Закрытое акционерное общество «Научно–Производственное Объединение «Эшелон»

УТВЕРЖДЕНО
НПЭШ.05002–01 32–ЛУ

КОМПЛЕКС ПРОТИВОДЕЙСТВИЯ ПРОГРАММНО-АППАРАТНЫМ ВОЗДЕЙСТВИЯМ (КП ПАВ) «РУБИКОН»

Руководство администратора

НПЭШ.05002-01 32
Листов 53

2016

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

АННОТАЦИЯ

Настоящее руководство администратора НПЭШ.05002-01 32 предназначено для ознакомления потребителей с технической информацией о программном изделии «Комплексе противодействия программно-аппаратным воздействиям (КП ПАВ) «Рубикон», НПЭШ.05002-01 (далее — комплекс, изделие «Рубикон», «Рубикон»), изготавливаемом согласно техническим условиям НПЭШ.05002-01 ТУ.

СОДЕРЖАНИЕ

1. Описание и работа 5
1.1. Назначение изделия 5
1.2. Минимальные требования к компьютеру, на который устанавливается «Рубикон» 5
2. Использование по назначению 6
2.1. Установка комплекса «Рубикон» 7
2.2. Описание старта и процедура проверки правильности старта 7
3. Сетевые настройки 9
3.1. Общие положения 9
3.2. Переназначение цветов интерфейсов 10
3.3. Настройка сетевых адресов 11
3.4. Назначение псевдонимов 12
3.5. Настройка статической маршрутизации 13
3.6. Настройка работы комплекса «Рубикон» в режиме моста 13
4. Межсетевой экран 15
4.1. Общие положения 15
4.2. Настройка правил межсетевого экрана 15
4.3. Настройка фильтрации пакетов 15
4.4. Трансляция сетевых адресов 16
4.5. Трансляция портов 16
4.6. Пример настройки правил МЭ для пропускания сетевых пакетов на определённый порт 18
4.7. Пример настройки правил МЭ для перенаправления портов 30
4.8. Расширенный режим фильтрации сетевых пакетов 35
4.8.1. Порт источника 35
4.8.2. Ограничение частоты следования пакетов 36
4.8.3. Включение извещения о применении правила по электронной почте 36
4.8.4. Включение локального извещения о применении правила 37
4.8.5. Временной диапазон применения правила 37
4.8.6. Фильтрация по битовой маске 37
4.8.7. Фильтрация по мандатным меткам 37
5. Система обнаружения вторжений 39
5.1. Интерфейсы, доступные для запуска СОВ 39
5.2. Запуск СОВ на физическом интерфейсе 39
5.3. Режимы обнаружения 40
5.3.1. Сигнатурный анализ 40
5.3.2. Эвристический анализ 40
5.4. База решающих правил 40

5.4.1. Загрузка новой базы решающих правил 40
5.4.2. Настройка решающих правил 42
6. Службы 45
6.1. Настройка точного времени 45
6.2. Горячее резервирование 45
7. Состояние 49
7.1. Обзор использования трафика 49
8. Журналирование 51
8.1. Настройка удаленного копирования журналов 51

1. ОПИСАНИЕ И РАБОТА

1.1. Назначение изделия

Изделие «Рубикон» НПЭШ.05002-01 предназначено для межсетевого экранирования, фильтрации сетевого трафика, обнаружения вторжений, коммутации и шлюзования.

1.2. Минимальные требования к компьютеру, на который устанавливается «Рубикон»

Таблица 1 – Минимальные требования к компьютеру, на который устанавливается «Рубикон»

Процессор	старше Intel Pentium IV
Оперативная память	512 Мбайт
Свободное место на диске	не менее 1 Гбайт
Дополнительные требования к аппаратуре	USB 2.0, наличие 4 Ethernet-портов

2. ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ

Изделие «Рубикон» реализует следующие основные функции:

- фильтрация сетевых пакетов на всех уровнях вплоть до прикладного с учетом любых значимых полей;
- аутентификация входящих и исходящих запросов;
- регистрация фильтруемых пакетов и учет сервисов прикладного уровня;
- дистанционная сигнализация попыток нарушения правил фильтрации;
- идентификация и аутентификация администратора комплекса;
- препятствование доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась;
- регистрация входа (выхода) администратора комплекса в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- регистрация запуска программ и процессов (заданий, задач);
- регистрация действия администратора комплекса «Рубикон» по изменению правил фильтрации;
- возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;
- проверка целостности своей программной и информационной части по контрольным суммам, как в процессе загрузки, так и динамически;
- процедура восстановления после сбоев и отказов оборудования;
- вывод журнальной информации на удаленный сервер;
- резервирование;
- обеспечение подключения локальных вычислительных сетей (ЛВС) к инфраструктуре имеющихся сетей передачи данных (СПД) и организации сетевых соединений для двунаправленного прохождения сетевых пакетов, удовлетворяющих требованиям стека протоколов TCP/IP;
- возможность построения единой сети на основе инфраструктуры имеющихся независимых друг от друга сегментов сетей передачи данных с обеспечением «прозрачных» сетевых соединений между подключаемыми локальными вычислительными сетями (прямая адресация из каждой ЛВС в каждую).
- возможность назначения восьми IP-адресов каждому физическому интерфейсу;
- трансляция сетевых адресов по портам, указанным в составе сетевого пакета (NAT);
- обеспечение статической маршрутизации сетевых пакетов по заданным маршрутам;
  Примечание — Предусмотрена возможность задания «шлюза по умолчанию».
- обеспечение организации сетевых соединений в незащищённом и защищённых режимах с использованием протокола TLS 1.0;
- фильтрация сетевых пакетов:

- по сетевым адресам получателя и отправителя;
- по номерам портов получателя, отправителя;
- по используемым протоколам транспортного уровня (TCP, UDP);
- по мандатным меткам;

Примечание — В случае отсутствия мандатной метки в составе сетевого пакета, фильтрация сетевых пакетов по признаку мандатной метки не проводится. Предусмотрена возможность полного отключения фильтрации сетевых пакетов по мандатным меткам.

- обеспечение функций системы обнаружения вторжений;
- возможность удаленного копирования системой защиты информации (СЗИ) изделия журналов аудита комплекса;
- возможнось задания точного времени посредством клиента точного времени (NTP-клиент).

Комплекс «Рубикон» обеспечивает выполнение требований руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) к 2 классу защищенности.

2.1. Установка комплекса «Рубикон»

Перед установкой системы необходимо ознакомиться с документацией на систему, в частности, с аппаратными требованиями, предъявляемыми изделием «Рубикон».

Для выполнения установки комплекса «Рубикон» необходимо произвести загрузку с установочного носителя комплекса «Рубикон».

Установка представляет собой неинтерактивный процесс, в процессе которого устанавливается система, происходит настройка оборудования и задаются параметры системы по умолчанию.

После установки комплекса «Рубикон» система имеет сетевой интерфейс с IP-адресом `192.168.1.1`, через который может производиться начальная настройка параметров комплекса «Рубикон». При дальнейшей настройке параметры администрирования можно изменить.

2.2. Описание старта и процедура проверки правильности старта

Старт комплекса «Рубикон» начинается с загрузки операционной системы.

По окончании загрузки работоспособность и правильность старта можно проверить, выполнив команду ping 192.168.1.1 на любом из компьютеров, подключенных к внутренней защищаемой сети. Если ответ комплекса «Рубикон» получен, то удостовериться в его работе можно, подключившись по защищенному https-соединению https://192.168.1.1:8443. В случае загрузки web-страницы можно приступать к работе с изделием «Рубикон».

Для выполнения административных действий существует пароль по умолчанию **radmin** для учетной записи **admin**. При первом подключении к административному интерфейсу пароль необходимо изменить на странице **Система** → **Пароли** (Рисунок 1).

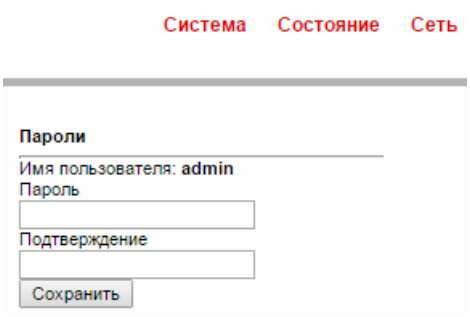


Рис. 1 – Система → Пароли

3. СЕТЕВЫЕ НАСТРОЙКИ

3.1. Общие положения

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

– физические сетевые интерфейсы:

1) красный: сетевой интерфейс, подключаемый к внешней сети. По умолчанию все пакеты, маршрутизируемые с красного интерфейса на зелёный (кроме пакетов, принадлежащих открытым TCP-сессиям), блокируются межсетевым экраном. На красном интерфейсе происходит трансляция сетевых адресов по портам, указанным в составе сетевого пакета;
2) зелёный: сетевой интерфейс, подключаемый к внутренней сети. По умолчанию все пакеты, маршрутизируемые между различными зелёными 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 разрешённых на странице **МЭ → Доступ к синему интерфейсу**.
4) оранжевый: демилитаризованная зона. По умолчанию все пакеты, маршрутизируемые с оранжевого интерфейса на зелёный (кроме пакетов, принадлежащих открытым TCP-сессиям), блокируются. При этом возможна настройка проброса портов с красного интерфейса на оранжевый для обеспечения работоспособности внешних сервисов;

– виртуальные сетевые интерфейсы:

1) IPSec — ipsecO, ipsecl, и т.д.;
2) OpenVPN — tunO, tunl, и т.д.;
3) Криптошлюз — vccO;
4) Мост — idsbr, brO, brl, и т.д.

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

Таблица 2 – Доступность политики в зависимости от цвета интерфейса

Интерфейс	Политика		
	Закрыто	Полуоткрыто	Открыто
Зелёный	√	√	√
Голубой	√	√	√
Оранжевый	√	×	√
Красный	√	×	×
OpenVPN	√	√	√
Мост	√	√	√
IPSec	√	√	√
Криптошлюз	√	√	√

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	Разрешён доступ в сеть	Разрешён доступ в сеть	Разрешён доступ в сеть и из сети
Исходящее	Доступ разрешён	Доступ разрешён	Доступ разрешён

3.2. Переназначение цветов интерфейсов

По умолчанию все физические интерфейсы изделия «Рубикон» являются зелёными. Для переназначения цветов интерфейсов необходимо:

- настроить администрирование комплекса «Рубикон» на странице **МЭ → Настройки межсетевого экрана** (Рисунок 2); по умолчанию первые четыре зелёных интерфейса помечены как административные, т.е. по ним разрешено администрирование комплекса «Рубикон»; цвет таких интерфейсов изменить нельзя, поэтому перед назначением цветов необходимо настроить администрирование;
- назначить цвета интерфейсов на странице **Сеть → Настройка адаптеров** (Рисунок 3); для этого напротив нужного интерфейса необходимо нажать кнопку редактирования, затем выбрать цвет интерфейса и для сохранения настроек нажать кнопку

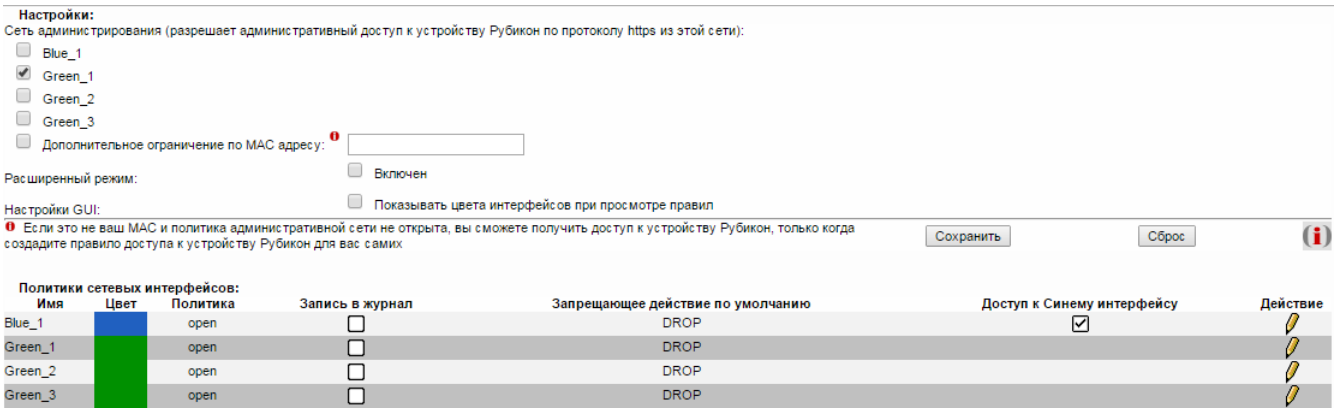


Рис. 2 – МЭ → Настройки межсетевого экрана

редактирования ещё раз; номера интерфейсов внутри цвета (напр., `GREEN 1`, `RED 2`) назначаются в инкрементивном порядке и не зависят от реальных имён интерфейсов;

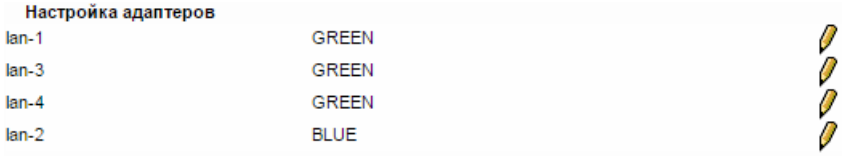


Рис. 3 – Сеть → Настройка адаптеров

– настроить сетевые адреса для изменённых интерфейсов (Рисунок 4).

После переназначения цветов интерфейсов для применения корректной политики МЭ необходимо перезагрузить комплекс «Рубикон», а также повторно настроить правила межсетевого экрана.

3.3. Настройка сетевых адресов

На странице настройки сетевых интерфейсов **Система** → **Интерфейсы** (Рисунок 4) задаются значения сетевых адресов, а также базовые настройки маршрутизации.

Для конфигурации сетевого адреса определённого интерфейса нужно ввести числовое значение адреса и маски сети (в полном числовом формате), а затем нажать кнопку **«Изменить»** напротив полей ввода. Новые значения присваиваются интерфейсу немедленно.

В поле «Шлюз» той страницы настройки интерфейсов вводится адрес шлюза по умолчанию. На указанный узел будут отправляться пакеты, для которых отсутствует актуальная запись в таблице маршрутизации.

Комплекс «Рубикон» может выполнять роль клиента службы DNS. Для корректной работы в таком режиме необходимо указать адрес как минимум одного сервера DNS и нажать кнопку **«Изменить»** напротив соответствующих полей ввода.

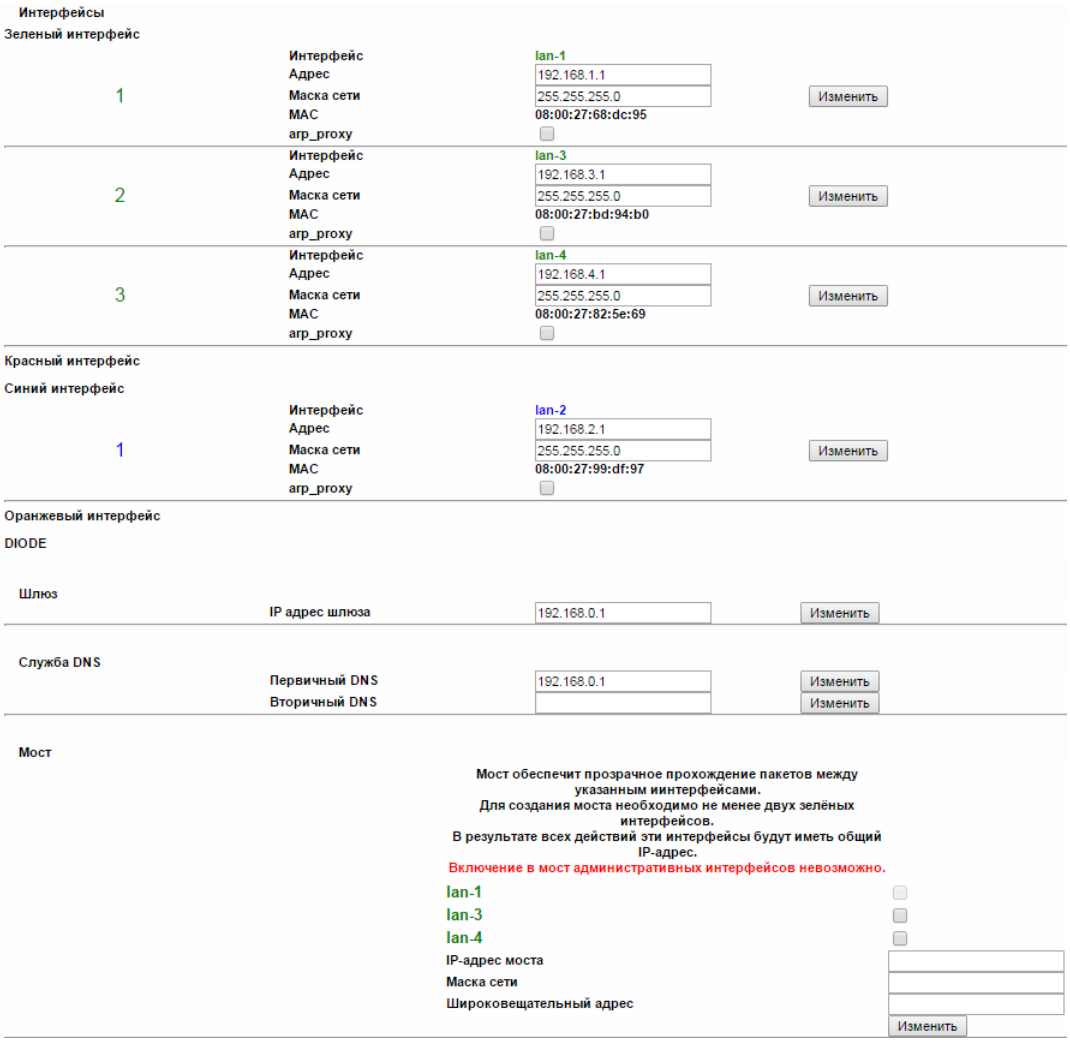


Рис. 4 – Система → Интерфейсы

3.4. Назначение псевдонимов

В изделии «Рубикон» существует возможность назначения до восьми IP-адресов каждому физическому интерфейсу. Данная возможность обеспечивается назначением псевдонимов интерфейсов в разделе **Сеть → Псевдонимы** (Рисунок 5).

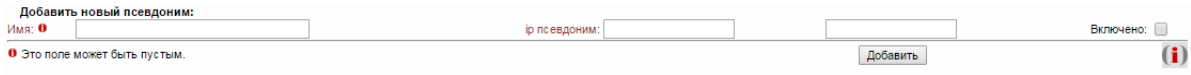


Рис. 5 – Сеть → Псевдонимы

Для задания псевдонима заполните необходимые поля и нажмите кнопку **«Добавить»** (Рисунок 6).

