УТВЕРЖДЕН
НПЕШ.465614.005РА-ЛУ

МЕЖСЕТЕВОЙ ЭКРАН И СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ «РУБИКОН»

Руководство администратора

НПЕШ.465614.005РА

Листов 173

2022

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

АННОТАЦИЯ

В данном документе содержатся сведения о функциях, структуре, системных настройках и особенностях администрирования изделия «Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005 (далее – «Рубикон», изделие).

В документе представлены инструкции по безопасным подготовке, первому запуску, настройке и установке изделия, его администрированию в ходе эксплуатации, даны необходимые описания интерфейса и инструкции по реализации основных функций администрирования.

Оформление программного документа «Руководство администратора» произведено по требованиям ЕСПД:

1) ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов;
2) ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов;
3) ГОСТ 19.104-78 ЕСПД. Основные надписи;
4) ГОСТ 19.105-78 ЕСПД. Общие требования к программным документам;
5) ГОСТ 19.106-78 ЕСПД. Общие требования к программным документам, выполненным печатным способом.

СОДЕРЖАНИЕ

1. Общие сведения 5

1.1. Назначение и область применения 5
1.2. Функциональные возможности изделия 6
1.3. Состав изделия 13
1.4. Подготовка к работе 23

2. Описание операций 29

2.1. Присвоение ролей 29
2.2. Просмотр сведений о программе 30
2.3. Настройка межсетевого экрана 31
2.4. Ограничение трафика 43
2.5. Приоритизация трафика 43
2.6. Создание межсетевого моста 44
2.7. Настройка дополнительного адреса сети (настройка псевдонима) 45
2.8. Добавление сети в группу адресов сетевых интерфейсов 46
2.9. Настройка фильтрации пакетов 46
2.10. Настройка прокси-сервера 54
2.11. Создание виртуального интерфейса GRE-туннеля 72
2.12. Создание туннеля GRE с использованием созданного интерфейса GRE 73
2.13. Настройка системы обнаружения вторжений 78
2.14. Трансляция сетевых адресов 84
2.15. Трансляция портов 84
2.16. Маскирование 86
2.17. Таблицы состояний 87
2.18. Настройка резервирования 88
2.19. Работа с журналами событий 93
2.20. Настройка автоматического восстановления 106
2.21. Проверка целостности программного обеспечения 114
2.22. Тестирование САВЗ 115
2.23. Процедуры обновления изделия 116
2.24. Настройки базы решающих правил 119

2.25. Процедуры обновления БРП 126
2.26. Процедура переустановки ПО 129

3. Текстовые сообщения 131

Приложение 1. Перечень принятых терминов и сокращений 133

Приложение 2. Перечень сообщений об ошибках и предупреждений 134

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и область применения

Изделие представляет собой программно-аппаратный комплекс, реализующий функции межсетевого экрана типа «А» второго класса защиты и системы обнаружения вторжений уровня сети второго класса защиты, используемый в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, и иной информации ограниченного доступа и обеспечивающее защиту от преднамеренного несанкционированного доступа или специальных воздействий на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена, с реализацией следующих функций безопасности:

1) контроль и фильтрация;

2) идентификация и аутентификация;

3) разграничение доступа к управлению изделием;

4) регистрация событий безопасности (аудит);

5) обеспечение бесперебойного функционирования и восстановление;

6) тестирование и контроль целостности;

7) преобразование сетевых адресов;

8) маскирование;

9) приоритизация информационных потоков;

10) управление (администрирование);

11) взаимодействие с другими средствами защиты информации;

12) управление параметрами системы обнаружения вторжений;

13) управление установкой обновлений (актуализации) базы решающих правил системы обнаружения вторжений;

14) анализ данных системы обнаружения вторжений;

15) сбор данных о событиях и активности в контролируемой информационной системе;

16) реагирование системы обнаружения вторжений.

1.2. Функциональные возможности изделия

«Рубикон» реализует следующие основные функциональные возможности:

1) возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации и всех операций передачи, контролируемой «Рубикон» информации к узлам информационной системы и от них;

2) возможность осуществлять фильтрацию для всех операций перемещения через межсетевой экран информации к узлам информационной системы и от них;

3) возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности субъектов и информации:

— сетевой адрес узла отправителя;

— сетевой адрес узла получателя;

— сетевой протокол, который используется для взаимодействия;

— интерфейс межсетевого экрана (на уровне сетевого адреса), через который проходит пакет;

— интерфейс межсетевого экрана (на физическом уровне).

4) возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности информации:

— сетевой протокол, который используется для взаимодействия;

— атрибуты, указывающие на фрагментацию пакетов;

— транспортный протокол, который используется для взаимодействия;

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

— разрешенные/запрещенные команды;

— разрешенный/запрещенный мобильный код;

— параметры команд;

— последовательности используемых команд;

— разрешенные/запрещенные протоколы прикладного уровня.

5) возможность явно разрешать информационный поток, базируясь на устанавливаемом администратором «Рубикон» наборе правил фильтрации, основанном на идентифицированных атрибутах;

6) возможность запрещать информационный поток, базируясь на устанавливаемом администратором «Рубикон» наборе правил фильтрации, основанном на идентифицированных атрибутах;

7) возможность блокирования всех информационных потоков, проходящих через нефункционирующий или функционирующий некорректно «Рубикон»;

8) возможность осуществлять политику фильтрации пакетов с учетом управляющих команд от взаимодействующих с «Рубикон» средств защиты информации других видов;

9) возможность осуществлять проверку каждого пакета по таблице состояний для определения того, не противоречит ли состояние (статус, тип) пакета ожидаемому состоянию;

10) возможность осуществлять проверку использования пользователями отдельных команд, для которых администратором «Рубикон» установлены разрешительные или запретительные атрибуты безопасности;

11) возможность осуществлять проверку использования пользователями отдельных команд (последовательностей отдельных команд), для которых администратором «Рубикон» установлены разрешительные или запретительные атрибуты безопасности;

12) возможность осуществлять проверку использования сетевых ресурсов, содержащих мобильный код, для которого администратором «Рубикон» установлены разрешительные или запретительные атрибуты безопасности;

13) возможность осуществлять проверку использования пользователями прикладного программного обеспечения (приложений), для которых администратором «Рубикон» установлены разрешительные или запретительные атрибуты безопасности;

14) возможность разрешать информационный поток, основываясь на результатах проверок;

15) возможность запрещать информационный поток, основываясь на результатах проверок;

16) возможность осуществлять фильтрацию пакетов с учетом управляющих команд от взаимодействующих с «Рубикон» средств защиты информации других видов, основанную на атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика;

17) возможность разрешать информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации;

18) возможность запрещать информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации;

19) возможность осуществлять фильтрацию при импорте (перехвате) информации сетевого трафика из-за пределов «Рубикон»;

20) возможность осуществлять передачу информационных потоков с переназначением сетевых адресов отправителя и (или) получателя (трансляция адресов и посредничество в передаче), фильтрацию при экспорте (передаче от своего имени) информации сетевого трафика за пределы межсетевого экрана;

21) возможность экспортировать (передавать от своего имени) информацию сетевого трафика при положительных результатах фильтрации и других проверок;

22) возможность осуществлять посредничество в передаче информации сетевого трафика, основанное на типе сетевого трафика;

23) возможность маскирования наличия «Рубикон» способами, затрудняющими нарушителям его выявление;

24) возможность осуществлять проверку параметров отдельных команд, для которых администратором «Рубикон» установлены допустимые или недопустимые значения параметров;

25) возможность осуществлять проверку последовательностей используемых отдельных команд, для которых администратором «Рубикон» установлены признаки допустимых и (или) недопустимых последовательностей;

26) возможность регистрации и учета выполнения проверок информации сетевого трафика;

27) возможность читать информацию из записей аудита уполномоченным администраторам;

28) возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита;

29) возможность оповещения уполномоченных лиц о критичных видах событий безопасности, в том числе – сигнализация о попытках нарушения правил «Рубикон»;

30) возможность выборочного просмотра данных аудита (поиск, сортировка, упорядочение данных аудита);

31) возможность регистрации возникновения событий, которые в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» включены в детализированный уровень аудита;

32) возможность идентификации администратора «Рубикон» до разрешения любого действия (по администрированию), выполняемого при посредничестве «Рубикон» от имени этого администратора;

33) возможность аутентификации администратора «Рубикон» до разрешения любого действия (по администрированию), выполняемого при посредничестве «Рубикон» от имени этого администратора;

34) возможность осуществления идентификации субъектов межсетевого взаимодействия до передачи «Рубикон» информационного потока получателю;

35) возможность осуществления аутентификации субъектов межсетевого взаимодействия до передачи «Рубикон» информационного потока получателю;

36) поддержку определенных ролей по управлению «Рубикон»;

37) возможность со стороны администраторов управлять режимом выполнения функций безопасности «Рубикон»;

38) возможность со стороны администраторов управлять данными «Рубикон», используемыми функциями безопасности «Рубикон»;

39) возможность со стороны администраторов управлять атрибутами безопасности;

40) возможность поддержки списка типов сетевого трафика для осуществления посредничества в передаче, предусматривающего разделение трафика по типам;

41) ассоциацию типов сетевого трафика из списка с конкретным сетевым трафиком для осуществления посредничества в передаче и обработки соответствующих типов сетевого трафика прокси-агентами;

42) возможность изменения области значений информации состояния соединения со стороны администраторов «Рубикон»;

43) возможность присвоения информации состояния соединения допустимых значений, таких как установление соединения, использование соединения, завершение соединения и других;

44) возможность ведения для каждого соединения таблицы состояний, основанной на информации состояния соединения;

45) предоставление возможности администраторам «Рубикон» модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для используемых пользователями отдельных команд для осуществления «Рубикон» фильтрации;

46) предоставление возможности администраторам «Рубикон» модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности использования сетевых ресурсов, содержащих отдельные типы мобильного кода, для осуществления «Рубикон» фильтрации;

47) предоставление возможности администраторам «Рубикон» модифицировать, удалять атрибуты безопасности, определяющие допустимые и (или) недопустимые значения параметров используемых отдельных команд, для осуществления «Рубикон» фильтрации;

48) предоставление возможности администраторам «Рубикон» модифицировать, удалять атрибуты безопасности, определяющие признаки допустимых и (или) недопустимых последовательностей используемых отдельных команд, для осуществления «Рубикон» фильтрации;

49) возможность перехода в режим аварийной поддержки, который предоставляет возможность возврата «Рубикон» к штатному функционированию;

50) возможность генерации надежных меток времени при проведении аудита безопасности;

51) возможность тестирования (самотестирования) функций безопасности «Рубикон» (контроль целостности исполняемого кода «Рубикон»);

52) возможность сохранения штатного функционирования «Рубикон» при некритичных типах сбоев;

53) возможность согласованно интерпретировать управляющие команды, атрибуты сетевого трафика и иные данные, получаемые от взаимодействующих с «Рубикон» средств защиты информации других видов;

54) поддержку правил интерпретации данных, получаемых от взаимодействующих с «Рубикон» средств защиты информации других видов;

55) возможность завершения работы или восстановления (для предусмотренных сценариев сбоев) штатного функционирования «Рубикон»;

56) возможность тестирования средств защиты информации других видов, взаимодействующих с «Рубикон», и управляющие команды которых использует «Рубикон» для управления потоками информации;

57) возможность при определенных типах сбоев/прерываний обслуживания автоматического возврата «Рубикон» к штатному функционированию;

58) возможность кластеризации «Рубикон»;

59) возможность приоритизации контроля и фильтрации разных информационных потоков, а также выделения ресурсов, доступных для разных информационных потоков, обрабатываемых одновременно (в течение определенного периода времени);

60) возможность сбора информации о сетевом трафике;

61) возможность выполнения анализа собранных данных «Рубикон» о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;

62) возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов;

63) возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа;

64) возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;

65) возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;

66) возможность задания правил фильтрации данных «Рубикон» с возможностью сохранения отфильтрованной информации в отдельных файлах;

67) возможность блокирования вторжений и нарушений безопасности, в том числе путем выдачи управляющих сигналов «Рубикон»;

68) уведомление администратора «Рубикон» об обнаруженных вторжениях по отношению к контролируемым узлам ИС и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления, отсылки сообщений электронной почты;

69) возможность автоматизированного обновления базы решающих правил;

70) возможность верификации целостности базы решающих правил (далее – БРП) системы обнаружения вторжений (далее – СОВ);

71) возможность маскирования наличия датчика «Рубикон» в составе контролируемой информационной системы (далее – ИС), противодействие выявлению его на сетевом уровне стандартными средствами операционной системы (далее – ОС);

72) возможность со стороны уполномоченных администраторов (ролей) управлять режимом выполнения функций безопасности «Рубикон»;

73) возможность со стороны уполномоченных администраторов (ролей) управлять данными «Рубикон» (установление и контроль ограничений и значений; внесения новых правил контроля в БРП СОВ);

74) поддержку определенных ролей для «Рубикон» и их ассоциацию с конкретными администраторами и пользователями ИС;

75) возможность локального и удаленного администрирования «Рубикон»;

76) наличие графического интерфейса администрирования «Рубикон»;

77) возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;

78) возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;

79) возможность читать информацию из записей аудита;

80) ограничение доступа к чтению записей аудита;

81) поиск, сортировку, упорядочение данных аудита.

1.3. Состав изделия

В состав изделия входят следующие основные компоненты:

1) аппаратная платформа с опционально предустановленными модулями расширения;

2) предустановленное программное обеспечение (далее – ПО) «Рубикон-А», обеспечивающее реализацию функциональных возможностей изделия.

Модель поставляемой в составе изделия аппаратной платформы и перечень дополнительных модулей расширения определяется вариантом исполнения изделия и его конфигурацией, в соответствии с Договором поставки. Указанная информация представлена в формуляре на поставляемое изделие.

1.3.1. Варианты исполнения «Рубикон»

Изделие поставляется в одном из следующих базовых вариантов исполнения:

1) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-01;

2) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-02;

3) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-03;

4) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-04;

5) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-05;

6) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-06;

7) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-07;

8) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-08;

9) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-09;

10) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-10;

11) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-11;

12) Межсетевой экран и система обнаружения вторжений «Рубикон» НПЕШ.465614.005-12.

