рубикон».

2.1.3 Процедуры и меры безопасности при распространении

Процедуры и меры безопасности, реализуемые при распространении КП ПАВ «Рубикон» к месту назначения. обеспечивают:

- идентификацию и целостность КП ПАВ «Рубикон» во время пересылки;
- обнаружение несанкционированных модификаций КП ПАВ «Рубикон»;
- блокирование попыток подмены КП ПАВ «Рубикон» от имени разработчика.

2.1.3.1 Контроль целостности программного обеспечения КП ПАВ «Рубикон»

Расчет эталонных контрольных сумм файлов программного обеспечения компонентов КП ПАВ «Рубикон», установленного на аппаратную платформу, осуществляется на этапе сборки и выполняется внутренними средствами КП ПАВ «Рубикон». При включении «Рубикон» выполняет контроль целостности установленных файлов. При выявлении несоответствия сохраненным значениям в веб-интерфейсе «Рубикон» отображается соответствующее уведомление.

2.1.3.2 Контроль целостности файлов установочного диска

Перечень файлов, записанных на установочный компакт-диск, а также их контрольные суммы представлены в формуляре на КП ПАВ «Рубикон», входящем в комплект поставки.

2.1.3.3 Контроль целостности аппаратной платформы

Корпус аппаратной платформы после установки программных и аппаратных компонентов КП ПАВ «Рубикон» опечатывается уникальным одноразовым стикером. Вскрыть корпус без разрушения стикера невозможно.

2.1.3.4 Контроль сохранности упакованного комплекта

Комплект КП ПАВ «Рубикон» упаковывают в пластиковый пакет, помещают в картонную коробку и заклеивают коробку скотчем с символикой АО «НПО «Эшелон». Упакованный комплект хранится на складе готовой продукции, оснащенном охранной сигнализацией.

2.1.3.5 Поддержка безопасности доставки

Доставка готовой продукции к месту назначения осуществляется силами разработчика. Выдача КП ПАВ «Рубикон» уполномоченному представителю заказчика осуществляется на основании документов, удостоверяющих полномочия представителя. Передача КП ПАВ «Рубикон» заказчику подтверждается актом сдачи-приемки КП ПАВ «Рубикон», на котором проставляются подписи и печати сторон.

2.2 Требования безопасности к среде ИТ

КП ПАВ «РУБИКОН» обеспечивает функциональное назначение при реализации пользователем следующих предварительных организационно-распорядительных мер:

– обеспечение сохранности оборудования и физической целостности системных блоков компьютеров;

– ведение журнала учета работы компьютеров, проведения регламентных мероприятий и внесения изменений в конфигурацию технических и программных средств;

– реализация мероприятий по антивирусной защите и обеспечение свободной от вирусов программной среды компьютеров.

К среде ИТ, в которой функционирует, предъявляются следующие требования безопасности, относящиеся к пользователю:

– регламентация запрета доступа непривилегированных пользователей из внешней сети в защищаемые сети по всем типам протоколов, за исключением специально созданной для такого доступа демилитаризованной сети;

– обеспечение физической сохранности технических средств (межсетевого экрана, СВТ, на котором он функционирует и терминалов, с которых выполняется его управление) и исключение возможности доступа к ним посторонних лиц;

– обеспечение установки, конфигурирования и управления КП ПАВ «Рубикон» в соответствии с эксплуатационной документацией.

3 СТРУКТУРА ПРОГРАММЫ

3.1 Подсистема обеспечения сетевого взаимодействия

3.1.1 Модуль фильтрации

Модуль фильтрации является ядром подсистемы обеспечения сетевого взаимодействия и используется для работы модуля управления состоянием, модуля тестирования и контроля целостности и модуля сетевого посредника. Модуль фильтрации осуществляет фильтрацию информационных потоков, основанную на следующих типах атрибутов безопасности:

– сетевой адрес узла отправителя и получателя;

– логический или физический сетевой интерфейс КП ПАВ «Рубикон», через который проходит пакет;

– сетевой протокол, который используется для взаимодействия;

– направление пакета (входящий/исходящий);

– транспортный протокол, который используется для взаимодействия;

– порты источника и получателя в рамках сеанса (сессии);

– флаг фрагментации;

– мандатная метка;

– команды (разрешенные/запрещенные), параметры команд; последовательности используемых команд - для FTP протокола;

– мобильный код (разрешенный/запрещенный) - для языков программирования Java и JavaScript;

– прикладное ПО (разрешенное/запрещенное) - для веб-браузеров (Internet Explorer, Mozilla Firefox, Google Chrome и др).

3.1.2 Модуль маршрутизации

Программный модуль КП ПАВ «Рубикон», предназначенный для выполнения статической маршрутизации.

3.1.3 Модуль преобразования адресов

Программный модуль КП ПАВ «Рубикон», позволяющий проводить трансляцию сетевых адресов (NAT) при экспорте информации сетевого трафика за пределы КП ПАВ

«Рубикон» и осуществлять замену сетевого адреса КП ПАВ «Рубикон» на маскирующий (подставной) адрес.

3.1.4 Модуль приоритизации

Программный модуль КП ПАВ «Рубикон», обеспечивающий приоритизацию информационных потоков на основе установленных приоритетов значений сетевого адреса и используемого порта.

3.1.5 Модуль управления состояниями

Программный модуль КП ПАВ «Рубикон», предназначенный для проверки каждого пакета по таблице состояний для определения того, не противоречит ли состояние пакета ожидаемому состоянию.

3.1.6 Модуль сетевого посредника

Программный модуль КП ПАВ «Рубикон», осуществляющий посредничество в передаче информации сетевого трафика, основанное на следующих типах атрибутов безопасности:

- сетевой адрес и порт отправителя и получателя;
- сетевой трафик (FTP, HTTP);
- разрешенные/ запрещенные атрибуты информации в заголовках пакетов.

3.1.7 Модуль настройки сетевых интерфейсов

Программный модуль КП ПАВ «Рубикон», осуществляет маскирование датчика СОВ на сетевом уровне и позволяет настраивать сетевые интерфейсы.

3.2 Подсистема идентификации / аутентификации

3.2.1 Модуль аутентификации веб-сервера

Модуль аутентификации веб-сервера обеспечивает идентификацию и аутентификацию администраторов КП ПАВ «Рубикон», а также идентификацию и аутентификацию субъектов межсетевого взаимодействия до передачи межсетевым экраном информационного потока получателю.

3.3 Подсистема бесперебойного функционирования и восстановления

3.3.1 Модуль тестирования и контроля целостности

Программный модуль КП ПАВ «Рубикон», обеспечивающий контроль целостности исполняемых файлов КП ПАВ «Рубикон» путем контрольного суммирования, а также проверку работоспособности служб КП ПАВ «Рубикон» и сетевого соединения.

3.3.2 Модуль восстановления

Программный модуль КП ПАВ «Рубикон», обеспечивающий автоматическое восстановление устойчивых и безопасных состояний HTTP сервера, прокси сервера, VPN сервера, сервиса аудита, службы времени, службы COB и DHCP.

3.3.3 Модуль кластеризации

Программный модуль КП ПАВ «Рубикон», обеспечивающий кластеризацию КП ПАВ «Рубикон» с помощью резервирования КП ПАВ «Рубикон».

3.4 Подсистема регистрации событий

Данная подсистема представлена модулем работы с журналом.

3.4.1 Модуль работы с журналом

Программный модуль КП ПАВ «Рубикон», предназначенный для создания, хранения и просмотра записей аудита. КП ПАВ «Рубикон» поддерживает уровни доступа (роли) пользователей. Все действия пользователей отслеживаются, и соответствующие записи помещаются в файлы регистрации событий безопасности. Модуль работы с журналом предоставляет уполномоченным пользователям (администратор КП ПАВ «Рубикон», аудитор КП ПАВ «Рубикон») возможность читать всю информацию из записей аудита, осуществлять поиск, сортировать записи аудита.

3.5 Подсистема взаимодействия с внешними системами

Данная подсистема состоит из следующих модулей:

1) Модуль взаимодействия с внешними СЗИ;
2) Модуль связи с сервером журналирования.

3.5.1 Модуль взаимодействия с внешними СЗИ

Программный модуль КП ПАВ «Рубикон», обеспечивающий взаимодействия КП ПАВ «Рубикон» с САВЗ по протоколу адаптации Интернет-контента (ICAP).

3.5.2 Модуль связи с сервером журналирования

Программный модуль КП ПАВ «Рубикон», обеспечивающий взаимодействие с сервером журналирования.

3.6 Подсистема управления

Данная подсистема состоит из нескольких модулей.

3.6.1 Модуль веб-сервера

Программный модуль КП ПАВ «Рубикон», обеспечивающий выполнение запросов пользователей.

3.6.2 Модуль преобразования конфигурации - браузера

Программный модуль КП ПАВ «Рубикон», обеспечивающий представление информации для пользователей.

3.7 Подсистема обнаружения вторжений

Подсистема обнаружения вторжений состоит из следующих модулей:

1) Агент обновления;
2) Модуль сигнатурного анализа сетевого трафика;
3) Модуль эвристического анализа сетевого трафика;
4) Модуль реагирования.

3.7.1 Агент обновления

Программный модуль КП ПАВ «Рубикон», предназначен для получения актуальной базы решающих правил СОВ с сервера обновлений.

3.7.2 Модуль сигнатурного анализа сетевого трафика

Программный модуль КП ПАВ «Рубикон» предназначен для поиска определенных в базе решающих правил СОВ сигнатур атак в сетевых пакетах.

3.7.3 Модуль эвристического анализа сетевого трафика

Программный модуль КП ПАВ «Рубикон», предназначен для обнаружения вторжений с помощью эвристического анализа.

3.7.4 Модуль реагирования

Программный модуль КП ПАВ «Рубикон», позволяет уведомлять администратора об обнаруженных вторжениях и выдачу управляющих сигналов межсетевому экрану.

3.8 Веб-интерфейс

3.8.1 Программа управления

Программный модуль КП ПАВ «Рубикон», позволяет решать задачи по администрированию СОВ.

3.9 Операционная система

3.9.1 Модуль выдачи меток времени

Программный модуль КП ПАВ «Рубикон», предоставляющий надежные метки времени для собственного использования (при генерации записей в журнале аудита).

3.9.2 Модуль захвата и разбора трафика

Программный модуль КП ПАВ «Рубикон», модуль предназначен для захвата, буферизации и управления последовательностью обработки сетевых пакетов.

3.10 Подсистема BIOS

3.10.1 Модуль BIOS

Программный модуль КП ПАВ «Рубикон», обеспечивающий инициализацию работы аппаратной платформы и передачу управления загрузчику ПО «Рубикон».

4 НАСТРОЙКА ПРОГРАММЫ

4.1 Установка ПО КП ПАВ «Рубикон»

ПО «Рубикон» поставляется в предустановленном варианте в составе КП ПАВ «Рубикон» и имеет настройки по умолчанию. Для целей администрирования в комплект поставки входит следующее ПО:

1) Установочный дистрибутив ПО «Рубикон» (поставляется на компакт-диске);

2) Патч «update-0.7-12», представленный файлом «update-0.7-12.x86_64.rpm», поставляемым на компакт-диске;

3) Патч «update-tls-0.2-1», представленный файлом «update-tls-0.2-1.x86_64.rpm», поставляемым на компакт-диске.

Перед установкой ПО «Рубикон» необходимо ознакомиться с требованиями к компьютеру, на котором функционирует ПО КП ПАВ «Рубикон», и с требованиями к ПО консоли управления (таблица 1).

Таблица 1 – Минимальные программно-аппаратные требования для консоли управления

Элемент среды функционирования	Параметры
Вычислительная платформа консоли управления КП ПАВ «Рубикон»	Процессор: частота не менее 1,2 ГГц Оперативная память: не менее 4 Гб Жесткий диск: не менее 120 ГБ Сетевая карта: не менее 100 Мбит/с
ОС консоли управления	ОС семейства Linux/Unix 64 bit: – Astra Linux Common Edition (Орел) не ниже 1.11; – Astra Linux Special Edition (Смоленск) не ниже 1.5; ОС семейства Microsoft Windows 64 bit: – Windows Server 2019; – Windows 10
Веб-браузер	Windows 10/Windows Server 2019: – IE (не ниже 11.1.17134.0); – Microsoft Edge (не ниже 42.17134.1.0); – Firefox не ниже 76.0.1 (64-битный); – Chrome (не ниже 83.0.4103.61); Astra Linux 1.6: – Firefox не ниже 60.0.2 (64-битный)

Для выполнения установки ПО КП ПАВ «Рубикон» необходимо произвести загрузку с установочного носителя КП ПАВ «Рубикон» (с компакт-диска), содержащего установочный дистрибутив ПО «Рубикон».

Установка представляет собой неинтерактивный процесс, в ходе выполнения которого устанавливается КП ПАВ «Рубикон», выполняется настройка оборудования и задаются параметры настроек по умолчанию.

По завершению процесса установки КП ПАВ «Рубикон» имеет сетевой интерфейс с IP-адресом 192.168.1.1. Сервер КП ПАВ «Рубикон» обрабатывает запросы пользователей. А веб-интерфейс обеспечивает предоставление информации, инструментарий настройки и конфигурирования для администратора и аудитора. Через веб-интерфейс может производиться начальная настройка параметров КП ПАВ «Рубикон». При дальнейшей настройке параметры администрирования можно изменить.

4.2 Описание старта и процедура проверки правильности старта

Старт КП ПАВ «Рубикон» начинается с включения кнопки питания аппаратной платформы, инициирующего загрузку необходимого ПО. По окончании загрузки ПО работоспособность и правильность старта КП ПАВ «Рубикон» можно проверить, выполнив команду «ping 192.168.1.1» на любом из компьютеров, подключенных к внутренней защищаемой сети.

Для прохождения процедур идентификации и аутентификации выполните следующие действия:

1) установите соединение с графическим интерфейсом КП ПАВ «Рубикон», подключившись по защищенному https-соединению https:// 192.168.1.1:8443;

2) введите идентификатор (логин) пользователя с ролью Администратор в текстовое поле «Имя пользователя» формы авторизации. По умолчанию «admin»;

3) введите пароль пользователя с ролью Администратор в текстовое поле «Пароль» формы авторизации. По умолчанию «radmin»;

4) нажмите кнопку «Вход».

При превышении трех неуспешных попыток ввода логина и пароля, доступ к КП ПАВ «Рубикон» будет заблокирован.

4.3 Установка необходимых обновлений (патчей)

При первом подключении к административному интерфейсу необходимо последовательно установить сначала файл патча «update-0.7-12.x86_64.rpm», затем файл

патча «update-tls-0.2-1.x86_64.rpm», поставляемых на компакт-диске «Программное изделие «Рубикон». Патч «update-0.7-12», патч «update-tls-0.2-1».

Для этого на странице «Система → Пакеты» (при необходимости, активировать эту страницу в разделе «Система → Настройка меню») выберите кнопкой «Browse» файл «update-0.7-12.x86_64.rpm» и нажмите кнопку «Загрузить новый пакет». Для установки патча выберите «Действие», отмеченное зеленой галочкой (рисунок 1).

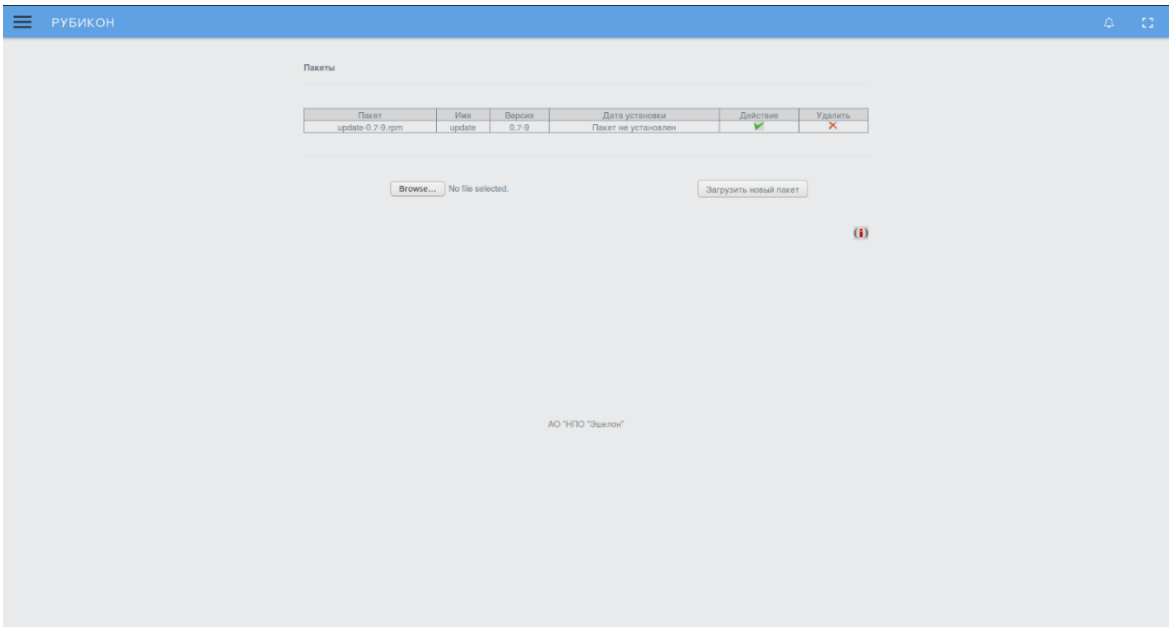


Рисунок 1 - Раздел «Система → Пакеты»

После установки пакета данные об этом отразятся в интерфейсе (рисунок 2).

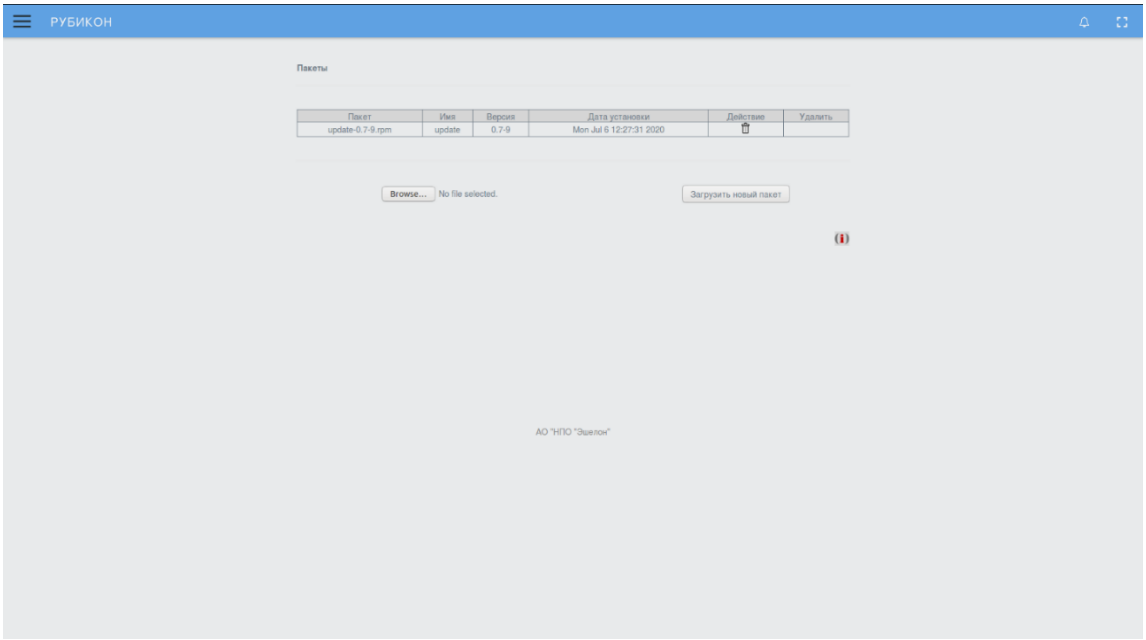


Рисунок 2 – Установка пакета обновлений

Список изменений, производимых пакетом, приведен в разделе 13.9.

Затем, на странице «Система → Пакеты» (страница должна быть активирована на предыдущем шаге) выберите кнопкой «Browse» файл «update-tls-0.2-1.x86_64.rpm» и нажмите кнопку «Загрузить новый пакет». Для установки патча выберите «Действие», отмеченное зеленой галочкой (рисунок 3).

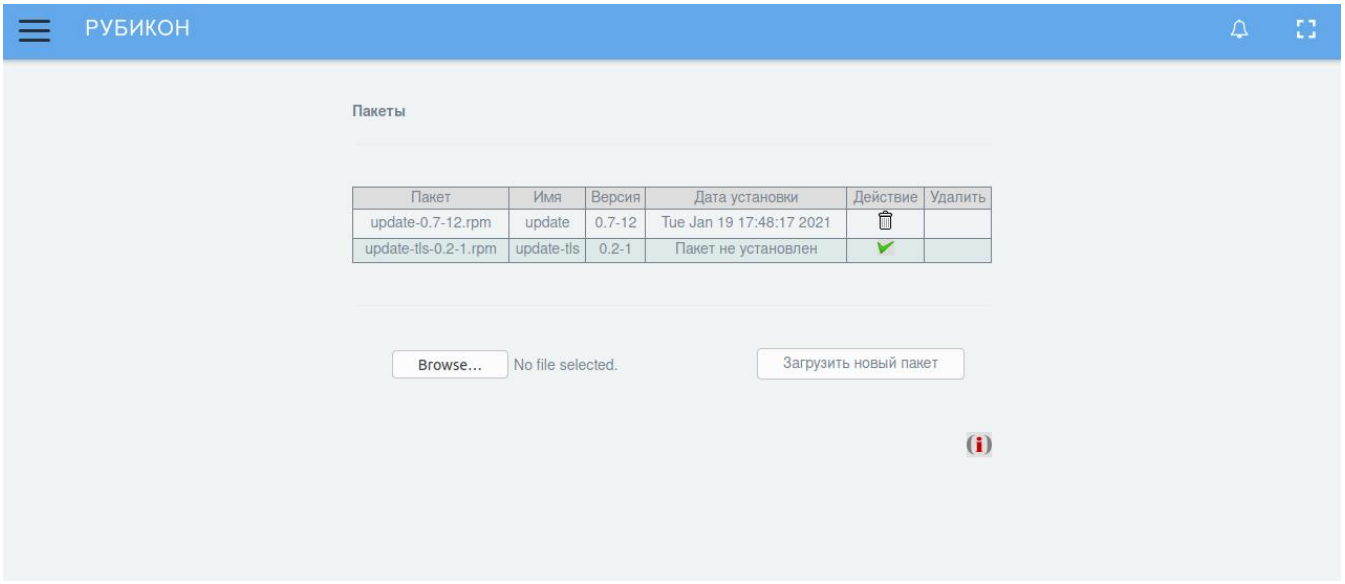


Рисунок 3 - Раздел «Система → Пакеты»

После установки пакета данные об этом отразятся в интерфейсе (рисунок 4).

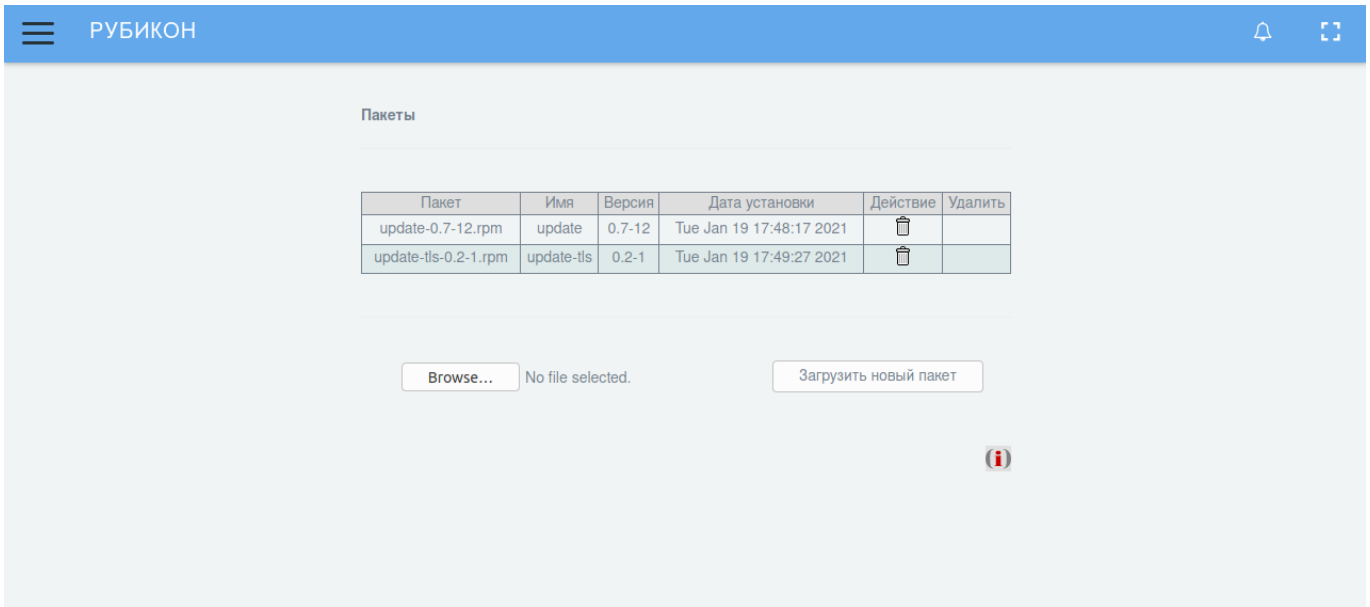


Рисунок 4 – Установка пакета обновлений

Список изменений, производимых пакетом, приведен в разделе 13.10.

Примечание – Действие «Удалить пакет», графически представленное символом корзины, предназначено исключительно для целей системного администрирования. По

умолчанию, для корректной работы КП ПАВ «Рубикон» после установки ПО «Рубикон» с установочного дистрибутива на аппаратную платформу, должны быть последовательно установлены патчи «update-0.7-12» и «update-tls-0.2-1».

После установки пакетов обновлений измените пароль на странице «Система → Пользователи» (рисунок 5).