Примечание — Параметр «Имя» следует вводить в формате *<название физического интерфейса>:<номер интерфейса>*.

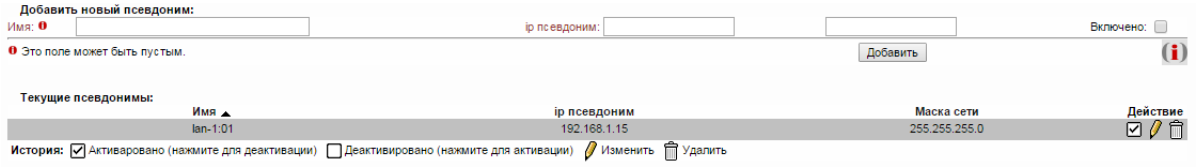


Рис. 6 – Добавление псевдонима

3.5. Настройка статической маршрутизации

В изделии «Рубикон» существует возможность задания статических маршрутов в ручном режиме. Для этого на странице **Сеть** → **Маршруты** (Рисунок 7) необходимо задать сеть, маску (в полном десятичном виде), промежуточный узел и интерфейс комплекса «Рубикон», через который он доступен, а также произвольное имя маршрута, состоящее из цифр и букв. В случае если все поля заполнены корректно и в соответствии с текущими сетевыми настройками, маршрут может быть добавлен (указанный интерфейс поднят, промежуточный узел доступен), изменения применяются незамедлительно.

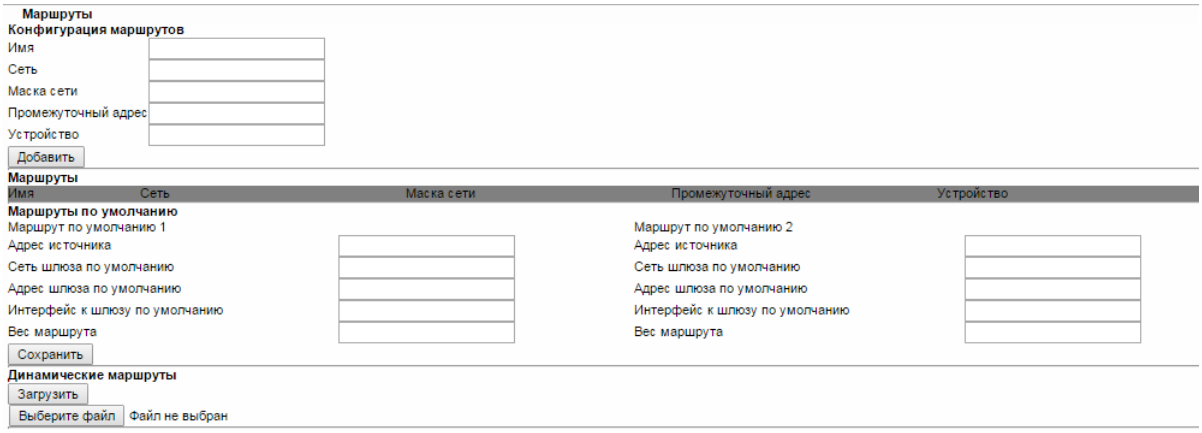


Рис. 7 – Сеть → Маршруты

Маршрут автоматически удаляется, если изменяются настройки (цвет, адрес, состояние) указанного сетевого интерфейса, либо если промежуточный узел становится недоступен.

Комплекс «Рубикон» не проверяет уникальность добавляемых маршрутов, т.е. не имеет защиты от т.н. «маршрутных петель». Корректность задаваемых маршрутов и отсутствие конфликтов маршрутизации должен проверять сетевой администратор.

3.6. Настройка работы комплекса «Рубикон» в режиме моста

В комплексе «Рубикон» существует возможность объединения нескольких зелёных интерфейсов в один с помощью технологии «bridge» (мост). После конфигурации этого режима выбранные интерфейсы потеряют свои IP-адреса и маршруты, а пакеты, приходящие на один

из объединённых интерфейсов, будут ретранслироваться на остальные интерфейсы, включённые в мост, **без обработки межсетевым экраном**. Правила межсетевого экрана должны настраиваться для виртуального интерфейса моста (`idsbr` или `brX`), а не для включённых в мост физических интерфейсов.

Для настройки режима моста нужно:

- пометить выбранные интерфейсы как неадминистративные на странице **МЭ** → **Настройки межсетевого экрана** (Рисунок 2);
- отметить галочками выбранные интерфейсы в секции «Мост» на странице настроек сетевых интерфейсов **Система** → **Интерфейсы** (Рисунок 4);
- по желанию задать сетевой адрес, маску и широковещательный адрес для моста;

  Примечание — Этот пункт можно опустить, если целью ставится настройка моста, не обнаружимого на сетевом уровне (напр., для режима СОВ). При задании данных полей интерфейсу «мост» (`idsbr`) назначается сетевой адрес, с помощью которого он может маршрутизироваться на сетевом уровне.
- нажать кнопку **«Изменить»** рядом с соответствующими полями ввода; изменения вступят в силу примерно через 30 секунд (точное время зависит от количества сетевых интерфейсов).

4. МЕЖСЕТЕВОЙ ЭКРАН

4.1. Общие положения

В комплексе «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: зелёный, красный, синий и оранжевый. Правила межсетевого экрана прикрепляются к имени интерфейса (напр., GREEN 1), поэтому после каждой смены ролей интерфейсов (см. 3.2.) необходимо перенастраивать правила МЭ в соответствии с текущими параметрами. Подробнее о настройке сетевых интерфейсов рассказано в разделе 3..

4.2. Настройка правил межсетевого экрана

В зависимости от роли сети настройка правил фильтрации осуществляется различными способами:

- фильтрация;
- трансляция сетевых адресов;
- трансляция портов.

4.3. Настройка фильтрации пакетов

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

Для настройки фильтрации пакетов необходимо выполнить следующие действия:

- настроить сетевые интерфейсы (Рисунок 4);
- перейти на страницу настройки правил фильтрации: **МЭ** → **Правила межсетевого экрана** (Рисунок 8);
- выбрать необходимое действие:
    1) для настройки фильтрации пакетов, следующих из одной сети в другую, нажать кнопку **«Другие из внутренней сети во внешнюю»**;
    2) для настройки административного доступа из зелёной, синей, оранжевой или виртуальной сети нажать кнопку **«Доступ к Рубикону»**;
    3) для настройки доступа к изделию «Рубикон» из красной сети нажать кнопку **«Доступ извне»**;
- настроить правило фильтрации, заполнив:
    1) информацию об источнике (интерфейс, сетевой адрес или адреса);

Рис. 8 – МЭ → Правила межсетевого экрана

2) информацию о месте назначения (интерфейс, сетевой адрес или адреса, протокол (службу) для которого определяется правило); при настройке административного доступа информация о месте назначения определяется параметрами комплекса «Рубикон»;
3) информацию о параметрах фильтруемых пакетов и решении о пропуске или отбрасывании их;

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

1) перейти к просмотру правила нажатием кнопки **«Следующий»**;
2) сохранить правило и вернуться к интерфейсу выбора необходимых действий по настройке правил нажатием кнопки **«Сохранить»**;
3) сбросить установленные параметры фильтрации нажатием кнопки **«Сброс»**;
4) выйти из интерфейса изменения правил без сохранения нажатием кнопки **«Отмена»**.

4.4. Трансляция сетевых адресов

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

4.5. 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 необходимо:

– настроить сетевые адреса красного и оранжевого или зелёного интерфейса (Рисунок 4);
– перейти на страницу настройки правил фильтрации: МЭ → Правила межсетевого экрана (Рисунок 8);
– нажать на кнопку «Перенаправление портов»;
– настроить правило фильтрации, заполнив (Рисунок 9):

1) информацию о параметрах источника пакета (адрес, порт);
2) номер протокола или сервис, который изделие «Рубикон» предоставляет в красную подсеть для доступа к требуемому узлу внутренней подсети;
3) информацию о месте назначения (интерфейс, адрес, порт, предоставляемый конкретным узлом);
4) информацию о параметрах фильтруемых пакетов и решении о пропуске или отбрасывании их;

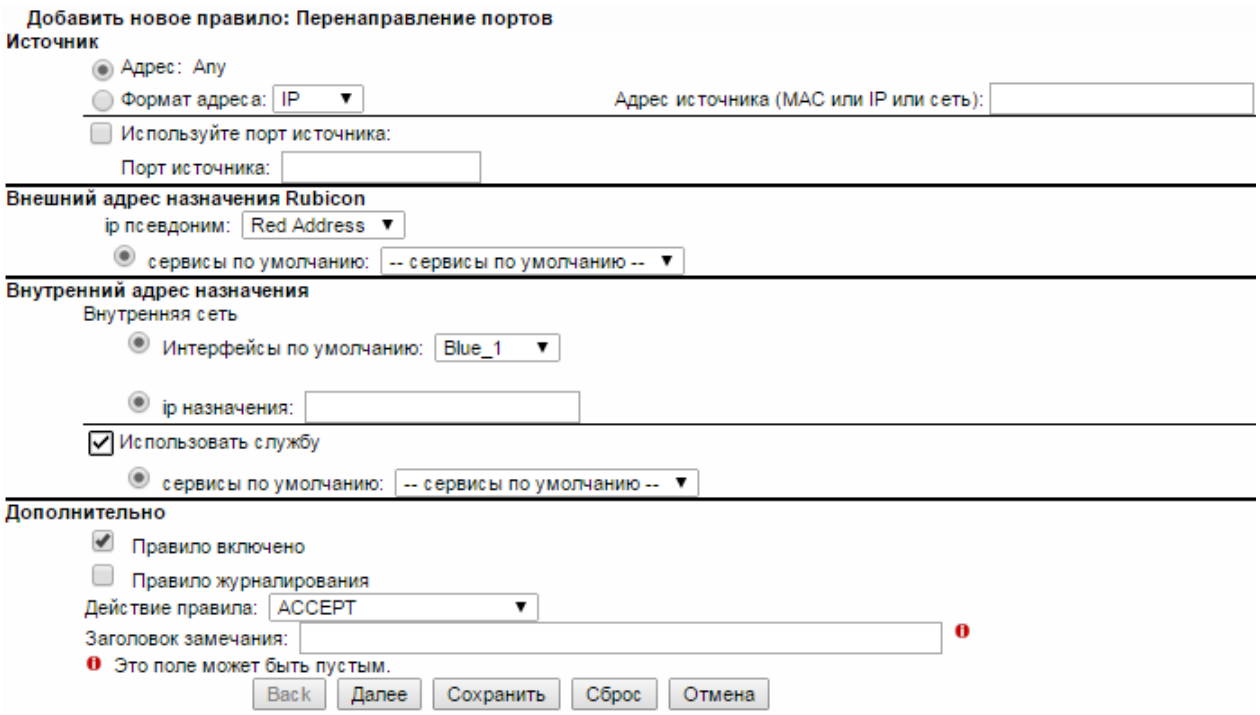


Рис. 9 – Правило «Перенаправление портов»

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

1) перейти к просмотру правила нажатием кнопки **«Далее»**;
2) сохранить правило и вернуться к интерфейсу выбора необходимых действий по настройке правил нажатием кнопки **«Сохранить»**;
3) сбросить установленные параметры фильтрации нажатием кнопки **«Сброс»**;

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

4.6. Пример настройки правил МЭ для пропускания сетевых пакетов на определённый порт

1) Настройка «Рубикона» без NAT.

Сетевая схема «Рубикона» без NAT представлена на рисунке 10.

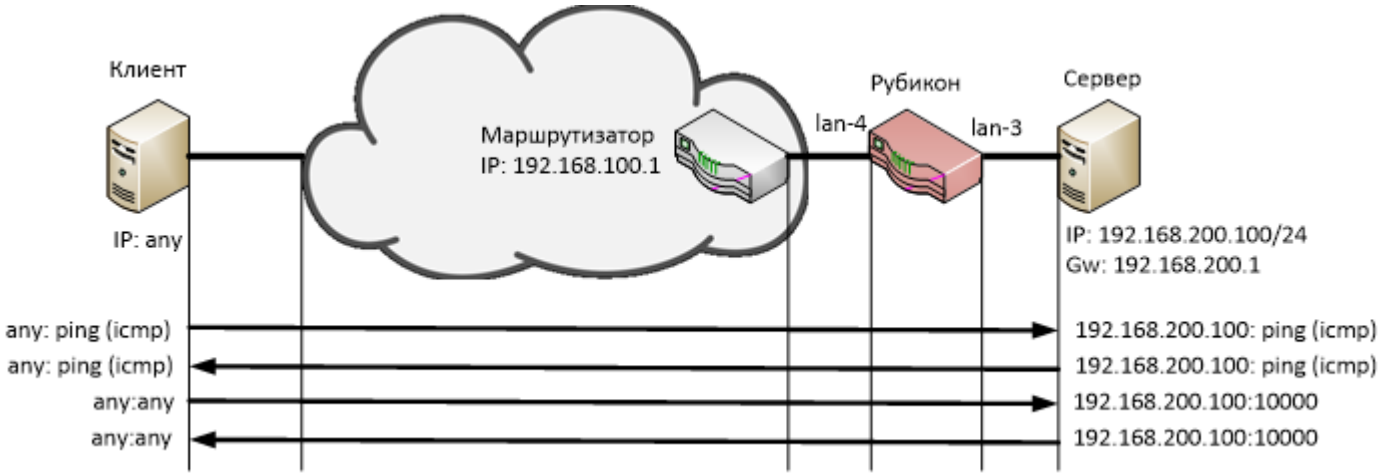


Рис. 10 – Сетевая схема «Рубикона» без NAT

Интерфейсы «Рубикона», участвующие в сетевом обмене, представлены в таблице 4.

Таблица 4 – Минимальные требования к компьютеру, на который устанавливается «Рубикон»

Интерфейсы	IP адрес	Маска сети	Политика
lan-3	192.168.200.1	255.255.255.0	зеленый
lan-4	192.168.100.100	255.255.255.0	зеленый
Шлюз по умолчанию	192.168.100.1		

Для настройки «Рубикона» без NAT необходимо:

– в веб-интерфейсе перейти на страницу: **МЭ→Настройка межсетевого экрана** и отключить администрирование интерфейсов, сняв галочки с интерфейсов в разделе «Настройки» и нажав «Сохранить»(Рисунок 11);

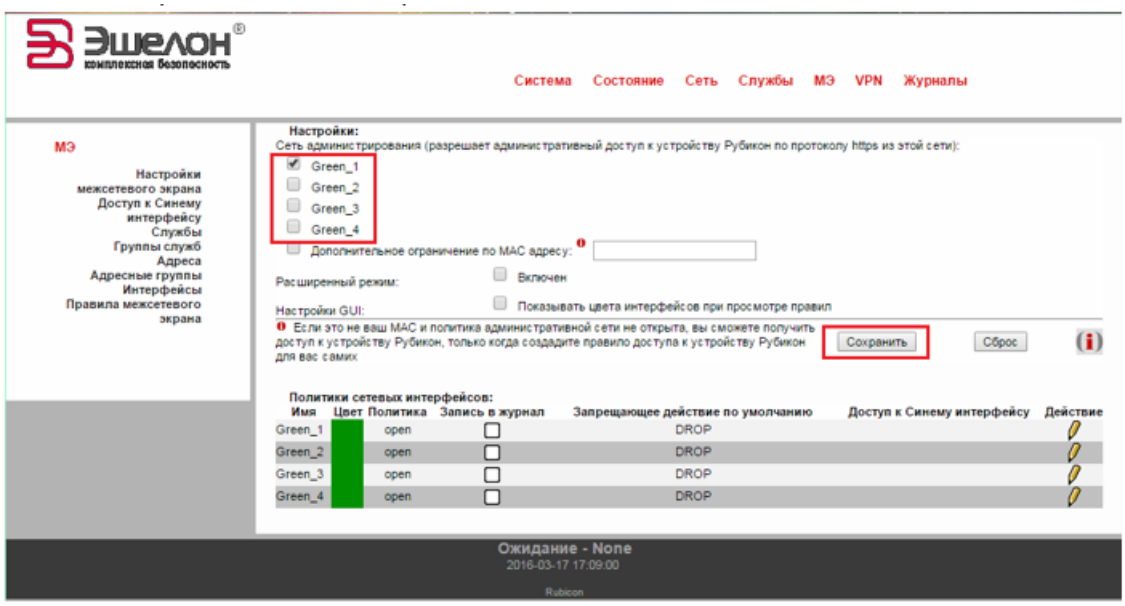


Рис. 11 – Отключение администрирования

– в веб-интерфейсе перейти на страницу: **Система→Интерфейсы** и настроить сетевые интерфейсы и маршрутизацию (Рисунок 12);

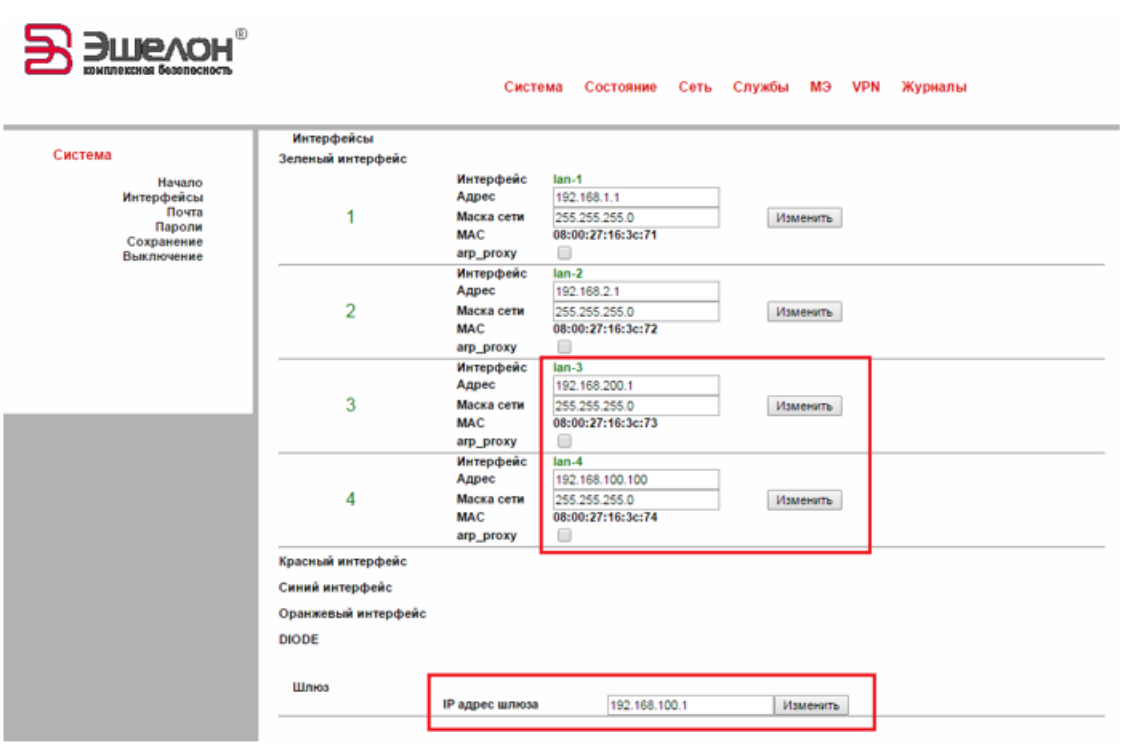


Рис. 12 – Настройки интерфейсов и маршрутизации

– в веб-интерфейсе перейти на страницу: **Состояние→Состояние сети** и проверить состояние сети (Рисунок 13);