1.3.2. Комплектность поставки

Состав комплекта поставки «Рубикон», в соответствии с вариантом исполнения, представлен в формуляре на изделие.

В зависимости от варианта исполнения «Рубикон» и договора поставки дополнительно могут поставляться модули расширения.

1.3.3. Требования к АРМ администратора

Для управления интерфейсом администрирования «Рубикон» используется графический веб-интерфейс, доступ к которому осуществляется с использованием веб-браузера.

Минимальные требования к автоматизированному рабочему месту (далее – АРМ) администратора указаны в таблице 1.

Таблица 1 – Минимальные требования к АРМ администратора «Рубикон»

Элемент среды функционирования	Параметры	
Вычислительная платформа АРМ администратора ПО «Рубикон-А»	Процессор на базе архитектуры	x86-x64/ARM
	Оперативная память, Гбайт, не менее	2
	Устройства ввода-вывода, не менее	– монитор; – клавиатура; – мышь; – 1xCOM-порт (RS-232)
	Поддержка дополнительных интерфейсов, не менее	– 1xEthernet 100/1000 Base-T
ОС АРМ администратора	ОС семейства Linux/Unix 32/64 бит	– Debian не ниже ver. 8; – Ubuntu не ниже ver. 16; – Astra Linux Common Edition (Орел) не ниже ver. 1.11; – Astra Linux Special Edition (Смоленск) не ниже ver. 1.5
	ОС семейства Microsoft Windows 64 бит	– Windows Server 2019; – Windows 10

Элемент среды функционирования	Параметры	
Веб-браузер	ОС семейства Linux/Unix 32/64 бит, не ниже	– Firefox (ver. 60.0.2, x64)
	ОС семейства Microsoft Windows 64 бит, не ниже	– IE (ver. 11.1.17134.0); – Microsoft Edge (ver. 42.17134.1.0); – Firefox (ver. 76.0.1 x64); – Chrome (ver. 83.0.4103.61)

1.3.4. Состав установочного дистрибутива ПО

Установочный дистрибутив представляет собой ISO-образ файловой системы «Рубикон» на носителе данных.

Контрольная сумма ISO образа «Рубикон» совпадает с контрольной суммой побитовой копии ISO образа на флеш-накопителе и представлена в формулярах на соответствующее исполнение «Рубикон».

Фиксацию контрольных сумм дистрибутива необходимо выполнять с использованием утилиты «Инспектор» программного комплекса «Средство анализа защищенности «Сканер-ВС» (Сертификат соответствия ФСТЭК России № 2204) по алгоритму «ФИКС (уровень 1)».

Для подсчета контрольных сумм флеш-накопителя необходимо в интерфейсе утилиты «Инспектор» программного комплекса «Средство анализа защищенности «Сканер-ВС» указать путь /dev/<имя партиции флеш-накопителя> и алгоритм «ФИКС (уровень 1)».

Состав и контрольные суммы неизменяемых исполняемых файлов ПО «Рубикон-А» после установки на аппаратную платформу должны соответствовать контрольным суммам, приведенным в документе «Технические условия. Приложение В НПЕШ.465614.005ТУ1», находящемся на электронном носителе с документацией из комплекта поставки.

1.3.5. Функциональная структура ПО

Функциональная структура ПО «Рубикон-А» представлена следующими подсистемами:

1) подсистема обеспечения сетевого взаимодействия;

2) подсистема идентификации / аутентификации;

3) подсистема бесперебойного функционирования и восстановления;

4) подсистема регистрации событий;

5) подсистема взаимодействия с внешними системами;

6) подсистема управления;

7) подсистема обнаружения вторжений;

8) веб-интерфейс;

9) операционная система;

10) подсистема BIOS.

1.3.5.1. Подсистема обеспечения сетевого взаимодействия

Подсистема обеспечения сетевого взаимодействия представлена следующими модулями:

1) модуль фильтрации;

2) модуль маршрутизации;

3) модуль преобразования адресов;

4) модуль приоритизации;

5) модуль управления состояниями;

6) модуль сетевого посредника;

7) модуль настройки сетевых интерфейсов.

1.3.5.1.1. 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:

1) сетевой адрес узла отправителя и получателя;

2) логический или физический сетевой интерфейс «Рубикон», через который проходит пакет;

3) сетевой протокол, который используется для взаимодействия;

4) направление пакета (входящий/исходящий);

5) транспортный протокол, который используется для взаимодействия;

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

7) флаг фрагментации;

8) мандатная метка;

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

10) мобильный код (разрешенный/запрещенный) для языка программирования JavaScript;

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

1.3.5.1.2. Модуль маршрутизации

Программный модуль «Рубикон» предназначен для выполнения статической маршрутизации.

1.3.5.1.3. Модуль преобразования адресов

Программный модуль «Рубикон», позволяющий проводить трансляцию сетевых адресов (NAT) при экспорте информации сетевого трафика за пределы «Рубикон» и осуществлять замену сетевого адреса «Рубикон» на маскирующий (подставной) адрес.

1.3.5.1.4. Модуль приоритизации

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

1.3.5.1.5. Модуль управления состояниями

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

1.3.5.1.6. Модуль сетевого посредника

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

1) сетевой адрес и порт отправителя и получателя;

2) сетевой трафик (FTP, HTTP);

3) разрешенные/ запрещенные атрибуты информации в заголовках пакетов.

1.3.5.1.7. Модуль настройки сетевых интерфейсов

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

1.3.5.2. Подсистема идентификации / аутентификации

Подсистема идентификации / аутентификации представлена модулем аутентификации веб-сервера.

1.3.5.2.1. Модуль аутентификации веб-сервера

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

1.3.5.3. Подсистема бесперебойного функционирования и восстановления

Подсистема бесперебойного функционирования и восстановления представлена следующими модулями:

1) модуль тестирования и контроля целостности;

2) модуль восстановления;

3) модуль кластеризации.

1.3.5.3.1. Модуль тестирования и контроля целостности

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

1.3.5.3.2. Модуль восстановления

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

1.3.5.3.3. Модуль кластеризации

Программный модуль «Рубикон» обеспечивает выполнение всех возможностей межсетевого экрана (далее – МЭ) при возникновении сбоев путем кластеризации.

Кластеризация предполагает резервирование двух изделий «Рубикон» в режиме «активный – пассивный».

1.3.5.4. Подсистема регистрации событий

Данная подсистема представлена модулем работы с журналом.

1.3.5.4.1. Модуль работы с журналом

Программный модуль «Рубикон», предназначенный для создания, хранения и просмотра записей аудита. «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 «Рубикон», аудитор «Рубикон») возможность читать всю информацию из записей аудита, осуществлять поиск, сортировать записи аудита.

1.3.5.5. Подсистема взаимодействия с внешними системами

Данная подсистема состоит из следующих модулей:

1) модуль взаимодействия с внешними средствами защиты информации (далее – СЗИ);

2) модуль связи с сервером журналирования.

1.3.5.5.1. Модуль взаимодействия с внешними СЗИ

Программный модуль «Рубикон», обеспечивающий взаимодействия «Рубикон» со средствами антивирусной защиты (далее – САВЗ) по протоколу адаптации Интернет-контента (ICAP).

1.3.5.5.2. Модуль связи с сервером журналирования

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

1.3.5.6. Подсистема управления

Данная подсистема представлена следующими модулями:

1) модуль веб-сервера;

2) модуль преобразования конфигурации браузера.

1.3.5.6.1. Модуль веб-сервера

Программный модуль «Рубикон», обеспечивающий выполнение запросов пользователей.

1.3.5.6.2. Модуль преобразования конфигурации браузера

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

1.3.5.7. Подсистема обнаружения вторжений

Подсистема обнаружения вторжений представлена следующими модулями:

1) модуль «Агент обновления»;

2) модуль сигнатурного анализа сетевого трафика;

3) модуль эвристического анализа сетевого трафика;

4) модуль реагирования.

1.3.5.7.1. Модуль «Агент обновления»

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

1.3.5.7.2. Модуль сигнатурного анализа сетевого трафика

Программный модуль «Рубикон», предназначенный для поиска определенных в базе решающих правил СОВ сигнатур атак в сетевых пакетах.

1.3.5.7.3. Модуль эвристического анализа сетевого трафика

Программный модуль «Рубикон», предназначенный для обнаружения вторжений с помощью эвристического анализа.

1.3.5.7.4. Модуль реагирования

Программный модуль «Рубикон», позволяющий уведомлять администратора об обнаруженных вторжениях и выдавать управляющие сигналы МЭ.

1.3.5.8. Веб-интерфейс

Веб-интерфейс реализует интерфейс модуля «Программа управления», позволяет решать задачи по администрированию СОВ.

1.3.5.9. Операционная система

Операционная система, помимо реализации профильных функций по умолчанию, дополнительно представлена следующими модулями:

1) модуль выдачи меток времени;

2) модуль захвата и разбора трафика.

1.3.5.9.1. Модуль выдачи меток времени

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

1.3.5.9.2. Модуль захвата и разбора трафика

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

1.3.5.10. Подсистема BIOS

Подсистема BIOS представлена модулем BIOS.

1.3.5.10.1. Модуль BIOS

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

1.4. Подготовка к работе

1.4.1. Действия по приемке изделия

Приемка изделия осуществляется в следующем порядке:

1) проверка комплектности;

2) проверка маркировки и пломбирования;

3) проверка контрольных сумм изделия.

1.4.1.1. Проверка комплектности

Проверку комплектности следует проводить методом оценки соответствия комплекта изделия и разделом «Комплектность» формуляра на изделие, если в Договоре поставки не указано иное.

1.4.1.2. Проверка маркировки и пломбирования

Проверку маркировки и пломбирования следует проводить методом оценки соответствия маркировки и пломбирования изделия и подразделами «Маркировка» и «Пломбирование» руководства по эксплуатации на изделие.

1.4.1.3. Проверка контрольных сумм изделия

Проверка контрольных сумм дистрибутива проводится с использованием утилиты «Инспектор» программного комплекса «Средство анализа защищенности «Сканер-ВС» (Сертификат соответствия ФСТЭК России № 2204) по алгоритму «ФИКС (уровень 1)».

Для подсчета контрольных сумм флеш-накопителя необходимо в интерфейсе утилиты «Инспектор» программного комплекса «Средство анализа защищенности «Сканер-ВС» указать путь /dev/<имя партиции флеш-накопителя> и алгоритм «ФИКС (уровень 1)».

Состав и контрольные суммы неизменяемых исполняемых файлов ПО «Рубикон-А» после установки на аппаратную платформу приведены в документе «Технические условия. Приложение В НПЕШ.465614.005ТУ1», находящемся на электронном носителе с документацией из комплекта поставки.

Результаты контрольного суммирования BIOS используемой аппаратной платформы представлены в формулярах на соответствующее исполнение «Рубикон». Контрольные суммы BIOS рассчитываются с использованием утилиты «Инспектор» программного комплекса «Средство анализа защищенности «Сканер-ВС» (Сертификат соответствия ФСТЭК России № 2204) по алгоритму «ФИКС (уровень 1)».

1.4.2. Требования по безопасной установке и настройке изделия

1.4.2.1. Требования к квалификации администратора

Администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию изделия, а также должен иметь профессиональные знания и практический опыт в области системного администрирования. Обязательны знакомство и практический опыт установки и администрирования серверных операционных систем семейства MS Windows и Linux, знание эксплуатационной документации изделия.

1.4.2.2. Организационные меры по обеспечению безопасной настройки и установки

При эксплуатации «Рубикон» в составе объектов информатизации, на которых производится обработка информации ограниченного доступа, должно быть обеспечено выполнение следующих организационных мер:

1) наличие администратора безопасности, отвечающего за корректную эксплуатацию «Рубикон»;

2) сохранение в защищенной форме идентификаторов (имен) и паролей (кодов) администратора «Рубикон»;

3) обеспечение физической сохранности технических средств (устройства «Рубикон», терминала или персональной электронно-вычислительной машины (далее – ЭВМ), использующейся в качестве терминала) и исключение возможности доступа к ним посторонних лиц;

4) обеспечение защиты АРМ администратора «Рубикон», в том числе, от деструктивного воздействия вредоносного ПО;

5) регламентацию использования дополнительного ПО, установленного на АРМ администратора «Рубикон»;

6) обеспечение сохранности оборудования и физической целостности системных блоков компьютеров;

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

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

К информационной среде, в которой функционирует «Рубикон», предъявляются следующие требования безопасности:

1) обеспечение регламентации запрета доступа непривилегированных пользователей из внешней сети в защищаемые сети по всем типам протоколов, за исключением специально созданной для такого доступа демилитаризованной сети;

2) обеспечение физической сохранности технических средств (МЭ, средства вычислительной техники, на котором он функционирует и терминалов, с которых выполняется его управление) и исключение возможности доступа к ним посторонних лиц;

3) обеспечение установки, конфигурирования и управления «Рубикон» в соответствии с эксплуатационной документацией.

1.4.2.3. Подготовка к эксплуатации

1.4.2.3.1. Перечень используемой эксплуатационной документации

Перечень эксплуатационных документов, с которым необходимо ознакомиться перед началом работы с изделием:

1) настоящий документ НПЕШ.465614.005РА «Межсетевой экран и система обнаружения вторжений «Рубикон». Руководство администратора»;

2) документ НПЕШ.465614.005РП «Межсетевой экран и система обнаружения вторжений «Рубикон». Руководство пользователя»;

3) руководство по эксплуатации на изделие (в соответствии с вариантом исполнения изделия);

4) формуляр на изделие (в соответствии с вариантом исполнения изделия).

1.4.2.3.2. Первый запуск устройства «Рубикон»

Первый запуск устройства «Рубикон» производится в следующем порядке:

1) последовательно выполнить действия, указанные в подразделе «Подготовка изделия к использованию» руководства по эксплуатации на изделие;

2) последовательно выполнить действия, указанные в подразделе «Подключение изделия» руководства по эксплуатации на изделие;

3) последовательно выполнить действия, указанные в подразделе «Включение изделия» руководства по эксплуатации на изделие;

Примечание – Для авторизации, как администратор, необходимо ввести логин и пароль. По умолчанию логин – **admin**. Пароль – **radmin**. В случае выполнения трех неуспешных попыток ввода логина и пароля – доступ к «Рубикон» будет заблокирован. Спустя 5 минут можно повторить попытку входа.