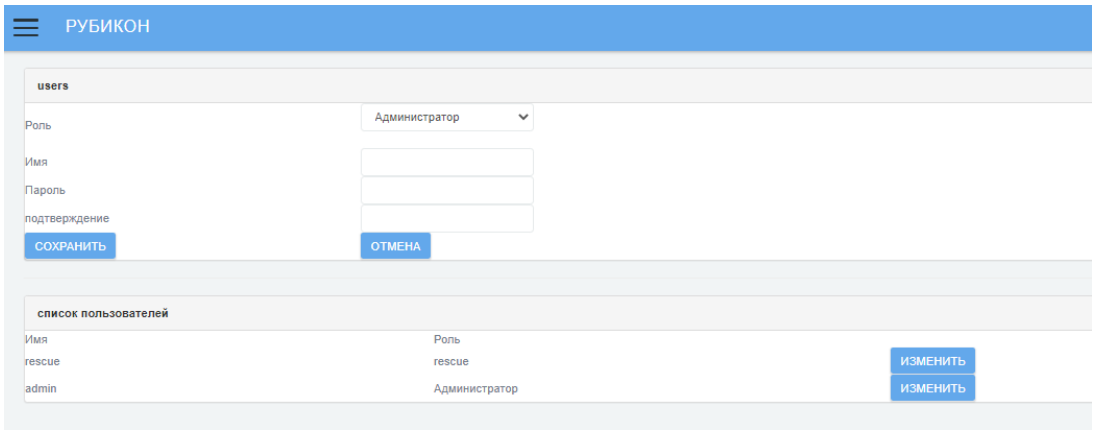


Рисунок 5 - Раздел «Система → Пользователи»

После выполнения указанных выше шагов пользователь с полномочиями администратора будет перенаправлен на стартовую страницу.

4.4 Роли

КП ПАВ «Рубикон» поддерживает следующие роли:

1) администратор - имеет доступ к просмотру веб-интерфейса и настройке КП ПАВ «Рубикон»;

2) аудитор - имеет доступ к просмотру веб-интерфейса, информации о конфигурации системы и журнальной информации, без возможности внесения изменений в настройки КП ПАВ «Рубикон»;

3) пользователь - не имеет доступа к просмотру веб-интерфейса (кроме стартовой страницы) и страницы установки соединения. Параметр IP-адрес при первоначальной установке имеет значение 192.168.1.1 и может быть изменен администратором. На странице установки соединения после нажатия кнопки «Установить соединение» КП ПАВ «Рубикон» фиксирует IP-адрес пользователя и предоставляет соответствующие правила, назначенные данному пользователю администратором на странице «Межсетевой экран → Правила межсетевого экрана»;

4) специальная роль «rescue» – используется для доступа с целью восстановления паролей и файла конфигурации через консоль восстановления при потерях паролей и

сбоях работы. По умолчанию: логин: «rescue»; пароль: «rescue». Пароль рекомендуется заменить при первой настройке КП ПАВ «Рубикон».

Для того чтобы добавить новых пользователей в разделе «Система → Пользователи» в ниспадающем списке «role» выберите роль (администратор, аудитор, пользователь), а затем заполните следующие текстовые поля (рисунок 6):

– «Имя»;

– «Пароль»;

– «Подтверждение».

Далее нажмите кнопку «Сохранить».

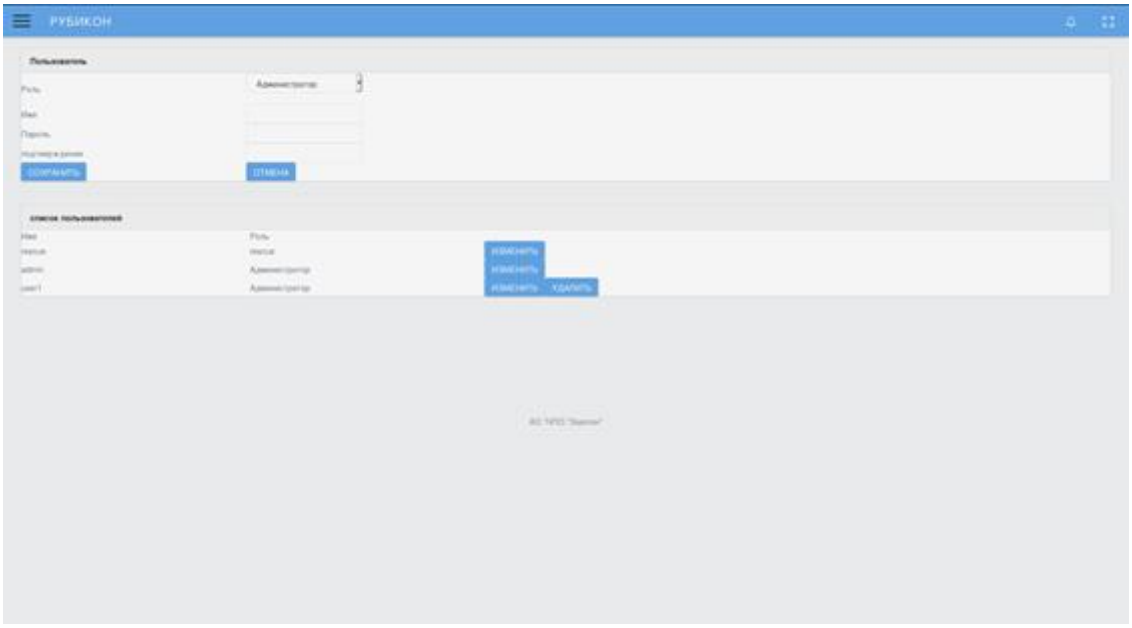


Рисунок 6 – Добавление пользователя

Список пользователей можно посмотреть в секции «список пользователей». При необходимости, можно удалить пользователя, нажав на кнопку «Удалить» напротив имени соответствующего пользователя.

Для работы с КП ПАВ «Рубикон» получите ваш логин и пароль у администратора.

4.5 О программе

После успешного прохождения процедуры авторизации администратор может просмотреть сведения о КП ПАВ «Рубикон» (версию, производителя и т.п.), перейдя в меню «Система → О программе» (рисунок 7).

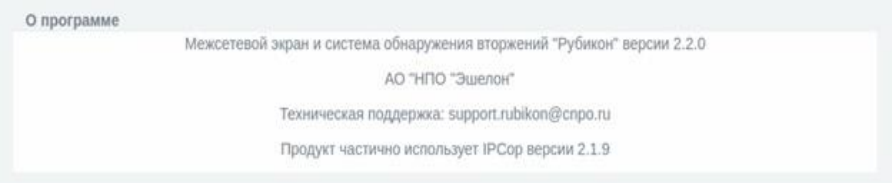


Рисунок 7 - Раздел «Система → О программе»

5 СЕТЕВЫЕ НАСТРОЙКИ

5.1 Общие положения

В зависимости от используемых функций в комплексе «Рубикон» предусмотрены следующие типы физических сетевых интерфейсов:

1) «красный»: сетевой интерфейс, подключаемый к внешней сети. По умолчанию все пакеты, маршрутизируемые с красного интерфейса на зеленый (кроме пакетов, принадлежащих открытым TCP-сессиям), блокируются межсетевым экраном. На красном интерфейсе происходит трансляция (преобразование) сетевых адресов: при прохождении пакета в «красную» сеть происходит замена адреса источника пакета, а при прохождении пакета из «красной» сети для установленных соединений происходит замена адреса назначения в соответствии с таблицей состояния соединений;

2) «зеленый»: сетевой интерфейс, подключаемый к внутренней сети. По умолчанию все пакеты, маршрутизируемые между различными зелеными интерфейсами, не блокируются;

3) «синий»: для этого интерфейса включен режим «белого списка», т.е. запрещены как входящие, так и перенаправляемые пакеты от всех адресов, кроме специально разрешенных на странице «МЭ → Доступ к синему интерфейсу».

4) «оранжевый»: демилитаризованная зона. По умолчанию все пакеты, маршрутизируемые с оранжевого интерфейса на зеленый (кроме пакетов, принадлежащих открытым TCP-сессиям), блокируются. При этом возможна настройка проброса портов с красного интерфейса на оранжевый (замена адреса (и порта) назначения для пакетов, приходящих на «красный» интерфейс на адрес (и порт) конкретного узла в «оранжевой» сети) для обеспечения работоспособности внешних сервисов.

Каждому интерфейсу можно назначить одну из следующих политик (таблица 2).

Таблица 2 - Доступность политики в зависимости от цвета интерфейса

Интерфейс	**Политика**		
	Закрыто	**Полуоткрыто**	**Открыто**
Зеленый	✓	✓	✓
Голубой	✓	✓	✓
Оранжевый	✓	×	✓
Красный	✓	×	×

В таблице 3 приведено описание правил, создаваемых по умолчанию при применении каждой из политик.

Таблица 3 - Описание сетевых политик

Тип правила	Политика		
	Закрыто	Полуоткрыто	Открыто
Входящее	Все соединения запрещены	DNS, DHCP, NTP, ICMP, Proxy	DNS, DHCP, NTP, ICMP, Proxy
Перенаправление	Разрешен доступ в сеть	Разрешен доступ в сеть	Разрешен доступ в сеть и из сети
Исходящее	Доступ разрешен	Доступ разрешен	Доступ разрешен

Примечание - Если в вашей сети используются статические IP-адреса или уже установлен DHCP сервер, то необходимо отключить его в настройках КП ПАВ «Рубикон».

Примечание - Если при установке новой сетевой карты в аппаратную платформу КП ПАВ «Рубикон» не был найден драйвер сетевой карты (или она была установлена позже), то интерфейсы этой карты отобразятся в веб-интерфейсе под именами eth"n", где "n" является номером интерфейса. В случае возникновения подобной ситуации обратитесь в техническую службу поддержки.

5.2 Назначение цветов интерфейсов

По умолчанию все физические интерфейсы изделия «Рубикон» являются зелеными. Для переназначения цветов интерфейсов выполните следующие действия:

1) Откройте следующую страницу «МЭ → Настройки межсетевого экрана» (рисунок 8).

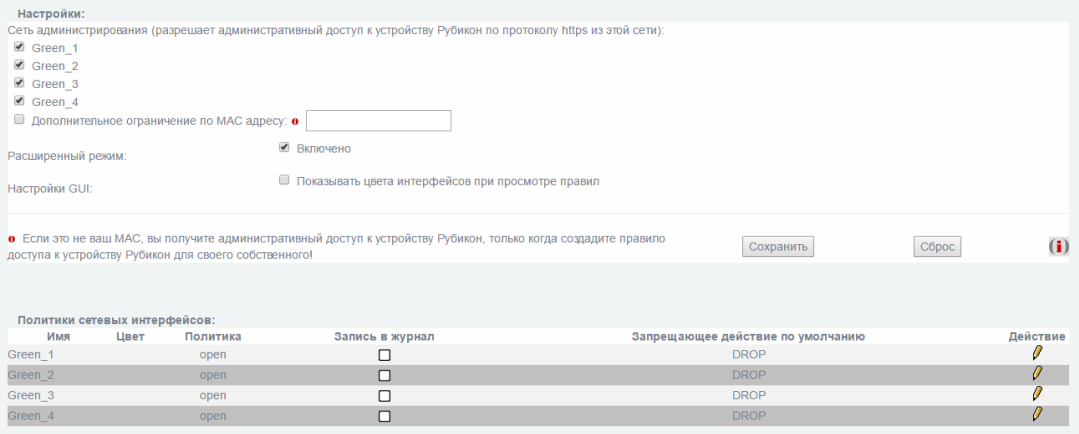


Рисунок 8 - Раздел «МЭ → Настройки межсетевого экрана»

2) по умолчанию первые четыре зеленых интерфейса помечены как административные, т.е. по ним разрешено администрирование КП ПАВ «Рубикон»; цвет таких интерфейсов изменить нельзя, поэтому перед назначением цветов настройте администрирование;

3) назначьте цвета интерфейсов на странице «Сеть → Настройка адаптеров» (рисунок 7), выполнив следующее:

4) назначьте цвета интерфейсов на странице «Сеть → Настройка адаптеров» (рисунок 9), выполнив следующее:

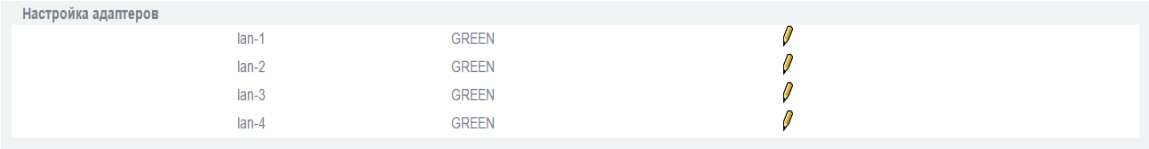


Рисунок 9 - Раздел «Сеть → Настройка адаптеров»

a) нажмите кнопку редактирования напротив требуемого интерфейса;

b) выберите цвет интерфейса;

c) нажмите кнопку редактирования, для сохранения настроек,

d) номера интерфейсов внутри цвета (например, GREEN 1, RED 2) назначаются в инкрементном порядке и не зависят от реальных имен интерфейсов;

e) настройте сетевые адреса для измененных интерфейсов в разделе «Система → Интерфейсы» (рисунок 10).

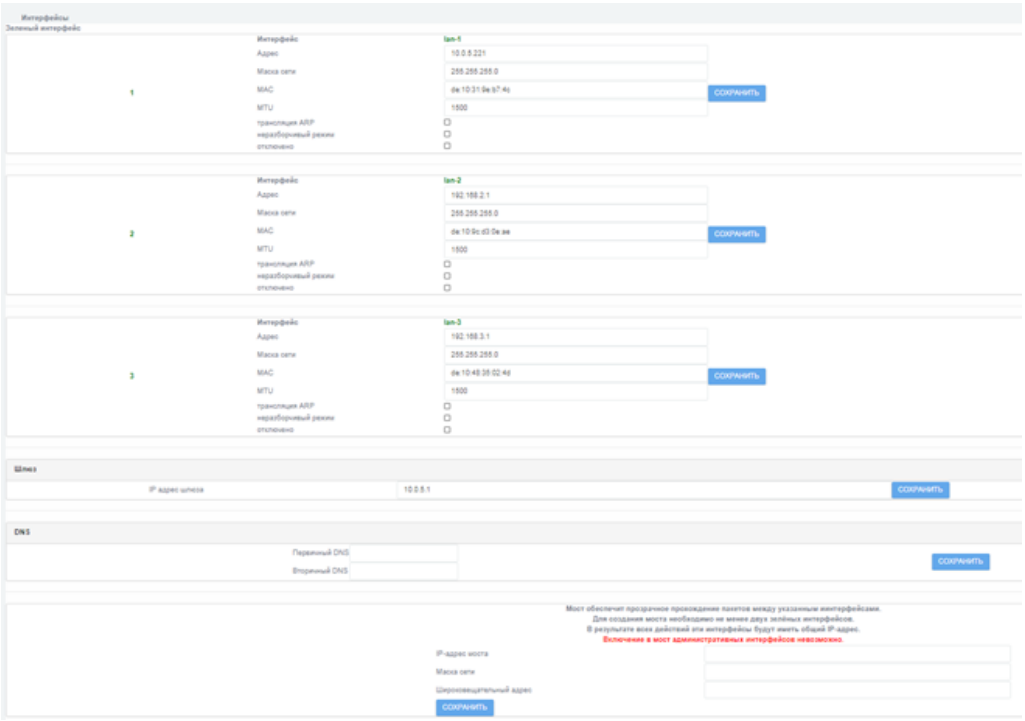


Рисунок 10 - Раздел «Система → Интерфейсы»

Раздел «Интерфейсы» предназначен для настройки сетевых интерфейсов и содержит следующие секции и поля в них:

1) «Интерфейсы»:

– «Интерфейс» - название и тип интерфейса;

– «Адрес» - IP адрес интерфейса;

– «Маска сети» - маска сети интерфейса;

– «MAC» - MAC адрес оборудования интерфейса;

– «MTU» - максимальный размер пакета, передаваемого по сетям;

– «трансляция ARP» - включение трансляции протокола, предназначенного для определения MAC-адреса интерфейса по известному IP-адресу интерфейса;

– «неразборчивый режим» - включение режима приема всех сетевых пакетов, появляющихся на сетевом адаптере независимо от назначения;

– «отключено» - отключение интерфейса;

2) «Шлюз»: «IP адрес шлюза» - IP адрес шлюза;

3) «DNS»:

– «Первичный DNS» - IP адрес первичного DNS-сервера;

– «Вторичный DNS» - IP адрес вторичного DNS-сервера.

Существует возможность отключения сетевого интерфейса установкой флажка «отключено» для данного интерфейса. При этом невозможно отключить сетевой интерфейс, входящий в группу административных.

Изменить список административных интерфейсов можно на странице «Межсетевой экран → Настройки межсетевого экрана».

5.3 Ограничение трафика

Раздел «Ограничение Трафика» предназначен для ограничения трафика по определенным интерфейсам и для выставления приоритета трафика для служб и содержит следующие секции:

1) «Настройки» - предназначена для настройки ограничения трафика по указанным интерфейсам и содержит следующие поля:

– «Скорость исходящих соединений (кбит/сек)» - параметр устанавливает скорость исходящих соединений;

– «Скорость входящих соединений (кбит/сек)» - параметр устанавливает скорость входящих соединений;

2) «Ограничение трафика по интерфейсам» - перечень ограничений трафика, распределяется по параметрам «Интерфейс», «Скорость исходящих соединений (кбит/сек)», «Скорость входящих соединений (кбит/сек)». Для удаления ограничения трафика необходимо нажать на иконку удаления.

3) «Изменить службу» содержит следующие поля:

– ниспадающий список «Приоритет» - выставляет приоритет для службы. Приоритеты назначаются статически в зависимости от установленных значений ограничения исходящего трафика: «Высокий» - 80 % от ограничения исходящего трафика, «Средний» - 60 % и «Низкий» - 40%;

– «Адрес» - адрес выбираемой службы;

– «Служба» - имя выбираемой службы;

– ниспадающий список «TCP» - выбор сетевого протокола.

4) «Список приоритетов трафика» - перечень ограничений трафика с приоритетами, распределяется по параметрам «Интерфейс», «Приоритет», «Адрес», «Служба», «Протокол». Для удаления ограничения трафика необходимо нажать на иконку удаления.

Примечание - Для настройки приоритетов трафика необходимо выставить ограничение входящего и исходящего трафика.

В разделе «Службы → Ограничение трафика» установите ограничение скорости для входящих и исходящих соединений (рисунок 11).

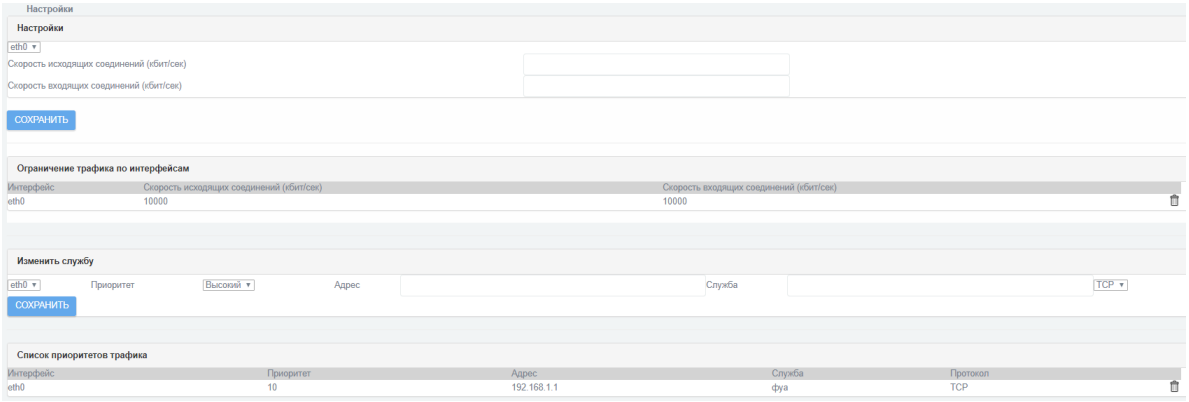


Рисунок 11 - Раздел «Службы → Ограничение трафика»

В секции «Настройки» выполните следующие действия:

1) выберите имя интерфейса в ниспадающем списке;

2) заполните текстовое поле «Скорость исходящих соединений (кбит/сек)»;

3) заполните текстовое поле «Скорость входящих соединений (кбит/сек)»;

4) нажмите кнопку «Сохранить».

В секции «Изменить службу» настройте приоритеты трафика (рисунок 11), для этого выполните следующие действия:

1) выберите имя интерфейса в ниспадающем списке;

2) выберите «Приоритет» в ниспадающем списке - высокий, средний или низкий;

3) заполните текстовое поле «Адрес»;

4) заполните текстовое поле «Служба»;

5) в ниспадающем списке выберите протокол TCP или UDP.

6) нажмите кнопку «Сохранить».

6 МЕЖСЕТЕВОЙ ЭКРАН

6.1 Общие положения

В КП ПАВ «Рубикон» за каждым сетевым интерфейсом закреплена определенная роль или набор особенностей взаимодействия с сетью и другими интерфейсами. Каждая роль или каждый сегмент сети определяется цветом: зеленый, красный, синий и оранжевый. Правила МЭ прикрепляются к имени интерфейса (например, GREEN 1), поэтому после каждой смены ролей интерфейсов (см. 5.2) необходимо перенастраивать правила МЭ в соответствии с текущими параметрами. Подробнее о настройке сетевых интерфейсов рассказано в разделе 5.

6.2 Настройка фильтрации пакетов

Фильтрация пакетов применяется для создания правил прохождения пакетов из зеленой сети в красную, синюю, оранжевую, организации взаимодействия между физическими и виртуальными сетями, а также для настройки административного доступа к КП ПАВ «Рубикон».

Для настройки фильтрации пакетов выполните следующие действия:

1) настройте сетевые интерфейсы;

2) перейдите на страницу настройки: «МЭ → Настройки межсетевого экрана» (рисунок 6);

3) в разделе «Расширенный режим» поставьте галочку напротив пункта «Включено»;

4) нажмите кнопку «Сохранить»;

5) перейдите на страницу «МЭ → Службы». В данном разделе можно создать свою службу, а можно посмотреть какие существуют службы по умолчанию.

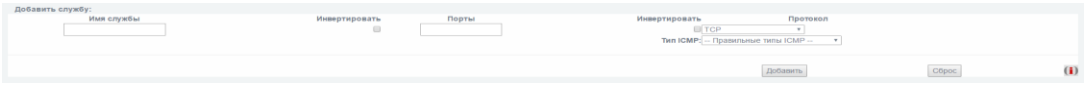


Рисунок 12 - Раздел «МЭ → Службы»

Для того, чтобы добавить свою службу для МЭ заполните следующее (рисунок 12):

– в текстовом поле «Имя службы» напишите имя службы;

– в текстовом поле «Порты» укажите номер порта, инвертируйте при необходимости;

– в ниспадающем списке «Протокол» выберите протокол, который будет использоваться, инвертируйте при необходимости;

– в ниспадающем списке «Тип ICMP» выберите тип ICMP (из ниспадающего списка «Правильные типы ICMP»);

6) нажмите кнопку «Добавить»;

7) перейдите на страницу настройки правил фильтрации «МЭ → Правила межсетевого экрана» (рисунок 13);

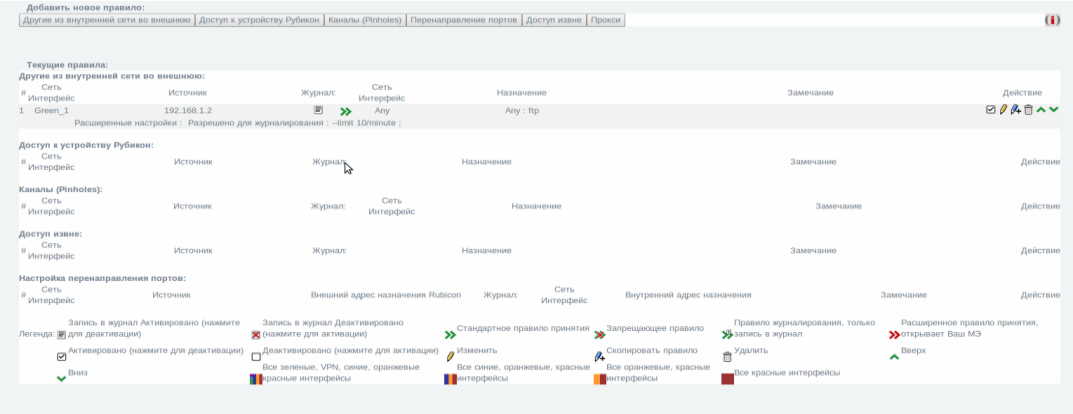


Рисунок 13 - Раздел «МЭ → Правила межсетевого экрана»

В данном разделе можно увидеть текущие правила. Текущие правила можно изменять, копировать, удалять, перемещать, активировать и деактивировать. Легенда указана внизу раздела.

8) выберите действие «Другие из внутренней сети во внешнюю»;

9) создайте правило (см. разделы 6.2.1-6.2.8);

10) перед тем, как сохранить и применить правило, нажмите кнопку «Далее» для предварительного просмотра (рисунок 14);

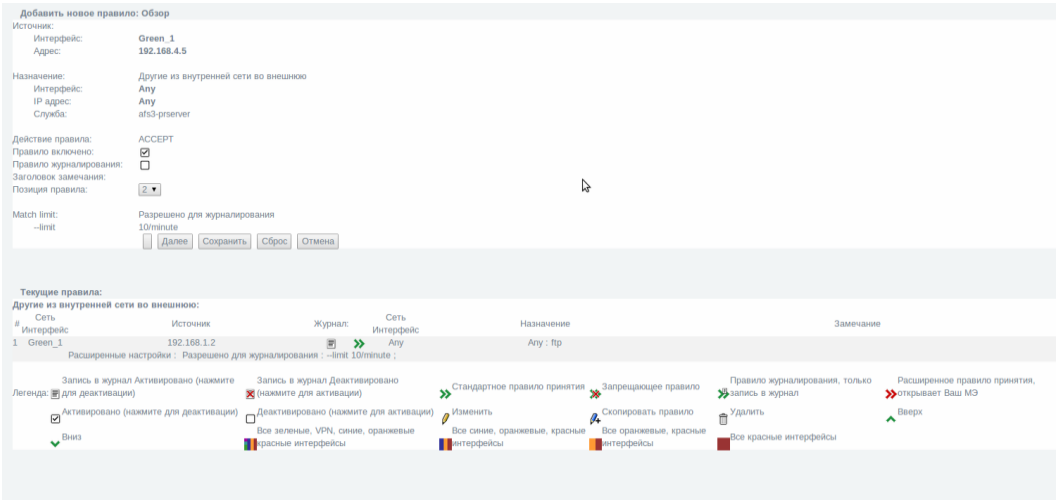


Рисунок 14 - Предварительный просмотр правила

Здесь вы можете сбросить настройки и перейти на предыдущую страницу, нажав кнопку «Сброс», или уйти со страницы интерфейса, нажав кнопку «Отмена».