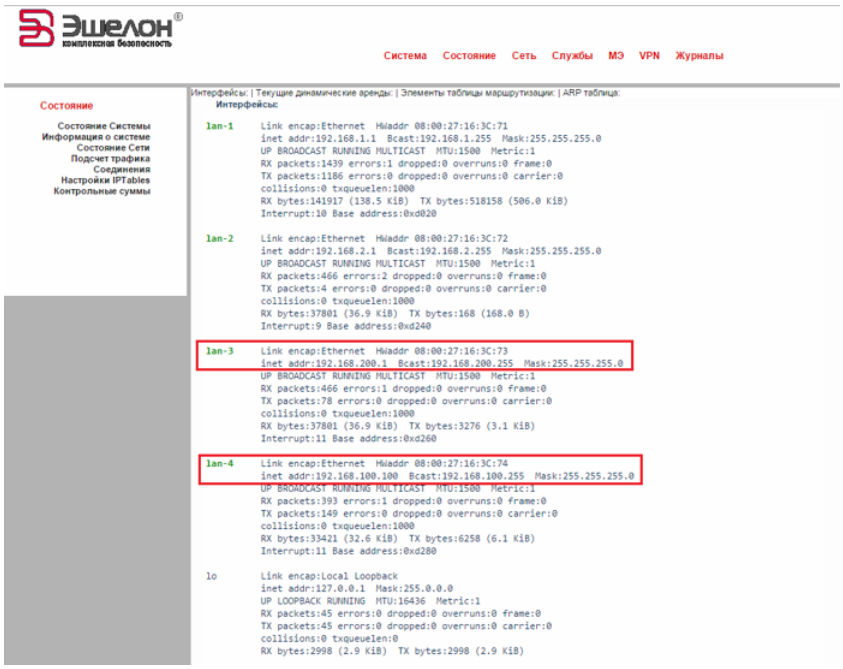


Рис. 13 – Проверка состояния сети

– в веб-интерфейсе перейти на страницу: **МЭ→Настройка межсетевого экрана** и включить расширенный режим СОВ (Рисунок 14);

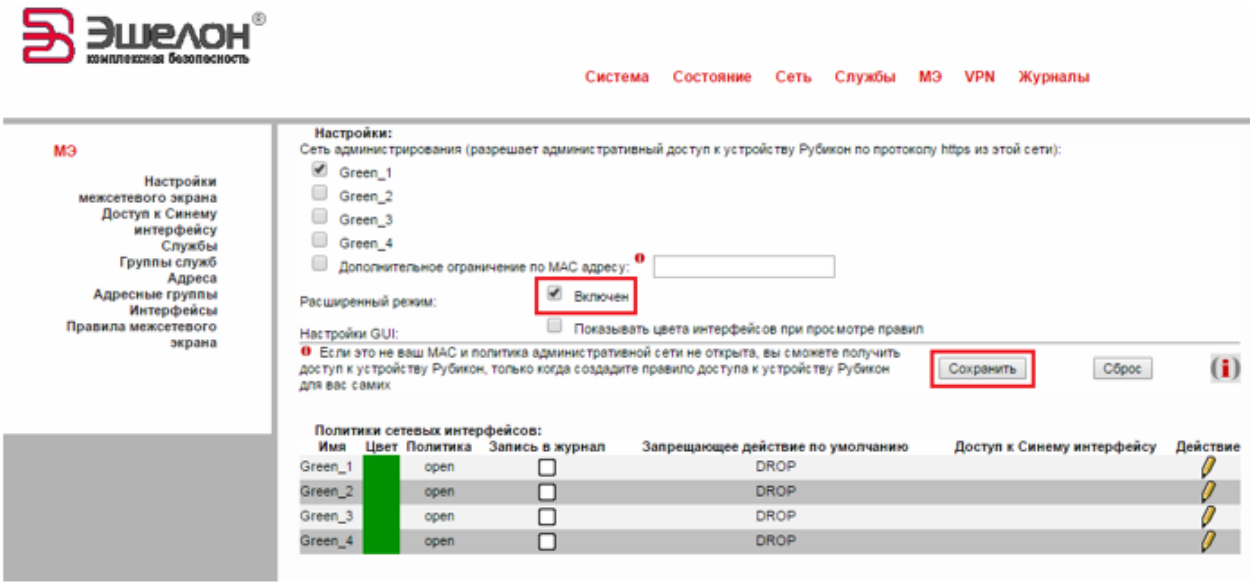


Рис. 14 – Включение расширенного режима СОВ

– в веб-интерфейсе перейти на страницу: **МЭ→Службы** и добавить службу 10000 для МЭ (Рисунок 15);

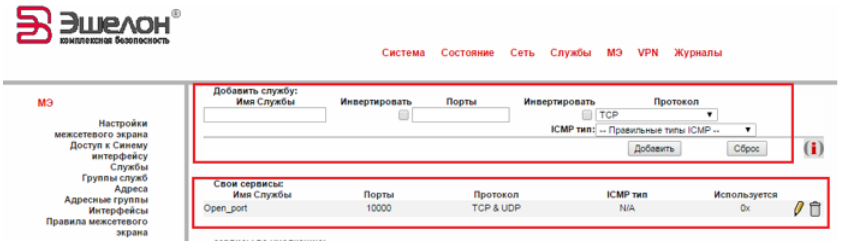


Рис. 15 – Добавление службы 10000

– в веб-интерфейсе перейти на страницу: **МЭ→Правила межсетевого экрана→Другие из внутренней сети во внешнюю** и добавить:

– ACCEPT: any:ping(icmp)→ 192.168.200.100:ping(icmp) (Рисунок 16);

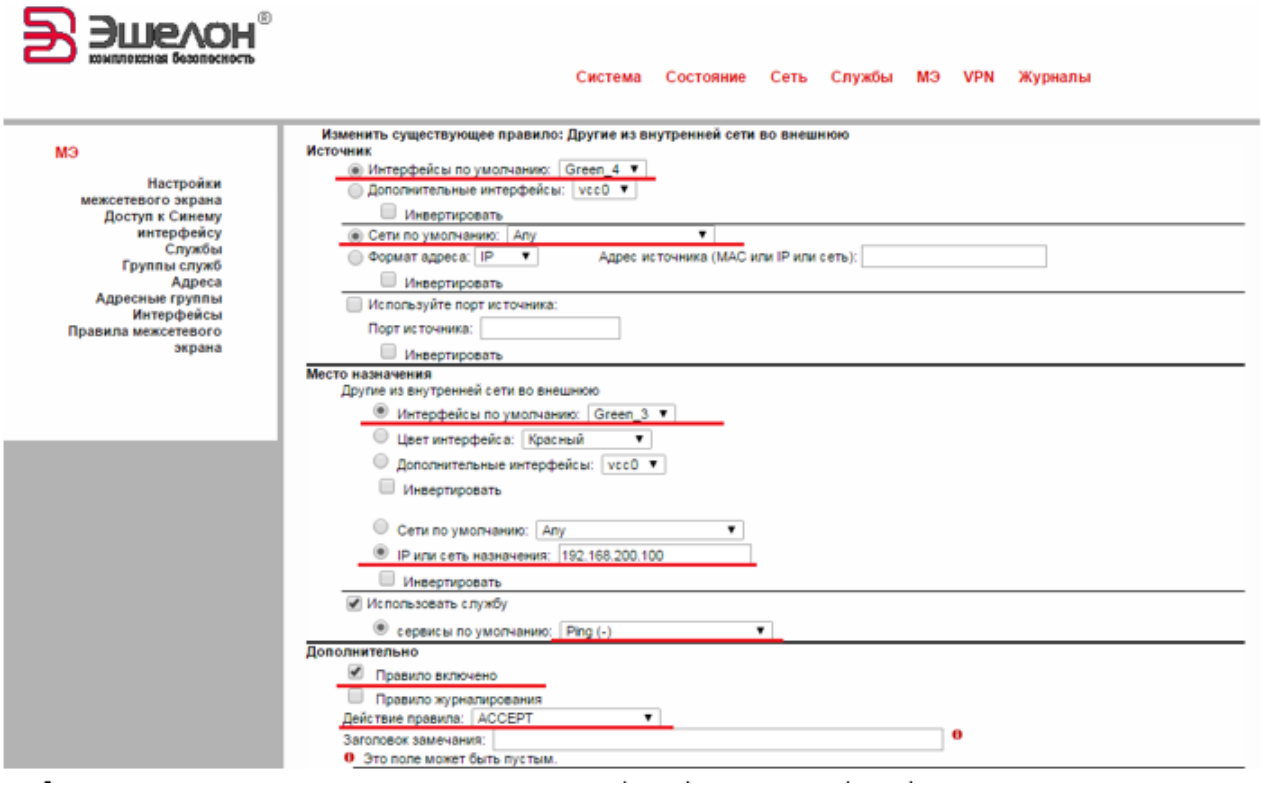


Рис. 16 – Добавление правила ACCEPT: any:ping(icmp)→ 192.168.200.100:ping(icmp)

– ACCEPT: 192.168.200.100:ping(icmp)→ any: ping(icmp)(Рисунок 17);

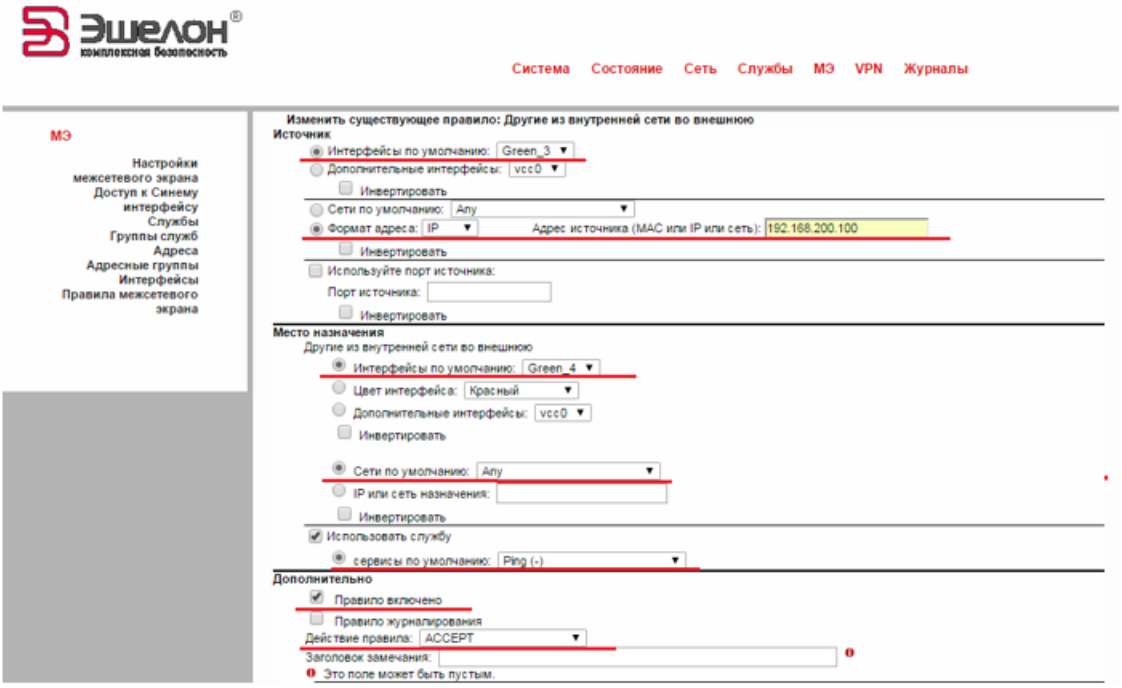


Рис. 17 – Добавление правила ACCEPT: 192.168.200.100:ping(icmp)→ any: ping(icmp)

– ACCEPT: any:any → 192.168.200.100:Open_port(10000)(Рисунок 18);

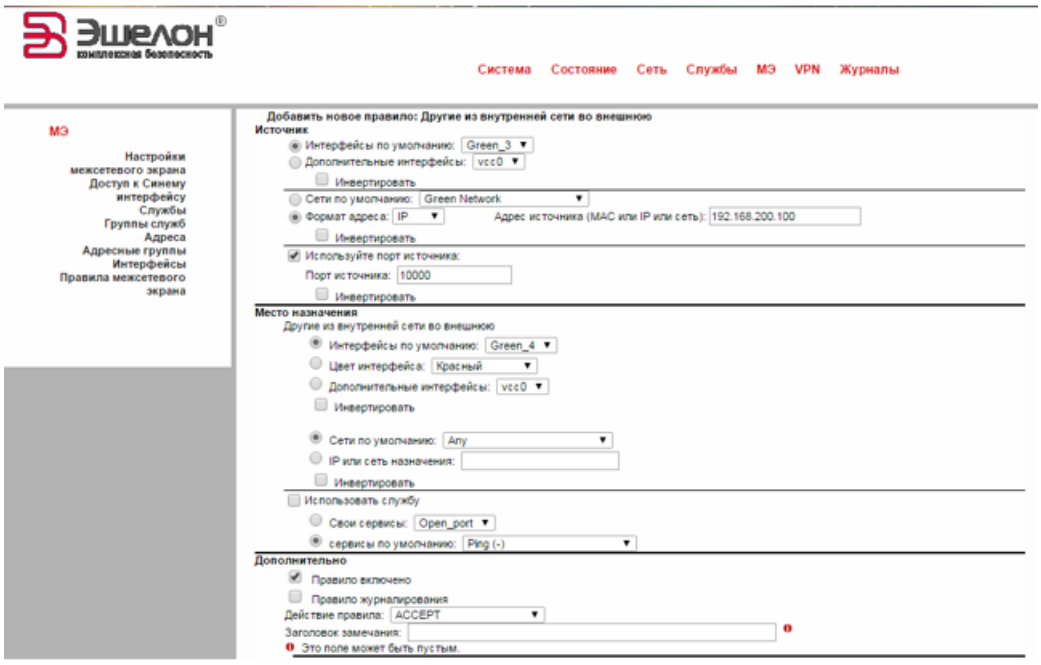


Рис. 18 – Добавление правила ACCEPT: any: any → 192.168.200.100:Open_port(10000)

– ACCEPT: 192.168.200.100: Open_port(10000)→ any: any (Рисунок 19);

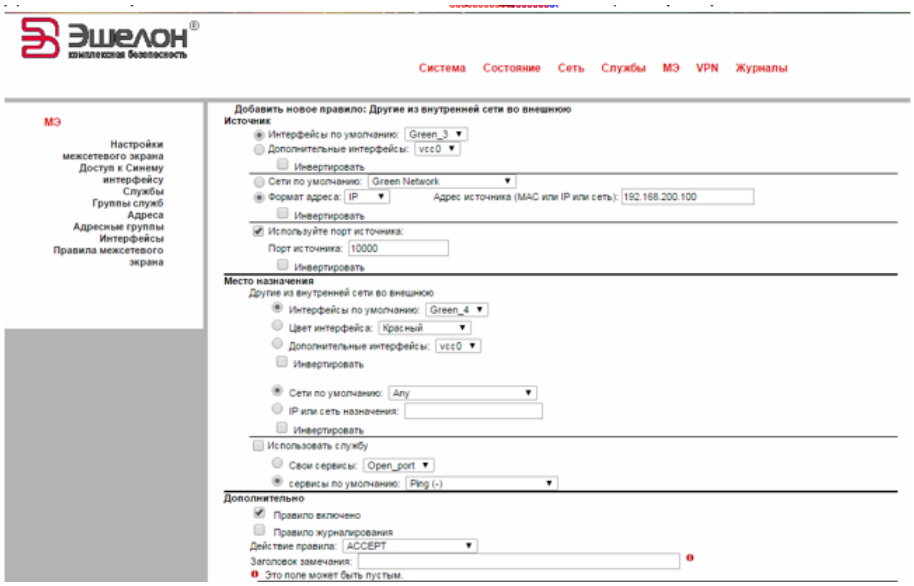


Рис. 19 – Добавление правила ACCEPT: 192.168.200.100: Open_port(10000)→ any: any ;

– DROP: any(lan-4) :all → any(lan-3):all (Рисунок 20);

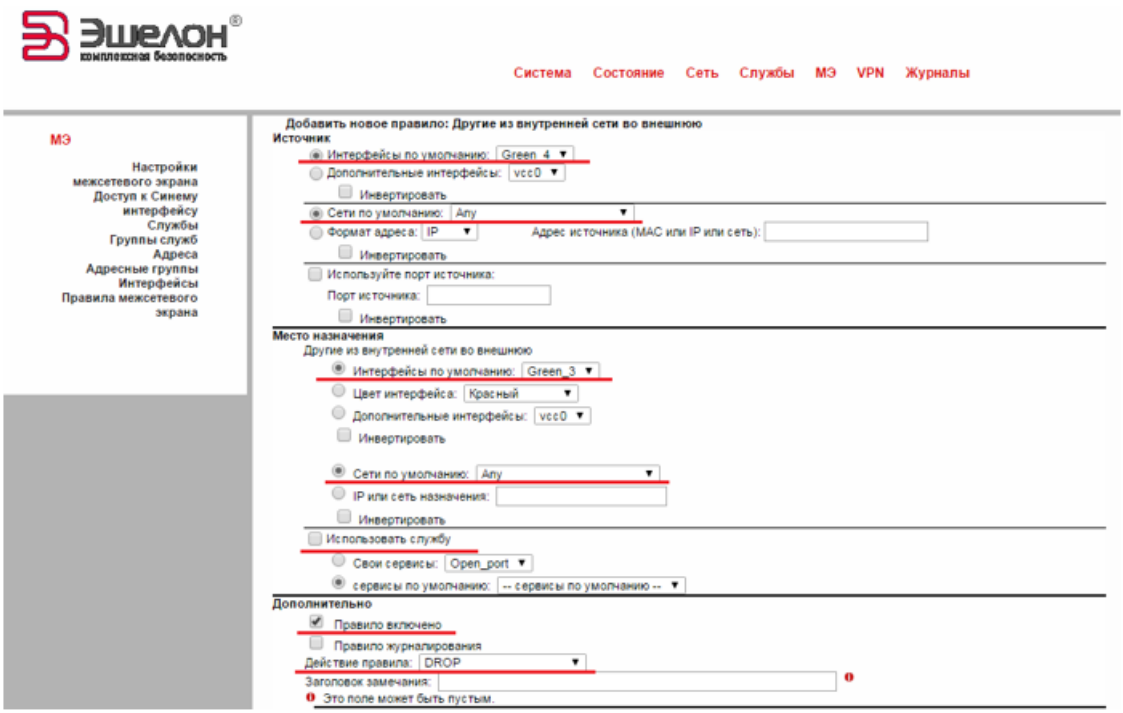


Рис. 20 – Добавление правила DROP: any(lan-4) :all → any(lan-3):all

– DROP: any(lan-3) :all → any(lan-4):all(Рисунок 21);