4) при первом подключении к административному интерфейсу, для обеспечения безопасности, пароль по умолчанию необходимо изменить на странице «Система – Пользователи» в главном меню веб-интерфейса изделия;

5) после выполнения указанных выше шагов пользователь с полномочиями администратора безопасности будет перенаправлен в раздел «Система», подраздел «Начало» (стартовая страница).

1.4.2.3.3. Настройка функций безопасности

Настройка функций безопасности устройства «Рубикон» осуществляется администратором безопасности охраняемого IT-сегмента в соответствии с Политикой информационной безопасности.

1.4.2.3.4. Установка устройства «Рубикон»

По окончании настройки функций безопасности устройство «Рубикон» должно быть установлено и подключено согласно монтажным схемам и схемам подключения защищаемой информационной системы.

1.4.2.3.5. Проверка целостности установленного ПО

Перед началом эксплуатации необходимо выполнить проверку контрольных сумм установленного ПО «Рубикон-А».

В изделии 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.

1.4.2.3.6. Проверка работоспособности

Проверка работоспособности считается выполненной при успешном выполнении процедур первого запуска и корректных результатах проверки контрольных сумм ПО «Рубикон-А», установленном на аппаратной платформе «Рубикон».

Подробно процедуры первого запуска и проверки работоспособности представлены в руководстве по эксплуатации изделия в разделе «Использование по назначению».

2. ОПИСАНИЕ ОПЕРАЦИЙ

2.1. Присвоение ролей

ПО «Рубикон-А» поддерживает присвоение пользователям следующих ролей:

1) «Администратор» – имеет доступ к просмотру веб-интерфейса и настройке «Рубикон»;

2) «Аудитор» – имеет доступ к разделам «Состояние» и «Журналы», без возможности внесения изменений в настройки «Рубикон»;

3) «Пользователь» – не имеет доступа к просмотру веб-интерфейса (кроме стартовой страницы) и страницы установки соединения «https://<ip-address>:8443/cgi-bin/connect.cgi». Параметр «ip-address» при первоначальной установке имеет значение 192.168.1.1 и может быть изменен администратором. На странице установки соединения после нажатия кнопки «Установить соединение» ПО «Рубикон-А» фиксирует IP-адрес пользователя и предоставляет соответствующие права, назначенные данному пользователю администратором в разделе «Межсетевой экран» подраздела «Правила межсетевого экрана».

Для того, чтобы добавить новых пользователей в подразделе «Пользователи» раздела «Система», в ниспадающем списке «Роль» выберите роль («Администратор», «Аудитор», «Пользователь»), затем заполните следующие текстовые поля (см. рис. 1):

1) «Имя»;

2) «Пароль»;

3) «Подтверждение».

Далее следует нажать кнопку «Сохранить».

Подраздел «Пользователи» раздела «Система»

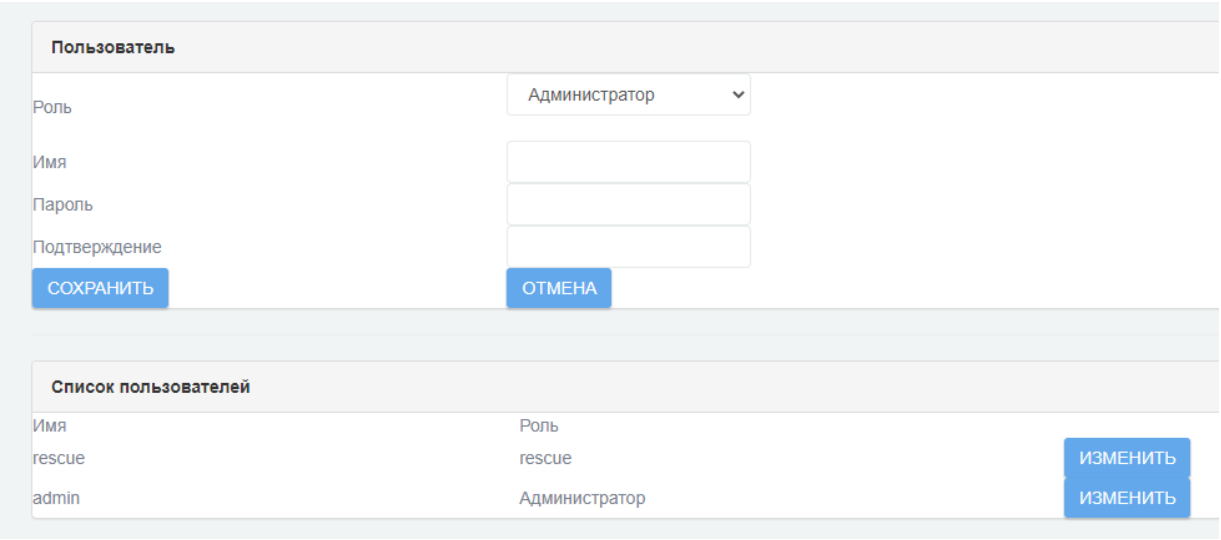


Рис. 1

Список пользователей отображается в блоке «Список пользователей». При необходимости, можно удалить пользователя или внести изменения в учетную запись.

Авторизация роли «Аудитор» и роли «Пользователь» выполняется аналогично авторизации роли «Администратор». Для работы с «Рубикон» пользователю необходимо получить логин и пароль у администратора безопасности.

2.2. Просмотр сведений о программе

После успешного прохождения процедуры авторизации администратор может вывести на экран сведения о «Рубикон» (версию, производителя и т.п.), перейдя в подраздел «О программе» раздела «Система» (см. рис. 2).

Подраздел «О программе» раздела «Система»

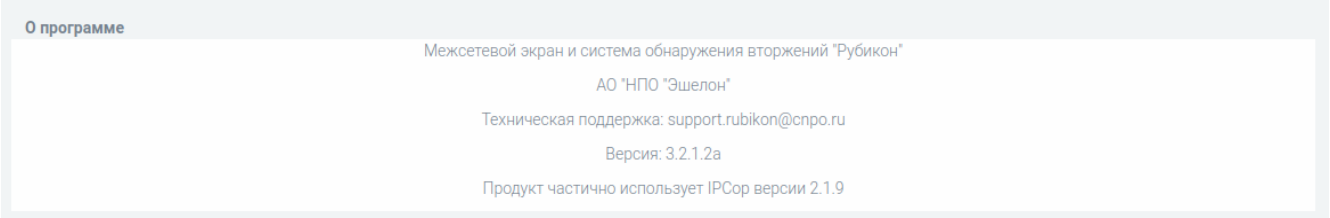


Рис. 2

2.3. Настройка межсетевого экрана

Для настройки МЭ войдите в раздел «Межсетевой Экран» и перейдите в подраздел «Настройки межсетевого экрана».

Подраздел «Настройки межсетевого экрана» предназначен для установки параметров администрирования МЭ. Общая настройка межсетевого экрана заключается в настройке административного доступа к межсетевому экрану, выборе режимов его работы, а также в установке политик по умолчанию на интерфейсах.

Цвет интерфейса – это набор стандартных правил и политик по отношению к пакетам, которые проходят через него. Цветовые политики позволяют избежать создания большого числа различных правил и сразу применить наиболее подходящую политику, которую в дальнейшем возможно доработать под конкретное применение настройкой правил МЭ.

Цветовые политики – определяют «поведения» правил МЭ при сетевом взаимодействии с данным сетевым интерфейсом и между сетевыми интерфейсами.

Пользовательские правила МЭ имеют **более высокий** приоритет, чем цветовые политики и могут их превосходить.

Сетевые интерфейсы можно разбить на две группы:

1) физические – определяются исходя из наличия физических сетевых адаптеров;

2) виртуальные – назначаются на физических интерфейсах или объединяют их в виртуальные интерфейсы.

Цветовые политики для физических интерфейсов представлены в таблице 2.

Таблица 2 – Цветовые политики для физических интерфейсов

Цвет интерфейса	Описание соответствующих правил и политик
Green (Зеленый)	Интерфейс используется для подключения к внутренней (доверенной) сети
Red (Красный)	Интерфейс используется для подключения к внешней сети, при этом на сетевом интерфейсе включается трансляция сетевых адресов (NAT) (потенциально опасная сеть)
Orange (Оранжевый)	Интерфейс для создания демилитаризованной зоны (далее – DMZ)

Цвет интерфейса	Описание соответствующих правил и политик
Blue (Синий)	Интерфейс, для подключения к локальной сети, узлы которой по умолчанию имеют возможность свободного прохождения в сеть красного интерфейса аналогично узлам в сети зеленого интерфейса, но имеют ограничения на доступ к узлам зеленых интерфейсов с помощью белого списка. Разрешения на доступ к узлам зеленых интерфейсов настраиваются на странице «Межсетевой экран» → «Доступ к синему интерфейсу»

По умолчанию цветовая политика на физических интерфейсах назначается **зеленая**. Такие интерфейсы являются **административными**, т.е. по ним разрешено администрирование «Рубикон» (см. рис. 3).

Цветовая политика на физических интерфейсах по умолчанию

Политики сетевых интерфейсов:

Имя	Цвет	Политика	Запись в журнал	Запрещающее действие по умолчанию	Доступ к Синему интерфейсу	Действие
Green_1		open	☐	DROP		
Green_10		open	☐	DROP		
Green_2		open	☐	DROP		
Green_3		open	☐	DROP		
Green_4		open	☐	DROP		
Green_5		open	☐	DROP		
Green_6		open	☐	DROP		
Green_7		open	☐	DROP		
Green_8		open	☐	DROP		
Green_9		open	☐	DROP		

Рис. 3

Чтобы назначить / изменить цветовую политику интерфейса, нужно перейти в подраздел «Настройка адаптеров» раздела «Сеть» (см. рис. 4 – 5).

Подраздел «Настройка адаптеров»

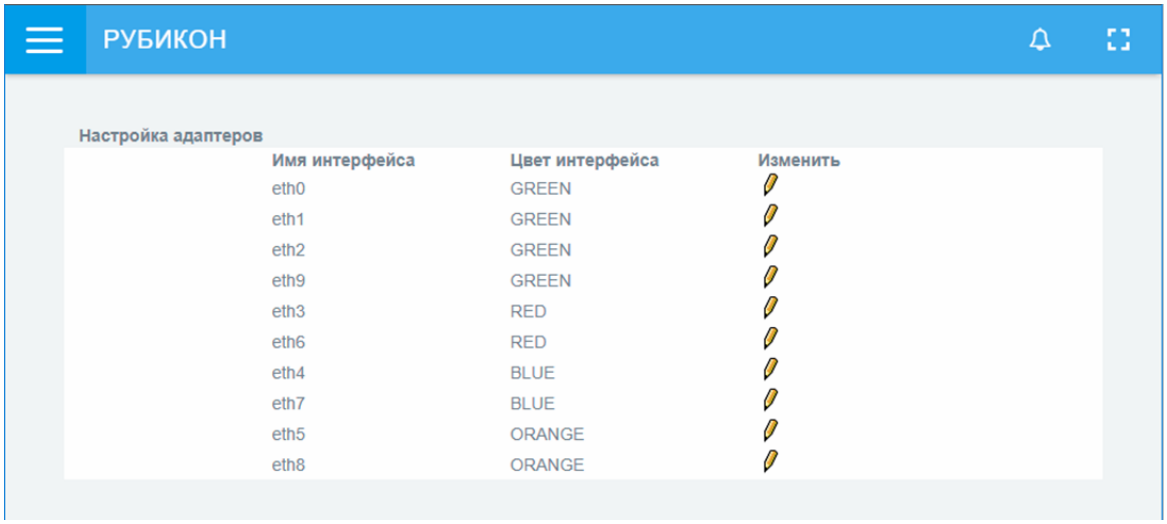


Рис. 4

Отображение цветовых политик интерфейсов

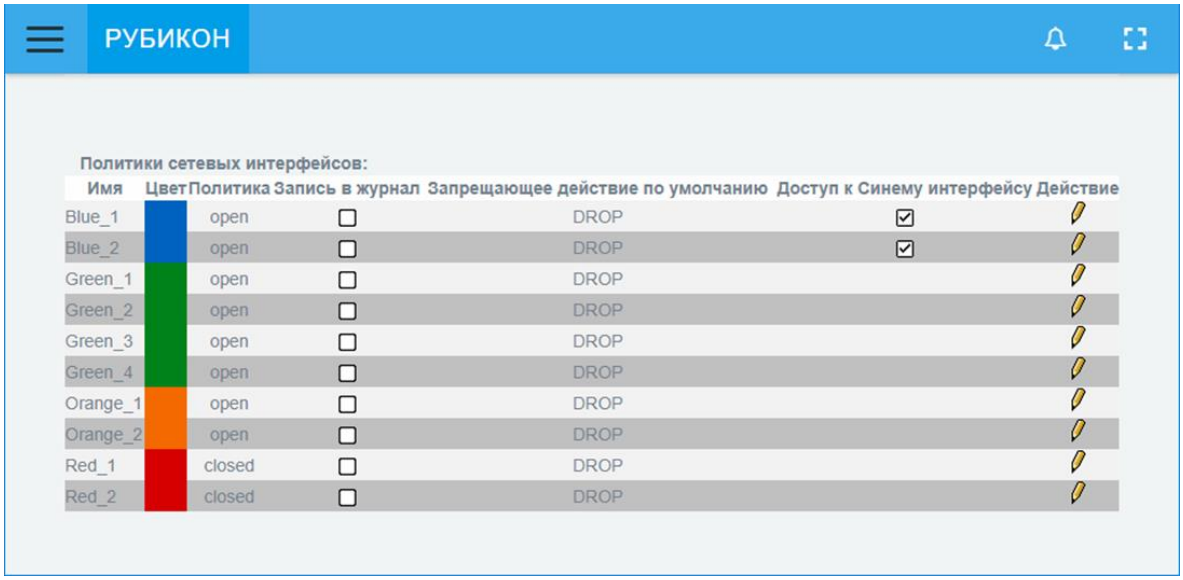


Рис. 5

Перед сменой цвета необходимо убедиться, что интерфейс **не является административным** (на странице «Межсетевой экран» → «Настройки межсетевого экрана»). **Система не позволит изменить цвет зеленого административного интерфейса.**