11) откорректируйте параметры правила при необходимости;

12) нажмите кнопку «Сохранить», чтобы сохранить параметры и включить правила.

6.2.1 Фильтрация по сетевому адресу отправителя

В разделе «Другие из внутренней сети во внешнюю → Источник» (рисунок 15):

1) поставьте переключатель в пункт меню «Формат адреса»;

2) в ниспадающем списке выберите значение «IP»;

3) в текстовом поле «Адрес источника (MAC или IP или сеть)» укажите IP-адрес отправителя.

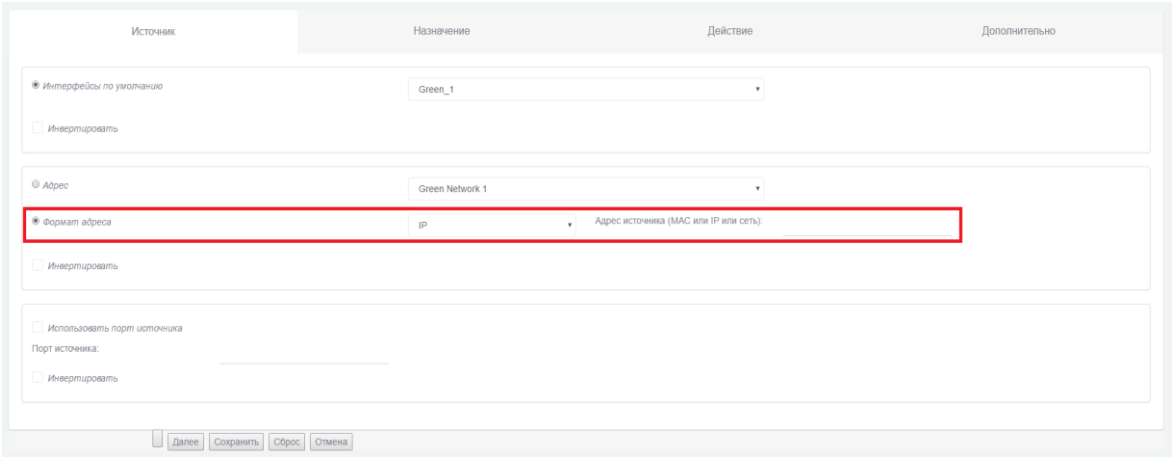


Рисунок 15 - Раздел «Источник»

6.2.2 Фильтрация по сетевому адресу получателя

В разделе «Другие из внутренней сети во внешнюю → Назначение» (рисунок 16):

1) поставьте переключатель в пункт меню «IP или сеть назначения»;

2) в текстовом поле укажите IP-адрес получателя.

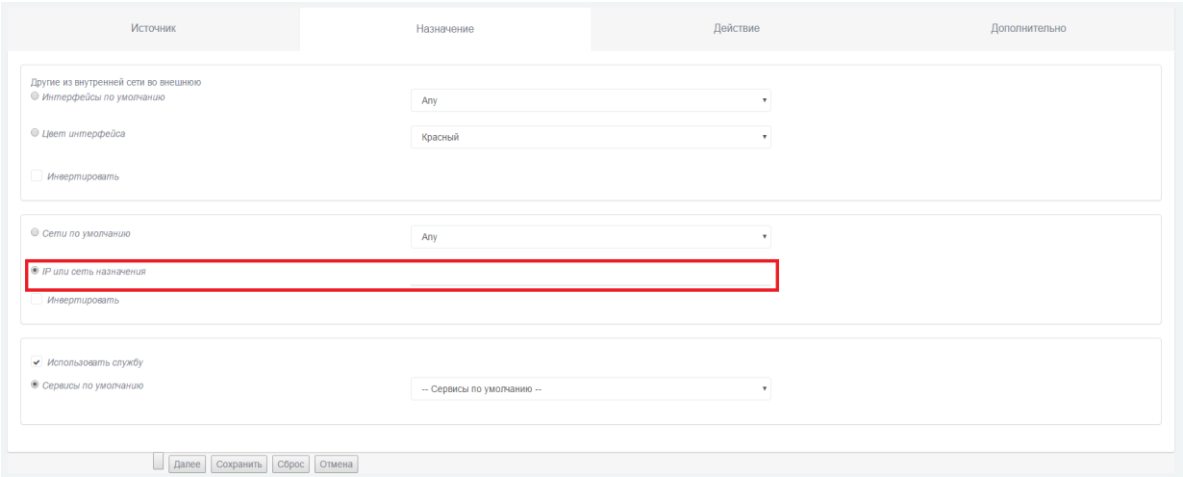


Рисунок 16 - Раздел «Назначение»

6.2.3 Фильтрация по сетевому протоколу

В разделе «Другие из внутренней сети во внешнюю → Назначение» (рисунок 17):

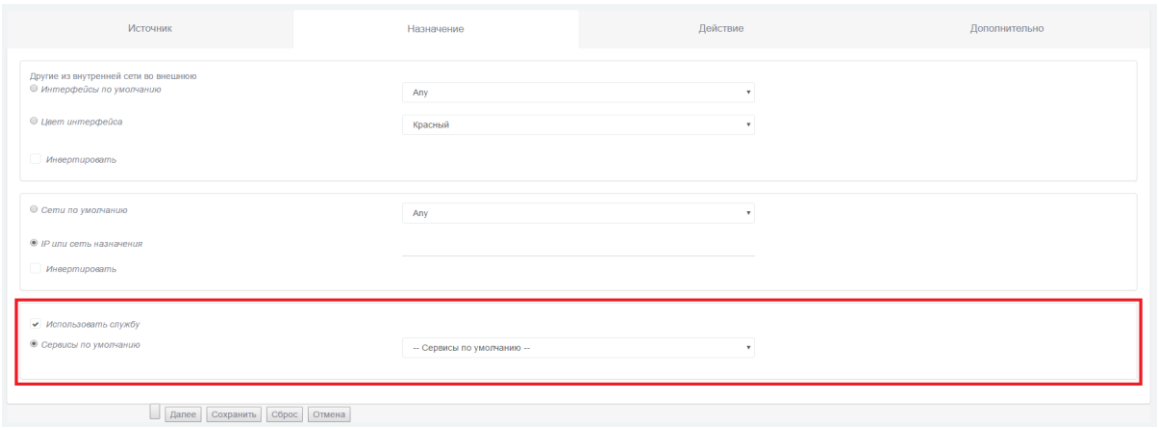


Рисунок 17 - Раздел «Назначение»

1) поставьте галочку напротив пункта «Использовать службу»;

2) поставьте переключатель в меню «Свои сервисы» или «Сервисы по умолчанию» в зависимости от того какую службу вы собираетесь выбрать;

3) в ниспадающем списке выберите службу, использующую сетевой протокол, по которому планируется осуществление фильтрации;

Например: выберите службу по умолчанию Ping. Служба Ping работает по сетевому протоколу ICMP.

6.2.4 Фильтрация по направлению пакета

Фильтрация по направлению пакета выполняется следующим образом:

1) заполните поля правила в разделе «Другие из внутренней сети во внешнюю → Источник» — для входящего пакета (рисунок 15);

2) заполните поля правила в разделе «Другие из внутренней сети во внешнюю → Назначение» — для исходящего пакета (рисунок 16).

6.2.5 Фильтрация по транспортному протоколу

В разделе «Другие из внутренней сети во внешнюю → Назначение» (рисунок 17):

1) поставьте галочку напротив пункта «Использовать службу»;

2) поставьте переключатель в меню «Свои сервисы» или «Сервисы по умолчанию» в зависимости от того какую службу вы собираетесь выбрать;

3) в ниспадающем списке выберите службу, использующую транспортный протокол, по которому планируется осуществление фильтрации.

Например: выберите службу по умолчанию domain. Служба DNS использует транспортный протокол UDP.

6.2.6 Фильтрация по портам источника и получателя

Фильтрация по портам источника и получателя выполняется следующим образом:

1) по портам источника — в разделе «Другие из внутренней сети во внешнюю → Источник» (рисунок 18):

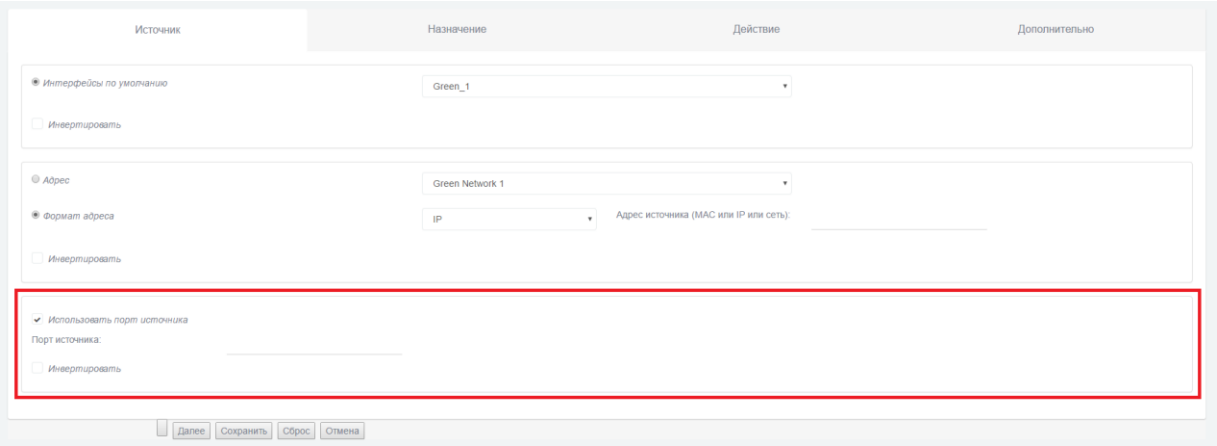


Рисунок 18 - Раздел «Источник»

Данный режим позволяет указывать порт, с которого поступают сетевые пакеты. Применяется в том случае, когда необходимо фильтровать ответные пакеты от сетевых сервисов (http-, ftp- серверы и т.п.), при этом порт назначения может не указываться, так как чаще всего он выбирается произвольно:

a) поставьте галочку напротив пункта «Использовать порт источника»,

b) в текстовом поле укажите порт источника, инвертируйте при необходимости.

2) По портам назначения — в разделе «Назначение»:

a) поставьте галочку напротив пункта «Использовать службу»,

b) поставьте переключатель в меню «Свои сервисы» или «Сервисы по умолчанию», в зависимости от того какую службу вы собираетесь выбрать.

c) в ниспадающем окне выберите необходимую службу.

Например, выберите службу по умолчанию https. Служба HTTPS использует порт 443.

6.2.7 Фильтрация по флагу фрагментации

В разделе «Другие из внутренней сети во внешнюю → Дополнительно → Фильтрация по маске (4 байта)» (рисунок 19):

1) поставьте галочку напротив пункта «Включить фильтрацию по битовой маске»;

2) если необходимо фильтровать фрагментированные пакеты:

a) в текстовом поле «смещение» укажите: «7»;

b) в текстовом поле «маска» укажите: «0xff000000»;

c) в текстовом поле «с» укажите: «0x00000000»;

d) в текстовом поле «по» укажите: «0x00000000»;

3) если необходимо фильтровать нефрагментированные пакеты:

a) в текстовом поле «смещение» укажите: «7»;

b) в текстовом поле «маска» укажите: «0xff000000»;

c) в текстовом поле «с» укажите: «0x01000000»;

d) в текстовом поле «по» укажите: «0x01000000».

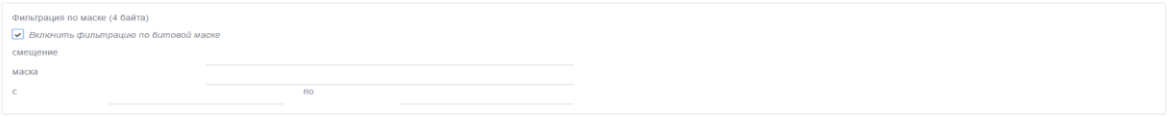


Рисунок 19 - Раздел «Фильтрация по маске» (4 байта)

6.2.8 Фильтрация по интерфейсу

На уровне сетевого адреса (рисунок 20):

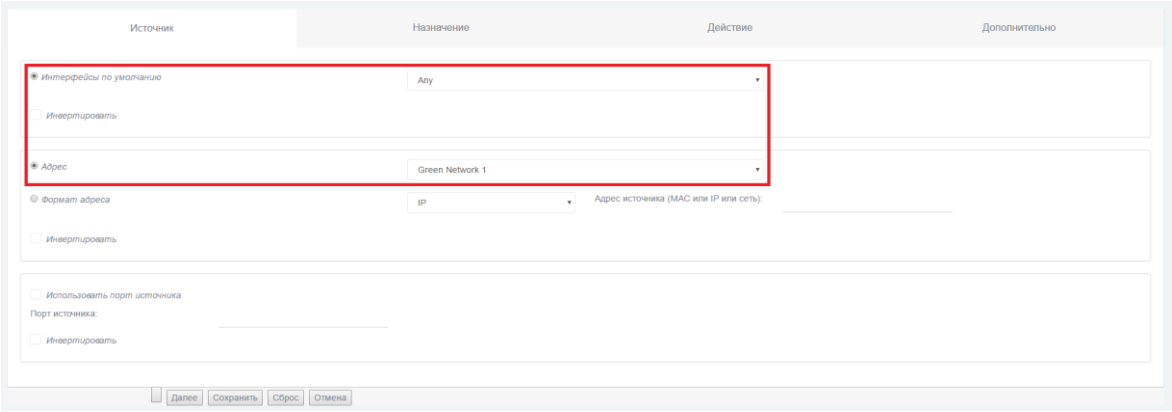


Рисунок 20 - Раздел «Доступ к устройству Рубикон → Источник»

1) на странице «МЭ → Правила межсетевого экрана» выберите действие «Доступ к устройству Рубикон»,

2) в разделе «Источник» поставьте переключатель в меню «Интерфейсы по умолчанию»,

3) в ниспадающем списке выберите значение «Any»,

4) поставьте переключатель в меню «Адрес»,

5) в ниспадающем списке выберите необходимое значение,

6) например, выберите сеть «Green network 1».

На уровне интерфейса (рисунок 21):

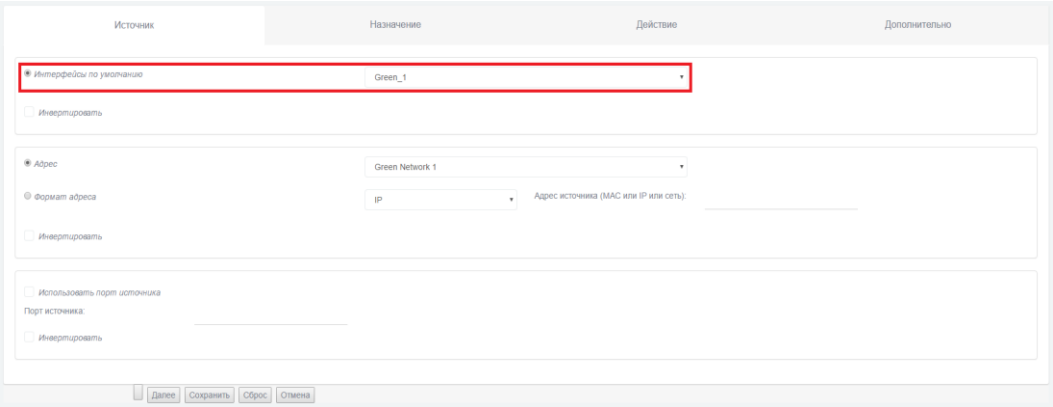


Рисунок 21 - Раздел «Доступ к устройству Рубикон → Источник»

1) на странице «МЭ → Правила межсетевого экрана» выберите действие «Доступ к устройству Рубикон»,

2) в разделе «Источник» поставьте переключатель в меню «Интерфейсы по умолчанию»;

3) в ниспадающем списке выберите необходимое значение, например, выберите интерфейс «GREEN_1».

Повторите действия пунктов 6.2.5-6.2.7.

6.3 Настройка прокси-сервера

Веб-прокси-сервер - это программа, которая делает запросы к веб-страницам от имени других компьютеров в сети. Прокси-сервер кэширует страницы, которые получает из интернета, поэтому если три пользователя запрашивают одну и ту же страницу, требуется только одна передача из сети Интернет. Если имеется ряд часто используемых веб-сайтов, это поможет сэкономить время на интернет-доступе.

6.3.1 FTP посредничество

Для того чтобы включить функции прокси-сервера в МЭ перейдите в раздел «Службы → FTP посредник» (рисунок 22).

– «enable ftp proxy» - поставьте соответствующий флажок, чтобы включить функции прокси-сервера в МЭ.

– «ftp proxy port» - введите порт, на котором прокси-сервер будет прослушивать запросы.

– «ftp blocked sequence» - введите последовательность FTP команд, которая будет блокироваться.

– нажмите кнопку «Сохранить».

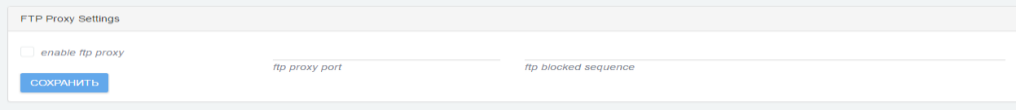


Рисунок 22 - Раздел «Службы → FTP посредник»

6.3.2 Сервисы безопасности FTP

Сервисы безопасности FTP дают возможность осуществлять проверку использования пользователем отдельных команд, их атрибутов безопасности и параметров.

Перейдите в раздел «Службы → FTP посредник» (рисунок 23):

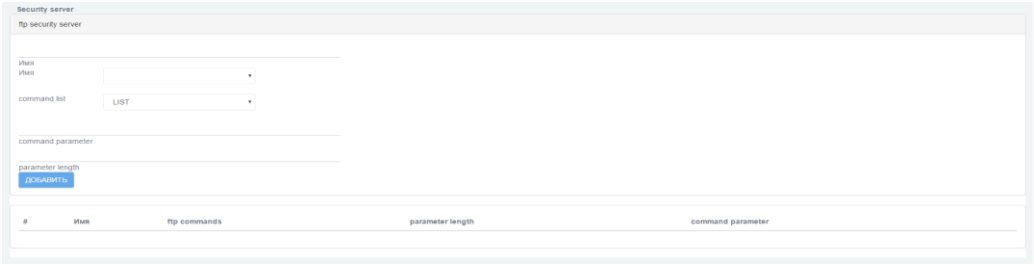


Рисунок 23 - Раздел «СОВ → ftp secsrv»

– «Имя» - укажите имя правила;

– «command list» - выберите команду из выпадающего списка;

– «command parameter» - укажите параметр, по которому будет происходить фильтрация;

– «parameter length» - укажите длину параметра;

– Нажмите кнопку «Добавить».

6.3.3 Веб-прокси

Перейдите в раздел «Службы → Прокси». Первая строка в данном разделе показывает, запущен или остановлен прокси-сервер (рисунок 24).

Секция «Настройки» разделена на три подсекции:

– общие параметры;

– прокси верхнего уровня;

– настройки журналирования.

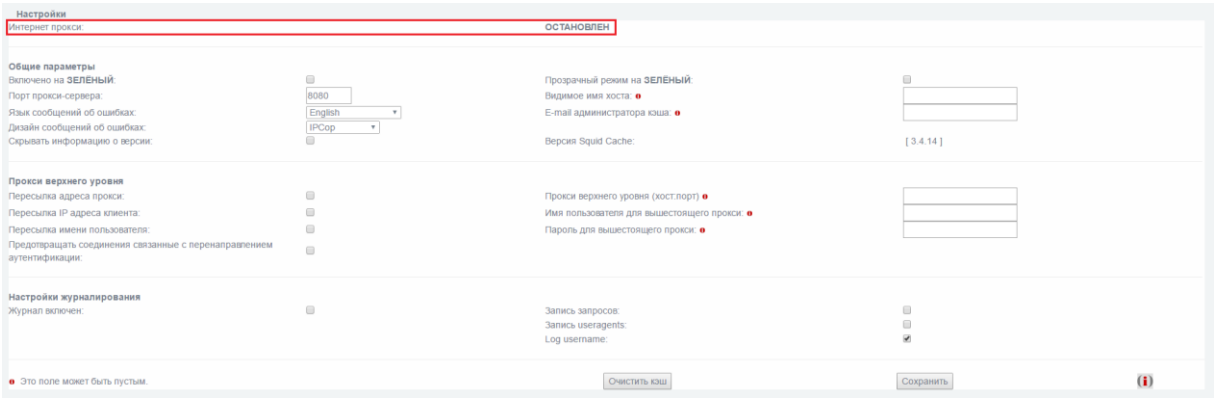


Рисунок 24 - Раздел «Службы → Прокси»

6.3.3.1 Общие параметры

Здесь вы можете настроить, чтобы прокси-запросы шли от вашей зеленой (частной) сети и/или синей (беспроводной) сети (если она установлена). Для этого отметьте соответствующие поля (рисунок 25):

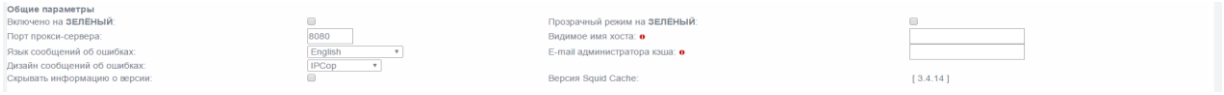


Рисунок 25 - Подсекция «Общие параметры»

– «Включено на ЗЕЛЕНЫЙ» поставьте соответствующий флажок, чтобы включить прокси-сервер для прослушивания запросов на выбранном интерфейсе (зеленый или синий). Если прокси-служба отключена, все клиентские запросы будут направлены непосредственно на адрес получателя.

– «Прозрачный режим на ЗЕЛЕНЫЙ» - если «прозрачный режим» включен, все запросы на 80 порту будут направлены к прокси-серверу без необходимости специальной настройки клиентов.

– «Порт прокси-сервера». Это порт, на котором прокси-сервер будет прослушивать запросы клиента. По умолчанию 8080. В прозрачном режиме, все клиентские запросы на 80 порту будут автоматически перенаправлены на этот порт.

– «Видимое имя хоста» - необязательное поле. Если вы хотите, чтобы клиентам отображалось другое имя в прокси-сообщениях об ошибках сервера, или для прокси-серверов верхнего уровня, то укажите его здесь. Если вы оставите это поле пустым, будет использоваться имя вашего КП ПАВ «Рубикон».

– «E-mail администратора кэша» - необязательное поле. Вы можете указать адрес электронной почты, который появляется клиентам в прокси-сообщениях об ошибках сервера. Если оставить его пустым, будет использоваться «веб-мастер».

– «Язык сообщений об ошибках». Вы можете выбрать язык, на котором прокси-сервер будет отображать сообщения об ошибках для клиентов.

– «Дизайн сообщений об ошибках». Вы можете выбрать дизайн, в котором сообщения об ошибках прокси-сервера отображаются на клиентах. Вы можете выбрать между «IPCop» и «Стандартный».

Дизайн «IPCop» включает хороший графический баннер, в то время как «Стандартный» дизайн обычно поставляется с Squid.

Примечание – В том случае, если определить «Видимое имя хоста», всегда будет использоваться «Стандартный» дизайн.

– «Скрывать информацию о версии». Отметьте этот флажок, чтобы предотвратить отображение версии Squid Cache в сообщениях об ошибках Squid клиентам.

– «Версия Squid Cache». Здесь отображаются установленные версии Squid Cache.

6.3.3.2 Прокси верхнего уровня

Эти параметры могут потребоваться в цепочке прокси окружения.

Если ваш провайдер требует использовать свой кэш для доступа к интернету, то укажите имя хоста и порт в текстовом поле «Прокси верхнего уровня». Если прокси вашего провайдера требует имя пользователя и пароль, заполните текстовые поля «Имя пользователя для вышестоящего прокси» и «Пароль для вышестоящего прокси» (рисунок 26):

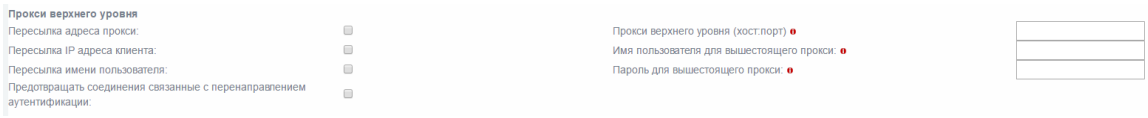


Рисунок 26 - Подсекция «Прокси верхнего уровня»

– «Пересылка адреса прокси». Включает HTTP VIA в поле заголовка. Если эта опция включена, эта информация будет добавлена к заголовку http.

Примечание - Если последний прокси в цепочке не удалит это поле, оно будет направлено на узел назначения!

Это поле будет скрыто по умолчанию.

– «Пересылка IP-адреса клиента». Включает HTTP X-FORWARDED-FOR в поле заголовка. Если эта опция включена, внутренний IP-адрес клиента будет добавлен к http-заголовку.

Это может пригодиться для источника ACL или входа на удаленный прокси-сервер.

Примечание - Если последний прокси в цепочке не удалит это поле, оно будет направлено на узел назначения.

Вместо того чтобы переслать «неизвестный», это поле будет полностью скрыто по умолчанию.

– «Пересылка имени пользователя». Если какой-либо тип аутентификации активирован, это поле позволит пересылать логин.

Это может пригодиться для пользователей на основе ACL или входа на удаленный прокси-сервер.