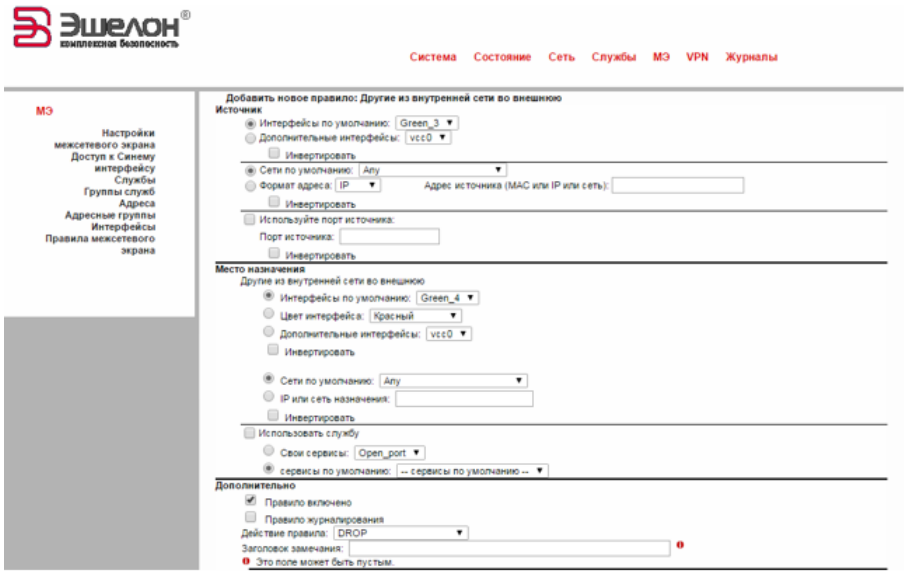


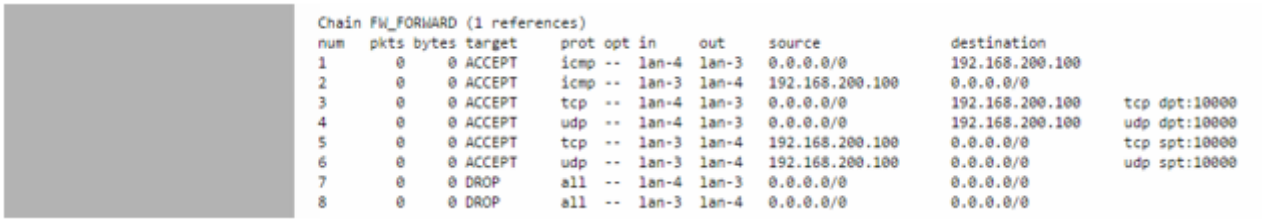
Рис. 21 – Добавление правила DROP: any(lan-3) :all → any(lan-4):all

Далее необходимо

– в веб-интерфейсе перейти на страницу: **МЭ→Правила межсетевого экрана** и проверить настройки сети (Рисунок 22);

Рис. 22 – Настройки сети

– в веб-интерфейсе перейти на страницу: **Состояние→ Настройки IP Tables→** и проверить добавленные правила(Рисунок 23).



```
Chain FW_FORWARD (1 references)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 ACCEPT     icmp --  lan-4  lan-3   0.0.0.0/0            192.168.200.100
2        0     0 ACCEPT     icmp --  lan-3  lan-4   192.168.200.100      0.0.0.0/0
3        0     0 ACCEPT     tcp  --  lan-4  lan-3   0.0.0.0/0            192.168.200.100     tcp dpt:10000
4        0     0 ACCEPT     udp  --  lan-4  lan-3   0.0.0.0/0            192.168.200.100     udp dpt:10000
5        0     0 ACCEPT     tcp  --  lan-3  lan-4   192.168.200.100      0.0.0.0/0           tcp spt:10000
6        0     0 ACCEPT     udp  --  lan-3  lan-4   192.168.200.100      0.0.0.0/0           udp spt:10000
7        0     0 DROP       all  --  lan-4  lan-3   0.0.0.0/0            0.0.0.0/0
8        0     0 DROP       all  --  lan-3  lan-4   0.0.0.0/0            0.0.0.0/0
```

Рис. 23 – Добавленные правила в IP Tables

2) Настройка «Рубикона» с NAT.

Сетевая схема «Рубикона» с NAT представлена на рисунке 24.

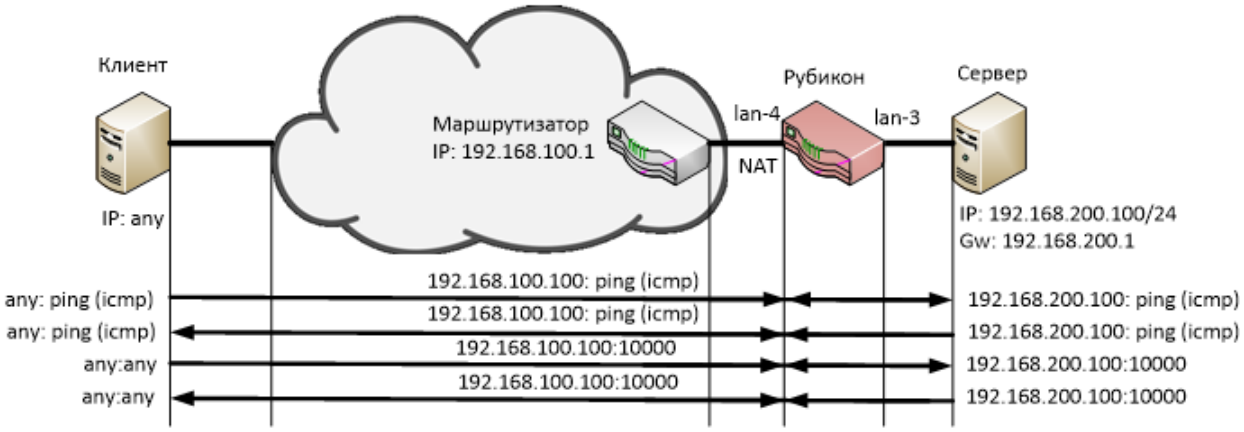


Рис. 24 – Сетевая схема «Рубикона» с NAT

Интерфейсы «Рубикона», участвующие в сетевом обмене, представлены в таблице 5.

Таблица 5 – Минимальные требования к компьютеру, на который устанавливается «Рубикон»

Интерфейсы	IP адрес	Маска сети	Политика
lan-3	192.168.200.1	255.255.255.0	зеленый
lan-4	192.168.100.100	255.255.255.0	красный (NAT)
Шлюз по умолчанию	192.168.100.1		

Для настройки «Рубикона» с NAT необходимо:

– в веб-интерфейсе перейти на страницу: **Сеть→Настройка адаптеров** и включить красную политику (NAT) на красном интерфейсе (Рисунок 25);

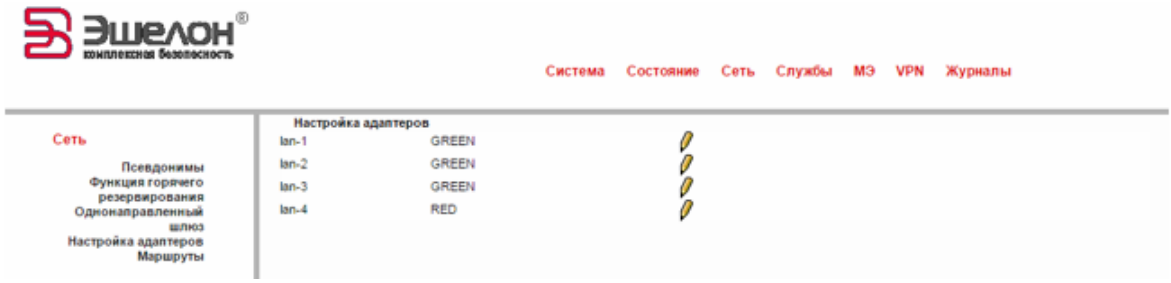


Рис. 25 – Подключение политики NAT

– в веб-интерфейсе перейти на страницу: **Система→Выключение** и перезагрузить «Рубикон»(Рисунок 26);

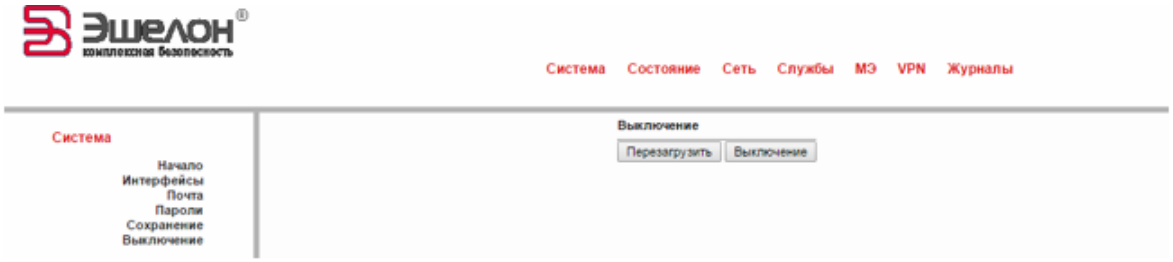


Рис. 26 – Окно перезагрузки «Рубикона»

Настраиваем сетевые интерфейсы и маршрутизацию

– в веб-интерфейсе перейти на страницу: **Система→Интерфейсы** и настроить сетевые интерфейсы и маршрутизацию(Рисунок 27);

– в веб-интерфейсе перейти на страницу: **Состояние→Состояние сети** и проверить состояние сети(Рисунок 28);

– в веб-интерфейсе перейти на страницу: **МЭ→Настройка межсетевого экрана** и включить расширенный режим СОВ (Рисунок 29);

– в веб-интерфейсе перейти на страницу: **МЭ→Службы** и службу 10000 для МЭ (Рисунок 30);

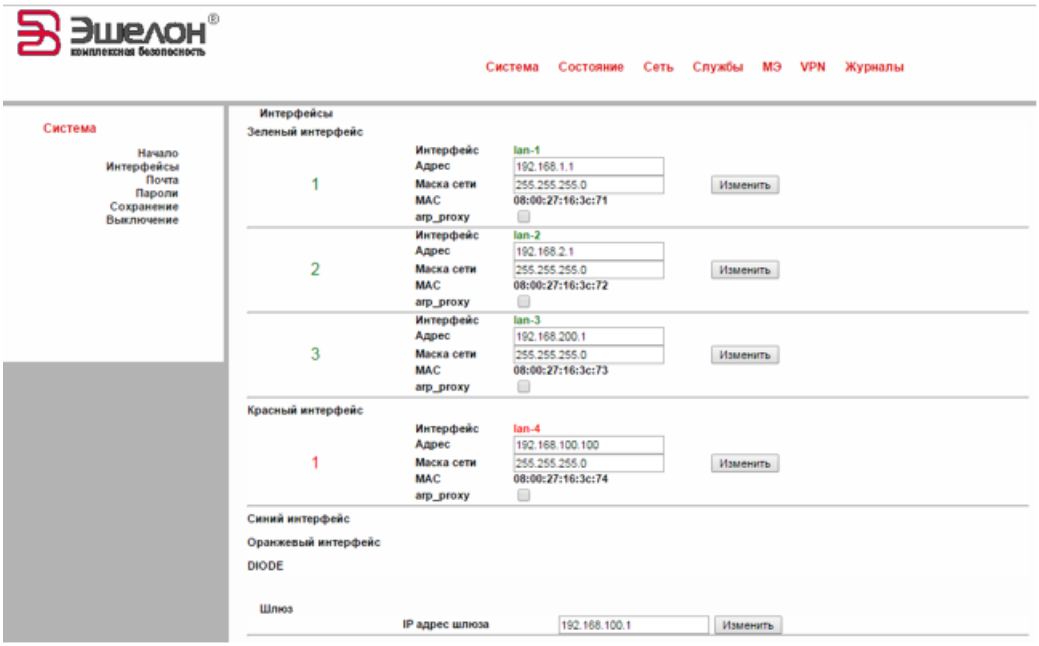


Рис. 27 – Настройка сетевых интерфейсов и маршрутизации

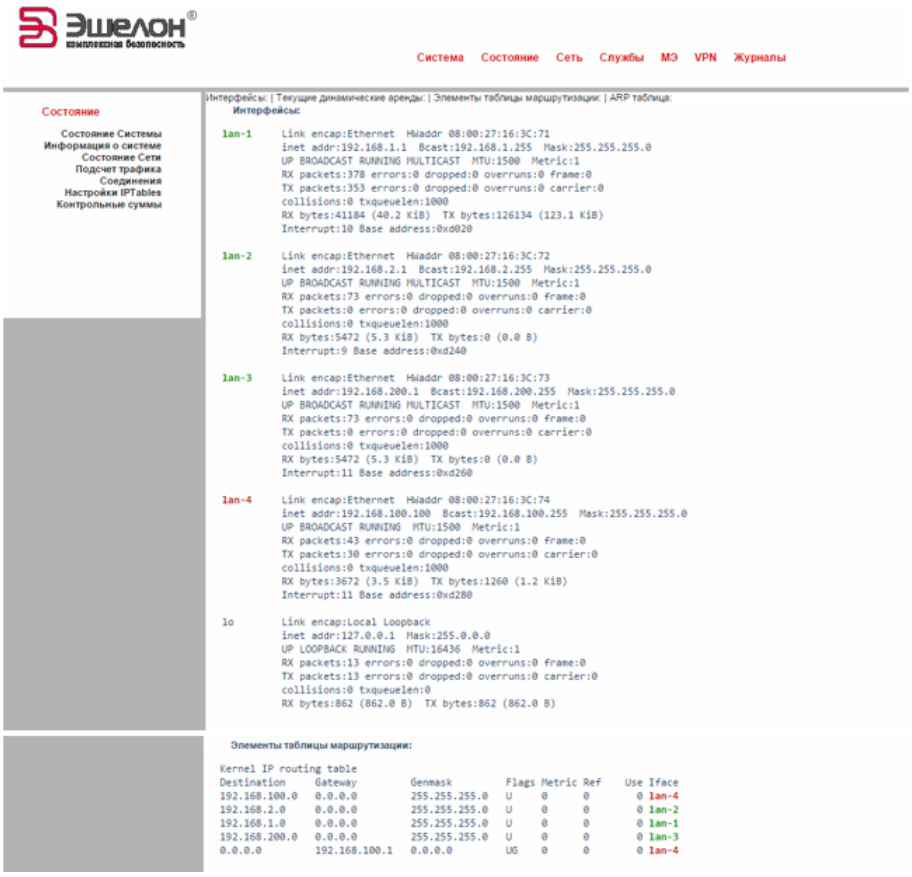


Рис. 28 – Состояние сети

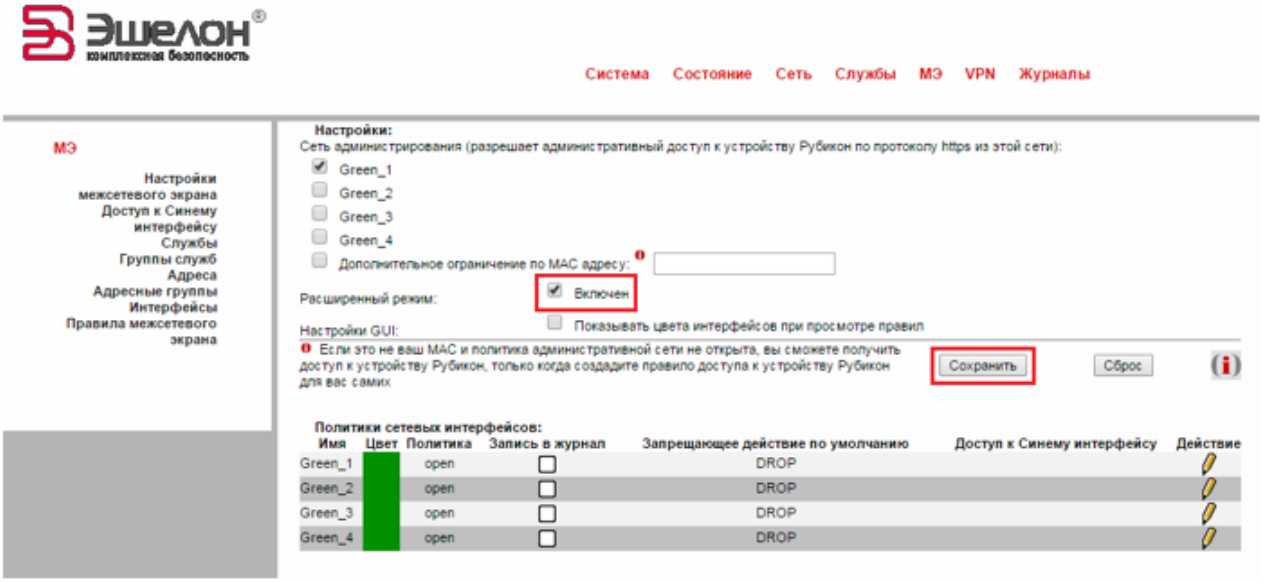


Рис. 29 – Включение расширенного режима СОВ

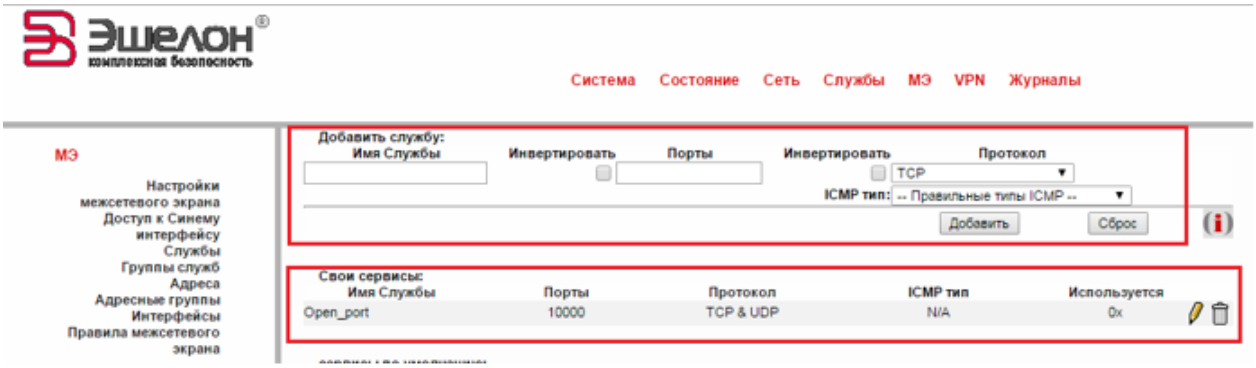


Рис. 30 – Добавление службы 10000 для межсетевого экрана

– в веб-интерфейсе перейти на страницу: **МЭ→Правила межсетевого экрана→Перенаправление портов** и добавить правила:

  – ACCEPT: 192.168.100.100:ping(icmp)→ 192.168.200.100: ping(icmp) (Рисунок 31);
  – ACCEPT: 192.168.100.100:Open_port(10000) → 192.168.200.100:Open_port(10000) (Рисунок 32);

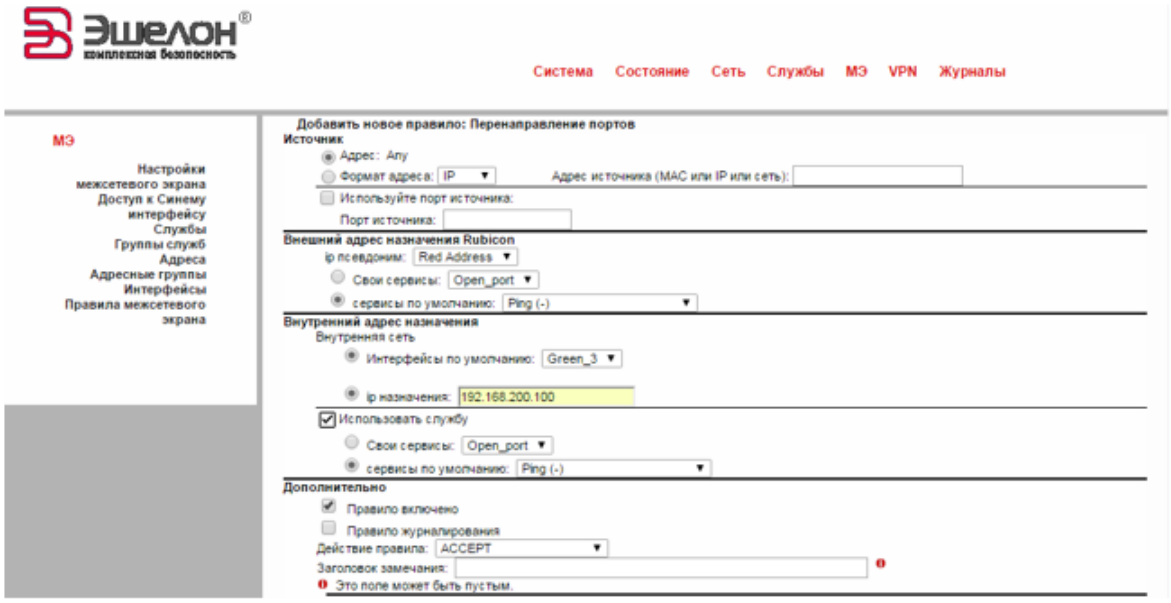


Рис. 31 – Добавление правила ACCEPT: 192.168.100.100:ping(icmp)→ 192.168.200.100: ping(icmp))

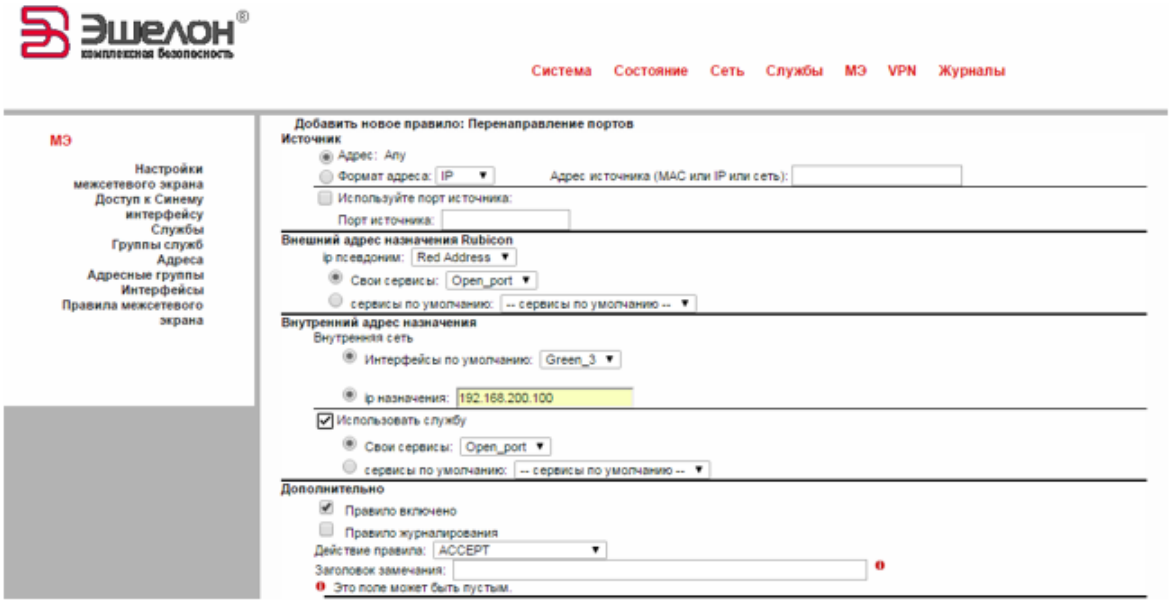


Рис. 32 – Добавление правила ACCEPT : 192.168.100.100 : Open_port(10000) → 192.168.200.100 : Open_port(10000)

Далее необходимо

– в веб-интерфейсе перейти на страницу: **МЭ→Правила межсетевого экрана→** и проверить настройки сети (Рисунок 33);
– в веб-интерфейсе перейти на страницу: **Состояние→ Настройки IP Tables→** и проверить добавленные правила(Рисунок 34, Рисунок **??**.

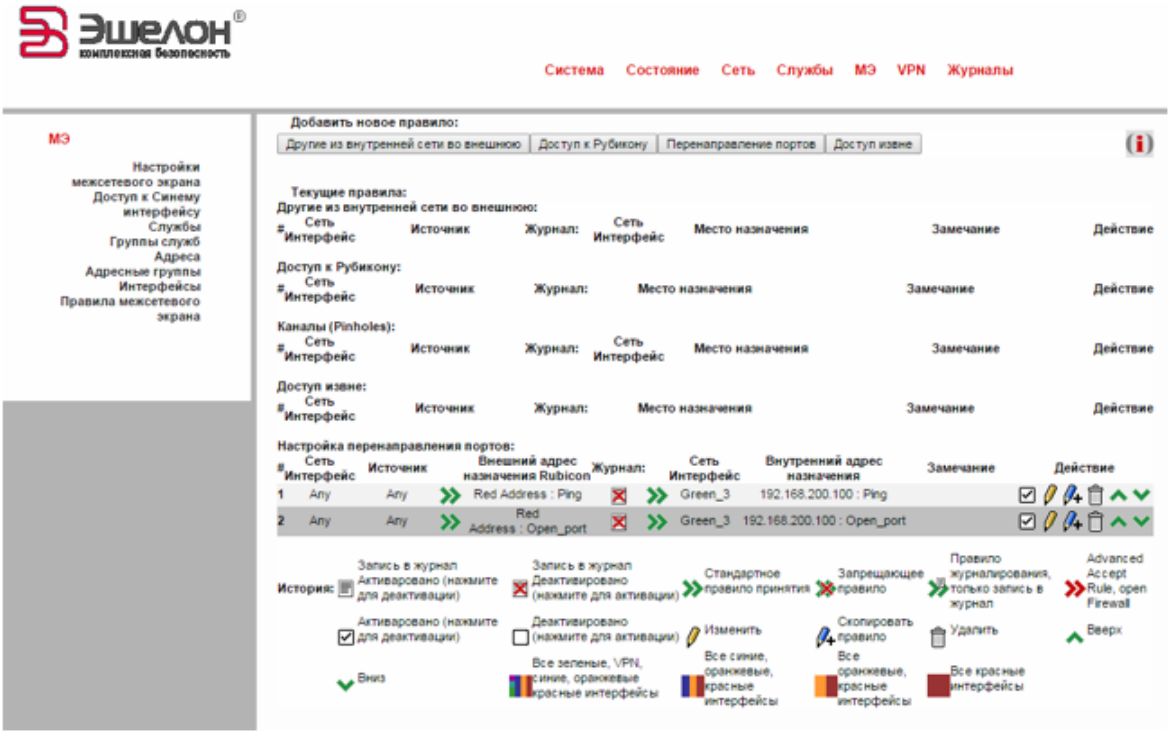


Рис. 33 – Настройки сети

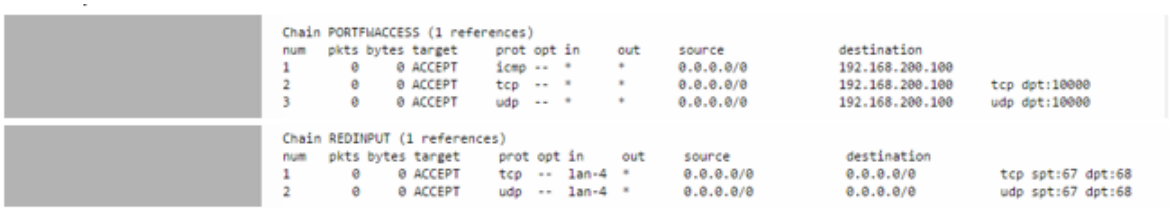


Рис. 34 – Таблица «filter» в IP Tables

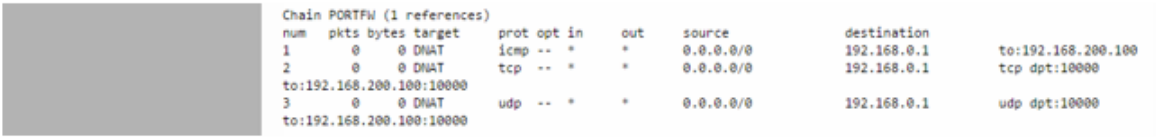


Рис. 35 – Таблица «NAT» в IP Tables

4.7. Пример настройки правил МЭ для перенаправления портов

Для доступа из красной сети в зеленую необходимо настроить перенаправление портов в правилах МЭ, в связи с тем, что на красном интерфейсе включается NAT.

Для этого необходимо:

– в веб-интерфейсе перейти на страницу: **МЭ→Настройки межсетевого экрана** и отключить администрирование интерфейса, на котором планируется изменить цвет (Рисунок 36);

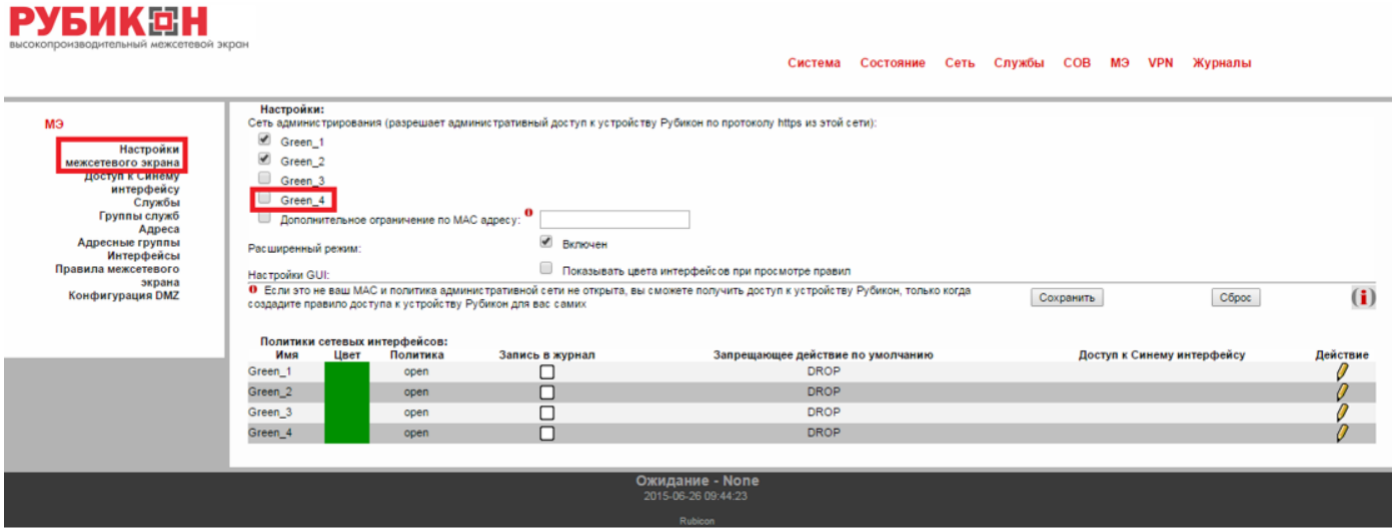


Рис. 36 – Отключение администрирования интерфейса

– в веб-интерфейсе перейти на страницу: **Сеть→Настройки адаптеров** и изменить цвет интерфейса на красный(Рисунок 37);

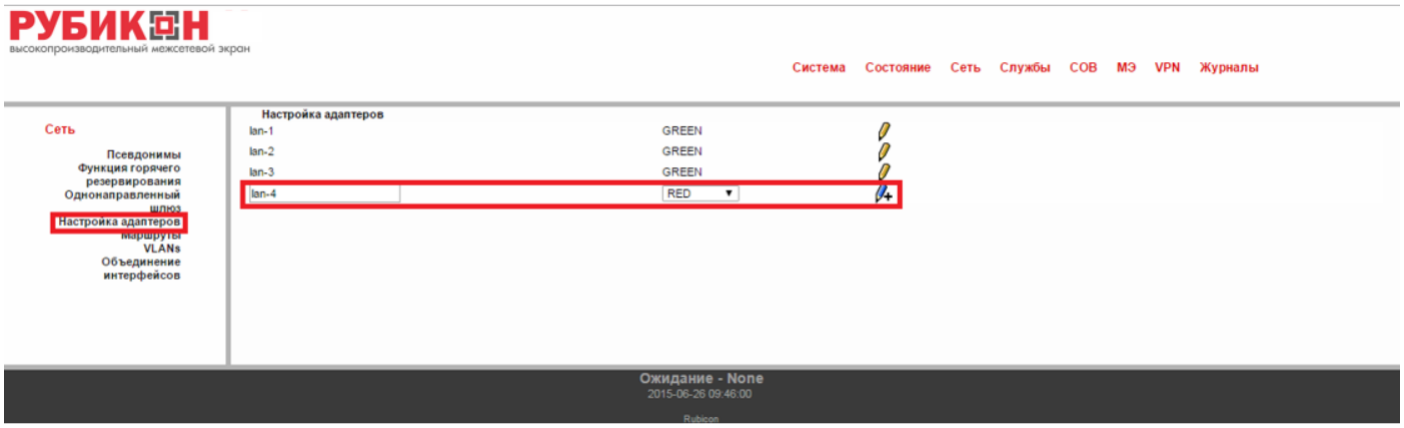


Рис. 37 – Изменение цвета интерфейса

– в веб-интерфейсе перейти на страницу: **Система→Выключение** и перезагрузить «Рубикон»(Рисунок 38);

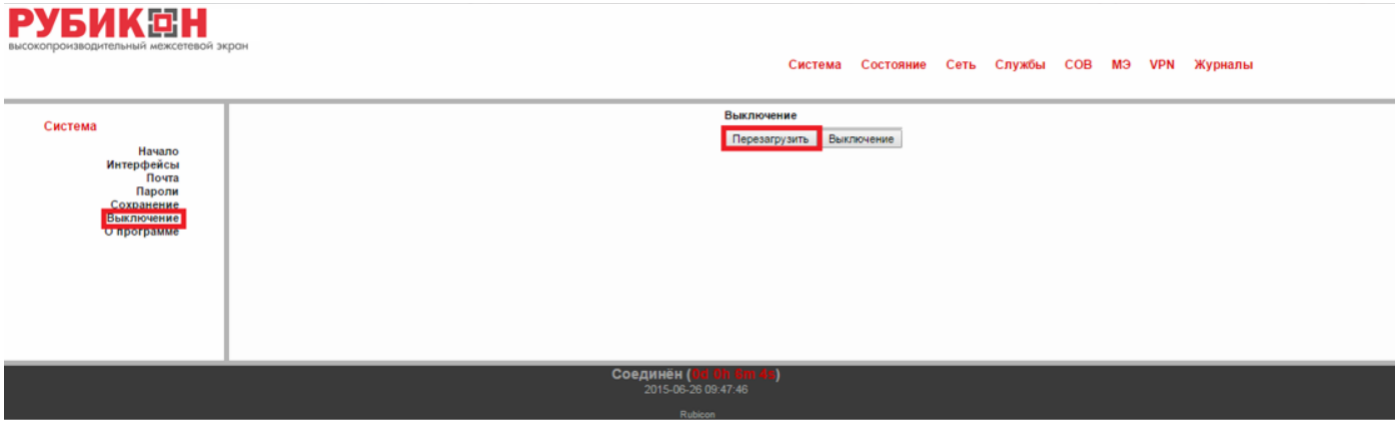


Рис. 38 – Перезагрузка «Рубикона»

В качестве примера рассмотрим следующий случай, представленный на рисунке 39:

– к «Рубикону» подключен web-сервер с IP адресом 192.168.2.100 и портом 8080;
– «Рубикон» подключен к глобальной сети через красный интерфейс (NAT);
– клиенту, находящемуся в глобальной сети, необходимо подключиться по протоколу http к web-серверу, который находится за NAT.

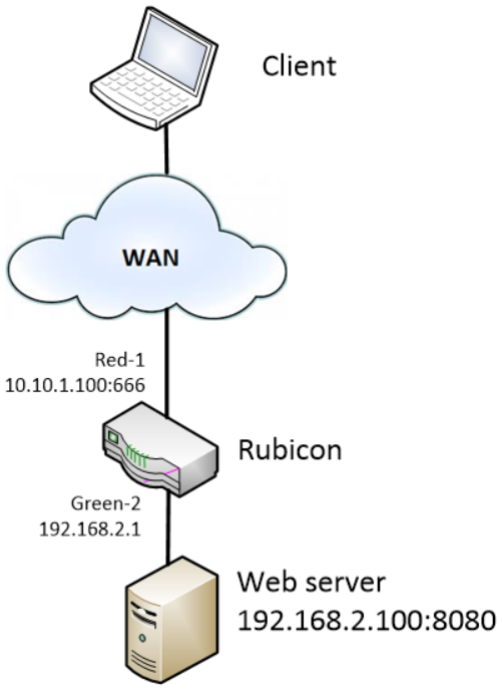


Рис. 39 – Схема стенда

Для доступа клиента к web-серверу через NAT необходимо настроить перенаправление портов в правилах МЭ «Рубикона». В качестве примера будем перенаправлять приходящий

пакет на IP адрес 10.10.1.100 с портом 666 на IP адрес 192.168.2.100 с портом 8080.