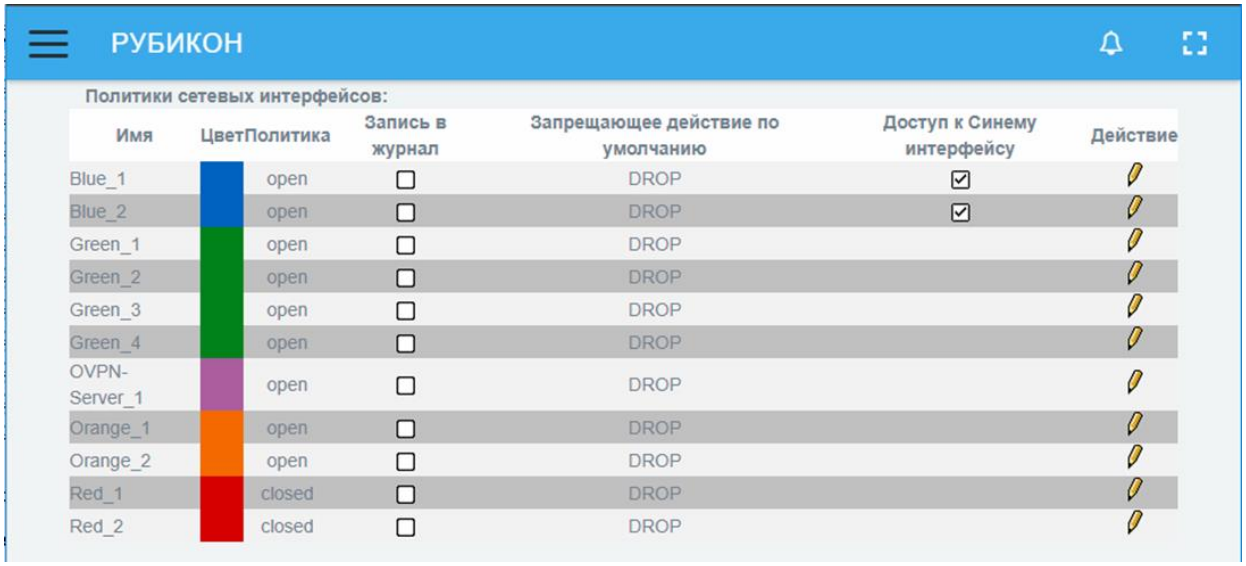
ВНИМАНИЕ!

СМЕНА ЦВЕТА ИНТЕРФЕЙСА ВСТУПАЕТ В СИЛУ ТОЛЬКО ПОСЛЕ ПЕРЕЗАГРУЗКИ.

Цветовые политики для виртуальных интерфейсов представлены на рис. 6 – 7.

Виртуальным интерфейсам **не назначаются** цветовые политики, за исключением OpenVPN. Правила цветовой политики МЭ для OpenVPN **аналогичны** зеленой цветовой политики.

Цветовые политики для виртуальных интерфейсов



Имя	ЦветПолитика	Запись в журнал	Запрещающее действие по умолчанию	Доступ к Синему интерфейсу	Действие
Blue_1	open	☐	DROP	☑	
Blue_2	open	☐	DROP	☑	
Green_1	open	☐	DROP		
Green_2	open	☐	DROP		
Green_3	open	☐	DROP		
Green_4	open	☐	DROP		
OVPN-Server_1	open	☐	DROP		
Orange_1	open	☐	DROP		
Orange_2	open	☐	DROP		
Red_1	closed	☐	DROP		
Red_2	closed	☐	DROP		

Рис. 6

Правила цветовых политик для виртуальных интерфейсов

#	Сеть Интерфейс	Источник	Журнал:		Сеть Интерфейс	Назначение	Замечание	Действие
1	Green_1	Any	☒	»	Red_1	Any : Ping		
2	Green_1	Any	☒	»	Orange_1	Any : Ping		
3	Green_1	Any	☒	»	Blue_1	Any : Ping		
4	Green_1	Any	☒	»	OVPN-Server_1	Any : Ping		
5	Green_1	Any	☒	»	vlan	Any : Ping		

Рис. 7

Для отслеживания состояний соединений различных интерфейсов используется отдельная цветовая легенда, которую можно увидеть на странице «Состояние» → «Соединения» (см. рис. 8).

Цветовая легенда состояний соединений различных интерфейсов

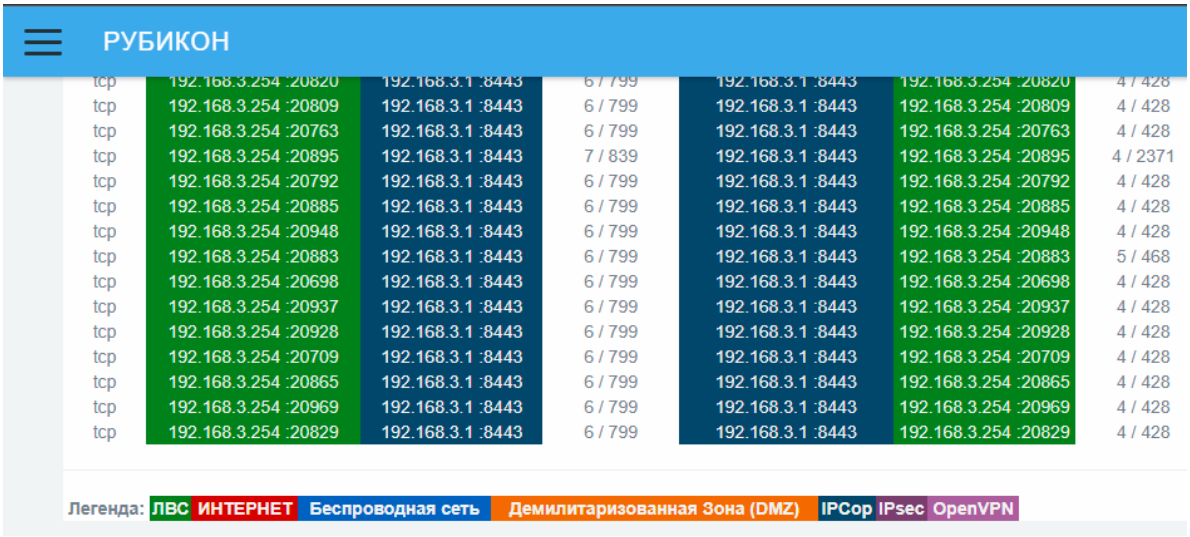


Рис. 8

Описание цветовой легенды состояний соединений различных интерфейсов представлена в таблице 3.

Таблица 3 – Описание цветовой легенды состояний соединений

Цвет	Значение	Описание
Зеленый	ЛВС	Сетевые пакеты от/к сети с зеленой цветовой политикой
Красный	Интернет	Сетевые пакеты от/к сети с красной цветовой политикой
Голубой	Беспроводная сеть	Сетевые пакеты от/к сети с синей цветовой политикой
Оранжевый	DMZ	Сетевые пакеты от/к сети с оранжевой цветовой политикой
Синий	IPCop	Сетевые пакеты от/к Рубикон
Насыщено фиолетовый	IPSec	Сетевые пакеты от/к сети IPSec
Светло фиолетовый	OpenVPN	Сетевые пакеты от/к сети OpenVPN
Бесцветный	–	Все остальные сетевые пакеты

Подраздел «Настройки межсетевого экрана» состоит из следующих блоков:

1) «Настройки»;

2) «Политики сетевых интерфейсов».

2.3.1. Блок «Настройки»

Блок «Настройки» (см. рис. 9) предназначен для ввода настроек МЭ.

Блок «Настройки»

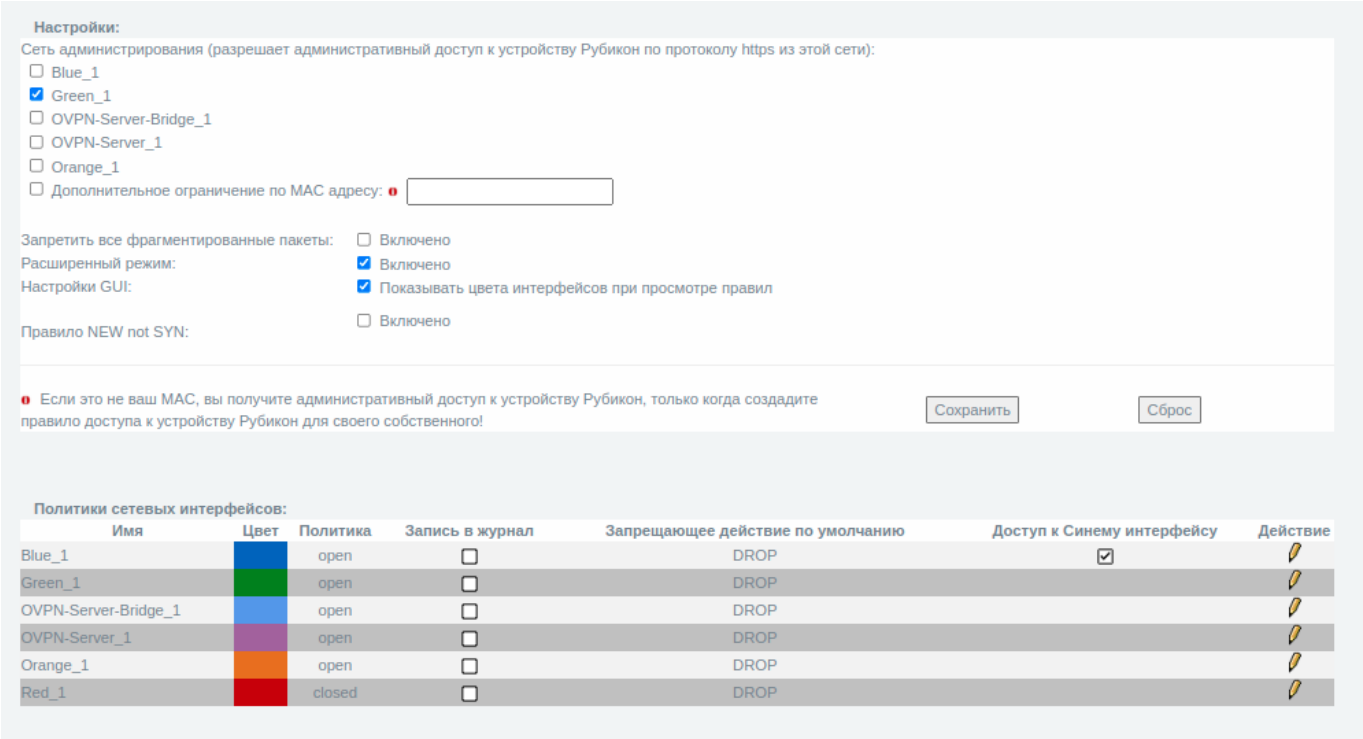


Рис. 9

Блок «Настройки межсетевого экрана» содержит элементы, указанные в таблице 4.

Таблица 4 – Описание элементов блока «Настройки»

Элемент	Описание
	Поле для ввода необходимой информации
	Поле с проставленным флажком (параметр включен)
	Пустое поле для проставления флажка (параметр выключен)
	Если это не ваш MAC, вы получите административный доступ к устройству «Рубикон», только когда создадите правило доступа к устройству «Рубикон» для своего собственного
Параметр «Green_1»	Сетевой интерфейс являющийся административным. По умолчанию все пакеты, маршрутизируемые между различными зелеными интерфейсами, не блокируются
Параметр «Дополнительное ограничение по MAC-адресу»	Включение MAC-адреса компьютера, с которого возможно администрирование МЭ. После установки данного параметра администрирование с других MAC-адресов будет невозможно
Поле «Дополнительное ограничение по MAC-адресу»	Предназначено для указания MAC-адреса компьютера, с которого возможно администрирование МЭ. После установки данного параметра администрирование с других MAC-адресов будет невозможно
Параметр «Запретить все фрагментированные пакеты»	При активации параметра сетевые пакеты с флагом фрагментации в IP-заголовке будут заблокированы
Параметр «Расширенный режим»	Предназначен для активации расширенного режима настроек МЭ
Параметр «Настройки GUI»	Предназначен для включения цветной индикации интерфейсов при просмотре правил МЭ
Параметр «Правило NEW not SYN»	Включение блокировки SYN-пакетов по протоколу TCP, для которых не было установлено соединение
Сохранить	Кнопка сохранения введенных данных
Сброс	Кнопка удаления введенных данных

2.3.2. Блок «Политики сетевых интерфейсов»

Блок «Политики сетевых интерфейсов» (см. рис. 10) содержит перечень политик сетевых интерфейсов.

Блок «Политики сетевых интерфейсов»

Политики сетевых интерфейсов:

Имя	Цвет	Политика	Запись в журнал	Запрещающее действие по умолчанию	Доступ к Синему интерфейсу	Действие
Blue_1		open	☐	DROP	☑	
Green_1		open	☐	DROP		
OVPN-Server-Bridge_1		open	☐	DROP		
OVPN-Server_1		open	☐	DROP		
Orange_1		open	☐	DROP		
Red_1		closed	☐	DROP		

Рис. 10

Блок «Политики сетевых интерфейсов» содержит перечень политик сетевых интерфейсов, распределенных по следующим параметрам:

1) «Имя»;

2) «Цвет»;

3) «Политика;

4) «Запись в журнал»;

5) «Запрещающее действие по умолчанию»;

6) «Доступ к Синему интерфейсу».

Блок «Политики сетевых интерфейсов» содержит элементы, указанные в таблице 5.

Таблица 5 – Описание элементов блока «Политики сетевых интерфейсов»

Элемент	Описание
Чекбокс « ☑ »	Чекбокс включения/отключения записи в журнал
Кнопка « »	Кнопка редактирования политики

Для изменения политики нажмите на кнопка « » в столбце «Действие» редактируемой политики. После этого вы перейдете в меню редактирования политики (см. рис. 11).