Примечание - Это работает для ACL или ведения журнала, и не работает, если вышестоящий прокси-сервер требует реального входа.

Эта пересылка ограничивается именем пользователя. Пароль не будет передан.

– «Предотвращать соединения связанные с перенаправлением аутентификации». Отключает пересылку Microsoft соединений, ориентированных на проверку подлинности (NTLM и Kerberos).

6.3.3.3 Настройки журналирования

– «Журнал включен». Если вы решите включить прокси, то можете также включить журнала веб-посещений, включив опцию «журнал включен». Это позволит прокси-серверу вести журнал системы, который может потребоваться для устранения неполадок (рисунок 27).

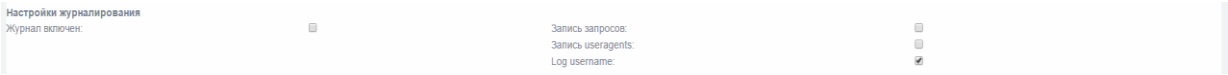


Рисунок 27 - Подсекция «Настройки журналирования»

Посещения через прокси можно увидеть, проверив прокси-логи веб-страницы. В журнале также включена поддержка прокси-графиков работы.

– «Запись запросов». Часть URL, содержащих динамические запросы будут удалены по умолчанию перед входом. Если включить опцию «запись запросов» то в журнале будет записан полный URL-адрес.

– «Запись useragents». Включение опции «запись useragents» позволит записывать строку useragent в лог файл /var/log/squid/user_agent.log. Этот параметр журнала используется только для отладки и результаты не отображаются графическим интерфейсом для просмотра журнала.

– «Log username». Включение опции «Log username» позволит записывать строку username в лог файл.

6.3.4 Расширенные настройки

Секция «Расширенные настройки» разделена на следующие подсекции:

- управление кэшем;
- порты назначения;
- контроль доступа по адресу;
- классные расширения;
- ограничение по времени;
- лимиты передачи;
- регулирование закачки;
- фильтр MIME типов;
- веб-браузер;
- конфиденциальность;
- redirectors;
- метод аутентификации.

6.3.4.1 Управление кэшем

Вы можете выбрать, сколько места на диске должно быть использовано для кэширования веб-страниц в разделе «Управление кэшем». Вы можете также установить размер самого маленького объекта в кэш от 0 до 4096 КБ (рисунок 28).

По причинам конфиденциальности, прокси не кэширует страницы, полученные через https или другие страницы, где имя пользователя и пароль передаются через URL-адрес.

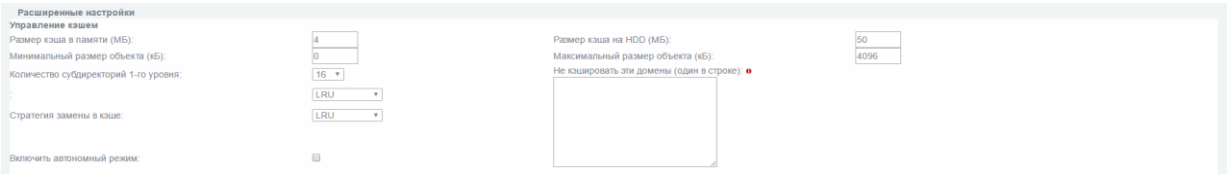


Рисунок 28 - Подсекция «Управление кэшем»

Примечание – Кэширование может занимать много места на вашем жестком диске. Если использовать большой кэш, то минимальный размер жесткого диска, указанный в документации, будет недостаточен.

Чем больше кэш вы выберете, тем больше памяти потребуется прокси-серверу для управления кэшем. Если вы работаете сейчас на машине с малым объемом памяти, не выбирайте большой кэш.

– «Размер кэша в памяти (Мб)» - это объем физической памяти, используемой для отрицательного кэширования и транзитных объектов. Это значение не должно превышать более 50% от установленной оперативной памяти. Минимальное значение составляет 1 МБ, по умолчанию 2 МБ.

Этот параметр не определяет максимальный размер процесса. Он только ставит ограничения на то, сколько дополнительной оперативной памяти будет использоваться прокси в качестве кэша объектов.

– «Размер кэша на HDD (Мб)» - это тот объем дискового пространства в мегабайтах, используемый для кэширования объектов. Значение по умолчанию - 50 Мб. Измените его в соответствии с вашей конфигурацией. Не указывайте здесь весь размер вашего диска. Вместо этого, если вы хотите Squid используйте 80% от вашего диска.

Если вы хотите настроить прокси-сервер без кэширования, выполните следующие действия:

Установите параметры «Размер кэша в памяти (Мб)» и «Размер кэша на HDD (Мб)» равными 0 Мб, чтобы полностью отключить кэширование.

– «Минимальный размер объекта (кБ)». Объекты меньше этого размера не будут сохранены на диске. Значение задается в килобайтах и по умолчанию равно 0 Кб, а это значит, что нет минимального значения.

– «Максимальный размер объекта (кБ)». Объекты больше этого размера не будут сохранены на диске. Значение задается в килобайтах и по умолчанию составляет 4 Кб. Если вы больше хотите увеличить скорость, чем сохранить пропускную способность, выйдите из этого минимума.

– «Количество субдиректорий 1-го уровня». Значение по умолчанию для кэша жесткого диска субдиректорий 1-го уровня равно 16.

Каждая директория 1-го уровня содержит 256 подкаталогов, поэтому значение 256 директорий 1-го уровня будет использовать в общей сложности 65536 директорий для кэша жесткого диска. Это значительно замедлит процесс запуска службы прокси, но может ускорить кэширование при определенных условиях.

Примечание - Рекомендуемое значение для 1-го уровня директорий равно 16. Увеличивайте это значение только тогда, когда это необходимо.

– «Стратегия замены в памяти». Параметр определяет, какие объекты удаляются из памяти, когда этого требует память. Политикой по умолчанию для замены в памяти является LRU.

Возможно изменение политики:

– «LRU»

Оригинальный список Squid, основанный на последней недавно использованной политике (Last Recently Used). Политика LRU хранит недавние ссылки на объекты. Например, он заменяет объекты, которые не использовались долгое время.

– «heap GDSF»

(The heap Greedy-Dual Size Frequency) политика оптимизирует объекты по скорости попаданий, сохраняя небольшие популярные объекты в кэше, потому что они имеют больший коэффициент попаданий. Она обеспечивает более низкий уровень совпадения байтов, чем LFUDA, так как она заменяет больше (возможно, популярных) объектов.

– «heap LFUDA»

(Least Frequently Used with Dinamic Aging) наименее часто использующиеся объекты с динамическим старением. Эта политика сохраняет популярные объекты в кэше независимо от коэффициента попаданий байтов, за счет скорости так как, один большой, популярный объект позволит предотвратить множество мелких, менее популярных объектов, которые не должны кэшироваться.

– «heap LRU»

(Last Recently Used policy implemented using a heap) Последняя недавно использованная политика, с использованием кучи. Работает как LRU, но отличается использованием кучи.

Примечание - При использовании политики замены LFUDA, значение параметра «Максимальный размер объекта (кБ)» должно быть больше размера по умолчанию 4096 КБ, чтобы максимизировать потенциальное улучшение скорости попадания байт реализованное LFUDA.

– «Стратегия замены в кэше». Замена параметра политики кэша решает, какие объекты останутся в кэше, а какие объекты будут исключены (заменены), чтобы создать пространство для новых объектов. Политикой по умолчанию для замены кэша является LRU.

– «Включить автономный режим». Включение этой опции позволит отключить проверку кэшированных объектов. Это дает доступ к более кэшированной информации (устаревшие кэшированные версии, с которыми исходный сервер уже соединился).

– «Не кэшировать эти домены» - необязательное поле. Список сайтов, запрос которых не может быть удовлетворен из кэша и ответ которых не кэшируется. Другими словами, используйте это, чтобы объекты не кэшировались.

6.3.4.2 Порты назначения

В этих полях содержатся списки разрешенных стандартных портов для http и зашифрованных SSL портов для https-запросов.

Порты могут быть определены как единый номер порта или как диапазон портов (рисунок 29).

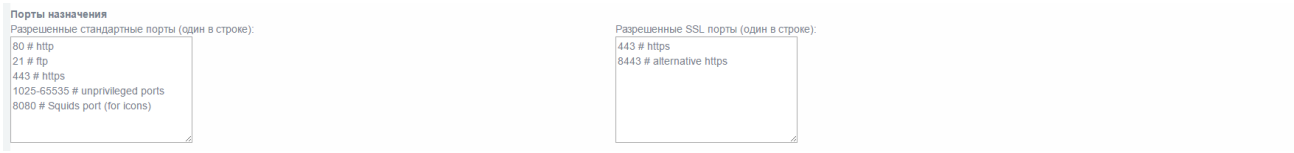


Рисунок 29 - Подсекция «Порты назначения»

6.3.4.3 Контроль доступа по адресу

Здесь можно контролировать доступ к прокси-серверу на основе сетевого адреса клиента (рисунок 30):

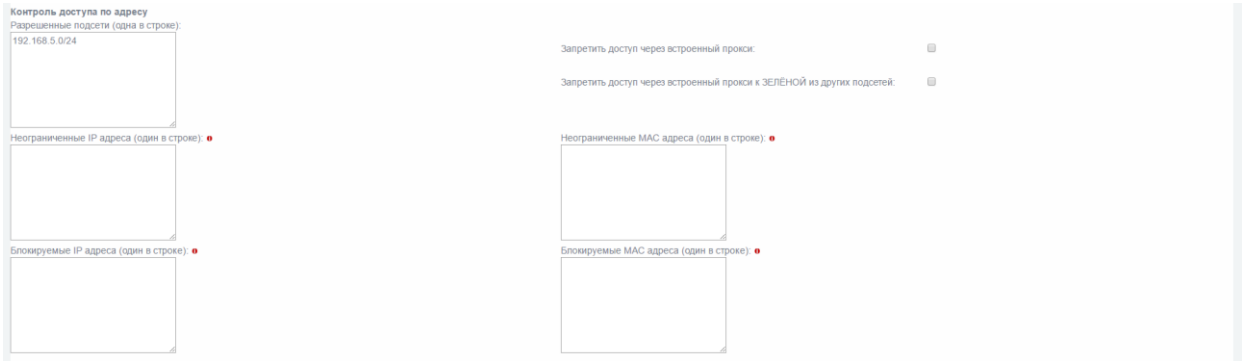


Рисунок 30 - Подсекция «Контроль доступа по адресу»

– «Разрешенные подсети». Для всех перечисленных подсетей разрешен доступ к прокси-серверу. По умолчанию зеленые и синие (если имеются) подсети перечислены здесь.

Вы можете добавить другие подсети, например, подсети за зелеными подсетями в крупных средах, в этот список. Доступ в интернет будет заблокирован для всех подсетей, которые здесь не перечислены.

– «Запретить доступ через встроенный прокси». Этот параметр предотвращает прямой доступ к http через встроенный прокси для локальных веб-серверов, в подсетях, определенных выше. Этот выбор переопределяет следующие два параметра, которые управляют доступом по протоколу http к зеленой подсети из синей подсети.

– «Запретить доступ через встроенный прокси к ЗЕЛЁНОЙ из других подсетей». Этот параметр предотвращает прямой http доступ через встроенный прокси веб-сервера к зеленой подсети из любой другой подсети (например, синей).

Например, пока разрешен доступ через встроенный прокси к зеленой и синей подсетям, все запросы, как правило, будут пересылаться на красную подсеть. Но если клиент из синей подсети хочет получить доступ к веб-серверу из зеленой подсети, встроенный прокси-сервер найдет короткий путь между синим и зеленым интерфейсом, независимо от правил МЭ.

Примечание - Для защиты вашего сервера, находящегося в зеленой подсети, рекомендуется включить эту опцию и использовать фильтр адресов или ДМЗ при необходимости.

– «Неограниченные IP-адреса» - необязательное поле. Для всех клиентских IP-адресов в этом списке будет переопределены следующие ограничения:

1) ограничения времени;

2) предельные размеры для запросов на загрузку;

3) регулирование загрузки;

4) проверка браузера;

5) фильтр MIME типов;

6) аутентификация (требуется по умолчанию для данных адресов, но может быть отключена);

7) одновременный вход одного пользователя на разных ЭВМ (доступно, только если включена проверка подлинности).

– «Неограниченные MAC-адреса» - необязательное поле. Для всех MAC-адресов клиентов в этом списке будет переопределены следующие ограничения:

1) ограничения времени;

2) предельные размеры для запросов на загрузку;

3) регулирование загрузки;

4) проверка браузера;

5) фильтр MIME типов;

6) аутентификация (требуется по умолчанию для данных адресов, но может быть отключена);

7) одновременный вход одного пользователя на разных ЭВМ (доступно, только если включена проверка подлинности).

Примечание - Прокси-сервер может определить MAC-адреса клиентов, настроенных для подсетей зеленых, синих или оранжевых интерфейсов.

– «Блокируемые IP-адреса» - необязательное поле. Все запросы от клиентов (IP-адресов или подсетей), перечисленные здесь, будут заблокированы.

– «Блокируемые MAC-адреса» - необязательное поле. Все запросы от клиентов в этом списке будут заблокированы.

6.3.4.4 Классные расширения

Классные расширения (ClassRoom Extensions) для прокси-сервера дают возможность делегировать административные задачи, чтобы пользователи без административных прав могли управлять веб-доступом через отдельную страницу (рисунок 31).

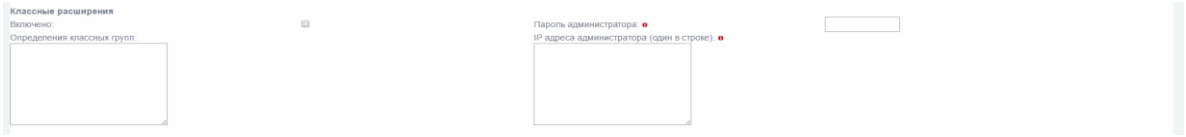


Рисунок 31 - Подсекция «Классные расширения»

– «Включено». Установите этот флажок, чтобы включить административный интерфейс управления веб-доступом.

– «Пароль администратора» - необязательное поле. Если этот пароль установлен, введите пароль для управления веб-доступом. Это необязательно, но по соображениям безопасности, либо установите пароль администратора, либо определите IP-адреса администратора.

– «IP-адреса администратора» - необязательное поле. Это поле позволяет определить IP-адреса, которые смогут управлять веб-доступом. Это необязательный элемент конфигурации, который может быть использован для повышения безопасности и упрощения управления, если вы не хотите, настраивать пароль администратора.

Высокий уровень безопасности достигается в том случае, если установлен пароль администратора, и IP ограничения, как будет описано ниже в разделе - уровни безопасности.

– «Определения классных групп» - определения классных групп вводятся в это поле. Определение классных групп имеют следующий формат:

```
[groupname]
client MAC address or client IP address or IP range or IP subnet
client MAC address or client IP address or IP range or IP subnet
```

```
client MAC address or client IP address or IP range or IP subnet
```

Ниже приведены примеры таких групп:

```
[Example group 1]
192.168.1.11
192.168.1.12
192.168.1.13
[Example group 2]
192.168.1.21-192.168.1.25
```

Каждая группа имеет уникальное имя. Имя группы заключено в квадратные скобки. Это имя будет отображаться в интерфейсе управления веб-доступом.

Каждая группа может иметь неограниченное количество адресов клиентов. Можно использовать смешанные адреса клиента в группе, но каждый адрес должен быть в одной строке. Вот некоторые примеры:

– один хост - MAC-адрес

```
01:23:45:67:89:0A
```

– один хост - IP-адрес

```
192.168.1.11
```

– диапазон хостов

```
192.168.1.21-192.168.1.25
```

– подсеть (обозначение маски подсети)

```
192.168.1.32/255.255.255.240
```

– подсеть (обозначение CIDR)

```
192.168.1.32/28
```

Уровни безопасности классных расширений:

– уровень 1: нет пароля, нет ограничения на IP-адреса - нет защиты. Все клиенты могут управлять веб-доступом без каких-либо ограничений. Не рекомендуется для рабочих сред.

Примечание – Рекомендуется использовать первый уровень только для отладки и тестирования.

– уровень 2: установлен пароль, нет ограничения на IP-адреса - низкий уровень защиты. Все клиенты могут управлять веб-доступом, но требуется пароль, для сохранения

изменений. Данный уровень безопасности рекомендуется в среде без специального компьютера администратора.

– уровень 3: нет пароля, установлены IP ограничения - низкий уровень безопасности. Все перечисленные клиенты могут изменять настройки веб-доступа. Клиенты идентифицируются по их IP-адресу, для сохранения изменений пароль не требуется.

Примечание - Если IP-адрес клиента не указан в списке, интерфейс управления веб-доступом появится в режиме «только для просмотра».

– уровень 4: установлен пароль и IP ограничения - высокий уровень безопасности. Самый высокий уровень безопасности для интерфейса управления веб-доступом. Только перечисленные клиенты могут изменять параметры, требуется пароль для сохранения изменений.

Примечание - Если IP-адрес клиента не указан в списке, интерфейс управления веб-доступом появится в режиме «только для просмотра».

6.3.4.5 Ограничения по времени

Эта подсекция определяет время активности веб-прокси. По умолчанию используется, для обеспечения доступа 24 часа в сутки, 7 дней в неделю (рисунок 32).

Рисунок 32 - Подсекция «Ограничения по времени»

Опция «Разрешить» разрешает веб-доступ, а опция «Запретить» блокирует веб-доступ в пределах выбранного периода времени. От выбора между «Разрешить» или «Запретить» будет зависеть время действия правила, которое вы хотите применить.

Временные ограничения не будут влиять на следующих клиентов:

– неограниченные IP-адреса;

– неограниченные MAC адреса;

– члены группы «Расширенный», если прокси-сервер использует «Локальную аутентификацию».

6.3.4.6 Лимиты передачи

Эта подсекция позволяет ввести ограничения на размер каждого скачанного и/или загруженного запроса. Значения приведены в килобайтах (КБ). Вы можете использовать данную подсекцию, чтобы запретить пользователям загружать большие файлы, из-за которых замедлится доступ в интернет для всех остальных пользователей (рисунок 33).

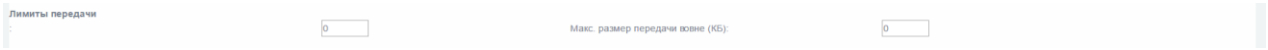


Рисунок 33 - Подсекция «Лимиты передачи»

Установите «Максимальный размер файла» и «Максимальный размер передачи вовне (КБ)». По умолчанию стоит «0», чтобы снять все ограничения.

Ограничения загрузки не коснутся следующих клиентов:

– неограниченные IP-адресов;

– неограниченные MAC-адресов;

– члены группы «Расширенный», если прокси-сервер использует «Локальную аутентификацию».

6.3.4.7 Регулирование закачки

Трафик загрузки может быть не ограничен, или ограничен для зеленого или синего интерфейса и/или хоста на основе типа содержимого (рисунок 34).

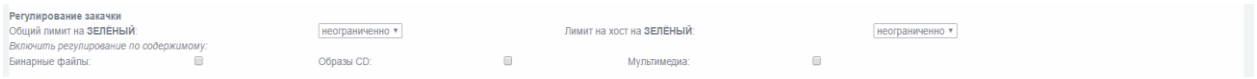


Рисунок 34 - Подсекция «Регулирование закачки»

Регулирование не повлияет на следующих клиентов:

– неограниченные IP-адреса;

– неограниченные MAC-адреса.

Ограничение трафика может быть определено для зеленого или синего интерфейса в качестве общего лимита, и для каждого узла. Используемый трафик для всех хостов будет ограничен общим лимитом.

По умолчанию, регулирование затрагивает все виды трафика, но регулирование может быть ограничено определенными типами контента. Однако это отключает регулирование для других типов контента.

Регулирование контента может быть применено к:

– бинарным файлам: bz2, bin, dmg, exe, sea, tar, tgz, zip и т.д.;

– CD-образам: ccd, cdi, img, iso, raw, tib и т.д.;

– мультимедийным файлам: aiff, avi, divx, mov, mp3, mp4, mpeg, qt и т.д.

6.3.4.8 Фильтр MIME типов

Фильтр MIME типов может быть настроен на блокирование содержимого в зависимости от его типа.

– «Включено». Если фильтр включен, проверяются все входящие заголовки MIME-типа.

– «Блокировать эти MIME типы» - необязательное поле. Если запрошенный MIME тип будет заблокирован, доступ к нему будет запрещен. Таким образом, Вы можете заблокировать контент, независимо от того, какой тип расширения имени файла используется.

Например, добавьте MIME типы в одной строке, если хотите заблокировать скачивание файлов Word:

```
application/msword
```

Или добавьте эти MIME типы, каждый тип в отдельной строке, если хотите заблокировать скачивание MPEG и QuickTime видео файлов:

```
video/mpeg
video/quicktime
```

– «Не фильтровать следующие направления» - необязательное поле. Используйте этот список, чтобы избежать фильтрации MIME конкретных адресатов. Это должен быть список, доменов или субдоменов, имена хостов, IP-адреса или URL, каждый на отдельной строке.

Ниже приведены примеры:

```
*.example.net
www.example.net
123.45.67.89
www.example.net/downloads
```

6.3.4.9 Веб-браузер

Настройка веб-браузера производится следующим образом:

– «Включить проверку браузера». Установите этот флажок, если хотите включить проверку браузера.

– «Разрешенные клиенты для веб-доступа». Установите соответствующий флажок / флажки для разрешенных клиентов (рисунок 35).

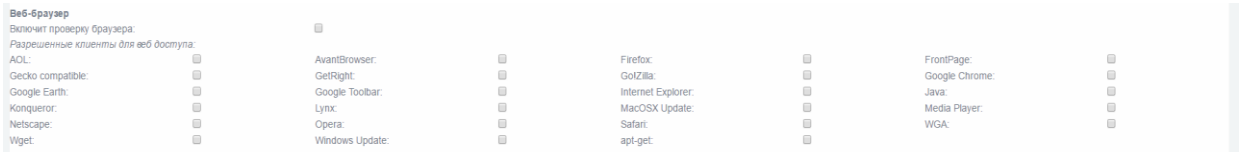


Рисунок 35 - Подсекция «Веб-браузер»

6.3.4.10 Конфиденциальность

В данной подсекции можно изменить некоторые поля заголовка http для защиты конфиденциальности (рисунок 36):

Рисунок 36 - Подсекция «Конфиденциальность»

– «Замена useragent посылаемого внешним сайтам» - необязательное поле. По умолчанию параметр useragent в данный момент, используемый веб-браузером будет предоставлен на внешние веб-сервера. Некоторые динамические веб-сайты генерируют контент в зависимости от представленной строки useragent. Эта строка также записывается в лог-файлы веб-сервера.

С опцией «замена useragent» у вас есть возможность переписать эту строку для всех своих клиентов. Для исходящих запросов поле заголовка useragent будет заменено прокси-сервером и передано на внешние сайты вместо исходной строки useragent. Это может быть полезно для защиты конфиденциальности или для обеспечения желаемого уровня совместимости.

– «Замена referer посылаемого внешним сайтам» - необязательное поле. При нажатии на гиперссылку, URL-адрес источника будет представлен сайту назначения. Эта опция может быть отключена путем введения пользователем определенной строки. Эта строка будет представлена вместо реального адреса. Опция может быть полезна для защиты конфиденциальности.

Примечание - Изменение referer нарушает стандарт http и иногда могут возникнуть трудности. Некоторые сайты блокируют запросы с неверным referer, чтобы защитить себя от так называемого внешнего связывания (deep link) или злоупотребления «кражей» графики с веб-сайта.

6.3.4.11 Redirectors

Redirectors работают с прокси для фильтрации и перенаправления веб-трафика на основе правил, которые могут включать в себя черные списки, белые списки, временные ограничения и т. д (рисунок 37):

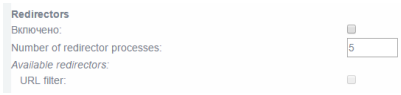


Рисунок 37 - Подсекция «Redirectors»

– «Включено». Установите флажок, чтобы включить перенаправление.

– «Number of redirector processes». Вы можете увеличить или уменьшить количество активных процессов фильтрации. Количество процессов зависит от производительности вашего оборудования, пропускной способности и числа одновременных клиентов. Значением по умолчанию является «5».

– «Available redirectors». Отображает список установленных redirectors, и показывает, какие из них активны. На рисунке 37 показано, что «URL-filter» неактивен.

6.3.4.12 Метод аутентификации

Веб-прокси предлагает несколько методов аутентификации пользователей (рисунок 38):

Рисунок 38 - Подсекция «Метод аутентификации»

– «Нет» (по умолчанию). Проверка подлинности отключена. Пользователи не должны авторизовываться, при доступе к веб-сайтам.

– «Локально». Этот метод аутентификации является наиболее оптимальным решением для домашних офисов. Пользователи проходят проверку подлинности для доступа к веб-сайтам, путем введения правильного имени пользователя и пароля.

– «identd». Этот метод аутентификации является наиболее оптимальным решением для сред, где:

a) проверка подлинности должна быть «скрытым» процессом, без введения логина и пароля;

b) прокси-служба должна работать в прозрачном режиме;

c) имя пользователя будет использоваться только для входа, а не для проверки подлинности.

Метод проверки подлинности identd требует identd-сервиса или daemon (программа, работающая в фоновом режиме и выполняющая определённые функции без ведома пользователя) запущенной на клиенте.

– «LDAP». Этот метод аутентификации является наиболее оптимальным решением для средних и крупных сетевых сред. Пользователи будут проходить аутентификацию при входе на веб-сайты, путем введения правильных имени пользователя и пароля. Учетные данные сверяются с внешним сервером с использованием облегченного протокола доступа к каталогам (LDAP).

Проверка подлинности LDAP будет полезна, если у вас уже есть служба каталогов в сети, и вы не хотите сохранять дополнительные учетные записи пользователей и пароли для веб-доступа.

– «Windows». Этот метод аутентификации является наиболее оптимальным решением для небольших и средних сетевых сред. Пользователям нужно будет аутентифицироваться при доступе к веб-сайтам. Учетные данные сверяются с внешним сервером, выступающего в качестве контроллера домена.