Для этого необходимо:

– в веб-интерфейсе перейти на страницу: **МЭ→Службы** и добавить дополнительную службу для web-сервера с протоколом TCP+UDP и портом 8080(Рисунок 40);

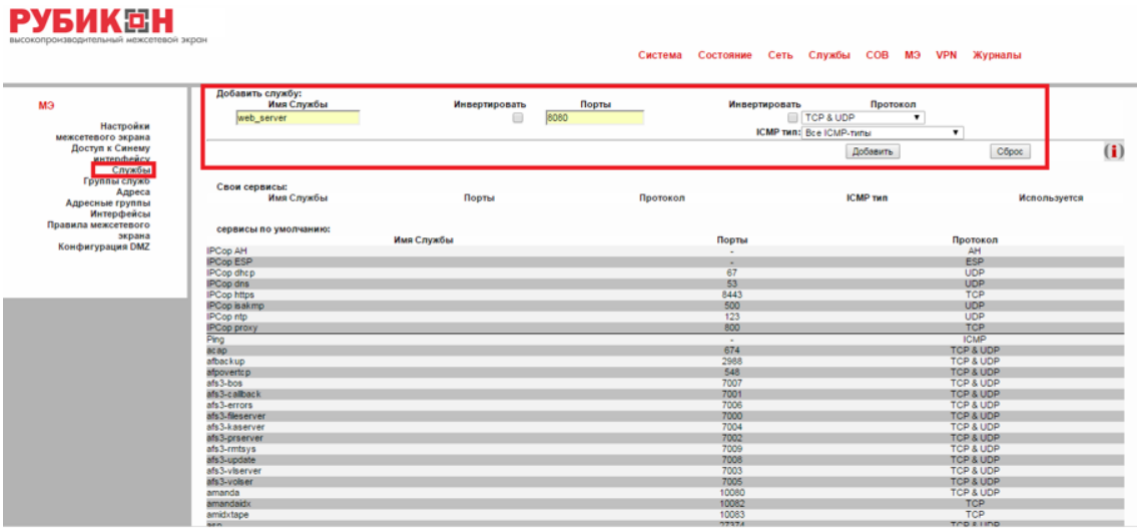


Рис. 40 – Добавление дополнительной службы для web-сервера с протоколом TCP+UDP и портом 8080

– в веб-интерфейсе перейти на страницу: **МЭ→Службы** и добавить дополнительную службу для красного интерфейса «Рубикона» с протоколом TCP+UDP и портом 666(Рисунок 41);

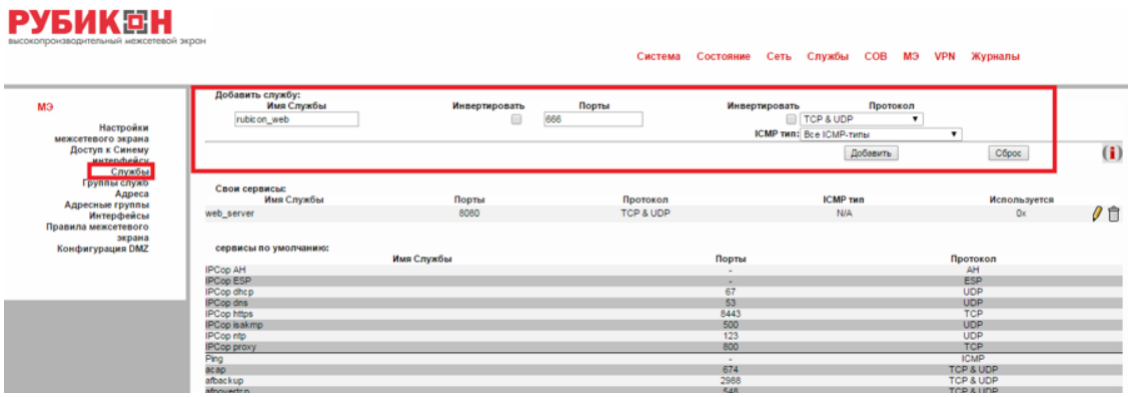


Рис. 41 – Добавление дополнительной службы для красного интерфейса «Рубикона» с протоколом TCP+UDP и портом 666

– в веб-интерфейсе перейти на страницу: **МЭ→Правила межсетевого экрана** и добавить правило МЭ «Перенаправление портов»(Рисунок 42);

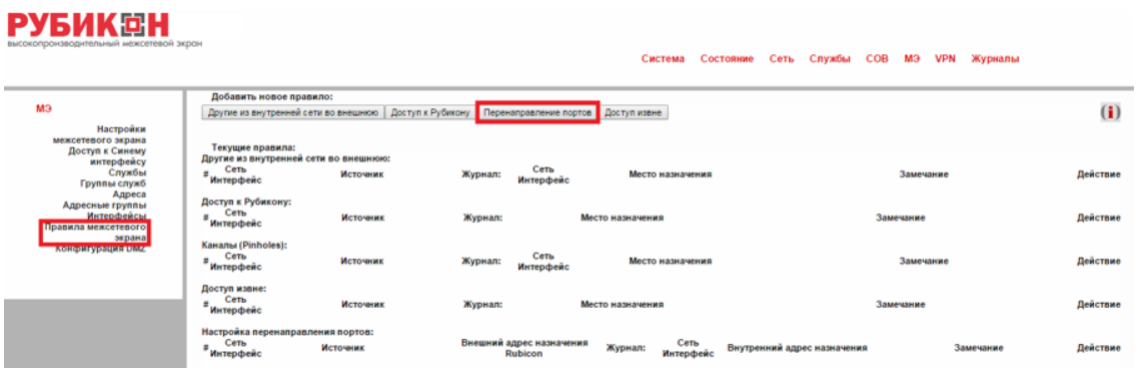


Рис. 42 – Добавление правила МЭ «Перенаправление портов»

Добавляем правила, как показано на рисунке 43, где

– 1 – Источник сетевых пакетов (в нашем случае клиент);
– 2 – Параметры красного интерфейса «Рубикона»;
– 3 – Параметры внутреннего адресата (в нашем случае web-сервера);
– 4 – Настройки действия правил.

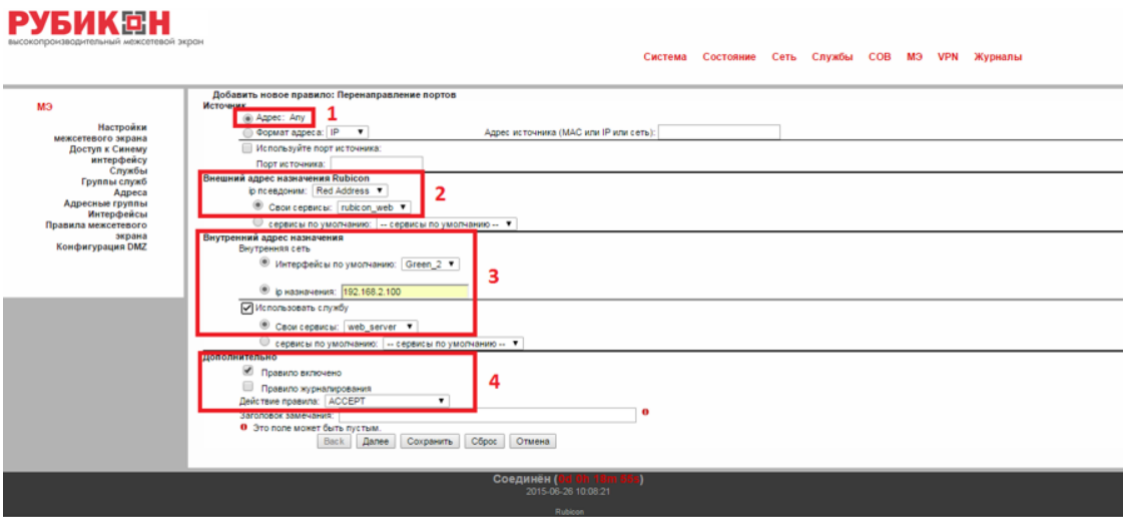


Рис. 43 – Добавление правил

Добавленные правила показаны на рисунке 44.

В итоге получим, что запрос клиента http://10.10.1.100:666 через web-браузер будет перенаправлен «Рубиконом» на web-сервер 192.168.2.100:8080. Ответ от web-сервера вернется обратно клиенту.

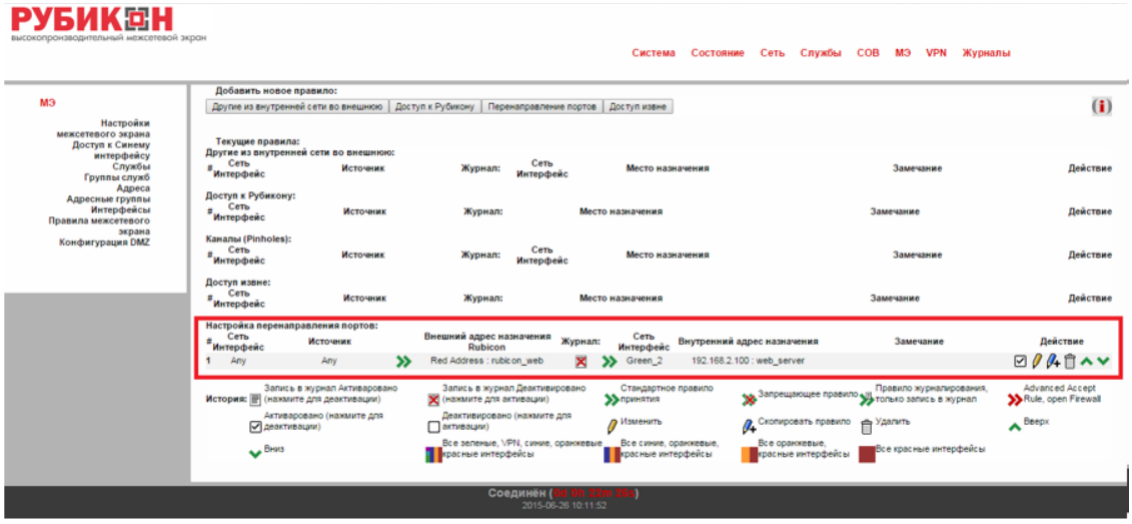


Рис. 44 – Проверка добавленных правил

4.8. Расширенный режим фильтрации сетевых пакетов

Расширенный режим настройки межсетевого экрана позволяет установить дополнительные параметры для фильтрации сетевых пакетов.

Для включения расширенного режима необходимо активировать данную возможность на странице **МЭ** → **Настройки межсетевого экрана** (Рисунок 2) (установив соответствующий переключатель) и сохранить сделанные настройки нажатием кнопки **«Сохранить»**. После установки расширенного режима при заполнении правил фильтрации будут доступны следующие дополнительные параметры.

4.8.1. Порт источника

Данный режим позволяет указывать порт, с которого поступают сетевые пакеты (Рисунок 45). Применяется в 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.

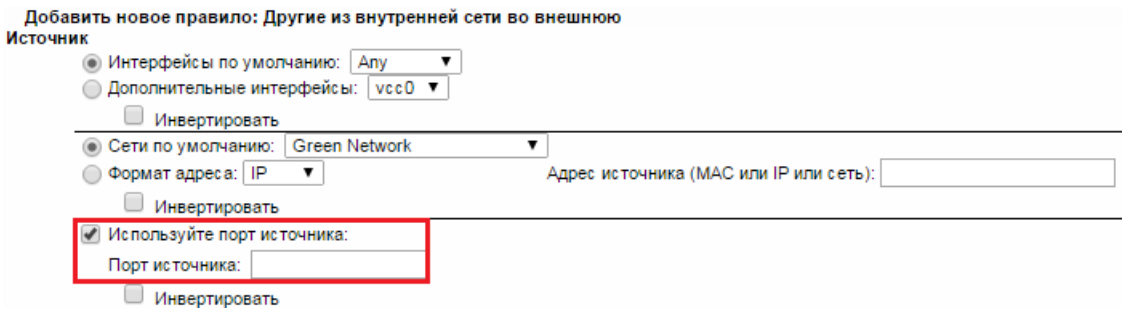


Рис. 45 – Порт источника

4.8.2. Ограничение частоты следования пакетов

Позволяет применять правила исходя из частоты следования пакетов (Рисунок 46). Можно выбрать одно из двух ограничений: средняя частота следования пакетов и превышение общего количества пакетов. Ограничения устанавливаются соответственно параметрами **limit avg** и **limit-burst**.

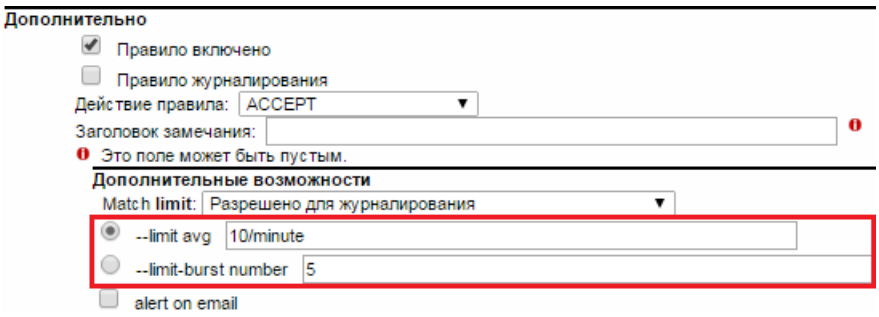


Рис. 46 – Ограничение частоты следования пакетов

4.8.3. Включение извещения о применении правила по электронной почте

При установлении переключателя **«alert on email»** (Рисунок 47) данная возможность позволяет извещать администратора о поступлении сетевого пакета, удовлетворяющего правилу, по электронной почте, параметры которой указываются в разделе **Система → Почта** (Рисунок 48).

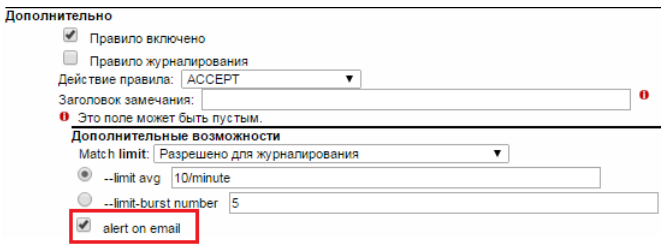


Рис. 47 – Включение извещения о правиле по электронной почте

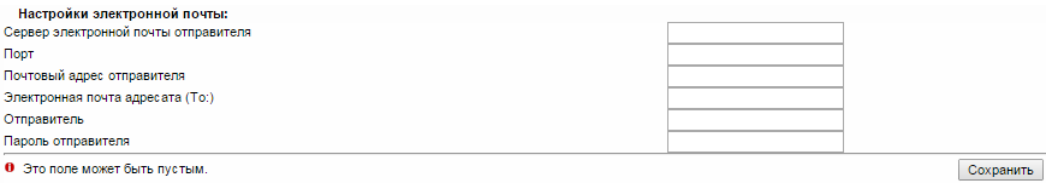


Рис. 48 – Система → Почта

4.8.4. Включение локального извещения о применении правила

При установлении переключателя **«alert locally»** данная возможность позволяет извещать администратора о поступлении сетевого пакета, удовлетворяющего правилу, во всплывающем окне на любой странице администрирования комплекса «Рубикон».

4.8.5. Временной диапазон применения правила

Позволяет установить временно́й диапазон применения правила. Необходимо установить переключатель **«Добавить временно́й диапазон»** (Рисунок 49) и выбрать число или дни недели применения правила, а также диапазон времени.

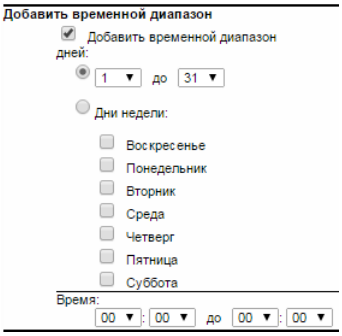


Рис. 49 – Временно́й диапазон применения правила

4.8.6. Фильтрация по битовой маске

Применяется включением переключателя **«Включить фильтрацию по битовой маске»** (Рисунок 50) и выставлением смещения и битовой маски относительно начала пакета.

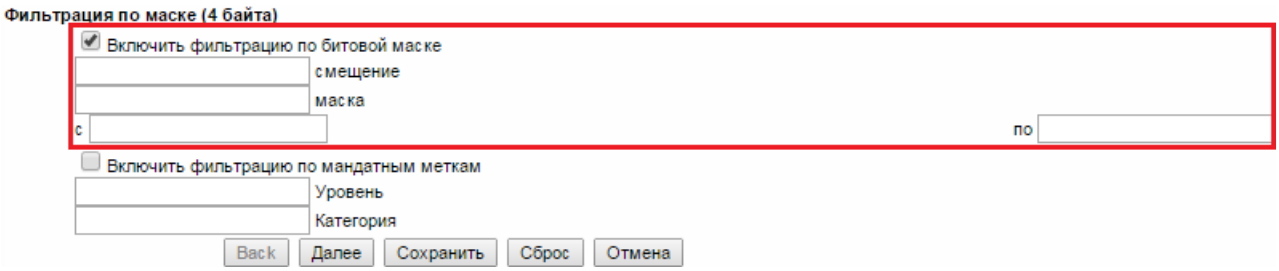


Рис. 50 – Фильтрация по битовой маске

4.8.7. Фильтрация по мандатным меткам

Позволяет фильтровать пакеты с установленными мандатными метками по RFC 1108. (Такие метки используются, например в ОС Astra Linux). Для включения правила фильтрации по мандатным меткам необходимо установить переключатель **«Включить фильтрацию по**

мандатным меткам» (Рисунок 51) и установить уровень (число от 0 до 127 в десятичном формате) и категорию (строка длины 8, состоящая из 0 и 1, согласно RFC 1108) для фильтрации в сетевом пакете.

В случае отсутствия мандатной метки в составе сетевого пакета, фильтрация сетевых пакетов по признаку мандатной метки не проводится.

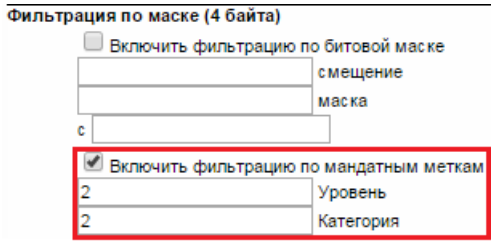


Рис. 51 – Фильтрация по мандатным меткам

5. СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

5.1. Интерфейсы, доступные для запуска СОВ

Модуль СОВ КП ПАВ «Рубикон» может быть запущен 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 комплекса (Службы → Обнаружение атак). Секция «Интерфейсы» представлена на рисунке 52.