Меню редактирования политики

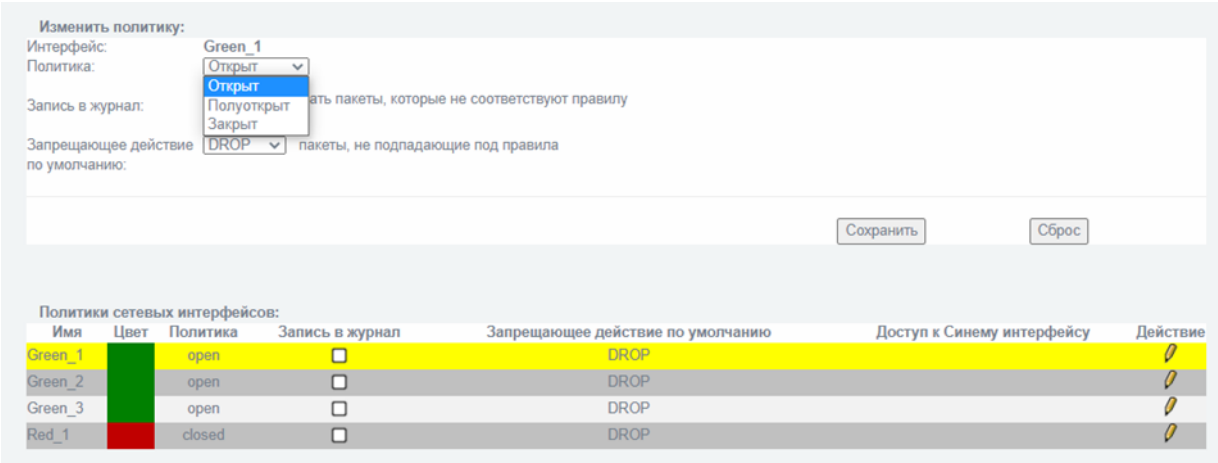


Рис. 11

Вы можете изменить тип политики, применяемой к редактируемому интерфейсу, в раскрывающемся меню из трех вариантов:

1) открыт (open);

2) полуоткрыт (half-open);

3) закрыт (closed).

Описание правил, создаваемых по умолчанию при применении каждой из политик представлено в таблице 6.

Таблица 6 – Описание сетевых политик

Тип правила	Политика		
	Закрыт	Полуоткрыт	Открыт
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

Описание политики фильтрации для разных типов интерфейсов представлено в таблице 7.

В таблице 7, приведено соответствие решений о фильтрации трафика между интерфейсами и «Рубикон» в зависимости от настроенной политики и типа правила, необходимого для разрешения (или запрещения) трафика.

Таблица 7 – Правила МЭ для разных цветовых политик

Направление сетевого пакета	Политика	Правило МЭ
Зеленая сеть → Доступ к Рубикон	open	Разрешен
Зеленая сеть → Доступ к Рубикон	half-open	Разрешен для определенных сервисов
Зеленая сеть → Красная сеть	open	Разрешен
Зеленая сеть → Красная сеть	half-open	Запрещено, для доступа необходимо создать правило МЭ
Зеленая сеть → Оранжевая сеть	open	Разрешен
Зеленая сеть → Оранжевая сеть	half-open	Запрещено, для доступа необходимо создать правило МЭ
Зеленая сеть → Синяя сеть	open	Разрешен
Зеленая сеть → Синяя сеть	half-open	Запрещено, для доступа необходимо создать правило МЭ
Зеленая сеть → Зеленая сеть	open	Разрешен
Зеленая сеть → Доступ к Рубикон	close	Запрещено, для доступа необходимо создать правило МЭ доступ к Рубикон
Зеленая сеть → Красная сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Зеленая сеть → Оранжевая сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Зеленая сеть → Синяя сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Зеленая сеть → Зеленая сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Красная сеть → Доступ к Рубикон	close	Запрещено, для доступа необходимо создать правило МЭ доступ к Рубикон
Красная сеть → Зеленая сеть	close	Запрещено, для доступа необходимо создать правило МЭ перенаправление портов
Красная сеть → Оранжевая сеть	close	Запрещено, для доступа необходимо создать правило МЭ перенаправление портов
Красная сеть → Синяя сеть	close	Запрещено, для доступа необходимо создать правило МЭ перенаправление портов

Направление сетевого пакета	Политика	Правило МЭ
Синяя сеть → Доступ к Рубикон	open	Разрешен
Синяя сеть → Доступ к Рубикон	half-open	Разрешен для определенных сервисов
Синяя сеть → Зеленая сеть	open	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Синяя сеть → Зеленая сеть	half-open	Запрещено, для доступа необходимо создать правило МЭ
Синяя сеть → Красная сеть	open	Разрешен
Синяя сеть → Красная сеть	half-open	Запрещено, для доступа необходимо создать правило МЭ
Синяя сеть → Оранжевая сеть	open	Разрешен
Синяя сеть → Оранжевая сеть	half-open	Запрещено, для доступа необходимо создать правило МЭ
Синяя сеть → Доступ к Рубикон	close	Запрещено, для доступа необходимо создать правило МЭ доступ к Рубикон
Синяя сеть → Зеленая сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Синяя сеть → Красная сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Синяя сеть → Оранжевая сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Оранжевая сеть → Доступ к Рубикон	open	Запрещено, для доступа необходимо создать правило МЭ доступ к Рубикон
Оранжевая сеть → Зеленая сеть	open	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Оранжевая сеть → Красная сеть	open	Разрешен
Оранжевая сеть → Синяя сеть	open	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Оранжевая сеть → Доступ к Рубикон	close	Запрещено, для доступа необходимо создать правило МЭ доступ к Рубикон
Оранжевая сеть → Зеленая сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Оранжевая сеть → Красная сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею
Оранжевая сеть → Синяя сеть	close	Запрещено, для доступа необходимо создать правило МЭ из внутренней сети во внешнею

Для включения записи в журнале о пакетах, не соответствующих правилу, поставьте «галочку» в чекбокс и нажмите кнопку « Сохранить » (см. рис. 12). После этого для выбранного интерфейса отобразится чекбокс « ☑ ».

Включение записи в журнале о пакетах, не соответствующих правилу

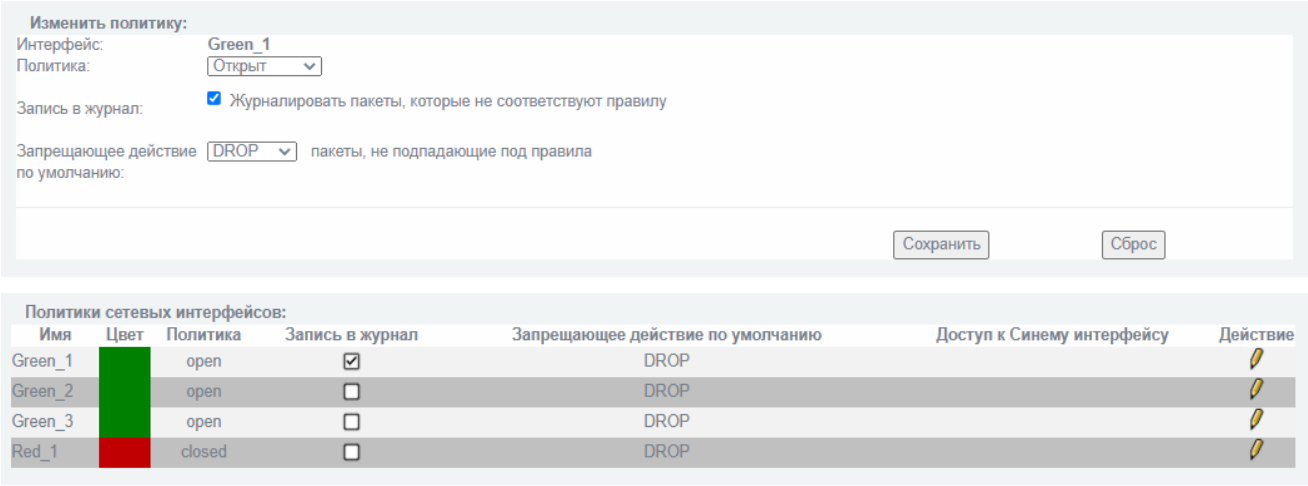


Рис. 12

Запрещающее действие по умолчанию можно выбрать из вариантов: DROP (Запретить) или REJECT (Отклонить) (см. рис. 13).

Запрещающее действие по умолчанию

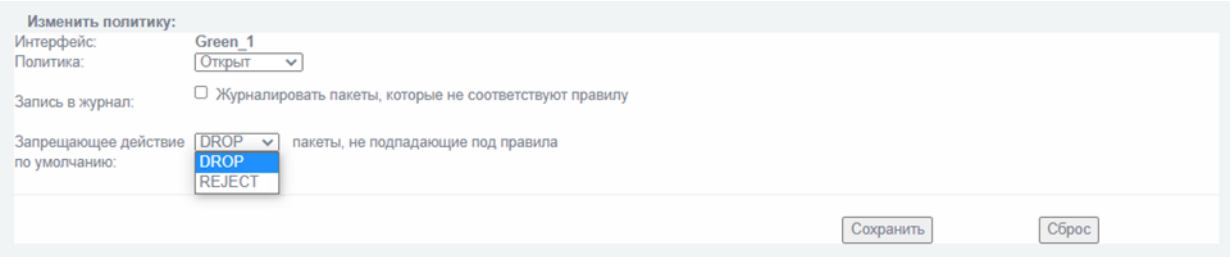


Рис. 13

DROP отклоняет пакет без уведомления. REJECT отклоняет пакет и отправляет ICMP сообщение «порт недоступен» отправителю.

2.4. Ограничение трафика

Для установки ограничения скорости для входящих и исходящих соединений необходимо выполнить следующие действия:

1) перейти в подраздел «Ограничение трафика» раздела «Службы» (см. рис. 14);

Подраздел «Ограничение трафика» раздела «Службы»

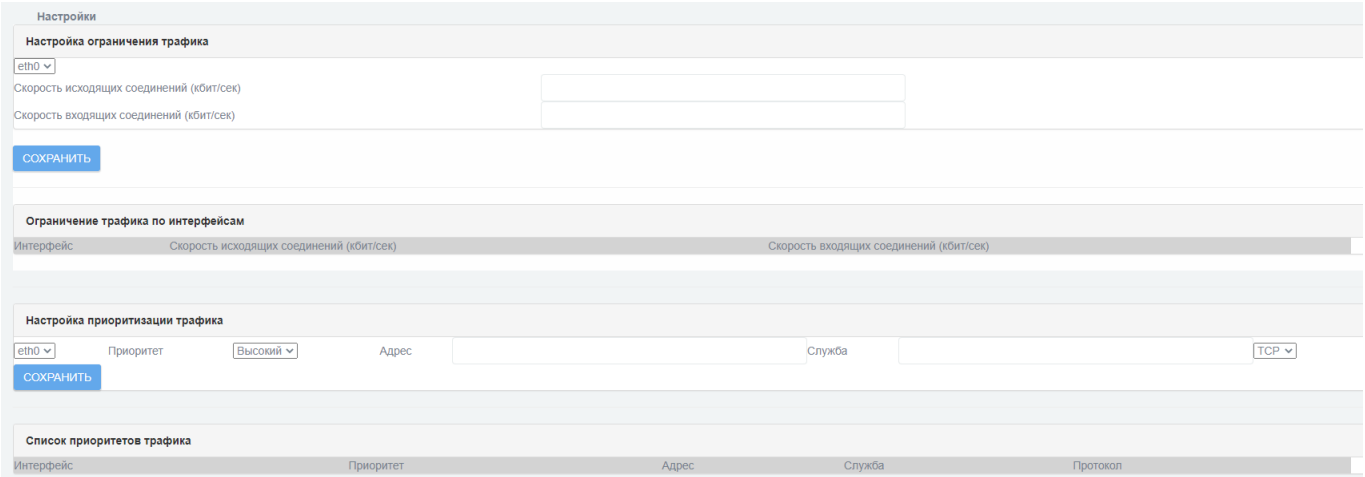


Рис. 14

2) в блоке «Настройки» выбрать имя интерфейса в выпадающем списке;

3) заполнить текстовое поле «Скорость исходящих соединений (кбит/сек)»;

4) заполнить текстовое поле «Скорость входящих соединений (кбит/сек)»;

5) нажать кнопку «Сохранить».

2.5. Приоритизация трафика

Для настройки приоритизации трафика необходимо настроить приоритеты трафика выполнив следующие действия:

1) перейти в подраздел «Ограничение трафика» раздела «Службы» и обратить внимание на блок «Настройка приоритизации трафика» (см. рис. 60);

Блок «Настройка приоритизации трафика»

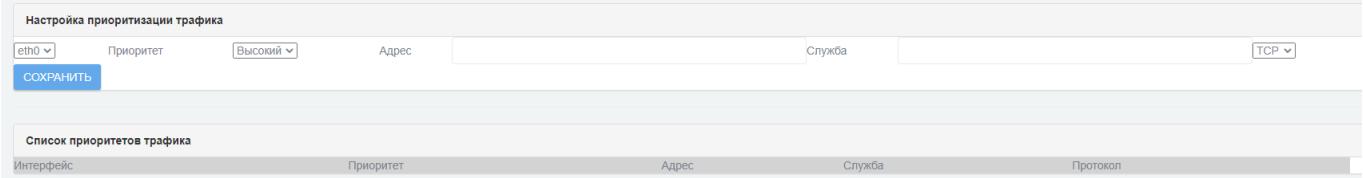


Рис. 15

2) выбрать имя необходимого интерфейса в выпадающем списке;

3) выбрать «Приоритет» в выпадающем списке – высокий, средний или низкий;

4) заполнить текстовое поле «Адрес»;

5) заполнить текстовое поле «Служба»;

6) выбрать в выпадающем списке протокол «TCP» или «UDP»;

7) нажать кнопку «Сохранить».