– «RADIUS». Этот метод аутентификации является наиболее оптимальным решением для небольших и средних сетевых сред. Пользователям нужно будет аутентифицироваться при доступе к веб-сайтам. Учетные данные сверяются с внешним сервером Radius.

Примечание - При использовании аутентификации и включении в веб-прокси лог-файлов, запрашиваемое имя пользователя будет зарегистрировано в дополнение к URL-адресу. Перед включением лог-файлов при использовании аутентификации, убедитесь, что не нарушаете существующих законов.

6.3.4.13 Включение взаимодействия с СЗИ

Настраивается возможность взаимодействия с антивирусом Касперского 5.5 для Proxy Server. Для этого в поле «ICAP URL» указывать в формате:

a) icap://addr:port/av/respmod, где addr и port это IP-адрес и порт антивируса.

b) «Enable ICAP». Для того чтобы включить возможность подключения чужого СЗИ, поставьте флажок (рисунок 39);

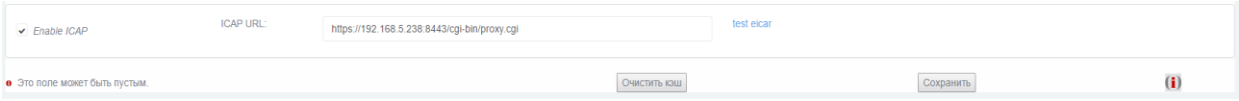


Рисунок 39 - Подсекция «Enable ICAP»

c) «ICAP URL». В текстовом поле напишите адрес СЗИ. Он будет использован при осуществлении функции прокси МЭ.

6.3.4.14 Включение фильтрации по мобильному коду

Включение фильтрации по мобильному коду выполняется следующим образом:

– «Enable script filter». Для того чтобы включить фильтрацию по скрипту, поставьте флажок (рисунок 40).

Рисунок 40 - Подсекция «Enable script filter»

– «Enable scripts». Для того чтобы включить поддержку скриптов, поставьте флажок. В текстовом поле напишите номер порта, к которому нужно обращаться.

6.3.5 Очистить кэш / сохранить

Процедура очистки/сохранения кэша:

– «Очистить кэш». Вы можете очистить все страницы из кэша прокси-сервера в любой момент нажатием кнопки «очистить кэш».

– «Сохранить». После внесения изменений, нажмите кнопку «Сохранить», чтобы применить их (рисунок 41).

Рисунок 41 - Очистить / сохранить кэш

6.4 Трансляция сетевых адресов

Трансляция сетевых адресов осуществляется автоматически на красном интерфейсе при прохождении сетевого пакета из зеленой подсети. Адрес источника пакета заменяется адресом красного интерфейса КП ПАВ «Рубикон». Изменение трансляции сетевых адресов не предусмотрено.

6.5 Маскирование

Для осуществления замены сетевого адреса на маскирующий адрес (подставной адрес) необходимо выполнить следующие действия:

– переназначьте цвет маскируемого интерфейса на красный - RED (см. раздел 5.2);

– перейдите в раздел «Система → Интерфейсы» (рисунок 42). В настройках красного интерфейса появится новое поле «mask address»;

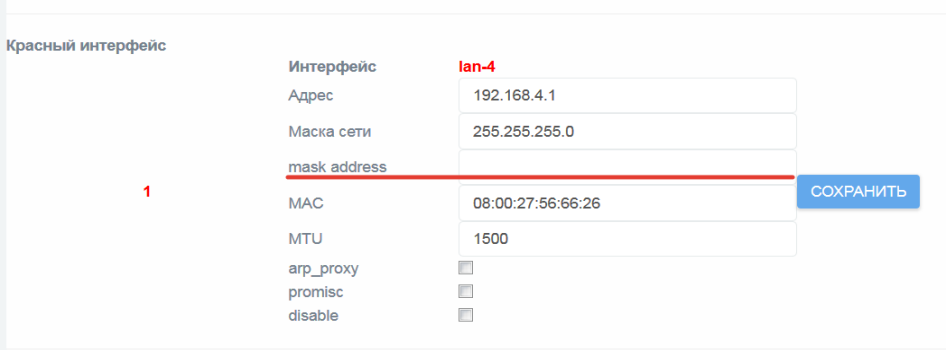


Рисунок 42 - Раздел «Система → Интерфейсы»

– введите маскирующий адрес, заполнив текстовое поле «mask address».

6.6 Трансляция портов

Трансляция портов осуществляется для обеспечения подключения узлов красной подсети к узлам, к которым необходим доступ извне, то есть для организации демилитаризованной зоны.

Для настройки трансляции портов выполните следующие действия:

– настройте сетевые адреса красного и оранжевого или зеленого интерфейса (рисунок 6);

– перейдите на страницу настройки правил фильтрации: «МЭ → Правила межсетевого экрана»;

– нажмите на кнопку «Перенаправление портов»;

– настройте правило фильтрации, заполнив:

1) в разделе «Источник» информацию о параметрах источника пакета (адрес, порт) (рисунок 46);

2) в разделе «Источник» номер протокола или сервис, который КП ПАВ «Рубикон» предоставляет в красную подсеть для доступа к требуемому узлу внутренней подсети (рисунок 43);

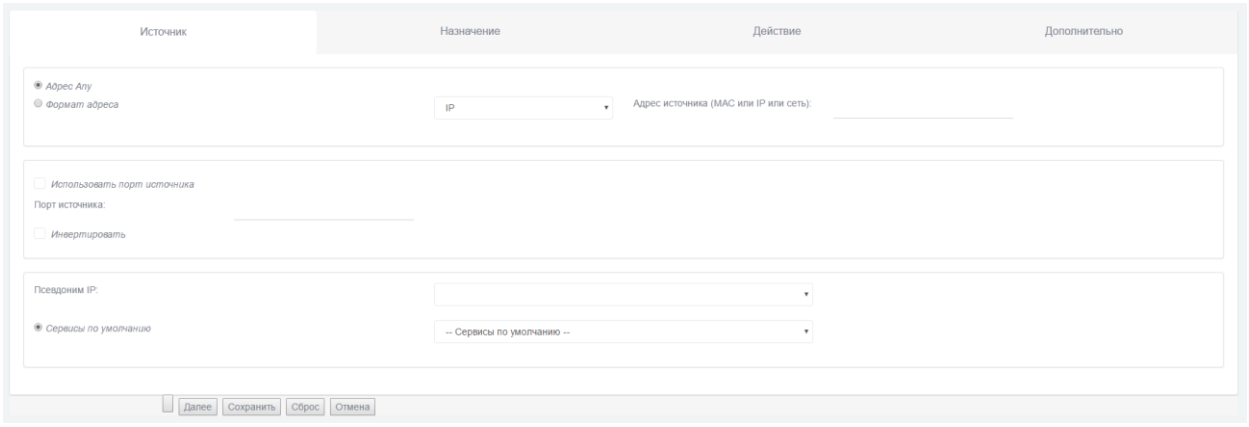


Рисунок 43 - Раздел «Источник»

3) в разделе «Назначение» информацию о месте назначения (интерфейс, адрес, порт, предоставляемый конкретным узлом) (рисунок 44);

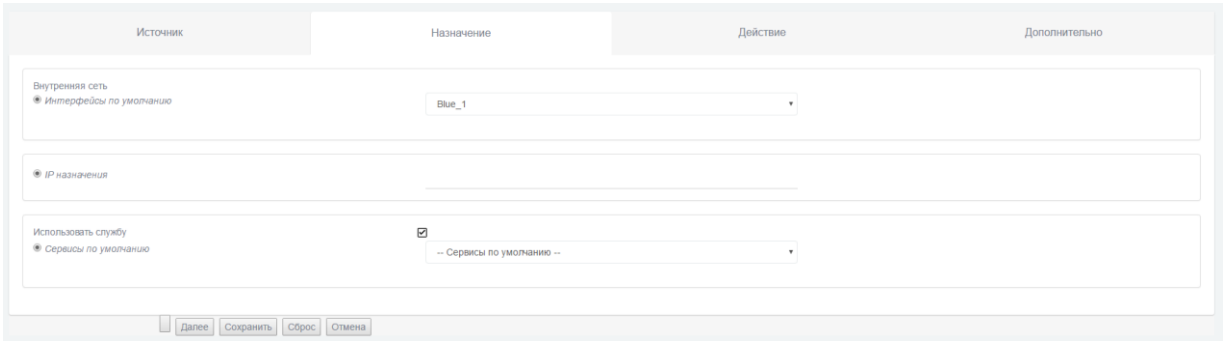


Рисунок 44 - Раздел «Назначение»

4) в разделе «Действие» информацию о параметрах фильтруемых пакетов и решении о пропуске или отбрасывании их (рисунок 45);

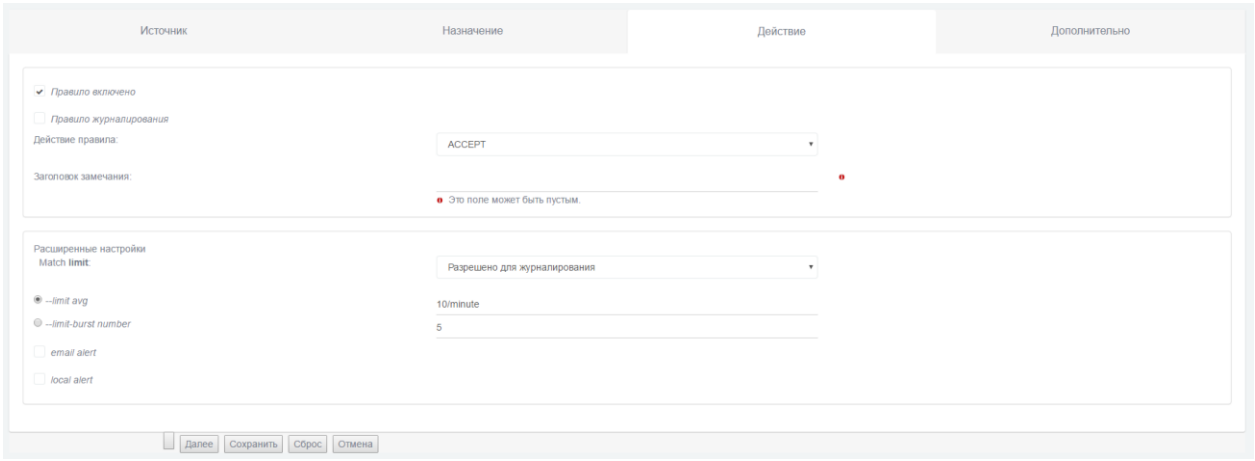


Рисунок 45 - Раздел «Действие»

– выберите необходимое действие для завершения операции по изменению текущего правила:

1) перейдите к просмотру правила нажатием кнопки «Далее»;

2) сохраните правило и вернитесь к интерфейсу выбора необходимых действий по настройке правил нажатием кнопки «Сохранить»;

3) сбросьте установленные параметры фильтрации нажатием кнопки «Сброс»;

4) выйдите из интерфейса изменения правил без сохранения нажатием кнопки «Отмена»;

6.7 Таблицы состояний

1) Перейдите на страницу состояний соединения «Состояние → Соединения».

2) В ниспадающем списке «Отображать» выберите значение «Состояние» (рисунок 46) или значение «Трафик» (рисунок 47).

3) Нажмите кнопку «Сохранить».

На рисунке 46 отображается таблица состояния всех соединений.

На рисунке 47 отображается таблица с информацией о трафике.

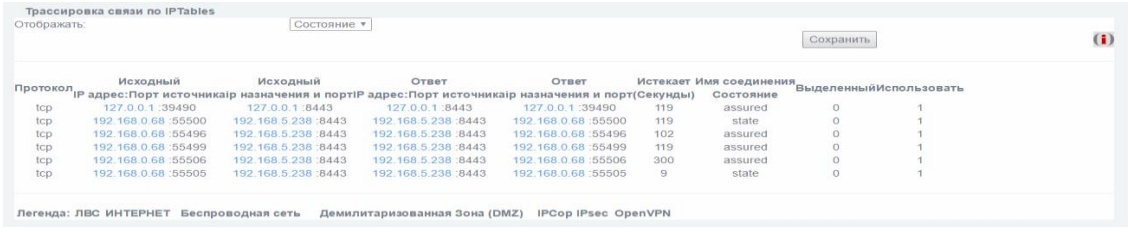


Рисунок 46 - Таблица состояний соединений

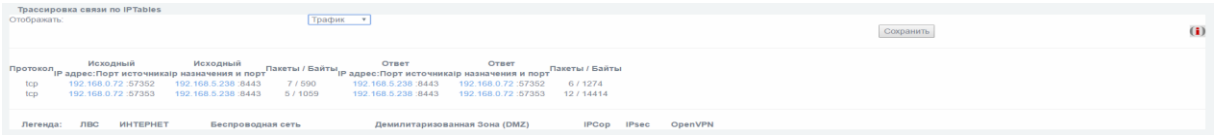


Рисунок 47 - Таблица с информацией о трафике

7 СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

7.1 Интерфейсы, доступные для запуска СОВ

СОВ может быть запущена в качестве отдельного процесса для любого из физических сетевых интерфейсов устройства. Указание о необходимости запуска процесса на том или ином интерфейсе осуществляется выбором соответствующего элемента управления в секции «Интерфейсы» на странице установки параметров «Службы → Обнаружение атак». Секция «Интерфейсы» представлена на рисунке 48.

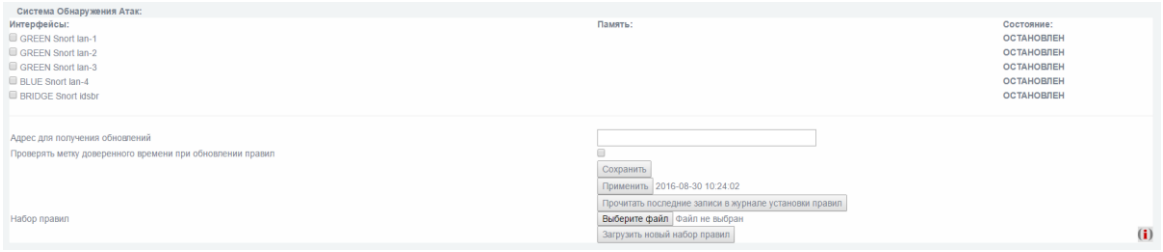


Рисунок 48 - Раздел «Службы → Обнаружение атак», секция «Интерфейсы»

7.1.1 Запуск на физическом интерфейсе

Для того, чтобы подключить СОВ к одному из физических интерфейсов, поставьте отметку напротив его названия в разделе «Службы → Обнаружение атак», секция «Интерфейсы» (рисунок 48).

После того как отметка поставлена, сохраните изменения, нажав кнопку «Сохранить». Появится надпись с дальнейшими указаниями (рисунок 49).

Рисунок 49 - Запуск СОВ на физическом интерфейсе

Чтобы применить сохраненные изменения, нажмите кнопку «Применить». Теперь СОВ запущена на выбранном интерфейсе (рисунок 50).

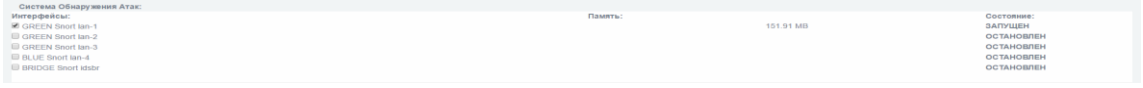


Рисунок 50 - СОВ запущена на интерфейсе Green Snort lan-1

7.2 Режимы обнаружения

В КП ПАВ «Рубикон» предусмотрено два режима обнаружения вторжений: сигнатурный анализ и эвристический анализ.

7.2.1 Сигнатурный анализ

Режим сигнатурного анализа предполагает наличие базы решающих правил (БРП), которая включает в себя сигнатуры известных атак. Корректная работа данного режима невозможна без актуальной БРП и напрямую зависит от набора правил.

7.2.2 Эвристический анализ

Режим эвристического анализа атак заключается в просмотре сетевого трафика на наличие элементов сканирования портов или узлов сети и выдаче решения о наличии сканирования в сегменте сети.

Для настройки режима эвристического анализа зайдите в раздел «СОВ → Настройка обнаружения сканирования».

Существует два элемента управления (рисунок 51): выбор протокола, и уровень срабатывания. Протокол определяет те сетевые пакеты, которые будут анализироваться. Уровень срабатывания определяет предполагаемую интенсивность сканирования злоумышленником.

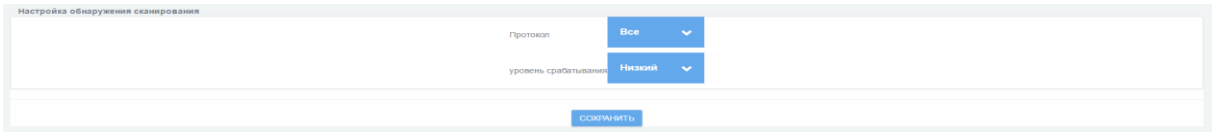


Рисунок 51 - Настройка режима эвристического анализа

Поле «Протокол» может принимать следующие значения:

- Все;
- TCP;
- UDP;
- ICMP;
- протокол IP.

Доступны три уровня срабатывания:

- низкий;
- средний;
- высокий.

7.3 База решающих правил

7.3.1 Загрузка новой базы решающих правил

Для настройки новой БРП загрузите в разделе «Службы → Обнаружение атак» следующие файлы (рисунок 52):

– метка времени в формате tsr: получена от сервера доверенного времени;

– непосредственно набор правил;

– файл УЦ: сертификат, выданный УЦ серверу доверенного времени.

Метка времени состоит из:

– контрольной суммы набора правил;

– времени создания метки;

– ЭП сервера доверенного времени, удостоверяющего целостность описанных выше данных;

– сертификата сервера доверенного времени.

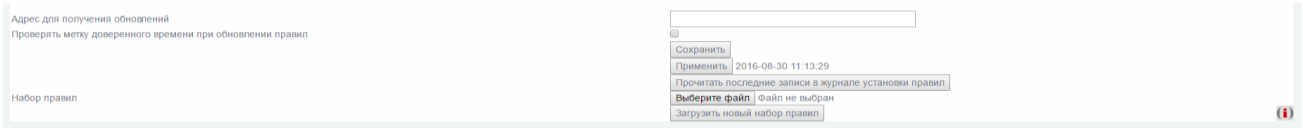


Рисунок 52 — Настройка БРП. Импорт файлов в систему

После того как все файлы выбраны, нажмите кнопку «Загрузить новый набор правил».

Примечание - Если хотя бы один из требуемых файлов не был загружен, после нажатия на кнопку «Загрузить новый набор правил» администратор увидит следующее сообщение (рисунок 53):

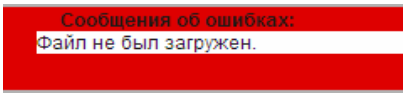


Рисунок 53 - Сообщение об ошибке

После загрузки происходит проверка:

– соответствия контрольной суммы загруженного набора правил контрольной сумме, указанной в метке времени;

– актуальности сертификата сервера доверенного времени, извлекаемого из метки времени.

В случае успешного прохождения проверки с помощью сертификата сервера доверенного времени проверяется ЭП метки времени. Если подпись верна, происходит

загрузка правил в хранилище СОВ и удаление временных файлов. Пользователю выводится предложение нажать кнопку «Применить» (рисунок 54), что обновит правила и перезапустит СОВ на выбранных интерфейсах.

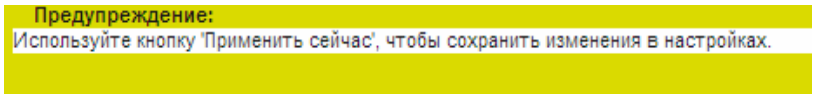


Рисунок 54 - Предложение применить внесенные изменения

После успешного перезапуска, а также по нажатию кнопки «Прочитать последние записи в журнале установки правил», администратор может увидеть информацию, представленную на рисунке 54.

При неуспешной проверке администратор увидит предупреждающее сообщение (рисунок 55):

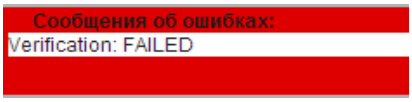


Рисунок 55 - Сообщение об ошибке

Данное сообщение означает что:

– один или более файлов выбраны ошибочно (неверный формат);

– все файлы корректного формата, но контрольная сумма загруженного набора правил не соответствует контрольной сумме, указанной в метке времени;

– сертификат сервера доверенного времени неактуален.

Справа от кнопки «Применить» отображается дата последнего изменения правил. Также отображаются сведения о результатах проверки метки времени. Результат проверки на рисунке 56 «done» означает успешное прохождение проверки. Можно также увидеть сведения о загружаемом наборе правил.

Рисунок 56 - Информация об установленных обновлениях

7.3.2 Настройка решающих правил

7.3.2.1 Включение/отключение решающих правил

Для включения (отключения) срабатывания конкретного решающего правила поставьте отметку напротив его названия в соответствующем контейнере в разделе «СОВ → Настройка правил СОВ».

Например, на рисунке 57 включены все правила, кроме «ATTAC_RESPONCES 403 Forbidden».

7.3.2.2 Включение/отключение уведомления по электронной почте для каждого правила

Для включения (отключения) уведомления администратора о срабатывании конкретного решающего правила выберите  для включения и  для отключения напротив названия правила в соответствующем контейнере в разделе «СОВ → Настройка правил СОВ».

Например, на рисунке 57 отключено уведомление обо всех правилах, кроме «ATTAC_RESPONCES command error».

7.3.2.3 Включение/отключение блокирования атаки с помощью межсетевого экрана

Для включения (отключения) блокирования атаки с помощью межсетевого экрана выберите  для включения и  для отключения напротив названия правила в соответствующем контейнере в разделе «СОВ → Настройка правил СОВ».

Например, на рисунке 57 включена возможность блокирования атаки межсетевым экраном при срабатывании правила «ATTAC_RESPONCES file copied ok», блокирование атаки межсетевым экраном при срабатывании других правил происходить не будет.

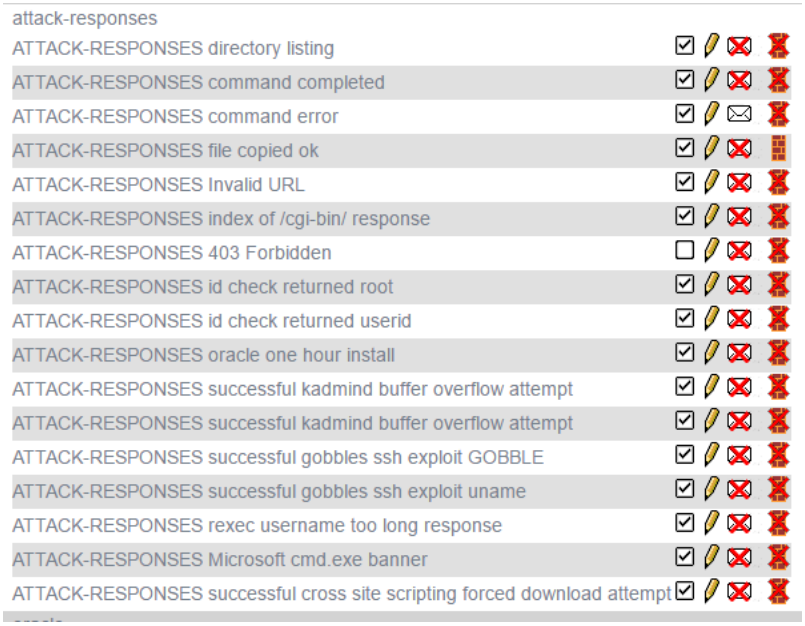


Рисунок 57 - Настройка решающих правил

8 РЕЗЕРВИРОВАНИЕ

8.1 Горячее резервирование

КП ПАВ «РУБИКОН» поддерживает технологию горячего резервирования. Пример, рассматривающий горячее резервирование красного интерфейса WAN, приведен ниже.

Пример: имеется два КП ПАВ «Рубикон», которые подключены в одну внешнюю сеть с основным IP адресом 10.10.10.1 и резервным IP адресом 10.10.10.2. Основной КП ПАВ «Рубикон» имеет IP адрес 192.168.3.1, а резервный КП ПАВ «Рубикон» - 192.168.3.2. Оба КП ПАВ «Рубикон» соединены между собой.

Создайте один общий виртуальный интерфейс, который будет переключаться между КП ПАВ «Рубикон». Для примера это IP адрес 10.10.10.3.