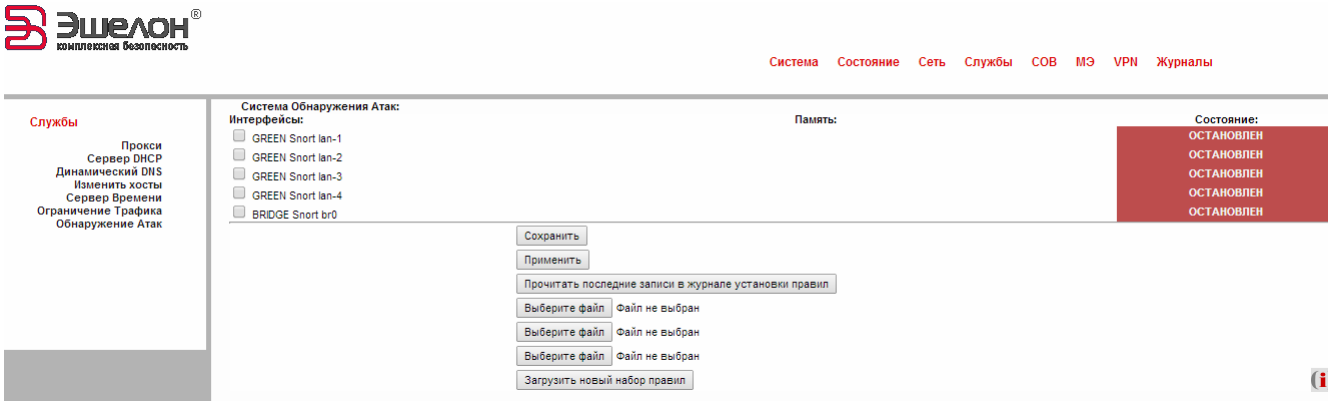


Рис. 52 – Раздел «Службы → Обнаружение атак», секция «Интерфейсы»

5.2. Запуск СОВ на физическом интерфейсе

Для того чтобы подключить модуль СОВ КП ПАВ «Рубикон» к одному из физических интерфейсов, необходимо поставить отметку напротив его названия в разделе **«Службы → Обнаружение атак»**, секция **«Интерфейсы»** (рисунок 52).

После того как отметка поставлена, администратор должен сохранить изменения, нажав кнопку Сохранить. Появится надпись, выделенная в рамку на рисунке 53.

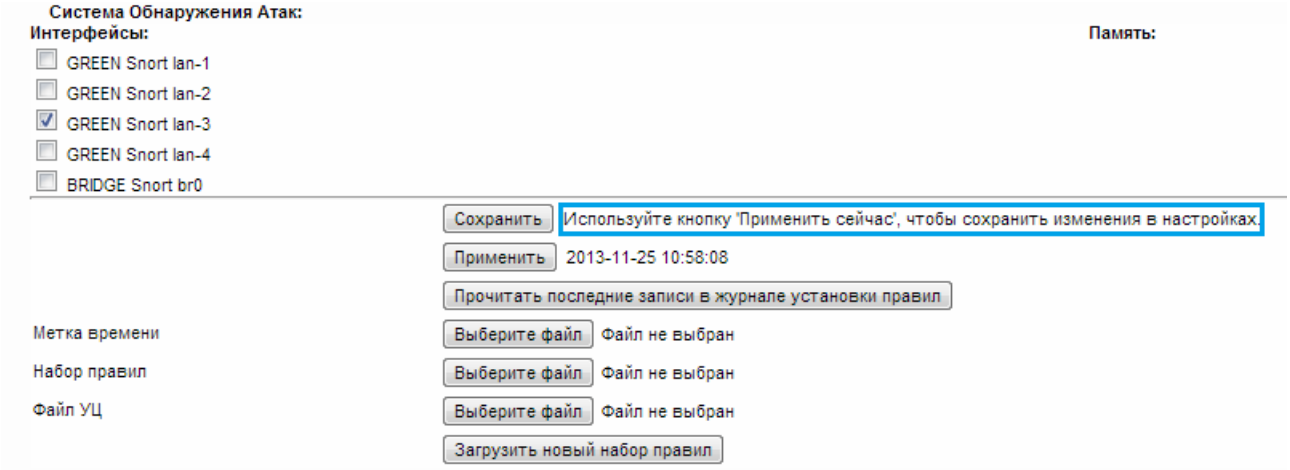


Рис. 53 – Запуск СОВ КП ПАВ «Рубикон» на физическом интерфейсе

Чтобы применить сохраненные изменения, необходимо нажать кнопку Применить. Теперь модуль СОВ КП ПАВ «Рубикон» запущен на выбранном интерфейсе (рисунок 54).

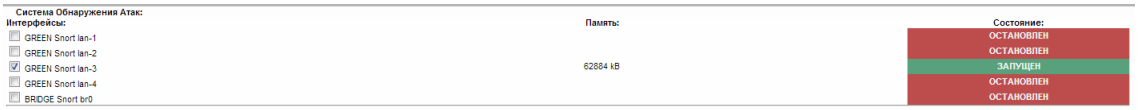


Рис. 54 – СОВ КП ПАВ «Рубикон» запущена на интерфейсе Green Snort lan-3

5.3. Режимы обнаружения

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

5.3.1. 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.

5.3.2. 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 необходимо зайти в раздел **«СОВ → Настройка обнаружения сканирования»**. Существует два элемента управления (рисунок 55): выбор протокола и уровень срабатывания. Протокол определяет те сетевые пакеты, которые будут анализироваться. Уровень срабатывания определяет предполагаемую интенсивность сканирования злоумышленником.

Рис. 55 – Настройка режима эвристического анализа

5.4. База решающих правил

5.4.1. Загрузка новой базы решающих правил

Для настройки новой БРП необходимо в разделе **«Службы → Обнаружение атак»** загрузить следующие файлы:

- 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.

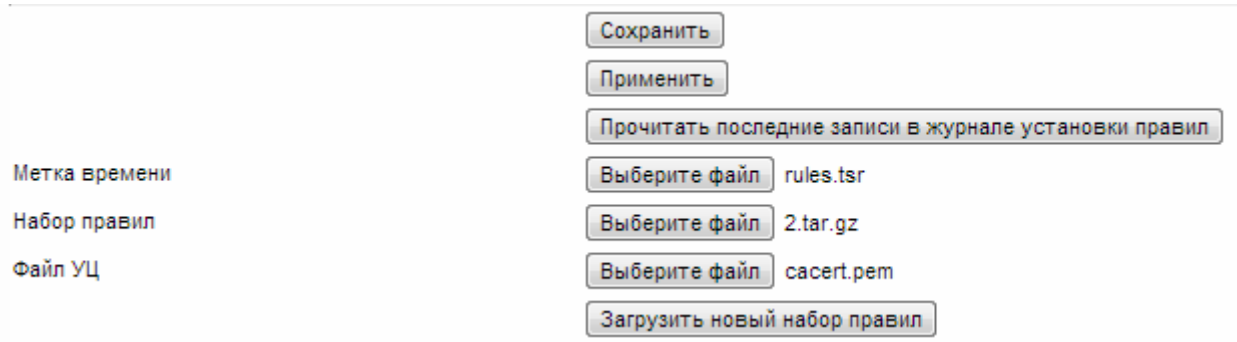


Рис. 56 – Настройка БРП. Импорт файлов в систему

После того как все файлы загружены, необходимо нажать 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:

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 и удаление временных файлов. Пользователю выводится предложение нажать кнопку Применить, что обновит правила и перезапустит СОВ КП ПАВ «Рубикон» на выбранных интерфейсах. После успешного перезапуска, а также по нажатию кнопки Прочитать последние записи в журнале установки правил, администратор может увидеть информацию, представленную на рисунке 57.

При неуспешной проверке администратор увидит предупреждающее сообщение:

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 (выделено в синюю рамку) отображается дата последнего изменения правил. В красную рамку обведены сведения о результатах проверки метки времени. Результат проверки на рисунке 57 «OK» означает успешное прохождение проверки. В рамку зеленого цвета выделены сведения о загружаемом наборе правил.

5.4.2. Настройка решающих правил

Для включения (отключения) срабатывания конкретного решающего правила необходимо поставить ☑ (снять ☐) отметку напротив его названия в соответствующем контейнере в разделе **«СОВ → Настройка правил СОВ»**. Например, на рисунке 58 включены все правила, кроме «ATTAC RESPONCES 403 Forbidden».

Для включения (отключения) уведомления администратора о срабатывании конкретного решающего правила необходимо выбрать ✉ для включения и ✉ для отключения напротив названия правила в соответствующем контейнере в разделе **«СОВ → Настройка правил СОВ»**. Например, на рисунке 58 отключено уведомление обо всех правилах, кроме «ATTAC RESPONCES command error».

Для включения (отключения) блокирования атаки с помощью межсетевого экрана необходимо выбрать для включения и для отключения напротив названия правила в соответствующем контейнере в разделе **«СОВ → Настройка правил СОВ»**. Например, на рисунке 58 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.

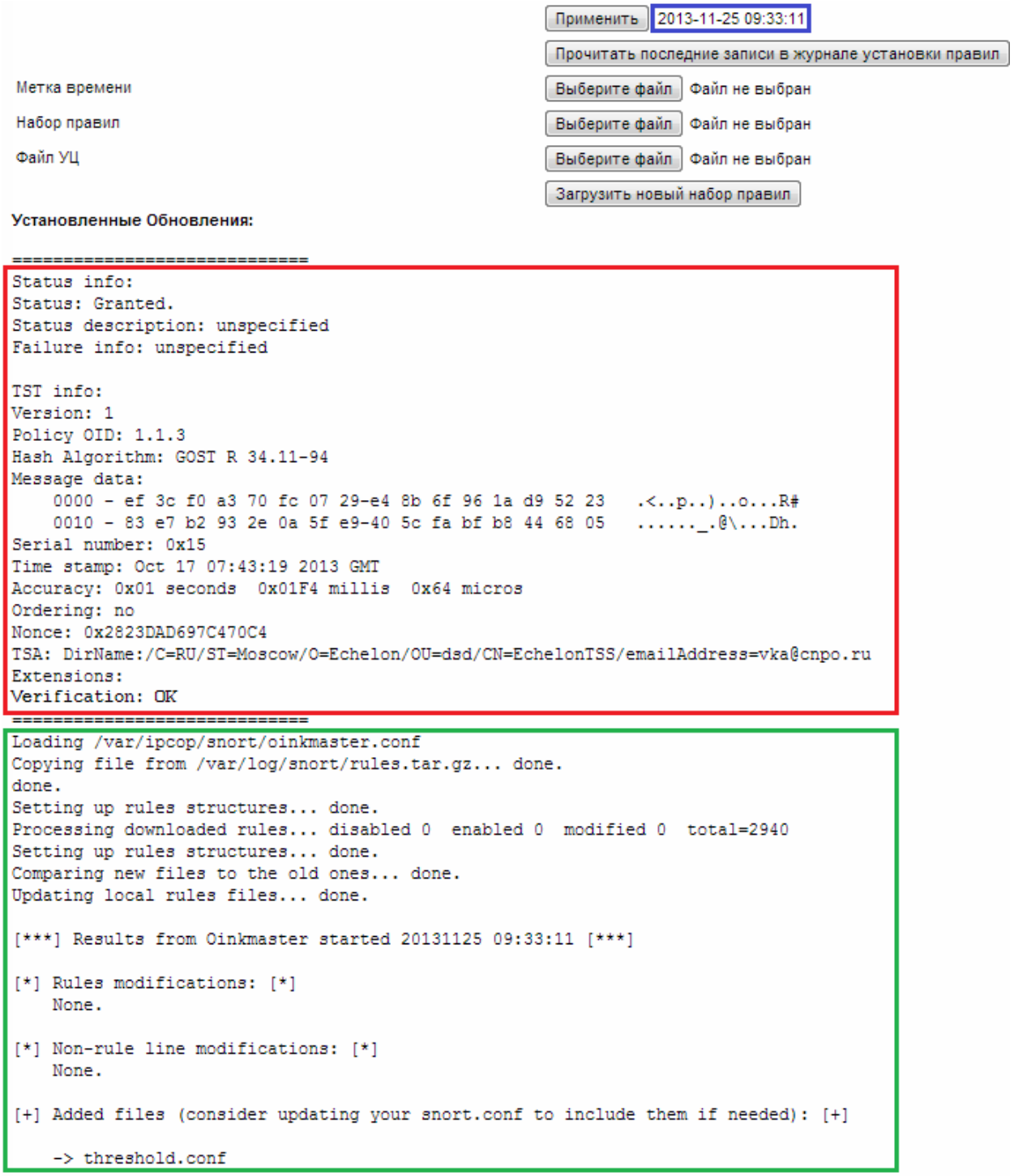


Рис. 57 – Информация об установленных обновлениях

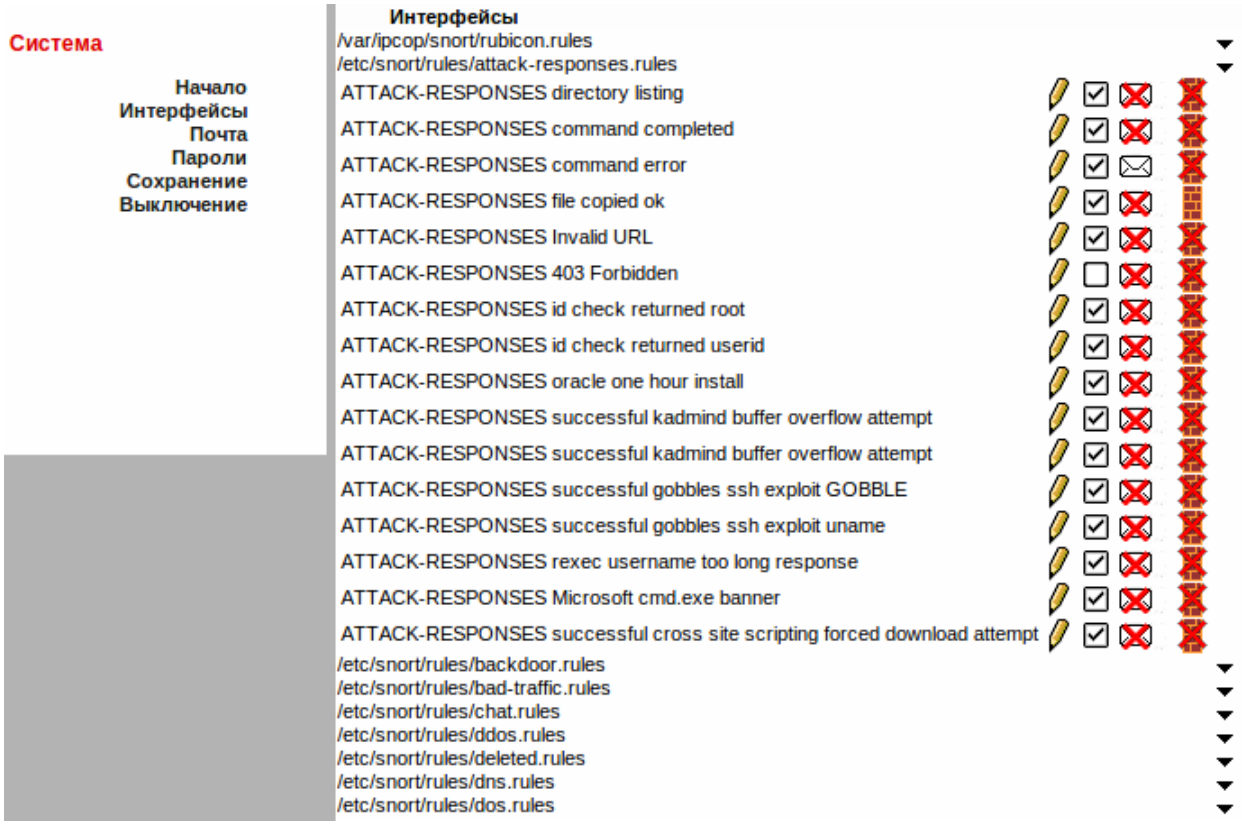


Рис. 58 – Настройка решающих правил

6. СЛУЖБЫ

6.1. Настройка точного времени

На изделии «Рубикон» установлен клиент точного времени (NTP-клиент). Для настройки NTP необходимо на странице **Службы → Сервер Времени** (Рисунок 59):

Рис. 59 – Настройка NTP

– задать первичный сервер NTP;
– при необходимости задать вторичный и третичный серверы NTP (для повышения отказоустойчивости системы получения точного времени);
– выбрать часовой пояс;
– активировать галочку **«Получить время от сетевого сервера времени»**;
– нажать кнопку **«Сохранить»**.

Примечание — При необходимости немедленного получения данных от сервера NTP можно воспользоваться кнопкой **«Получить время с сервера NTP»**.

6.2. Горячее резервирование

ПАК «Рубикон» поддерживает технологию горячего резервирования. Пример, рассматривающий горячее резервирование красного интерфейса WAN, приведен ниже.

Пусть имеются два комплекса «Рубикона»,которые подключены в одну внешнюю сеть с основным IP адресом 10.10.10.1 и резервным IP адресом 10.10.10.2. Основной «Рубикон » имеет IP адрес 192.168.3.1, а резервный «Рубикон» – 192.168.3.2. Оба «Рубикона» соединены между собой.

Схема подключения представлена на рисунке 60.

Необходимо создать один общий виртуальный интерфейс, который будет переключаться между «Рубиконами». Для примера это IP адрес 10.10.10.3, как показано на рисунке 61.