2.6. Создание межсетевого моста

Для создания нового межсетевого моста необходимо выполнить следующие действия:

1) перейти в подраздел «Мосты» раздела «Сеть» (см. рис. 16);

Подраздел «Мосты» раздела «Сеть»

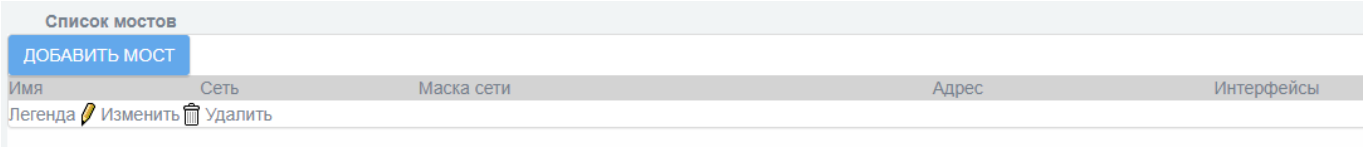


Рис. 16

2) создайте новый мост, нажав кнопку «Добавить мост» и введите произвольное имя моста;

3) задайте необходимые значения в полях «Сеть», «Маска сети» и «Адрес»;

4) укажите связываемые мостом интерфейсы, активировав соответствующие чекбоксы справа от имен доступных для выбора интерфейсов;

5) для завершения настройки нажмите кнопку «Добавить».

Созданный мост отобразится в информационной таблице «Список мостов» (см. рис. 17).

Отображение добавленного моста в информационной таблице «Список мостов»

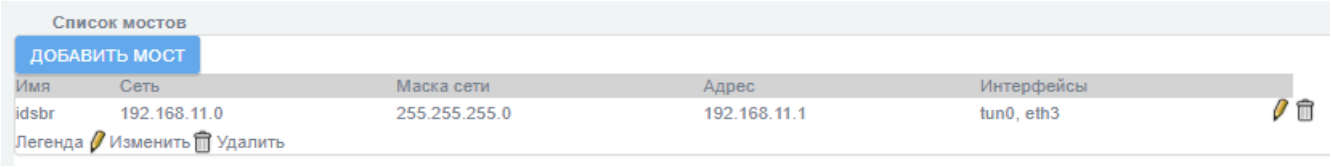


Рис. 17

2.7. Настройка дополнительного адреса сети (настройка псевдонима)

Для настройки дополнительного адреса сети (настройки псевдонима) необходимо выполнить следующие действия:

1) перейти в подраздел «Адреса» раздела «Межсетевой экран»;

2) в поле «Имя» ввести информацию, которая будет представлять данный адрес в правилах межсетевого экрана;

3) выбрать формат адреса IP из выпадающего списка (выбор MAC необходим для указания одиночного MAC-адреса сетевого устройства);

4) ввести необходимый адрес в поле «Адрес» (например, 11.0.0.0);

5) ввести маску сети в поле «Маска сети» (например, 255.255.255.0);

6) применить введенные параметры с помощью кнопки «Добавить».

Введенная сеть будет отображена в информационной таблице «Дополнительные адреса» (см. рис. 18).

Отображение введенной сети в информационной таблице «Дополнительные адреса»

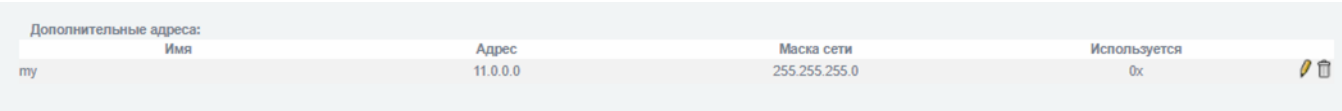


Рис. 18

2.8. Добавление сети в группу адресов сетевых интерфейсов

Для настройки объединения в группу сети и адресов сетевых интерфейсов необходимо выполнить следующие действия:

1) перейти в подраздел «Группы адресов» раздела «Межсетевой экран»;

2) заполнить поле «Имя группы адресов» для присвоения символьного обозначения группе (данное имя будет использоваться в правилах фильтрации);

3) активировать чекбокс «Сети по умолчанию» и в выпадающем списке «Сети по умолчанию» выбрать необходимую для объединения сеть;

4) для применения настройки нажать кнопку «Добавить»;

5) далее необходимо активировать чекбокс «Имя группы адресов» и выбрать уже внесенное ранее имя группы адресов в выпадающем списке «Имя группы адресов»;

6) активировать чекбокс «Дополнительные адреса»;

7) в выпадающем списке «Дополнительные адреса» выбрать нужную сеть;

8) для завершения настройки нажмите кнопку «Добавить».

Настроенная группа будет отображена в информационной таблице «Группы адресов» (см. рис. 19).

Отображение настроенной группы в информационной таблице «Группы адресов»

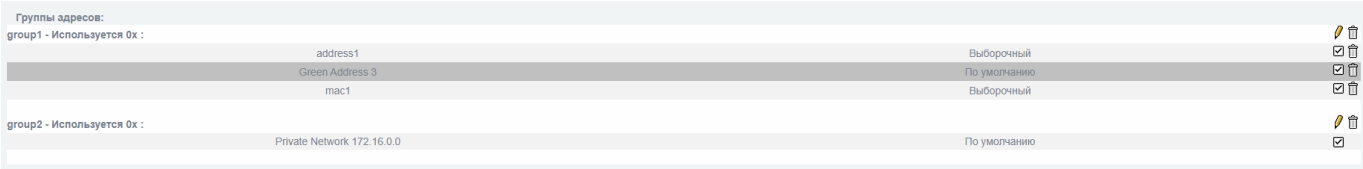


Рис. 19

2.9. Настройка фильтрации пакетов

Для настройки фильтрации пакетов необходимо выполнить следующие действия:

1) предварительно настройте необходимые сетевые интерфейсы;

2) перейти в подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран»;

3) активировать чекбокс «Включено» для функции «Расширенный режим» и нажать кнопку «Сохранить»;

4) перейти в подраздел «Службы» раздела «Межсетевой экран», (см. рис. 20) где при необходимости можно создать новую службу или выбрать службу по умолчанию;

Подраздел «Службы» раздела «Межсетевой экран»

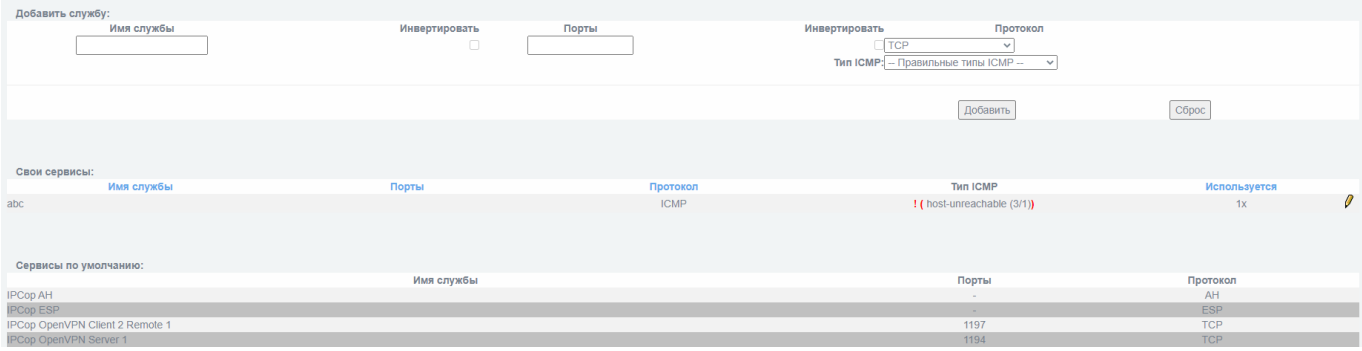


Рис. 20

5) для добавления новой службы необходимо в текстовом поле «Имя службы» задать имя новой службы;

6) в текстовом поле «Порты» указать номер порта и инвертировать при необходимости (функция активируется чекбоксом «Инвертировать»);

7) в выпадающем списке «Протокол» выбрать протокол, который будет использоваться (инвертировать при необходимости);

8) в выпадающем списке «Тип ICMP» выбрать тип ICMP;

9) нажать кнопку «Добавить»;

10) для дальнейшей настройки правил фильтрации перейти в подраздел «Правила межсетевого экрана» раздела «Межсетевой экран» (см. рис. 21); в данном разделе отображаются актуальные правила. Актуальные правила возможно изменять, копировать, удалять, перемещать, активировать и деактивировать. Легенда указана внизу подраздела;

Подраздел «Правила межсетевого экрана» раздела «Межсетевой экран»

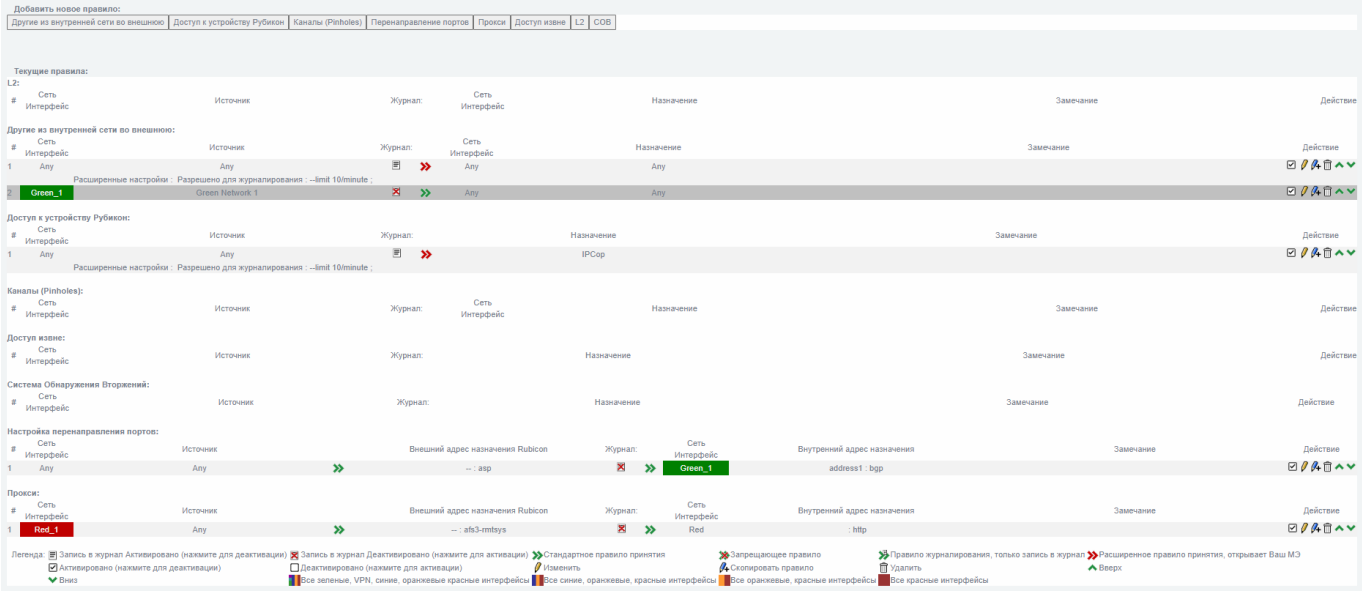


Рис. 21

11) для настройки нового правила фильтрации необходимо нажать кнопку «Другие из внутренней сети во внешнюю» для открытия одноименной страницы;

12) создать правило, заполнив необходимые поля;

13) перед тем, как сохранить и применить новое правило, нажать кнопку «Далее» для предварительного просмотра (см. рис. 22). На данной странице есть возможность сбросить настройки и перейти на предыдущую страницу, нажав кнопку «Сброс», или уйти со страницы без сохранения изменений, нажав кнопку «Отмена»;

14) откорректировать введенные параметры для правила при необходимости;

15) нажать кнопку «Сохранить» для сохранения параметров и включения нового правила.

Предварительный просмотр правила

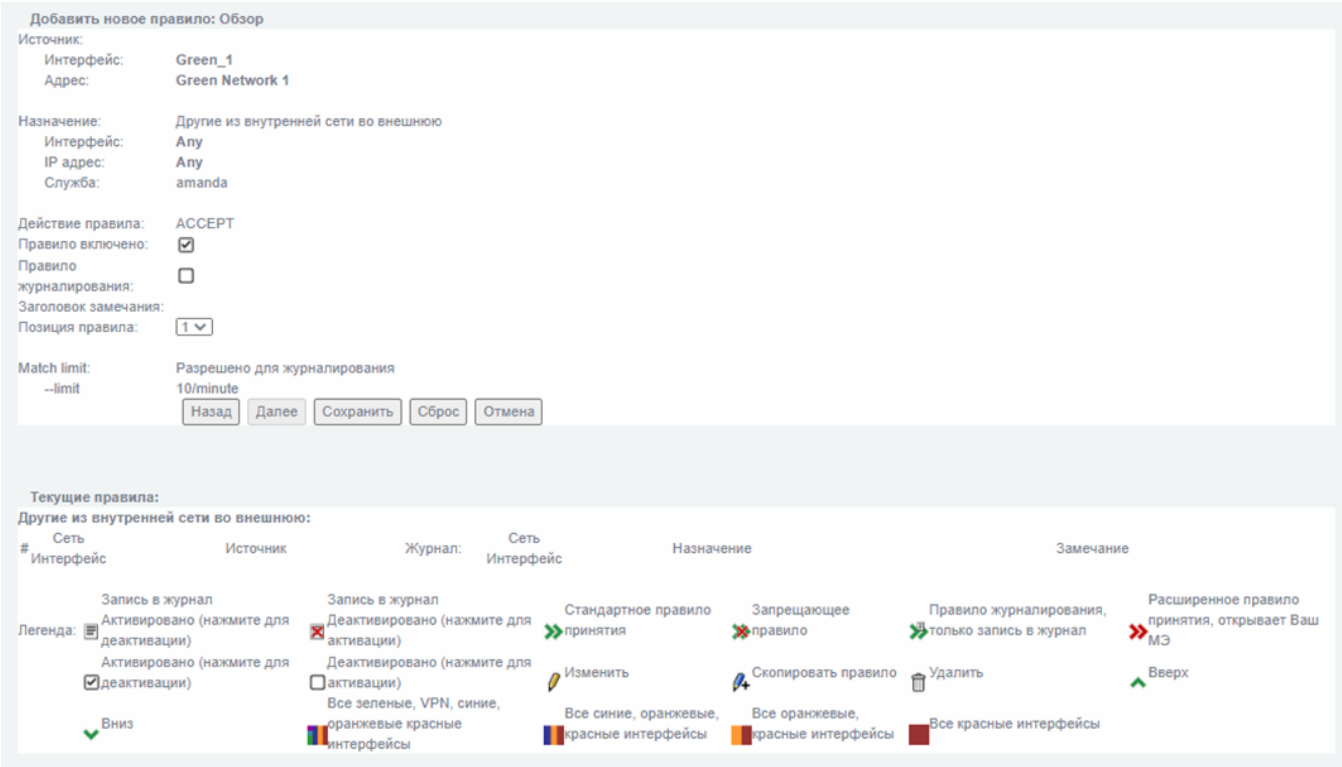


Рис. 22

2.9.1. Настройка фильтрации по сетевому адресу отправителя

Для настройки фильтрации по сетевому адресу отправителя необходимо выполнить следующие действия:

1) перейти на странице «Другие из внутренней сети во внешнюю» на вкладку «Источник» (подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран»);

2) активировать чекбокс «Формат адреса» и в одноименном выпадающем списке выбрать значение «IP»;

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

2.9.2. Настройка фильтрации по сетевому адресу получателя

Для настройки фильтрации по сетевому адресу получателя необходимо выполнить следующие действия:

1) перейти на странице «Другие из внутренней сети во внешнюю» на вкладку «Назначение» (подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран»);

2) активировать чекбокс «IP или сеть назначения» и в одноименном текстовом поле ввести IP-адрес получателя;

3) для применения правила для **всех** служб выключите чекбокс «Использовать службу»;

4) для применения правила для конкретной службы выберите ее из выпадающего списка «Сервисы по умолчанию»;

5) для проверки правила нажмите кнопку «Далее» или нажмите кнопку «Сохранить» для сохранения созданного правила без его проверки.