Для настройки горячего резервирования для данного примера выполните следующие действия:

– в веб-интерфейсе перейдите на страницу: «Сеть → Функция горячего резервирования» и нажмите кнопку редактирования нужного интерфейса (рисунок 58);

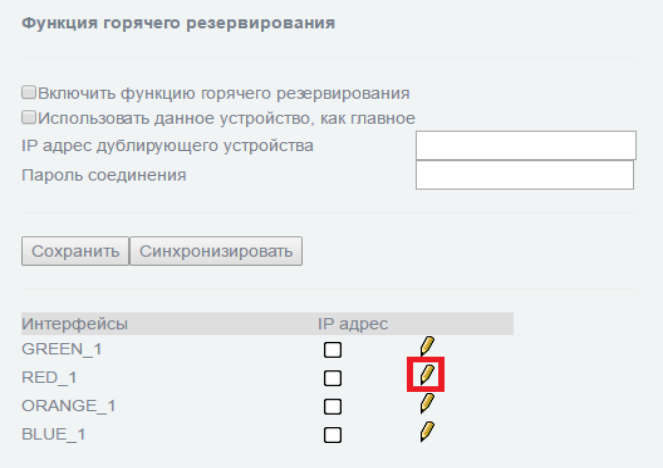


Рисунок 58 - Раздел «Сеть → Функция горячего резервирования»

– укажите общий виртуальный IP адрес и нажмите кнопку «Сохранить» (рисунок 59);

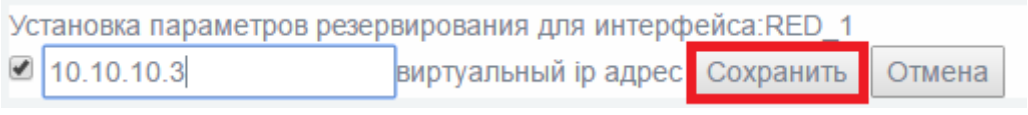


Рисунок 59 - Общий IP адрес

– заполните поля для основного КП ПАВ «Рубикон» с указанием необходимых IP адресов, по которым КП ПАВ «Рубикон» соединены между собой (рисунок 60)

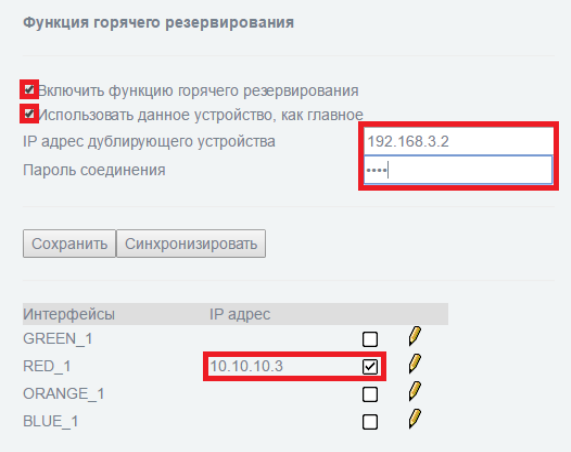


Рисунок 60 - Настройка основного КП ПАВ «Рубикон»

– заполните поля для резервного копирования КП ПАВ «Рубикон» с указанием необходимых IP адресов, по которым КП ПАВ «Рубикон» соединены между собой (рисунок 61);

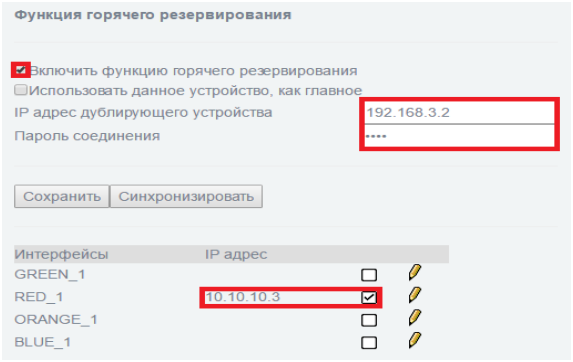


Рисунок 61 - Настройка резервного КП ПАВ «Рубикон»

Пароли соединения между основным и резервным КП ПАВ «Рубикон» должны совпадать.

Для проверки правильности настройки горячего резервирования зайдите в веб-интерфейсе на страницу «Состояние → Состояние сети» и вы увидите данные, аналогичные представленным на рисунке 62.

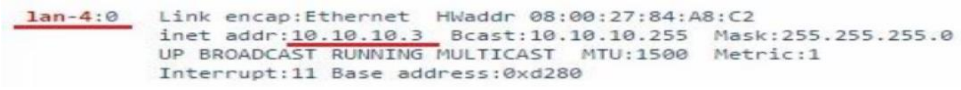


Рисунок 62 - Настройка резервного КП ПАВ «Рубикон»

9 ЖУРНАЛ СОБЫТИЙ

9.1 Общие положения

В КП ПАВ «Рубикон» есть четыре вида журналов:

1) журнал МЭ;
2) журнал обнаружения атак;
3) журнал обнаружения сканирования;
4) системный протокол - позволяет отслеживать сбои и восстанавливать работу КП ПАВ «Рубикон».

Журнал содержит информацию обо всех действиях, производимых в системе. Регистрируемые события:

– запуск выполнения функций аудита;
– попытка авторизации;
– успешная авторизация;
– неудачная авторизация;
– действия, предпринимаемые в ответ на возможные нарушения безопасности;
– чтение информации из записей аудита;
– параметры, используемые при просмотре;
– все модификации конфигурации аудита, происходящие во время сбора данных аудита;
– разрешения на запрашиваемые информационные потоки;
– все попытки импортировать данные пользователя;
– все попытки экспортировать информацию;
– все модификации режима выполнения функций;
– все модификации значений данных;
– использование функций управления;
– модификация группы пользователей - исполнителей роли;
– каждое использование прав, представленных ролью;
– все модификации значений атрибутов безопасности;
– обнаружение сбоя функций безопасности, если аудит возможен;
– факт возникновения сбоя или прерывания обслуживания;
– возобновление нормальной работы;
– тип сбоя или прерывания обслуживания;

– невозможность возврата к безопасному состоянию после сбоя функций безопасности, если аудит возможен;

– изменения внутреннего представления времени;

– предоставление меток времени;

– выполнение тестирования внешних сущностей и протоколирование результатов тестирования;

– выполнение и результаты самотестирования функций безопасности;

– успешное использование механизмов согласования данных функций безопасности;

– использование механизмов согласования данных функций безопасности;

– идентификация функций безопасности, данные которых интерпретируются;

– обнаружение модифицированных данных функций безопасности;

– любой сбой, обнаруженный функциями безопасности;

– завершение выполнения функций аудита.

Журналы можно хранить локально или отправлять на удаленный сервер (подробнее в разделе 9.2.4).

9.2 Настройка параметров отображения и ведения журналов

Для настройки параметров отображения и ведения журналов перейдите в раздел «Журналы → Настройки». Откроется страница, представленная на рисунке 63.

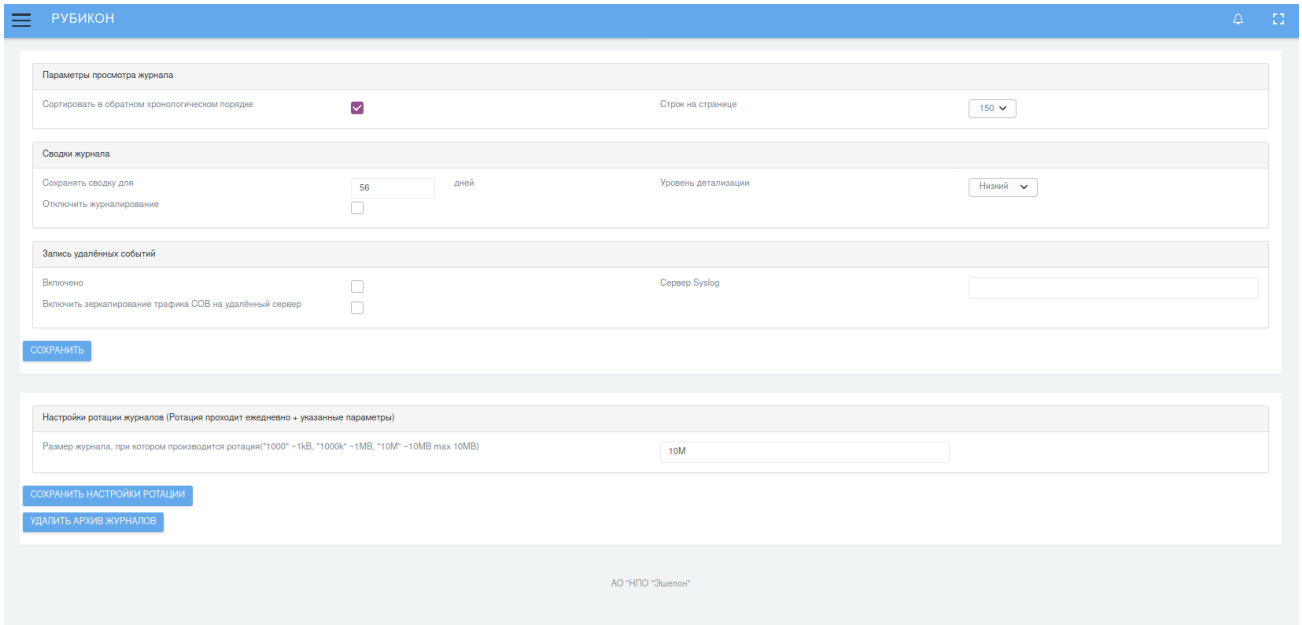


Рисунок 63 — Страница настройки параметров отображения журналов

Для настройки администратору доступны следующие параметры:

a) Настройки просмотра журнала;
b) Сводки журнала;
c) Запись удаленных событий;
d) Записывать в «Системный протокол».

9.2.1 Настройки просмотра журнала

Параметр «Отсортировать в обратном хронологическом порядке» предназначен для установления отображения записей журналов в обратном хронологическом порядке.

Параметр «Строк на странице» предназначен для установления количества строк, отображаемых на одной странице журнала.

9.2.2 Сводки журнала

Параметр «Сохранять сводку для» предназначен для указания временного периода хранения сводки журнала (в днях). После истечения указанного срока записи удаляются из журнала.

Параметр «Уровень детализации» может принимать следующие значения:

– низкий;
– средний;
– высокий.

Отметка напротив пункта «Отключить журналирование» позволяет отключить запись всех системных событий и обнаруженных с помощью КП ПАВ «Рубикон» атак, а также отправку записей на удалённый сервер (если эта опция была включена ранее).

9.2.3 Запись удаленных событий

Параметр «Включено» предназначен для включения возможности журналирования событий на удаленный сервер.

Строка ввода «Сервер Syslog», предназначена для указания адреса удаленного syslog-сервера.

Параметр «Включить зеркалирование трафика СОВ на удаленный сервер» позволяет отправлять трафик СОВ на удаленный сервер.

9.2.4 Записывать в «Системный протокол»

В секции «Записывать в «Системной протокол» можно выбрать, какие категории системного протокола хранить локально, а какие отправлять на удаленный сервер.

9.2.5 Настройки ротации журналов

Задайте «Количество файлов старых журналов, которые необходимо сохранить на устройстве» в текстовом поле.

Задайте «Размер журнала, при котором производится ротация («1000» ~1kB, "1000k" ~1MB, "10M" ~10MB, max 10MB)» в текстовом поле.

Перейдите по ссылке «Посмотреть статистику ротированных журналов», для просмотра статистики.

Для сохранения внесенных изменений в настройки параметров отображения и ведения журналов нажмите кнопку «Сохранить».

9.3 Сервер времени

Перейдите в раздел «Службы → Сервер времени» (рисунок 64).

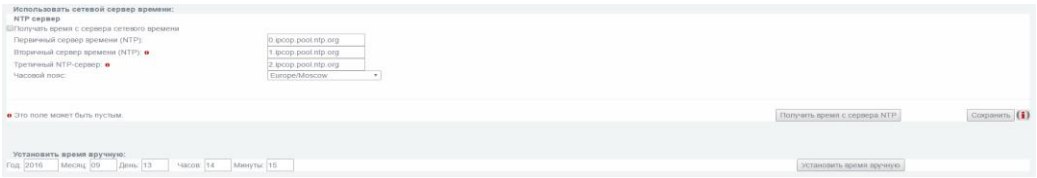


Рисунок 64 - Раздел «Службы → Сервер времени»

В разделе можно указать сервер, который будет передавать временные метки для журналирования, для этого выполните следующие действия:

1) поставьте флажок напротив параметра «Получать время с сервера сетевого времени»;

2) заполните текстовое поле «Первичный сервер времени (NTP)»;

3) заполните текстовое поле «Вторичный сервер времени (NTP)» (необязательное поле);

4) заполните текстовое поле «Третичный NTP-сервер»;

5) в ниспадающем списке «Часовой пояс» выберите город;

6) нажмите кнопку «Сохранить».

Если вы хотите установить время вручную, перейдите в секцию «Установить время вручную» (рисунок 64).

9.4 Сводка журнала

Для просмотра общего отчета о работе системы перейдите в раздел «Журналы → Сводка журнала». Страница отображения общего отчета о системе представлена на рисунке 65.

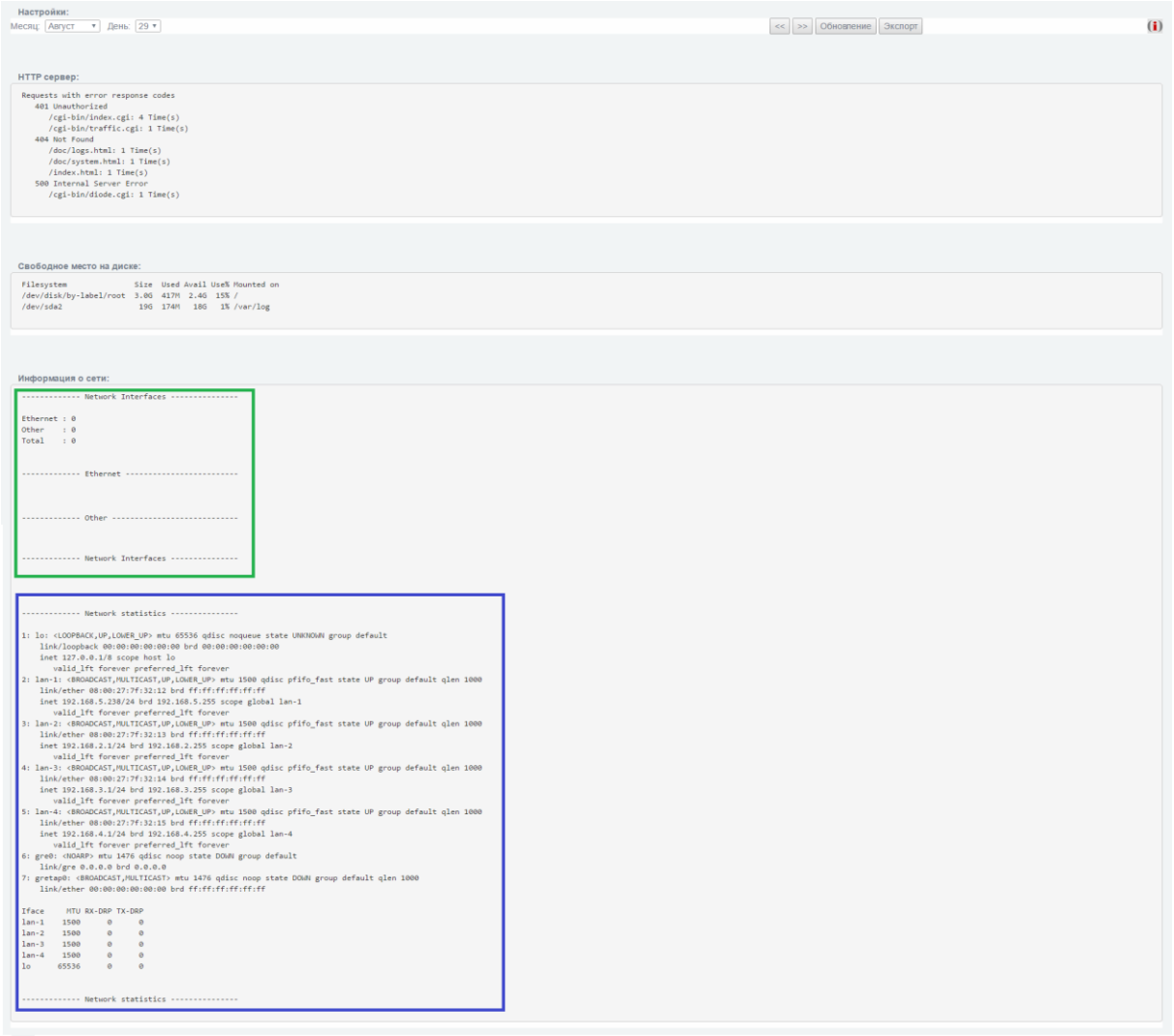


Рисунок 65 - Страница отображения общего отчета о системе

Как видно из рисунка 65, общий отчет о работе КП ПАВ «Рубикон» состоит из четырех секций.

9.4.1 Настройки

Администратору предоставляется возможность выбора конкретного дня, за который необходимо просмотреть отчет (рисунок 66).

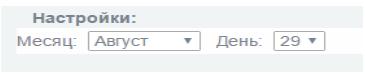


Рисунок 66 - Секция «Настройки»

9.4.2 HTTP сервер

В секции «HTTP сервер приведено перечисление исследованных сайтов и запросов с кодами ошибок (рисунок 67).

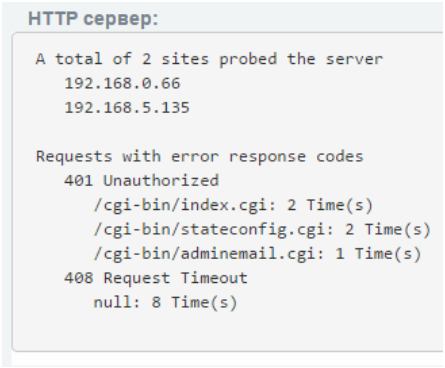


Рисунок 67 - Секция «HTTP сервер»

9.4.3 Свободное место на диске

Секция представляет собой сводную таблицу с данными об используемых файловых системах (рисунок 68).

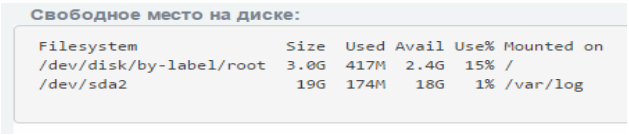


Рисунок 68 - Секция «Свободное место на диске»

9.4.4 Информация о сети

Информация в этой секции состоит из двух блоков:

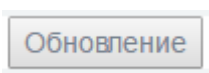
– сведения о сетевых интерфейсах (Network Interfaces): на рисунке 65 выделено в рамку зеленого цвета;

– сведения о конфигурации сетевых интерфейсов (Network Statistics): на рисунке 65 выделено в рамку синего цвета.

На странице общего отчета о работе системы есть ряд кнопок:

предназначена для перехода к странице информации на один день раньше;

предназначена для перехода к странице информации на один день позже;



предназначена для обновления информации для выбранного периода времени;

Экспорт — *предназначена для экспорта информации в формате .txt.*

9.5 Журнал межсетевого экрана

Чтобы посмотреть журнал межсетевого экрана, перейдите в раздел «Журналы → Журнал межсетевого экрана». Откроется страница, изображенная на рисунке 69.

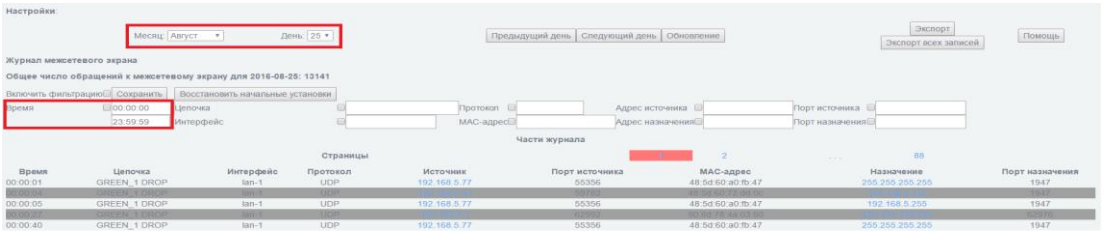


Рисунок 69 - Раздел «Журналы → Журнал межсетевого экрана»

На странице журнала межсетевого экрана предусмотрена возможность выборочного просмотра записей. Для просмотра информации журнала, отсортированной по какому-либо параметру, включите фильтрацию. Для этого выставите отметку напротив соответствующего пункта и нажмите кнопку «Сохранить».

Загрузить события из журнала можно за период равный одним суткам. Для этого укажите день и месяц текущего года (рисунок 69).

Возможно ограничить промежуток времени, за который будут отображены события выбранных суток, путем выставления конкретных временных рамок (рисунок 69).

На странице журнала межсетевого экрана есть ряд кнопок:

Предыдущий день — *предназначена для перехода к странице информации на один день раньше;*

Следующий день — *предназначена для перехода к странице информации на один день позже;*

Обновление — *предназначена для обновления информации для выбранного периода времени;*

Экспорт — *предназначена для экспорта информации в формате .txt;*

Экспорт всех записей — *предназначена для экспорта всей информации в формате .zip*

Восстановить начальные установки — *предназначена для сброса всех параметров фильтров.*

Доступны следующие параметры для настройки фильтрации журнала межсетевого экрана:

- время;
- цепочка;
- интерфейс;
- протокол;
- источник;
- порт источника;
- MAC-адрес;
- назначение;
- порт назначения.

На рисунках 70 - 72 приведены примеры журналов межсетевого экрана, отсортированных по адресу источника, порту источника и MAC-адресу соответственно.

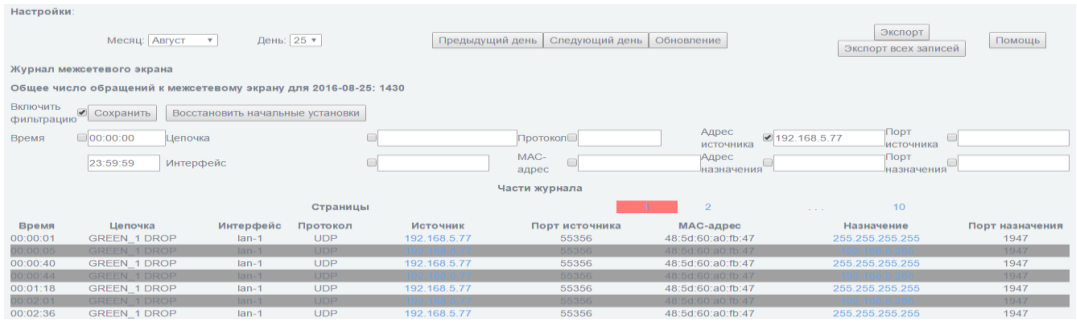


Рисунок 70 - Пример журнала МЭ, фильтр по адресу источника: 192.168.5.77

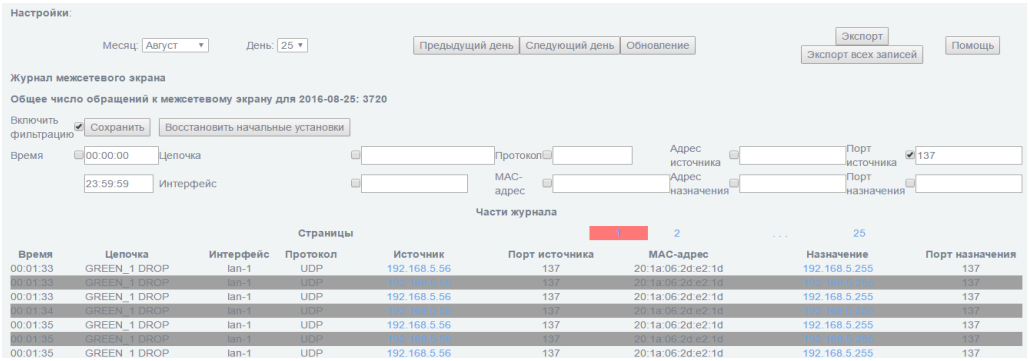


Рисунок 71 - Пример журнала МЭ, фильтр по порту источника: 137

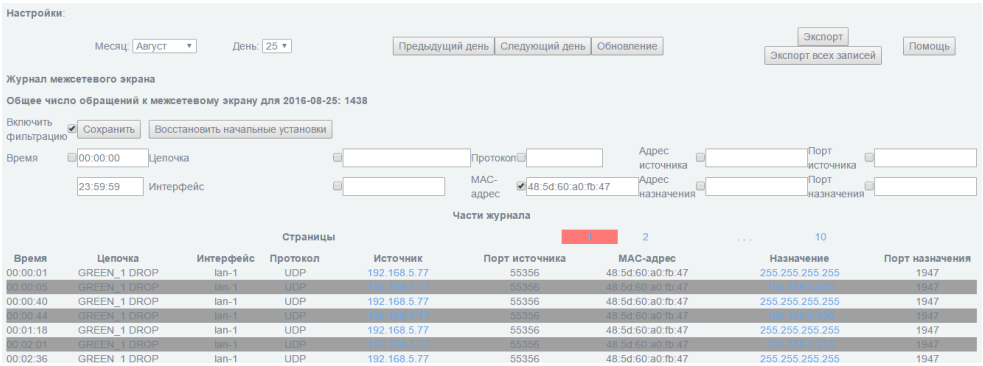


Рисунок 72 - Пример журнала МЭ, фильтр по MAC-адресу: 48:5d:60:a0:fb:47

9.6 Журнал обнаружения атак

Чтобы просмотреть журнал обнаруженных атак СОВ, необходимо перейдите в раздел «Журналы → Журнал обнаружения атак». Откроется страница, изображенная на рисунке 73.

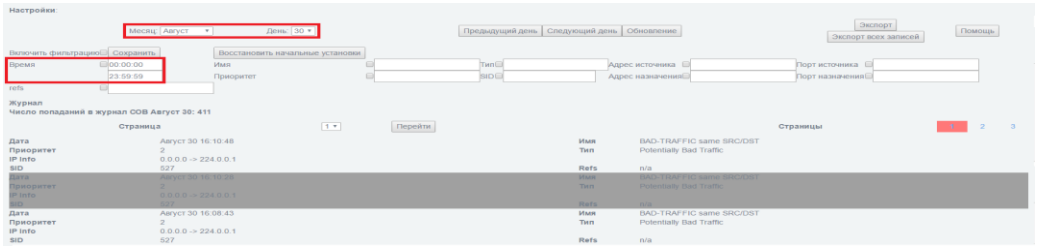


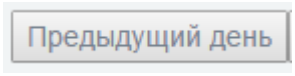
Рисунок 73 - Раздел «Журналы → Журнал обнаружения атак»

На странице журнала обнаружения атак предусмотрена возможность выборочного просмотра записей. Для просмотра информации журнала, отсортированной по какому-либо параметру, включите фильтрацию. Для этого выставите отметку напротив соответствующего пункта и нажмите кнопку «Сохранить».

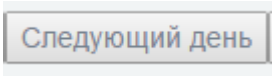
Загрузить события из журнала можно за период равный одним суткам. Для этого укажите день и месяц текущего года (рисунок 76).

Возможно ограничить промежуток времени, за который будут отображены события выбранных суток, путем выставления конкретных временных рамок (рисунок 76).

На странице журнала обнаружения атак есть ряд кнопок.



предназначена для перехода к странице информации на один день раньше;



предназначена для перехода к странице информации на один день позже;

Обновление	*предназначена для обновления информации для выбранного периода времени;*
Экспорт	*предназначена для экспорта информации в формате .txt;*
Экспорт всех записей	*предназначена для экспорта всей информации в формате .zip*
Восстановить начальные установки	*предназначена для сброса всех параметров фильтров.*

Доступны следующие параметры для настройки фильтрации журнала обнаружения атак:

- имя;
- приоритет;
- тип;
- SID (Security Identifier);
- адрес источника;
- адрес назначения;
- порт источника;
- порт назначения;
- refs (ссылка на описание уязвимости).