Для настройки горячего резервирования для данного примера необходимо:

– в веб-интерфейсе перейти на страницу: **Сеть→Функция горячего резервирования** и нажать кнопку редактирования нужного интерфейса (Рисунок 62);

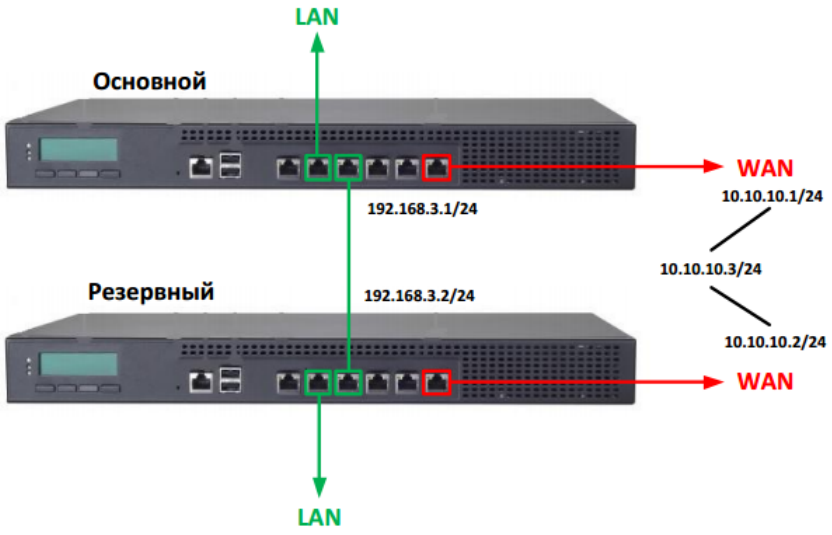


Рис. 60 – Схема подключения горячего резервирования

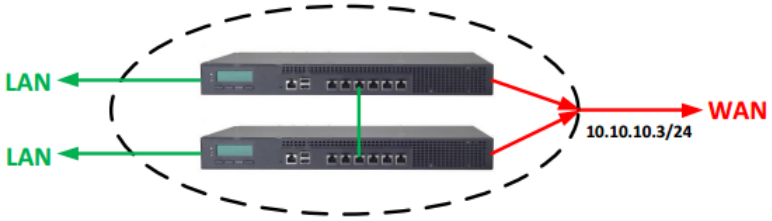


Рис. 61 – Общий виртуальный интерфейс для двух «Рубиконов»

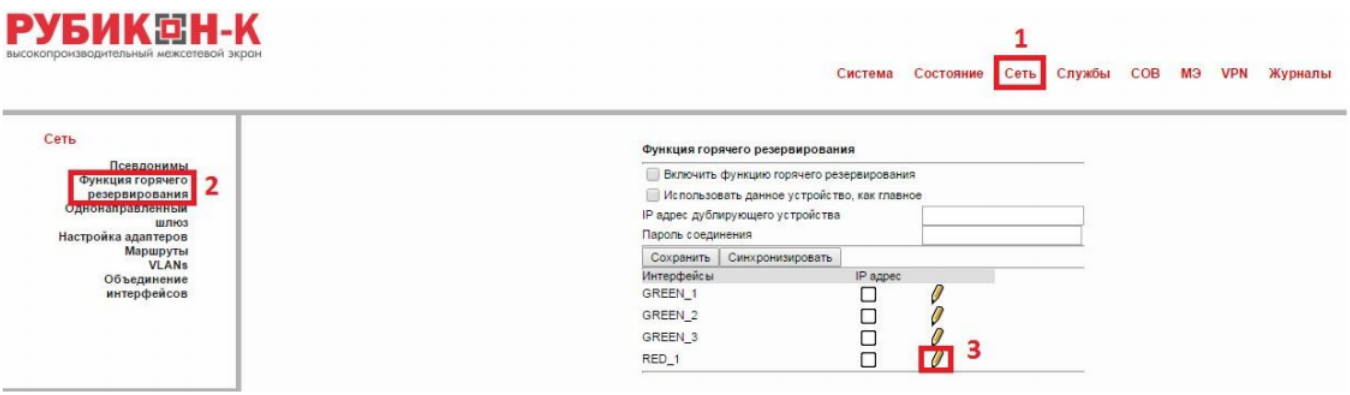


Рис. 62 – Сеть→Функция горячего резервирования

– указать общий виртуальный IP адрес и нажать кнопку «Сохранить»(Рисунок 63);

заполнить поля для основного «Рубикона» с указанием необходимых IP адресов, по которым «Рубиконы» соединены между собой (Рисунок 64);

заполнить поля для резервного «Рубикона» с указанием необходимых IP адресов, по которым «Рубиконы» соединены между собой (Рисунок 65);

Пароли соединения между основным и резервным «Рубиконами» должны совпадать.

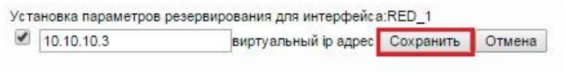


Рис. 63 – Общий IP адрес

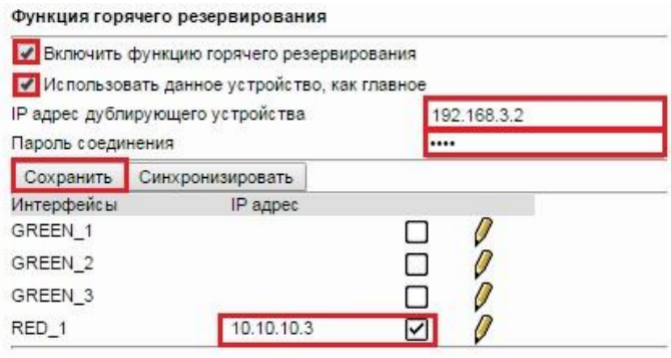


Рис. 64 – Настройка основного «Рубикона»

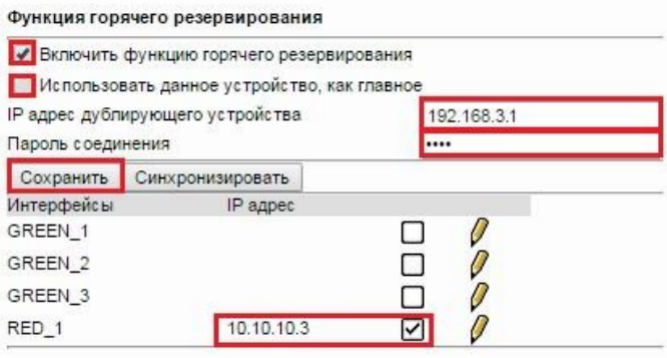


Рис. 65 – Настройка резервного «Рубикона»

Для проверки правильности настройки горячего резервирования необходимо в веб-интерфейсе зайти на страницу **Сеть→Состояние сети** и увидеть данные, аналогичные представленным на рисунке 66.

Рис. 66 – Настройка резервного «Рубикона»

7. СОСТОЯНИЕ

7.1. Обзор использования трафика

В КП ПАВ «Рубикон» предусмотрена возможность обзора использованного трафика. Чтобы перейти к настройкам обзора использования трафика, необходимо перейти в раздел **«Состояние → Подсчет трафика»** (рисунок 67).

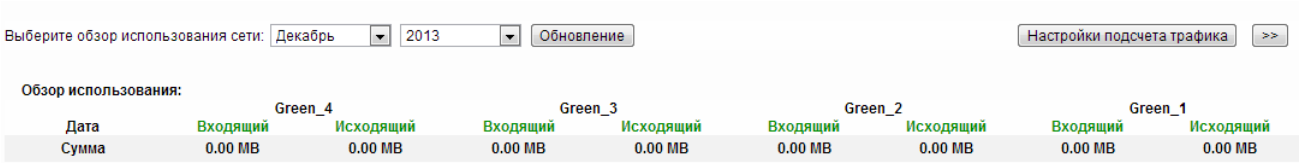
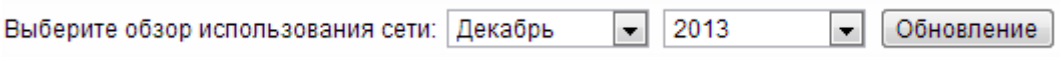
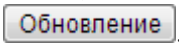


Рис. 67 – «Состояние → Подсчет трафика»

На данной странице предлагается выбрать период обзора использования сети:



После указания месяца и года, за который требуется просмотреть использованный трафик, требуется нажать кнопку 

.

Для конкретизации периода обзора использованного трафика необходимо нажать кнопку

. Откроется страница, представленная на рисунке 68.

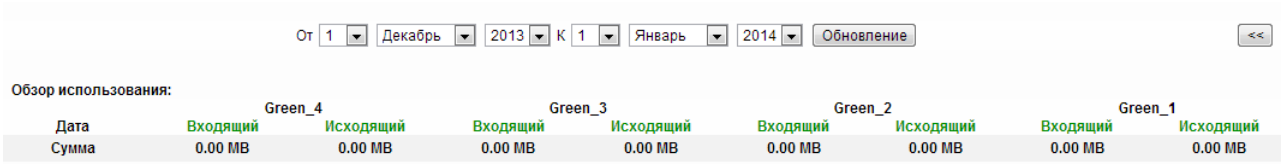
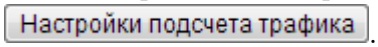


Рис. 68 – «Состояние → Подсчет трафика», детализация периода обзора

Чтобы перейти к настройкам подсчета трафика, необходимо нажать кнопку 

. Откроется страница, представленная на рисунке 69.

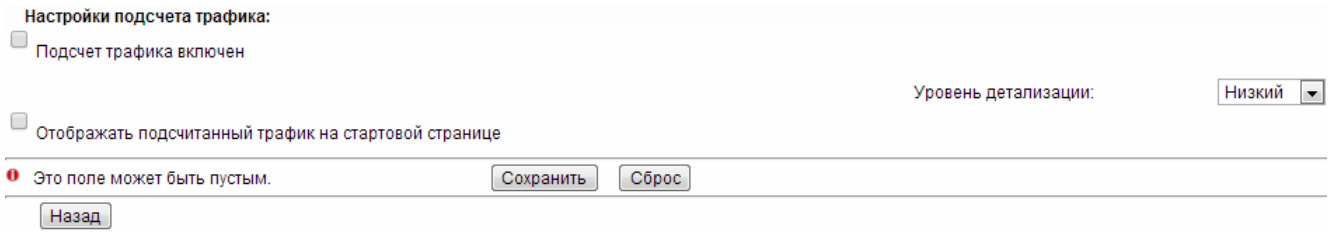
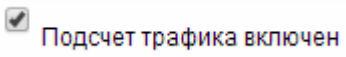


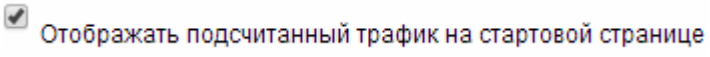
Рис. 69 – Страница настроек подсчета трафика

Для включения подсчета трафика необходимо поставить отметку напротив соответствующего пункта:

Для отключения подсчет трафика отметку необходимо снять.



Предусмотрена возможность отображения подсчитанного трафика на стартовой странице. Для включения данной опции необходимо поставить отметку напротив соответствующего пункта:



После сохранения настроек на стартовой странице можно увидеть подсчитанный трафик (рисунок 70).

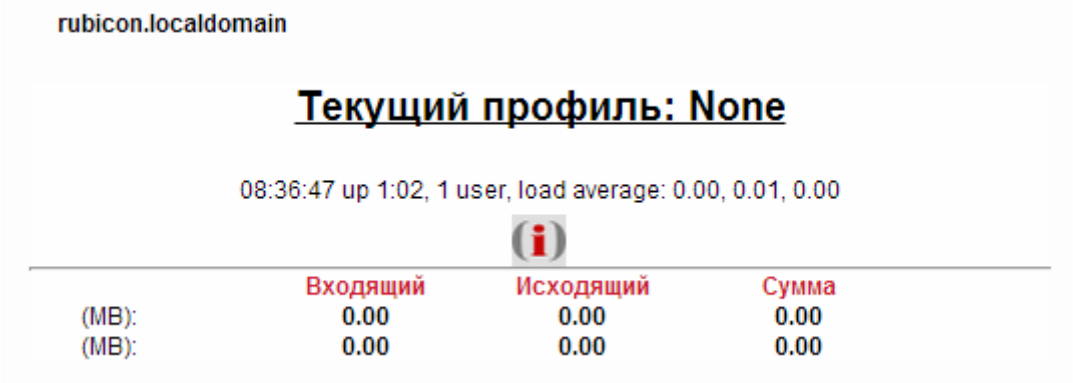


Рис. 70 – Стартовая страница с отображением подсчитанного трафика

Для настройки уровня детализации подсчитанного трафика необходимо выбрать значение из списка:

Уровень детализации при отображении подсчитанного трафика принимает два значения:

– низкий (по умолчанию);
– высокий.

На странице настроек подсчета трафика есть ряд кнопок:
Назад предназначена для перехода к странице «Состояние → Подсчет трафика»;
Сохранить предназначена для сохранения настроек;
Сброс предназначена для возвращения к настройкам по умолчанию.

8. ЖУРНАЛИРОВАНИЕ

8.1. Настройка удаленного копирования журналов

Для удаленного копирования системой защиты информации (СЗИ) изделия журналов «Рубикон» на АРМ, работающий под управлением ОС МС ВС 5.0, необходимо выполнить следующие действия.

1) Установить на АРМ пакет rsyslog-3.22.1-3vniins1, выполнив команды:

cd *<путь до каталога с пакетом rsyslog-3.22.1-3vniins1>*

rpm -i rsyslog-3.22.1-3vniins1.rpm

2) В веб-интерфейсе управления изделием «Рубикон» обратиться к разделу **Журналы** → **Настройка журнала**, вписать IP-адрес АРМ в поле «Сервер Syslog» и поставить отметку напротив пункта «Включено» в разделе **«Запись удаленных событий»**. Сохранить настройки, нажав кнопку **«Сохранить»** (Рисунок 71).

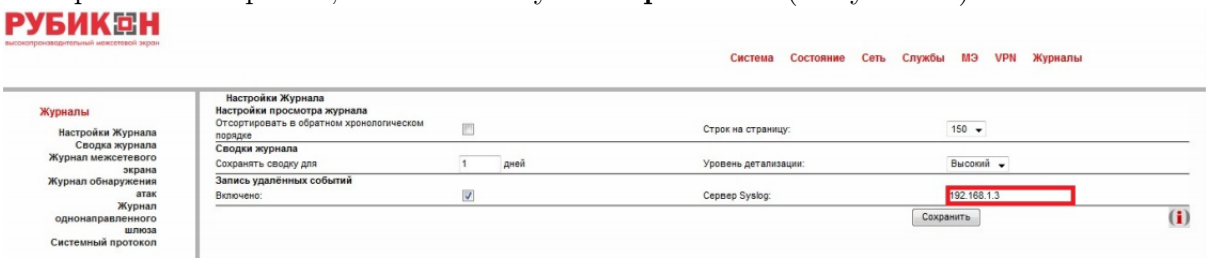


Рис. 71 – Настройка удаленного журналирования

3) В консоли АРМ изменить конфигурационный файл Syslog-сервера /etc/sysconfig/rsyslog, изменив строку, выделенную в рамку (Рисунок 72). Сохранить изменения в файле.

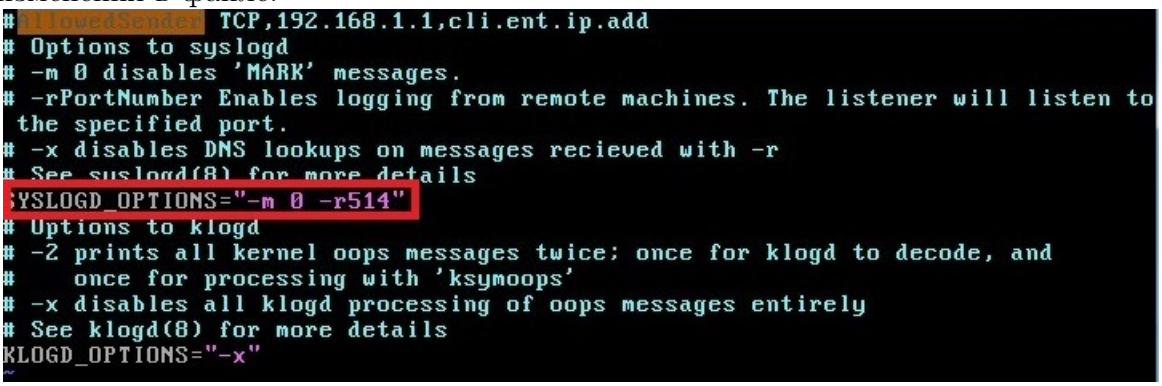


Рис. 72 – Настройка удаленного журналирования

4) В консоли АРМ изменить конфигурационный файл /etc/rsyslog, добавив в него строки, соответствующие источникам данных из сети (Рисунок 73). Сохранить изменения в файле.

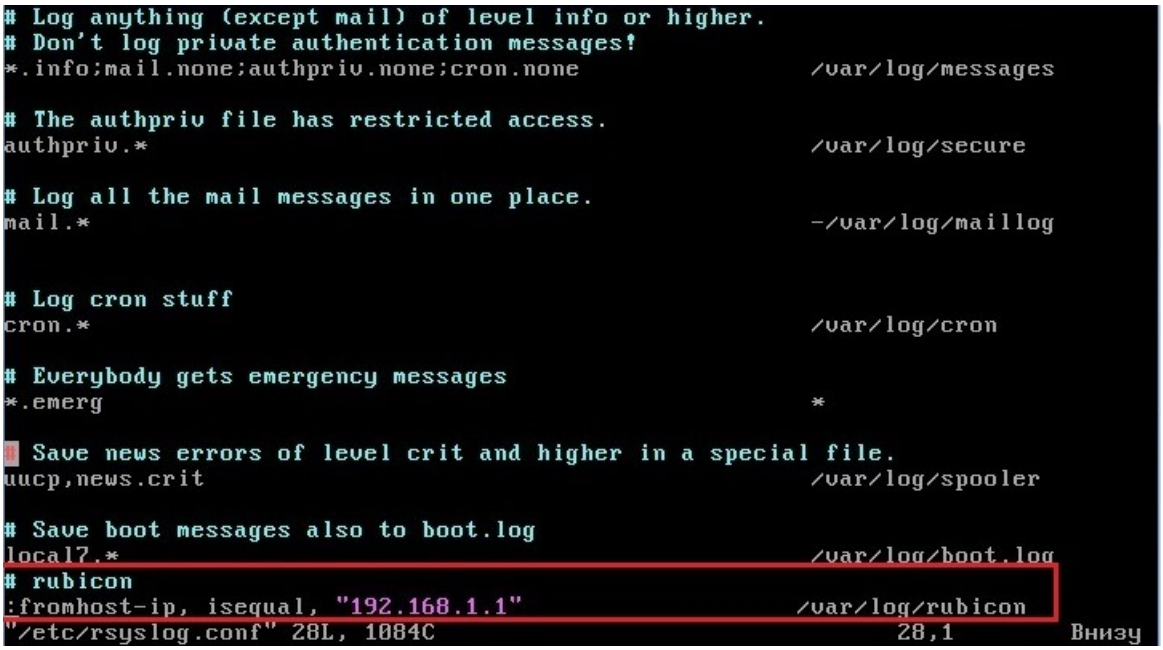


Рис. 73 – Настройка удаленного журналирования

Примечание — В примере на рисунке 73 192.168.1.1 — IP-адрес исчтоника событий, а /var/log/rubicon — путь к файлу, в который будут записаны журналы событий.

5) В настройках iptables отркыть порт 514, набрав команду в консоли АРМ или создав скрипт (Рисунок 74). Сохранить это правило таким образом, чтобы оно действовало и после перезапуска системы.

Рис. 74 – Настройки iptables: открытие порта 514

6) Перезапустить rsyslog-сервер командами:

cd /etc/init.d

./syslog stop

./rsyslog restart

./syslog start

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					