2.9.3. Настройка фильтрации по сетевому протоколу, который используется для взаимодействия

Для настройки фильтрации по сетевому протоколу, который используется для взаимодействия необходимо выполнить следующие действия:

1) перейти на странице «Другие из внутренней сети во внешнюю» на вкладку «Назначение» (подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран»);

2) активируйте чекбокс «Использовать службу»;

3) активируйте чекбокс «Свои сервисы» или «Сервисы по умолчанию» в зависимости от того, какую службу вы собираетесь выбрать;

4) в выпадающем списке выбрать службу, использующую сетевой протокол, по которому планируется осуществление фильтрации (см. рис. 23).

Настройка вкладки «Назначение»

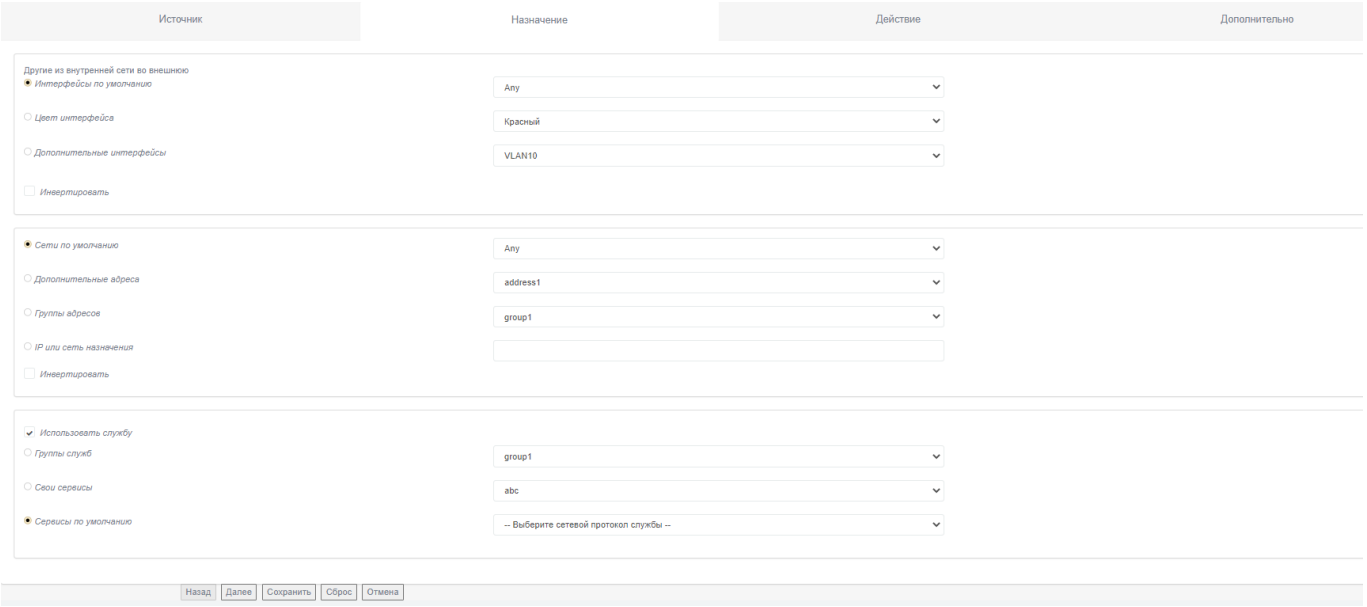


Рис. 23

2.9.4. Настройка фильтрации по направлению пакета

Для настройки фильтрации по направлению пакета необходимо выполнить следующие действия:

1) перейти на странице «Другие из внутренней сети во внешнюю» на вкладку «Источник» (подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран»);

2) заполнить поля правила на вкладке «Источник» страницы «Другие из внутренней сети во внешнюю» для входящего пакета;

3) перейти на вкладку «Назначение» страницы «Другие из внутренней сети во внешнюю» и заполнить поля правила для исходящего пакета;

4) сохранить введенные настройки.

2.9.5. Настройка фильтрации по транспортному протоколу, который используется для взаимодействия

Для настройки фильтрации по транспортному протоколу, который используется для взаимодействия необходимо выполнить следующие действия:

1) перейти на странице «Другие из внутренней сети во внешнюю» на вкладку «Назначение» (подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран»);

2) активируйте чекбокс «Использовать службу»;

3) активируйте чекбокс «Свои сервисы» или «Сервисы по умолчанию» в зависимости от того, какую службу вы собираетесь выбрать;

4) в выпадающем списке выбрать службу, использующую сетевой протокол, по которому планируется осуществление фильтрации.

2.9.6. Настройка фильтрации по портам источника и получателя в рамках сеанса (сессии)

Данная настройка 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.

2.9.6.1. Для настройки фильтрации по портам источника необходимо выполнить следующие действия:

1) перейти на странице «Другие из внутренней сети во внешнюю» на вкладку «Источник» (подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран»);

2) активировать чекбокс «Использовать порт источника»;

3) в текстовом поле «Порт источника» ввести порт источника и инвертировать его при необходимости (активировав чекбокс «Инвертировать»).

2.9.6.2. Для настройки фильтрации по портам назначения необходимо выполнить следующие действия:

1) перейти на странице «Другие из внутренней сети во внешнюю» на вкладку «Назначение» (подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран»);

2) активировать чекбокс «Использовать службу»;

3) активируйте чекбокс «Свои сервисы» или «Сервисы по умолчанию» в зависимости от того, какую службу вы собираетесь выбрать;

4) выбрать необходимую службу.

2.9.7. Настройка фильтрации по интерфейсу, через который проходит пакет

2.9.7.1. Для настройки фильтрации по интерфейсу, через который проходит пакет на уровне сетевого адреса, необходимо выполнить следующие действия:

1) перейти на страницу «Доступ к устройству Рубикон», нажав одноименную кнопку в подразделе «Правила межсетевого экрана» раздела «Межсетевой экран»;

2) на вкладке «Источник» активировать чекбокс «Интерфейсы по умолчанию»;

3) в выпадающем списке «Интерфейсы по умолчанию» выбрать значение «Any»;

4) активировать чекбокс «Адрес», в выпадающем списке «Адрес» выбрать необходимое значение (например, выберите сеть «Green Network 1»);

5) нажать кнопку «Сохранить» для сохранения введенных параметров.

2.9.7.2. Для настройки фильтрации по интерфейсу, через который проходит пакет на физическом уровне, необходимо выполнить следующие действия:

1) перейти на страницу «Доступ к устройству Рубикон», нажав одноименную кнопку в подразделе «Правила межсетевого экрана» раздела «Межсетевой экран»;

2) на вкладке «Источник» активировать чекбокс «Интерфейсы по умолчанию»;

3) в выпадающем списке «Интерфейсы по умолчанию» выбрать необходимый интерфейс;

4) нажать кнопку «Сохранить» для сохранения введенных параметров.

2.10. Настройка прокси-сервера

Веб-прокси-сервер – это программа, которая генерирует запросы к веб-страницам от имени других компьютеров в сети. Прокси-сервер кэширует страницы, которые получает из интернета, поэтому если 3 пользователя одновременно запрашивают одну и ту же веб-страницу, требуется только одна передача из сети Интернет. Если имеется ряд часто используемых веб-сайтов, это поможет сэкономить время на интернет-доступе.

2.10.1. FTP посредничество

Для включения функции прокси-сервера необходимо выполнить следующие действия:

1) перейти в подраздел «FTP посредник» раздела «Службы» (см. рис. 24);

Подраздел «FTP посредник» раздела «Службы»

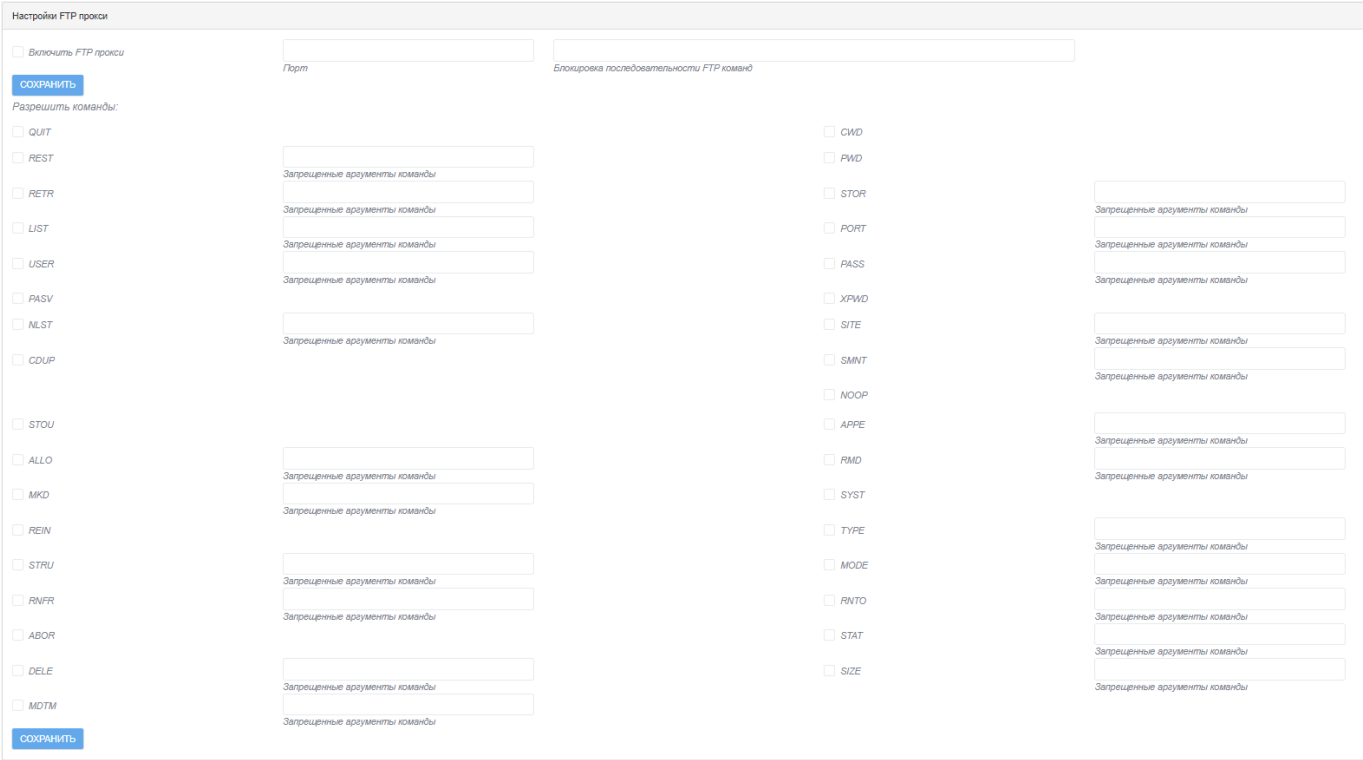


Рис. 24

2) активировать чекбокс «Включить FTP прокси» для включения функции прокси-сервера в межсетевом экране;

3) ввести номер порта (на котором прокси-сервер будет прослушивать запросы) в текстовое поле «Порт»;

4) ввести последовательность FTP команд, которая будет блокироваться, в текстовое поле «Блокировка последовательности FTP команд» (не обязательно);

5) нажать кнопку «Сохранить» для сохранения введенных параметров.

2.10.2. Настройка веб-прокси

Подраздел «Прокси» раздела «Службы» состоит из следующих блоков и секций:

1) блок «Настройки», который включает в себя:

— секцию «Общие параметры»;

— секцию «Прокси верхнего уровня»;

— секцию «Настройки журналирования».

2) блок «Расширенные настройки», который включает в себя:

— секцию «Управление кэшем»;

— секцию «Порты назначения»;

— секцию «Контроль доступа по адресу»;

— секцию «Классные расширения (CRE)»;

— секцию «Список URL фильтрации»;

— секцию «Ограничение по времени»;

— секцию «Лимиты передачи»;

— секцию «Регулирование закачки»;

— секцию «Фильтр MIME типов»;

— секцию «Веб-браузер»;

— секцию «Конфиденциальность»;

— секцию «Redirectors»;

— секцию «Метод аутентификации»;

— секцию «Включить взаимодействие с сервером ICAP»;

— секцию «Включить фильтрацию скриптов на дополнительном порту».