На рисунках 74 - 76 приведены примеры журналов обнаружения атак, отсортированных по SID, имени и типу соответственно.

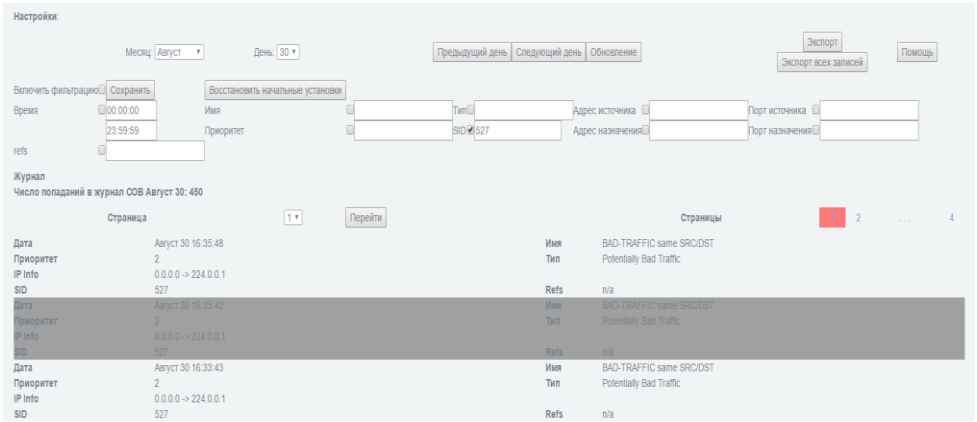


Рисунок 74 — Пример журнала обнаружения атак, фильтр по SID: 527

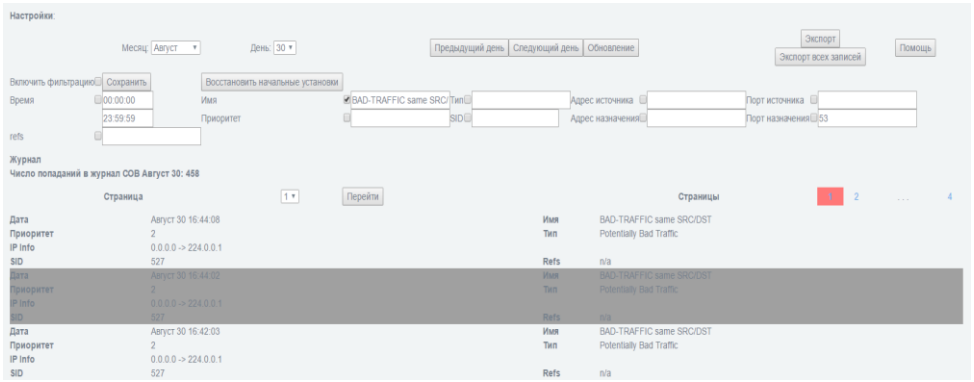


Рисунок 75 — Пример журнала обнаружения атак, фильтр по названию: BAD-TRAFFIC same SRC/DST

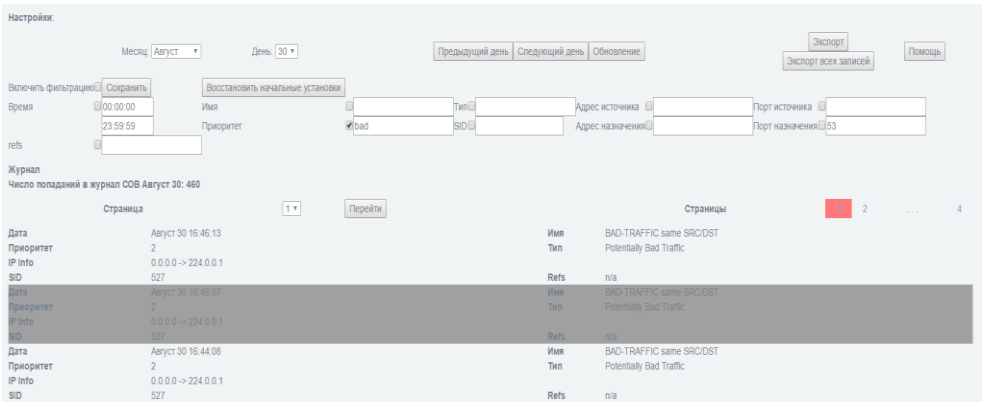


Рисунок 76 — Пример журнала обнаружения атак, фильтр по типу: bad

9.7 Журнал обнаружения сканирования

Записи обо всех попытках сканирования сети хранятся в разделе «Журналы → Журнал обнаружения сканирования» (рисунок 77).

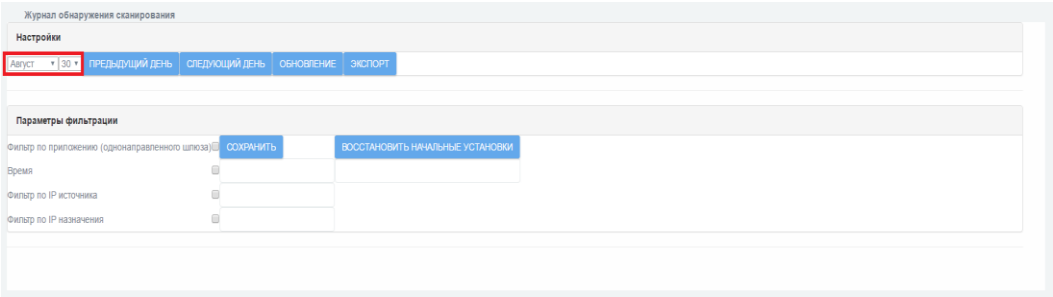
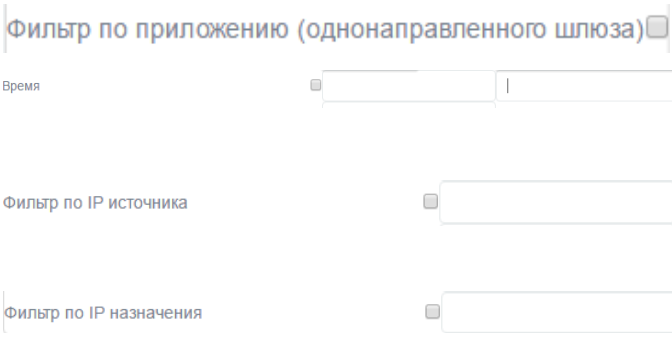


Рисунок 77 - Раздел «Журналы → Журнал обнаружения сканирования»

Загрузить события из журнала можно за период равный одним суткам. Для этого укажите день и месяц текущего года (рисунок 77).

В секции «Параметры фильтрации» предусмотрен ряд фильтров. Для того чтобы включить фильтрацию, поставьте соответствующую отметку и нажмите кнопку «Сохранить».

Доступны следующие параметры для фильтрации:



фильтр по приложению;

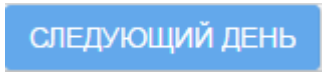
фильтр по времени: (в формате XX:YY:ZZ);

фильтр по IP-адресу источника;

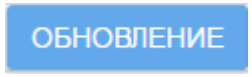
фильтр по IP-адресу назначения.

На странице журнала обнаружения сканирования есть ряд кнопок.

предназначена для перехода к странице информации на один день раньше;

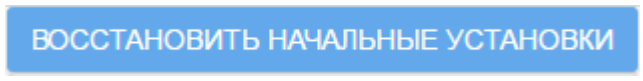


предназначена для перехода к странице информации на один день позже;



предназначена для обновления информации для выбранного периода времени;

предназначена для экспорта информации в формате .txt;



предназначена для сброса всех параметров фильтров.

9.8 Системный протокол

Для просмотра системного протокола КП ПАВ «Рубикон» перейдите в раздел «Журналы → Системный протокол». Откроется страница, изображенная на рисунке 78.

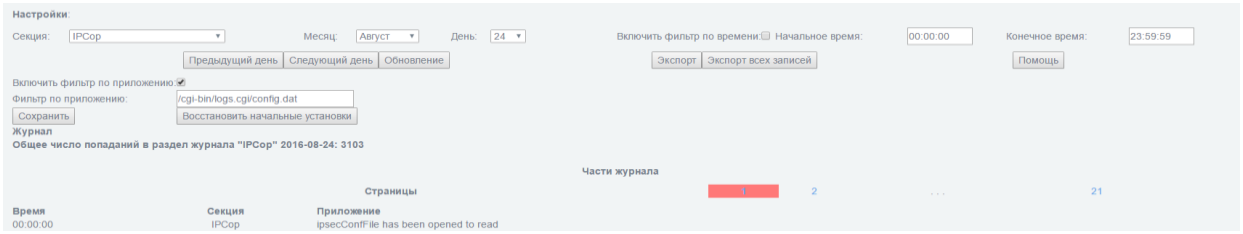
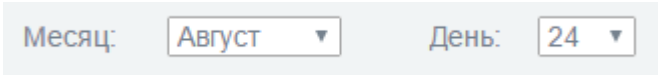


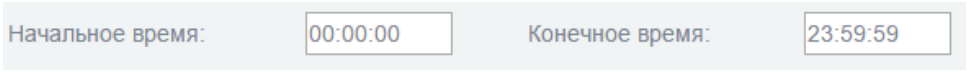
Рисунок 78 - Раздел «Журналы → Системный протокол»

Доступны следующие параметры для настройки фильтрации системного протокола:

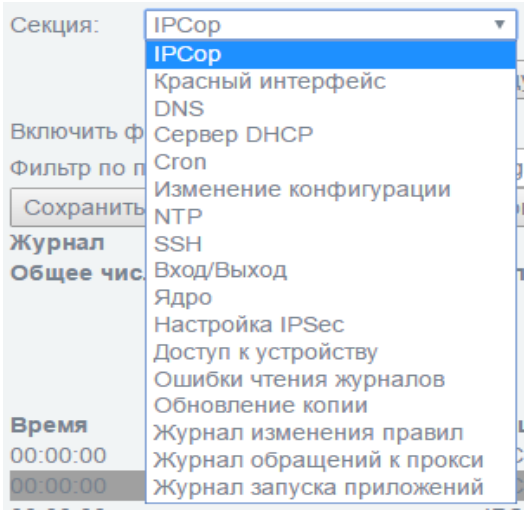
По дате:



По времени:



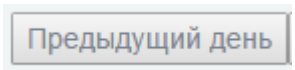
По секции:



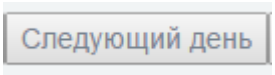
По приложению:

Примечание - Для настройки фильтров по времени и по приложению должны стоять отметки напротив соответствующих пунктов «Включить фильтр по времени» и «Включить фильтр по приложению».

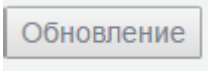
На странице системного протокола есть ряд кнопок.



предназначена для перехода к странице информации на один день раньше;



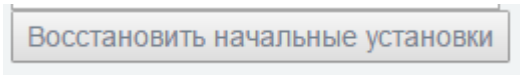
предназначена для перехода к странице информации на один день позже;



предназначена для обновления информации для выбранного периода времени;

предназначена для экспорта информации в формате .txt;

предназначена для экспорта всей информации в формате .zip



предназначена для сброса всех параметров фильтров.

На рисунках 79 и 80 приведены примеры фильтрации системного протокола по секции «IPCop» и журналу запуска приложений соответственно.

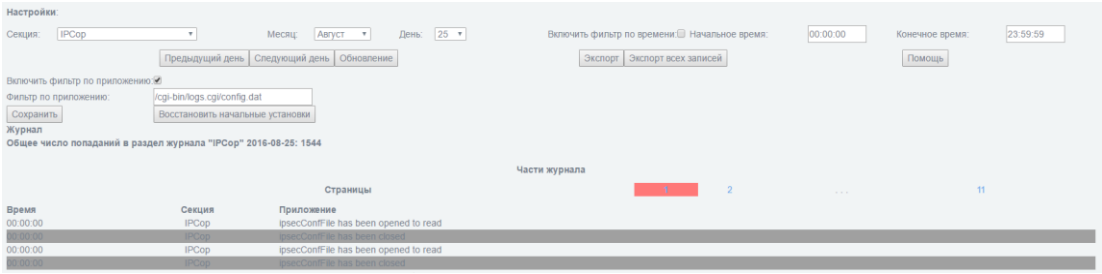


Рисунок 79 — Пример фильтрации системного протокола по секции «IPCop»

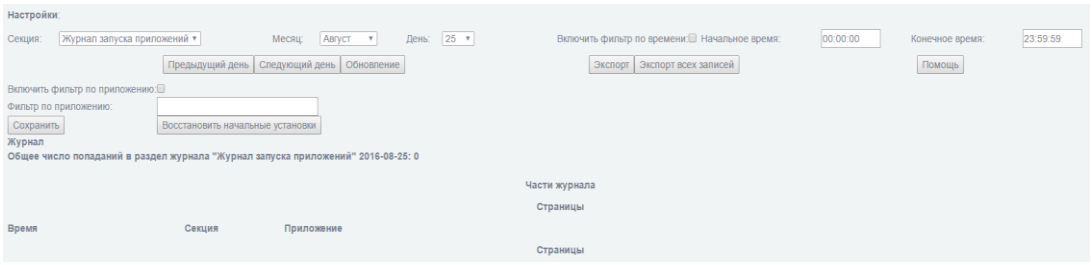


Рисунок 80 — Пример фильтрации системного протокола по секции «Журнал запуска приложений»

9.9 Настройка уведомлений

В случае попыток нарушения правил КП ПАВ «Рубикон» и при обнаружении критичных событий безопасности в шапке веб-интерфейса появляется соответствующее сообщение. При нажатии на кнопку вы можете получить более подробную информацию о возникшей проблеме в виде всплывающего окна (рисунок 81).

Рисунок 81 - Новые уведомления КП ПАВ «Рубикон»

Также КП ПАВ «Рубикон» позволяет настроить уведомление администратора об обнаруженных атаках по электронной почте. Для настройки уведомления по электронной почте перейдите в раздел «Система → Почта» (рисунок 82).

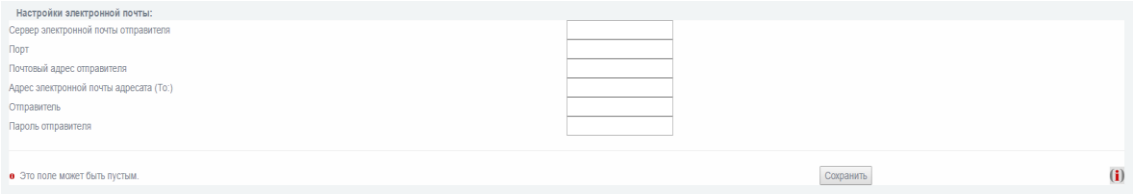


Рисунок 82 - Раздел «Система → Почта»

Для подтверждения правильности внесенной информации нажмите кнопку «Сохранить». После этого, уведомления об обнаруженных атаках будут приходить на электронную почту.

10 АВТОВОССТАНОВЛЕНИЕ

10.1 Действия системы в случае сбоя

Вы можете установить действия, которые сделает система в случае выявления сбоя, в зависимости от типа сбоя.

Перейдите в раздел «Система → Автовосстановление» (рисунок 83).

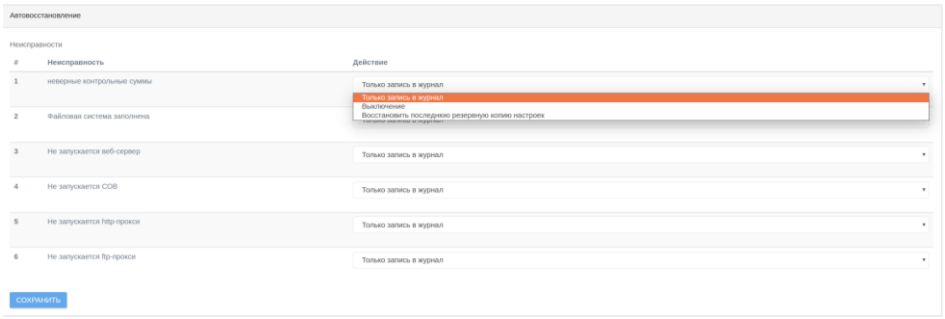


Рисунок 83 - Раздел «Система → Автовосстановление»

В разделе представлено 6 типов сбоя и в ниспадающих списках приведены опции восстановления при разных неисправностях:

1) неверные контрольные суммы:

– только запись в журнал,

– выключение,

– восстановить последнюю резервную копию настроек,

2) файловая система заполнена:

– только запись в журнал,

– выключение,

– исправить,

3) не запускается веб-сервер:

– только запись в журнал,

– выключение,

– исправить,

– восстановить последнюю резервную копию настроек,

4) не запускается СОВ:

– только запись в журнал,

– выключение,

– исправить,

– восстановить последнюю резервную копию настроек.

5) не запускается http-прокси:

– только запись в журнал,

– выключение,

– исправить,

– восстановить последнюю резервную копию настроек.

6) не запускается ftp-прокси:

– только запись в журнал,

– выключение,

– исправить,

– восстановить последнюю резервную копию настроек.

В случае сбоя в журнале аудита регистрируются следующие сообщения (рисунок 84):

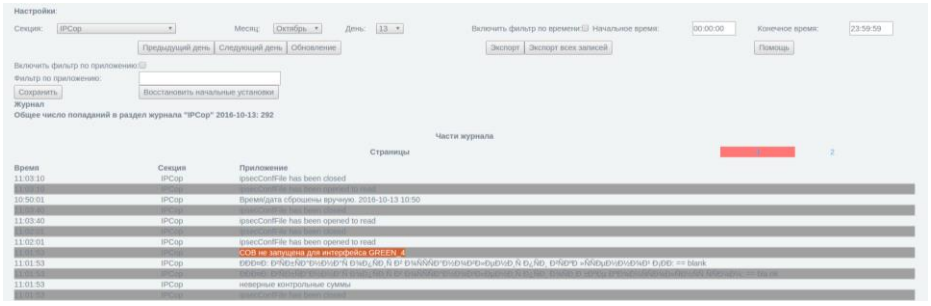


Рисунок 84 - Сообщение от утилиты восстановления

1) «файл конфигурации системы автоматического восстановления не найден» - сообщение появляется при ошибке чтения файла конфигурации утилиты автоматического восстановления;

2) «неверные контрольные суммы» - индикация ошибки;

3) «не удалось восстановить конфигурацию из резервной копии» - сообщение появляется при ошибке восстановления из резервной копии (самой новой из имеющихся);

4) «не удалось выключить Рубикон» - сообщение появляется при ошибке выключения Рубикон;

5) «критически мало места на жёстком диске» - индикация ошибки;

6) «не удалось очистить /var/log/archives» - сообщение появляется в случае ошибки действия «Исправить» при неисправности «мало места на ЖД»;

7) «директория /var/log/archive очищена, но места на жёстком диске недостаточно для стабильной работы» - сообщение появляется в случае, если старые логи очищены, но места на диске всё равно мало;

8) «не удалось перезапустить веб-сервер» - сообщение появляется в случае ошибки действия «Исправить» при неисправности «веб-сервер не запущен»;

9) «СОВ не запущена для интерфейса» - индикация ошибки;

10) «не удалось перезапустить СОВ для интерфейса»;

11) «http-прокси не запущен» - индикация ошибки;

12) «не удалось перезапустить http-прокси»;

13) «ftp-прокси не запущен» - индикация ошибки;

14) «не удалось перезапустить ftp-прокси»;

10.2 Консоль восстановления

Консоль восстановления создана для возможности восстановления системы в случае неработоспособности или отсутствия доступа к веб-интерфейсу.

Консоль восстановления реализуется посредством подключения к аппаратной платформе КП ПАВ «Рубикон» монитора и клавиатуры. При первом включении устройства на мониторе отображается информация об автозагрузке и выводится поле ввода логина и пароля (см. рисунок 85).

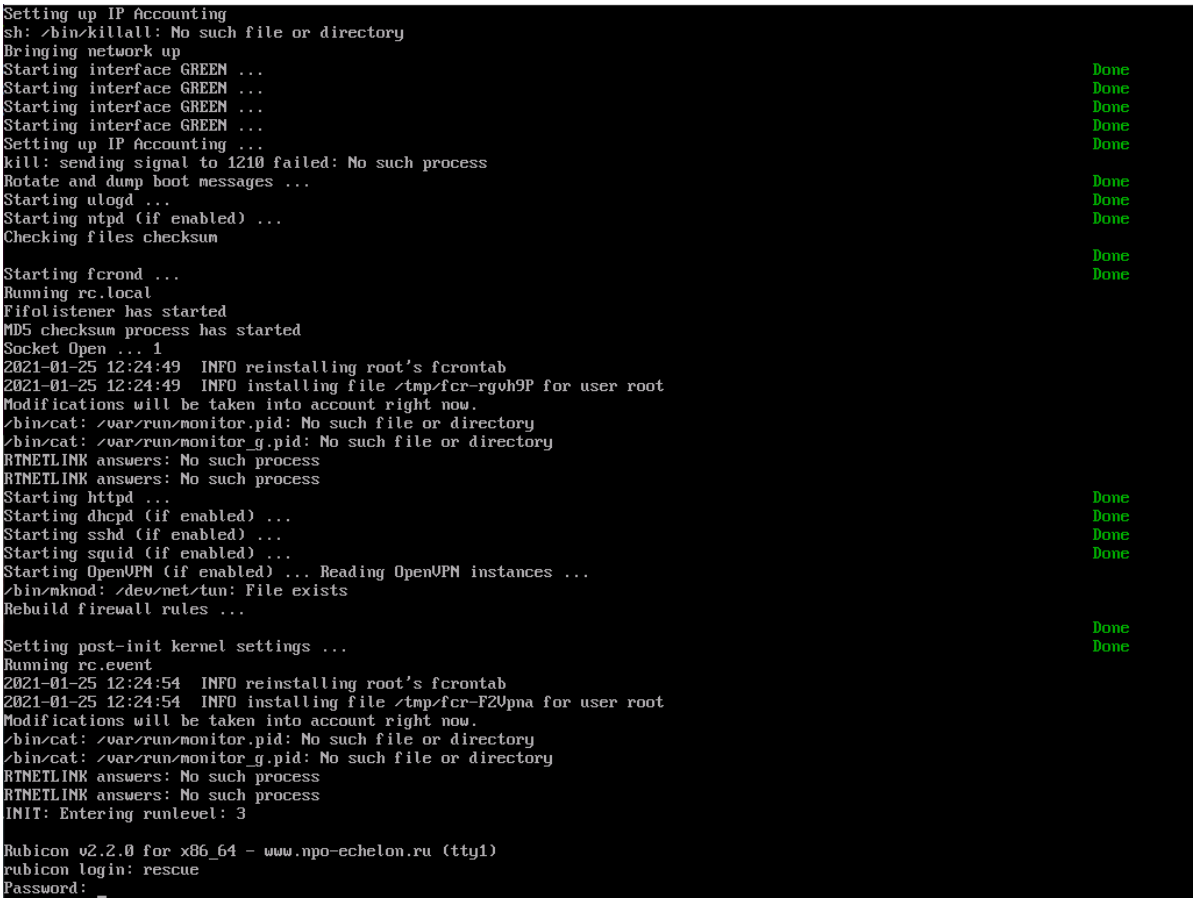


Рисунок 85 – Информация об автозагрузке и поле ввода логина и пароля

После ввода пароля открывается командная строка (рисунок 86).

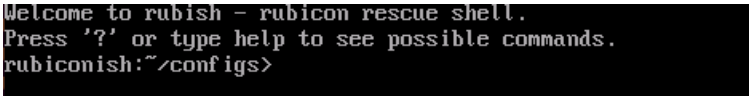


Рисунок 86 – Командная строка

При нажатии на клавишу «?» или вводе команды «Help» на экран выводится перечень и краткое описание доступных к использованию в консоли команд (рисунок 87).

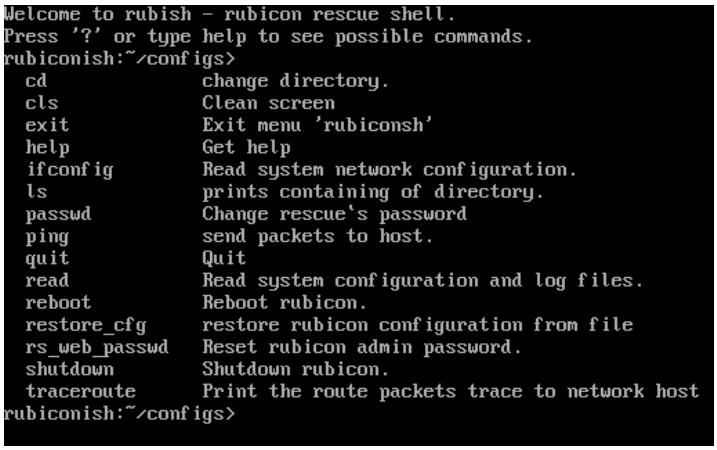


Рисунок 87 – Перечень и краткое описание доступных к использованию команд консоли

cd «опционально path name» — команда позволяет осуществить переход в папку /home, /var/logs, /configs, cd без параметров осуществляет переход в папку /configs.

cls — команда очистки экрана.

exit (а также «q» и «ctrl-d» «quit») — выход.

ls «опцинальные параметры» — команда выводит список файлов и папок в указанном каталоге. Принимает до 10 параметров, например:

```
rubiconish:~/>ls -l
drwxrwxr-x   2 root root  4096     28 13:50 bin
drwxr-xr-x   4 root root  1024     26 18:21 boot
```

Для просмотра доступных параметров введите команду «ls -help».

ping «опциональные параметры» «хост» — команда запускает пинг указанного хоста (по имени или по хосту). Принимает до 10 параметров, например:

```
rubiconish:~/configs>ping -c 2 8.8.8.8
  PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
  64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=69.5 ms
  64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=67.7 ms
  --- 8.8.8.8 ping statistics ---
```

```
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 67.775/68.683/69.591/0.908 ms
rubiconish:~/configs>
```

Для просмотра доступных параметров введите команду «ping -help».

read «filename» — позволяет посмотреть содержимое файла, выход по нажатию кнопки «q».

restore_cfg «файл» (опционально «--hadrware») — команда позволяет восстановить конфигурацию КП ПАВ «Рубикон». Если добавить параметр «--hardware», то также будут восстановлены настройки физических интерфейсов. Файлы в формате *.dat находятся в папке /home/httpd/html/backup.

traceroute «опциональные параметры» «хост» — команда позволяет определить маршрут до хоста. Принимает до 9 параметров:

- reboot — команда перезагрузки ЭВМ.
- shutdown — команда выключения ЭВМ.
- passwd — команда позволяет сменить пароль для пользователя rescue.
- rs_web_passwd — команда позволяет сбросить пароль администратора для web-интерфейса КП ПАВ «Рубикон». Пароль по умолчанию: radmin.
- ifconfig «опционально -a» — команда выводит конфигурацию интерфейсов. Доступен один опциональный параметр -a.

Все команды, введенные пользователем, сохраняются в текстовый файл /var/log/rubicon_shell_log.

При старте консоли пишется строка:

```
New session started. «имя пользователя» «дата» «время»
```

Все команды пишутся в формате:

```
«команда с параметрами» «пользователь» «время»
```

Файл с логами не доступен для редактирования. При попытке открыть его будет выдана ошибка, говорящая о том, что файл не найден.

Примечание – Использование консоли восстановления производится исключительно в целях восстановления и требует предварительного прохождения соответствующего обучения в компании АО «Эшелон». Ошибочно или произвольно введенные параметры команд могут послужить причиной некорректной работы КП ПАК «Рубикон».

11 ПРОВЕРКА ПРОГРАММЫ

11.1 Контроль целостности исполняемых файлов и файлов конфигурации

В КП ПАВ «Рубикон» предусмотрена возможность верификации целостности исполняемых файлов и файлов конфигурации администратором после успешного прохождения им процедуры авторизации.

Контроль целостности исполняемых файлов и файлов конфигурации проверяется с периодичностью 1 час и по запросу администратора.

Для контроля целостности исполняемых файлов и файлов конфигурации зайдите в раздел «Состояние → Контрольные суммы» и нажмите кнопку «Проверить контрольные суммы».

При наличии ошибок контрольных сумм исполняемых файлов и файлов конфигурации, результаты проверки будут отображены под надписью «Ошибки» (рисунок 88).

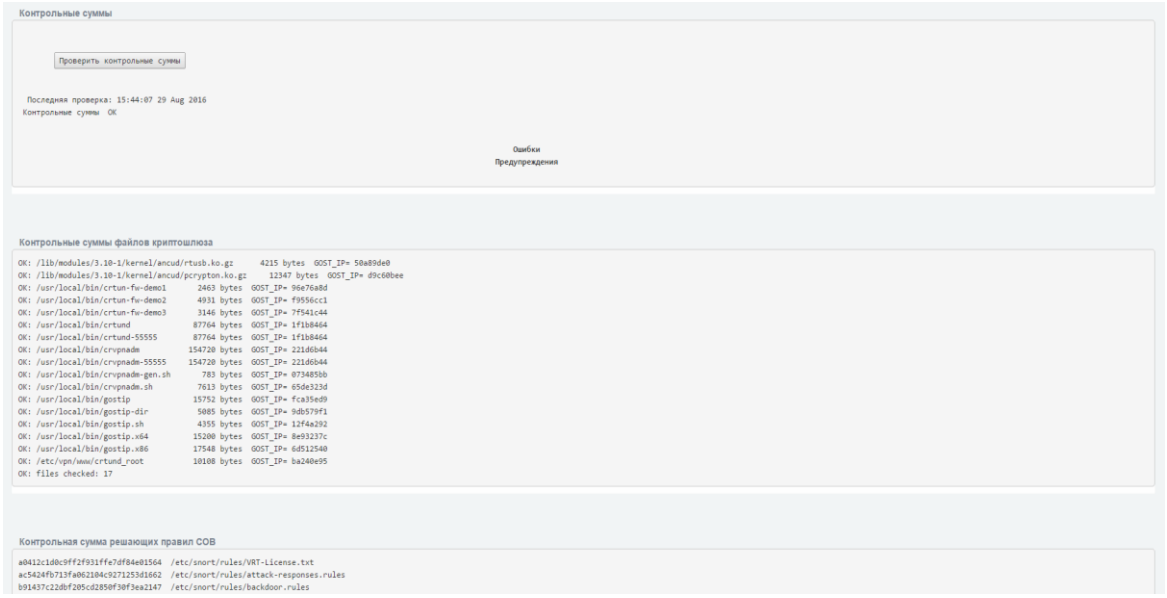


Рисунок 88 - Ошибка верификации контрольных сумм файлов КП ПАВ «Рубикон»

11.2 Тестирование САВЗ

Перейдите в раздел «Службы → Прокси» (рисунок 89).

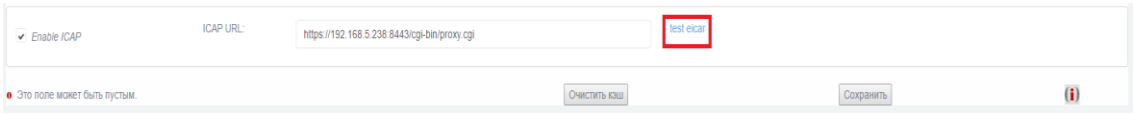


Рисунок 89 - Тестирование САВ3

Перейдите по ссылке «test eicar». После перехода по ссылке, будет выполнено тестирование САВ3.

12 ДЕЙСТВИЯ ПОСЛЕ СБОЯ ИЛИ ОШИБКИ

Большинство ошибок можно разделить на два типа:

1) Ошибки конфигурации:

– некорректные сетевые настройки,

– некорректные настройки фильтрации пакетов,

– некорректные правила СОВ.

Чаще всего их можно исправить переконфигурированием КП ПАВ «Рубикон», либо восстановлением из ранее сделанной резервной копии, либо восстановлением с установочного носителя.

2) Ошибки оборудования:

– выход из строя сетевых контроллеров,

– выход из строя дисковых накопителей.

В случае выхода из строя оборудования КП ПАВ «Рубикон» эксплуатировать нельзя, оборудование подлежит замене.

Возможны перезагрузки КП ПАВ «Рубикон», вызванные сбоями в питании. При кратковременном сбое КП ПАВ «Рубикон» может перезагрузиться самостоятельно, но чаще всего требуется включение вручную. При выключении КП ПАВ «Рубикон» сохраняются настройки и состояние сервисов, которые автоматически восстанавливаются после запуска. Однако для контроля ошибок рекомендуется не ранее чем через 30 секунд после запуска вручную проверять состояние запущенных сервисов.

13 ПРОЦЕДУРЫ ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

13.1 Общий порядок поставки обновлений

Доставка обновлений КП ПАВ «Рубикон» осуществляется с использованием сетевых протоколов передачи данных (загрузка с сервера АО «Научно-производственное объединение «Эшелон» – далее разработчик), параметры сервера обновлений: https://brp.cnpo.ru/brp/.

Процедура выпуска обновлений КП ПАВ «Рубикон» выглядит следующим образом:

– анализ сообщений о недостатках и потребностей пользователей;

– проектирование и разработка обновления продукта с учетом проведенного анализа;

– тестирование обновленного «Рубикон»;

– оценка влияния обновлений на функции безопасности «Рубикон»;

– выпуск документа «release notes», содержащего информацию об обновлении, процедур его получения, установки и верификации;

– при необходимости выпуск новой версии эксплуатационной документации;

– получение одобрения регулятора на внесение изменений в сертифицированное средство защиты информации;

– отгрузка файлов на сервер обновлений;

– предоставление обновлений пользователям для загрузки через закрытую часть сервера обновлений разработчика.

– доступ к закрытой части сервера обновлений разработчика осуществляется при условии действующей технической поддержки и регистрационных данных для входа в закрытую часть сервера обновлений (логин и пароль).

В течение жизненного цикла продукта могут выпускаться следующие типы выпускаемых обновлений:

a) пакет обновления основной версии (Feature Pack) - обновленная основная версия с добавлением новых функциональных возможностей; выпускается раз в год в течение жизни основной версии, является полнофункциональной версией продукта;

b) патч (Bugfix) - исправление недостатков продукта в основной версии или пакете обновления, выпускается по мере необходимости;

с) пакет модификаций (Service Pack) - дистрибутив, содержащий все патчи, выпущенные за период после последней сертификации или инспекционного контроля. Выпускается в случае накопления большого количества патчей.

13.2 Процедуры и меры безопасности при обновлениях

13.2.1 Оповещение покупателя КП ПАВ «Рубикон» об обновлении

Разработчик ведет учет покупателей КП ПАВ «Рубикон». Выполняется первичная регистрация следующей информации: наименование организации, адрес организации, номер знака соответствия. С целью получения сведений о выходе обновлений программного обеспечения покупателю необходимо отправить на rubikon@npo-echelon.ru контактную информацию, содержащую ФИО и электронный адрес лица, обеспечивающего администрирование «Рубикон». В теме письма необходимо указать «Рубикон. Получение доступа к закрытой части». В ответ придёт электронное письмо с регистрационными данными (логин и пароль) для входа в закрытую часть сервера обновлений.

Уведомление пользователей о выпуске обновления КП ПАВ «Рубикон» выполняется с использованием рассылки электронных почтовых сообщений с адреса электронной почты support.rubikon@cnpo.ru. Разработчик направляет документ «release notes» в адрес зарегистрированных пользователей. Данный документ содержит описание обновления, процедур получения и контроля целостности обновления, процедур тестирования, установки, применения и верификации.

Аналогичным способом разработчик осуществляет уведомление при выпуске обновлений правил БРП.

13.2.2 Доставка и контроль целостности обновления

Обновления программного обеспечения КП ПАВ «Рубикон» и BIOS аппаратной платформы, успешно прошедшие контроль влияния на безопасность изделия, публикуются в закрытой части сервера разработчика. Доступ пользователей к закрытой части сервера осуществляется с использованием регистрационных данных (логин и пароль), а также наличия действующей технической поддержки. Получение регистрационных данных описано в п. 13.2.1.

При публикации обновлений КП ПАВ «Рубикон» также публикуется файл сертификата его подписи. После получения обновления пользователь имеет возможность выполнить проверку его легитимности.

13.3 Тестирование обновления программного обеспечения

Обновления программного обеспечения необходимо тестировать на стенде перед их непосредственной установкой. Пример стенда для тестирования (рисунок 90).

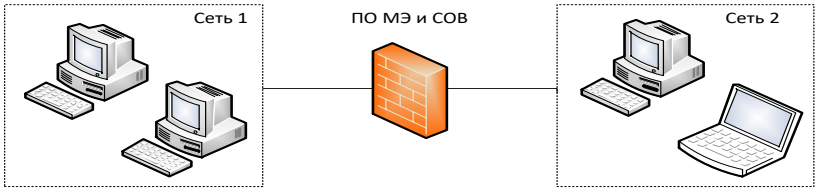


Рисунок 90 - Пример стенда для тестирования обновлений программного обеспечения КП ПАВ «Рубикон»

Тестирование обновлений программного обеспечения КП ПАВ «Рубикон» включает в себя следующие этапы:

1) задание правил фильтрации на КП ПАВ «Рубикон»;
2) проверка выполнения заданный правил на стенде.

Тестирование считается успешно пройдённым, если заданные правила выполняются в полном объеме.

13.4 Установка и применение обновления программного обеспечения

Обновление программного обеспечения КП ПАВ «Рубикон» устанавливается аналогично программному обсечению КП ПАВ «Рубикон». Подробнее процедуры установки и применения обновлений программного обеспечения описаны в разделе 4.1 «Установка ПО КП ПАВ «Рубикон».

13.5 Контроль установки обновления

Критерием правильности установки обновления программного обеспечения является доступность веб-интерфейса КП ПАВ «Рубикон» и отображение информации о новой версии программного обеспечения в разделе «Система» подразделе «О программе».

13.6 Верификация применения обновления

Подробнее процедуры верификации применения обновления программного обеспечения описаны в документе «Программно-аппаратный комплекс «Комплекс

противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с поддержкой виртуальных сетей». НПЕШ.465614.002. Тестовая документация. НПЕШ.465614.002 ТД».

13.7 Предоставление обновлений для проведения внешнего контроля

Процедура предоставления внешнего контроля уполномоченной организации:

a) уполномоченная организация обращается к Разработчику для предоставления доступа к обновлениям;

b) разработчик предоставляет организации доступ к серверу обновления на оговоренный срок.

Методика тестирования обновлений содержится в документе «Программно-аппаратный комплекс «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с поддержкой виртуальных сетей». НПЕШ.465614.002. Тестовая документация. НПЕШ.465614.002 ТД 01».

После проведение тестирования должны составляться протоколы и акты испытаний, которые должны оформляться в соответствии с ЕСКД.

13.8 Анализ влияния обновлений на безопасность КП ПАВ «Рубикон»

Обновление программного обеспечения КП ПАВ «Рубикон» будет влиять на все функции безопасности в связи с тем, что дистрибутив программного обеспечения при наличии новой версии обновляется целиком. В зависимости от типа обновления степень влияния на отдельные функции безопасности различается. Для определения степени влияния необходимо произвести тестирование КП ПАВ «Рубикон» согласно методикам, указанным в документе «Программно-аппаратный комплекс «Комплекс противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон» с поддержкой виртуальных сетей». НПЕШ.465614.002. Тестовая документация. НПЕШ.465614.002 ТД 01».

При наличии влияния обновления на ЗБ разработчик выпускает новую версию ЗБ.

13.9 Патч «update-0.7-12»

Патч «update-0.7-12» производит следующие изменения:

1) модифицирует работу функции ограничения трафика (выставление ограничений для входящего и исходящего трафика);

2) обеспечивает отслеживание переполнения и очистку диска для хранения журналов при ротации журналов;

3) модифицирует процедуру изменения роли пользователя таким образом, что исчезает необходимость ввода пароля для этого действия;

4) исключает страницу ввода паролей в разделе меню «Система», дублирующую функции страницы настройки прав и полномочий пользователей;

5) корректирует работу элементов управления, отвечающих за отключение сетевых интерфейсов, на странице настройки;

6) обеспечивает дополнительную проверку запуска сетевого моста после перезагрузки системы.

13.10 Патч «update-tls-0.2-1»

Патч «update-tls-0.2-1» производит следующие изменения:

1) вносит изменения в службы веб-сервера для возможности работы с более стойкими группами Диффи-Хелмана (длиной больше 1024 бит);

2) осуществляет замену сертификата веб-сервера, сгенерированный с ключом RSA 4096 бит и с использованием алгоритма хэширования SHA512;

3) вносит изменения в конфигурацию веб-сервера для запрещения работы со слабыми алгоритмами шифрования.

14 ПРОЦЕДУРЫ ОБНОВЛЕНИЯ БРП

14.1 Общий порядок поставки БРП

Доставка обновлений БРП осуществляется с использованием сетевых протоколов передачи данных (загрузка с сервера разработчика), параметры сервера обновлений: https://brp.cnpo.ru/brp/upd_rubicon_mo_rules.tar.gz.

Разработчик осуществляет проверку, адаптацию обновлений от различных компаний-поставщиков обновлений БРП (далее – поставщик БРП).

14.2 Локализация и противодействие новому типу вторжения (атаки)

14.2.1 Фиксация появления нового типа вторжения

Обновление БРП является важным аспектом эффективного функционирования системы обнаружения вторжения.

Поставщик БРП осуществляют постоянный мониторинг появления новых сетевых атак. Обнаруженные атаки локализуются, и на их основе формируется ежемесячное обновление.

Разработчик на постоянной основе осуществляет загрузку, проверку и анализ обновлений от поставщика БРП.

Кроме того, разработчик независимо от поставщика БРП осуществляет постоянный мониторинг появления новых сетевых угроз. На основании проведенного мониторинга разработчик может пополнить обновленную БРП собственными правилами, а также модифицировать полученные от поставщика БРП правила.

Существует два механизма, которые используются для обнаружения новых типов вторжений:

– исследовательские работы разработчика;

– акты рекламации, поступающие от пользователей сертифицированного изделия «Рубикон».

Исследовательские работы предусматривают анализ открытых источников данных сети «Интернет», содержащих сведения об уязвимостях программного обеспечения: cve.mitre.org, secunia.com, nvd.nist.gov, cvedetails.com.

При получении акта рекламации выполняется анализ вторжения, описание которого не присутствует в текущей БРП. Выполняются тестовые атаки и исследования на стенде

предприятия-разработчика для изучения атаки и формирования ее признаков. По результатам изучения нового типа вторжения устанавливается его актуальность и признаки, которые могут быть использованы для его обнаружения.

14.2.2 Предоставление обновления

Процедура предоставления покупателям обновлений БРП в общем случае выглядит следующим образом:

1) загрузка обновлений с серверов поставщика БРП, предоставляющих обновления БРП для разработчика;
2) проверка целостности загруженных обновлений;
3) обработка БРП;
4) тестирование работоспособности СОВ с обновленными правилами;
5) оценка влияния обновленных БРП на функции безопасности СОВ;
6) подготовка к отгрузке обновленных БРП:
   a) формирование архива с БРП;
   b) формирование файла сертификата подписи;
   c) отгрузка файлов на сервер обновлений;
7) предоставление обновлений БРП клиентам для загрузки через закрытую часть сервера обновлений разработчика.
8) доступ к закрытой части сервера обновлений разработчика осуществляется при условии действующей технической поддержки и регистрационных данных для входа в закрытую часть сервера обновлений (логин и пароль).

14.3 Процедуры и меры безопасности при обновлении БРП

14.3.1 Оповещение об обновлении

Разработчик ведет учет покупателей «Рубикон». Выполняется первичная регистрация следующей информации: наименование организации, адрес организации, номер знака соответствия. С целью получения сведений о выходе новых правил БРП, покупателю необходимо отправить на rubikon@npo-echelon.ru контактную информацию, содержащую ФИО и электронный адрес лица, обеспечивающего администрирование «Рубикон». В теме письма необходимо указать «Рубикон. Получение доступа к закрытой части». В ответ придёт электронное письмо с регистрационными данными (логин и пароль) для входа в закрытую часть сервера обновлений.

Уведомление пользователей о выпуске обновления БРП выполняется с использованием рассылки электронных почтовых сообщений.

При необходимости получения консультации по тому или иному правилу в обновленной БРП пользователю следует обратиться в техническую поддержку предприятия-изготовителя.

14.3.2 Доставка и контроль целостности БРП

Обновления БРП, успешно прошедшие контроль влияния на безопасность «Рубикон», публикуются в закрытой части сервера разработчика. Доступ пользователей к закрытой части сервера осуществляется с использованием учетной записи и пароля. Получение учётной записи описано в п 14.3.1. При публикации обновления БРП публикуется файл сертификата его подписи. После получение обновления БРП пользователь имеет возможность выполнить контроль его легитимности.

14.4 Предоставление обновлений для проведения внешнего контроля

Процедура предоставления внешнего контроля уполномоченной организации реализуется следующим образом:

1) уполномоченная организация обращается к Разработчику для предоставления доступа к обновлениям;

2) Разработчик предоставляет организации соответствующее ПО для осуществления контроля (ПО СОВ);

3) Разработчик предоставляет организации доступ к серверу обновления на оговоренный срок.

Анализ влияния обновления БРП на безопасность КП ПАВ «Рубикон» выполняется на стенде Разработчика (рисунок 91).

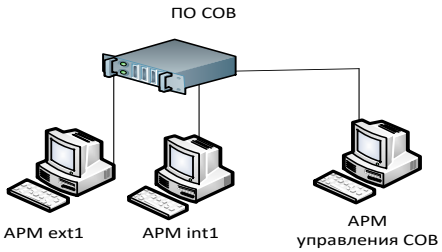


Рисунок 91 - Схема стенда анализа влияния обновления БРП на безопасность КП ПАВ «Рубикон»

14.5 Настройки BIOS

Имеется возможность осуществлять управление загрузкой с удаленного АРМ посредством консольного перенаправления. Консольное перенаправление позволяет наблюдать и конфигурировать систему с удаленной терминальной АРМ, перенаправляя клавиатурный ввод и текстовый вывод на последовательный порт.

Базовая система ввода-вывода позволяет перенаправлять консольный ввод/вывод на последовательный порт. Сконфигурировав порт, можно получать удаленный доступ ко всей загрузочной последовательности через COM-порт.

Следующие шаги иллюстрируют, как можно воспользоваться этой функцией:

1) Подключите консольный нуль-модемный кабель одной стороной в консольный порт системы, а другой стороной в последовательный порт удаленного АРМ;

2) Выставите следующие настройки в меню установки BIOS (BIOS Setup Menu):

BIOS > Advanced > Remote Access Configuration > Serial Port Mode > [115200, 8, n, 1];

3) Перейти на вкладку «Save & Exit» и сохранить изменения, выбрав «Save Changes and Exit»;

4) Сконфигурируйте последовательный порт на удаленном АРМ. Ниже приведен пример для платформы Windows XP:

a) Нажмите кнопку «Пуск», перейдите в меню Программы> Стандартные> Связь и запустите программу HyperTerminal;

b) Введите имя нового подключения и выберите любую иконку, нажмите «OK»;

c) Из выпадающего меню «Подключаться через» выберите соответствующий COM-порт на удаленном АРМ и нажмите «OK»;

d) Установите скорость обмена 115200, «Нет» в ниспадающем списке «Управление потоком», 8 бит данных, «Нет» в ниспадающем списке «Четность» и 1 стоповый бит.

Для того, чтобы отключить удаленное управление в настройках меню установки BIOS (BIOS Setup Menu), выполнить: BIOS> Advanced> Console Redirection> [Disabled]; далее перейти на вкладку «Save & Exit» и сохранить изменения, выбрав «Save Changes and Exit». Для установки пароля BIOS в настройках меню установки (BIOS Setup Menu), выполнить:

– BIOS >Security>Administrator Password и установить пароль;

– перейти на вкладку «Save & Exit» и сохранить изменения, выбрав «Save Changes and Exit».

15 СООБЩЕНИЯ АДМИНИСТРАТОРУ

15.1 Сообщения, регистрируемые при функционировании «Рубикон»

Сообщения веб-интерфейса «Рубикон» представлены в таблице 4.

Таблица 4 - Сообщения веб-интерфейса «Рубикон»

Код	Сообщение	Описание
102	Processing (идет обработка)	Информирование клиента о необходимости сбросить время ожидания ответа от сервера
200	Ok (Хорошо)	Запрос клиента обработан корректно
202	Accepted (принято)	Запрос от клиента принят на обработку, но обработка не завершена
204	No Content (нет содержимого)	Запрос обработан, но в ответ были переданы только заголовки без тела сообщения
301	Moved Permanently (постоянное перемещение)	Ресурс был постоянно перенесен на новый URL
302	Moved Temporarily (временное перемещение)	Ресурс был временно перенесен на новый URL
303	See Other (перенаправление)	Данные располагаются по другому URL
307	Temporary Redirect (временное перенаправление)	Ресурс временно доступен по другому URL
308	Permanently Redirect (постоянное перенаправление)	Ресурс постоянно доступен по другому URL
400	Bad Request (плохой запрос)	Сервер обнаружил в запросе клиента синтаксическую ошибку
401	Unauthorized (не авторизован)	Для доступа к запрашиваемому ресурсу требуется аутентификация
403	Forbidden (запрещено)	Сервер обработал запрос, но доступ к ресурсу для клиента запрещен
404	Not Found (не найден)	Сервер обработал запрос, но ресурс не найден

Код	Сообщение	Описание
405	Method Not Allowed (метод не разрешен)	Указанный клиентом метод нельзя применить к текущему ресурсу
406	Not Acceptable (неприемлемо)	Ошибки в заголовке запроса
408	Request Timeout (истекло время ожидания)	Время ожидания сервером данных от клиента истекло
410	Gone (удален)	Ресурс больше не находится по данному URL адресу
411	Length Required (необходима длина)	Клиент должен указать Content-Length для запроса к серверу
413	Payload Too Large (слишком большая полезная нагрузка)	Слишком большое тело в запросе
414	URI Too Long (URI слишком длинный)	Слишком длинный URI в запросе
429	Too Many Requests (слишком много запросов)	Клиент отправляет слишком много запросов за короткое время
431	Request Header Fields Too Large (поля заголовка запроса слишком длинные)	Слишком длинный заголовок в запросе
434	Requested host unavailable (адрес не доступен)	Запрашиваемый адрес недоступен
500	Internal Server Error (внутренняя ошибка сервера)	Любая внутренняя ошибка сервера
501	Not Implemented (не реализовано)	Сервер не поддерживает возможности, необходимые для обработки запроса
503	Service Unavailable (сервис недоступен)	Сервер временно не может обрабатывать запросы
505	HTTP Version Not Supported (версия HTTP не поддерживается)	Сервер не поддерживает указанную в запросе версию протокола http
510	Not Extended (нет расширения)	Сервер не поддерживает расширение, использующее клиентом

Сообщения, которые регистрируются при функционировании «Рубикон» записываются в локальный журнал и передаются на удаленный сервер по протоколу syslog.

Сообщения имеют следующий формат:

<время и дата> <наименование> <сообщение>

где:

<время и дата> – время фиксации события;

<наименование> – наименование компонента;

<сообщение> – информационное сообщение от компонента, которое формируется в свободной форме.

Наименование компонента является источником события и может иметь следующие значения:

- kernel –ядро системы;
- httpdaccess – доступ к устройству через веб-интерфейс;
- cron – планировщик задач;
- ipcop – сетевой модуль;
- red – модель функционирования NAT;
- dns – модуль DNS;
- dhcp – модуль DHCP;
- ntp – модуль NTP;
- auth – модуль аутентификации;
- installpackage – модуль установки пакетов;
- ipsec – модуль VPN;
- rules – модуль правил межсетевого экрана;
- errorlog – модуль легирования ошибок;
- audit – модуль аудита;
- proxy – модуль proxy;
- log – модуль логирования;
- idsadm – модуль настройки СОВ;
- snort – модуль СОВ;

Ошибку в компоненте можно определить по наличию в сообщении компонента одного из ключевых слов: error/failed/ошибка.

Предупреждение в компоненте можно определить по наличию в сообщении компонента одного из ключевых слов: warning/предупреждение.