Для настройки веб-прокси необходимо выполнить следующие действия:

1) перейти в подраздел «Прокси» раздела «Службы». Первая строка в данном разделе показывает запущен или остановлен прокси-сервер;

2) последовательно настроить необходимые блоки и секции настроек подраздела.

2.10.2.1. Настройка секции «Общие параметры»

Для настройки секции «Общие параметры» (см. рис. 25) необходимо выполнить следующие действия:

1) чекбокс «Включено на первом ЗЕЛЕНОМ интерфейсе» необходимо активировать чтобы включить прокси-сервер для прослушивания запросов на выбранном интерфейсе. Если прокси-служба отключена, все клиентские запросы будут направлены непосредственно на адрес получателя;

Секция «Общие параметры»

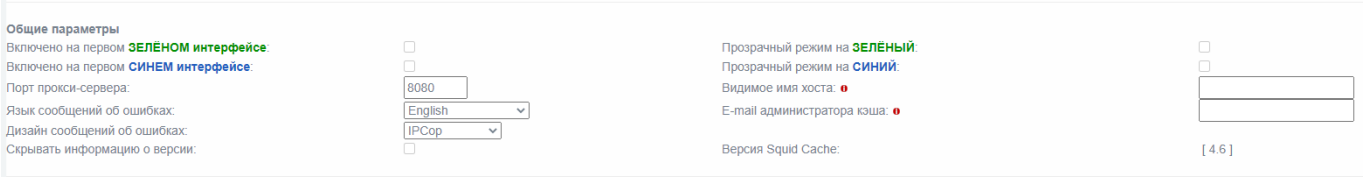


Рис. 25

2) чекбокс «Прозрачный режим на ЗЕЛЕНЫЙ» необходимо активировать для включения «прозрачного» режима, тогда все запросы на 80 порту будут направлены к прокси-серверу без необходимости специальной настройки клиентов;

3) поле «Порт прокси-сервера» необходимо заполнить для определения на каком порту прокси-сервер будет прослушивать запросы клиента. По умолчанию установлено – 8080. В прозрачном режиме все клиентские запросы на 80 порту будут автоматически перенаправлены на этот порт;

4) поле «Видимое имя хоста» – необязательное поле. Заполнять нужно если необходимо, чтобы клиентам отображалось другое имя в прокси-сообщениях об ошибках сервера, или для прокси-серверов верхнего уровня. Если оставить это поле пустым, будет использоваться имя вашего изделия;

5) поле «E-mail администратора кэша» – необязательное поле. Здесь задается адрес электронной почты, который будет отображаться в прокси-сообщениях об ошибках сервера. Если оставить его пустым, будет использоваться «веб-мастер»;

6) сделать выбор в выпадающем списке «Язык сообщений об ошибках». Это необходимо для выбора языка, на котором прокси-сервер будет отображать сообщения об ошибках для клиентов;

7) сделать выбор в выпадающем списке «Дизайн сообщений об ошибках». Это необходимо для выбора дизайна, в котором сообщения об ошибках прокси-сервера отображаются на клиентах. Вы можете выбрать между «IPCop» и «Стандартный». Дизайн «IPCop» включает улучшенный графический баннер, в то время как «Стандартный» дизайн обычно поставляется с «Squid»;

8) активировать чекбокс «Скрывать информацию о версии» для предотвращения отображения версии Squid Cache в сообщениях об ошибках Squid клиентам;

9) перейти к настройке следующей необходимой секции в блоке.

2.10.2.2. Настройка секции «Прокси верхнего уровня»

Настройка данных параметров может 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, следует заполнить текстовые поля «Имя пользователя для вышестоящего прокси» и «Пароль для вышестоящего прокси».

Для настройки секции «Прокси верхнего уровня» (см. рис. 26) необходимо выполнить следующие действия:

1) активировать чекбокс «Пересылка адреса прокси» если необходимо включение HTTP VIA в поле заголовка. Если чекбокс активирован, эта информация будет добавлена к заголовку HTTP. Если последний прокси в цепочке не удалит это поле, оно будет направлено на узел назначения. Данное поле будет скрыто по умолчанию;

Секция «Прокси верхнего уровня»

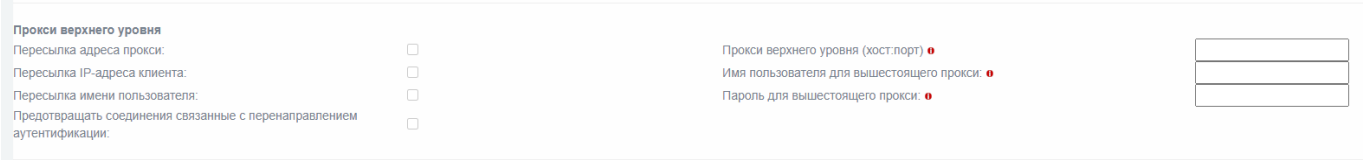


Рис. 26

2) активировать чекбокс «Пересылка IP-адреса клиента» (при необходимости). Включает HTTP X-FORWARDED-FOR в поле заголовка при активации. Если эта функция включена, внутренний IP-адрес клиента будет добавлен к HTTP-заголовку; это может пригодиться для источника ACL или входа на удаленный прокси-сервер. 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;

3) активировать чекбокс «Пересылка имени пользователя» (при необходимости). Если какой-либо тип аутентификации активирован, эта функция позволит пересылать логин; это может пригодиться для пользователей на основе ACL или входа на удаленный прокси-сервер. 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;

4) активировать чекбокс «Предотвращать соединения связанные с перенаправлением аутентификации» (при необходимости). Отключает пересылку Microsoft-соединений, ориентированных на проверку подлинности (NTLM и Kerberos);

5) перейти к настройке следующей необходимой секции в блоке.

2.10.2.3. Настройка секции «Настройки журналирования»

Для настройки секции «Настройки журналирования» (см. рис. 27) необходимо выполнить следующие действия:

1) активировать чекбокс «Журнал включен» (при необходимости). Если необходимо включить прокси, то следует также включить журнал веб-посещений, включив опцию «журнал включен». Это позволит прокси-серверу вести журнал, который может потребоваться для устранения неполадок; посещения через прокси можно отследить, проверив прокси-логи веб-страницы. В журнале также включена поддержка прокси-графиков работы;

Секция «Настройки журналирования»

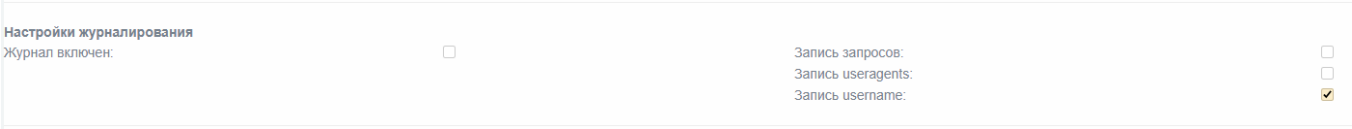


Рис. 27

2) активировать чекбокс «Запись запросов» (при необходимости). Часть URL, содержащих динамические запросы будут удалены по умолчанию перед входом. Если включить функцию «запись запросов», то в журнале будет записан полный URL-адрес;

3) активировать чекбокс «Запись useragents» (при необходимости). Включение функции «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;

4) активировать чекбокс «Запись username» (при необходимости). Включение данной функции позволит записывать имя пользователя (параметр «username») в журнал;

5) нажать кнопку «Очистить кэш», если необходима очистки файла, создаваемого прокси-сервером;

6) нажать кнопку «Сохранить» для сохранения введенных ранее настроек;

7) для более детальной настройки перейти к следующему блоку «Расширенные настройки».

2.10.2.4. Настройка секции «Управление кэшем»

Данная секция предназначена для определения сколько места на диске должно быть использовано для кэширования веб-страниц. Вы можете также установить минимальный и максимальный размер объекта в кэше.

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

Следует учитывать, что данные кэша могут занимать много места на жестком диске. Если настроить слишком **большой кэш**, то минимальный размер жесткого диска, указанный в документации, будет **недостаточен**. Чем больший размер кэша выбирается, тем больше оперативной памяти потребуется прокси-серверу для управления кэшем.

2.10.2.4.1. Настройка прокси-сервера без кэширования

Для настройки прокси-сервера без кэширования необходимо выполнить следующие действия:

1) установить в полях «Размер кэша в памяти (МБ)» и «Размер кэша на HDD (МБ)» значения равными 0 МБ, чтобы полностью отключить кэширование;

2) сохранить настройки, нажав кнопку «Сохранить» внизу блока «Расширенные настройки» подраздела «Прокси» раздела «Службы».

2.10.2.4.2. Настройка прокси-сервера с кэшированием

Для настройки секции «Управление кэшем» (см. рис. 28) необходимо выполнить следующие действия:

1) заполнить поле «Размер кэша в памяти (МБ)» для установки размера кэша в памяти. Это необходимо для указания объема 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 используемой физической памяти. Он только ставит ограничения на то, сколько дополнительной оперативной памяти будет использоваться прокси в качестве кэша объектов;

Секция «Управление кэшем»

Рис. 28

2) заполнить поле «Размер кэша на HDD (МБ)». Это необходимо для указания объема дискового пространства в мегабайтах, используемого для кэширования объектов. Значение по умолчанию – 50 МБ. Измените его в соответствии с вашей конфигурацией. **Не следует указывать весь размер используемого диска.** Рекомендуется для Squid использовать 80 % от вашего диска;

3) заполнить поле «Минимальный размер объекта (кБ)». Объекты меньше указанного размера не будут сохранены на диске. Значение задается в килобайтах и по умолчанию равно 0 кБ, а это значит, что минимальное значение не установлено;

4) заполнить поле «Максимальный размер объекта (кБ)». Объекты больше указанного размера не будут сохранены на диске. Значение задается в килобайтах и по умолчанию составляет 4 кБ;

5) установить необходимое для работы значение в выпадающем списке «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. Рекомендуемое значение для 1-го уровня директорий равно 16. **Увеличивать это значение следует только тогда, когда это необходимо.**

6) установить необходимое значение в выпадающем списке «Стратегия использования памяти». Выбранная стратегия определяет, какие объекты удаляются из памяти, когда это требуется. Стратегия по умолчанию для замены в памяти является **LRU**. Для выбора доступны следующие варианты стратегий:

— «LRU» (Last Recently Used). Стратегия сохранения ссылок последних запрошенных объектов. Иначе говоря, заменяются объекты, которые не использовались долгое время;

— «heap GDSF» (The heap Greedy-Dual Size Frequency). Стратегия оптимизирует хранение объектов по частоте попадания, сохраняя небольшие часто встречающиеся объекты в кэше, потому что они имеют больший коэффициент попаданий в кэш. Она обеспечивает более низкую оптимизацию размера выдачи страниц из кэша, чем LFUDA, так как из кэша в преимущественно удаляются объекты большего размера (возможно, часто попадающиеся);

— «heap LFUDA» (Least Frequently Used with Dinamic Aging) – наименее часто использующиеся объекты с динамическим устареванием. Эта стратегия сохраняет часто встречающиеся объекты в кэше независимо от размера страниц. Максимизируется размер выдачи страниц из кэша, но при этом количество совпадений страниц в кэше может не быть оптимальным, так как, большие, часто встречающиеся объекты препятствуют кэшированию нескольких более мелких реже встречающихся объектов. При использовании политики замены LFUDA, значение параметра «Максимальный размер объекта (кБ)» должно быть больше размера по умолчанию 4096 кБ, чтобы максимизировать потенциальную оптимизацию размера выдачи страниц из кэша, реализованную LFUDA;

— «heap LRU» (Last Recently Used policy implemented using a heap). Стратегия сохранения ссылок последних запрошенных объектов с использованием динамически распределенной памяти. Работает как LRU, но отличается использованием динамически распределенной памяти.

7) установить необходимое значение в выпадающем списке «Стратегия замены в кэше». Замена стратегии кэша влияет на то, какие объекты останутся в кэше, а какие объекты будут исключены (заменены), чтобы создать пространство для новых объектов. Стратегией по умолчанию для замены кэша является LRU;

8) активировать чекбокс «Включить автономный режим». Включение данной функции позволит отключить проверку кэшированных объектов. Это дает доступ к устаревшим версиям кэшированных страниц, которые появились в кэше на момент первоначального соединения с сервером;

9) ввести (при необходимости) перечень доменов в поле «Не кэшировать эти домены». Необходимо для создания перечня сайтов, запрос которых не может быть удовлетворен из кэша и ответ которых не кэшируется. Данное поле не обязательно к заполнению;

10) перейти к настройке секции «Порты назначения».

2.10.2.5. Настройка секции «Порты назначения»

В полях данной секции содержатся списки разрешенных стандартных портов для HTTP и зашифрованных SSL портов для HTTPS-запросов.

Порты могут быть указаны как единый номер порта или как диапазон портов (см. рис. 29).

Секция «Порты назначения»

Рис. 29

Для настройки секции «Порты назначения» необходимо выполнить следующие действия:

1) заполнить поле «Разрешенные стандартные порты (один в строке)». Необходимо вписывать каждый разрешенный стандартный порт в отдельную строку;

2) заполнить поле «Разрешенные SSL порты (один в строке)». Необходимо вписывать каждый разрешенный SSL-порт в отдельную строку;

3) перейти к настройке секции «Контроль доступа по адресу».

2.10.2.6. Настройка секции «Контроль доступа по адресу»

Настройка данной секции позволяет контролировать доступ к прокси-серверу на основе сетевого адреса клиента (см. рис. 30).

Секция «Контроль доступа по адресу»

Рис. 30

Для настройки секции «Контроль доступа по адресу» необходимо выполнить следующие действия:

1) заполнить поле «Разрешенные подсети (одна в строке)». Это необходимо для разрешения доступа к прокси-серверу всех перечисленных в поле подсетей. По умолчанию зеленые и синие (если имеются) подсети перечислены здесь. Возможно 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;

2) заполнить поле «Неограниченные IP-адреса (один в строке)». Не обязательное поле. Это необходимо чтобы для всех клиентских IP-адресов в данном списке действовали следующие ограничения:

— ограничение времени;

— предельные размеры для запросов на загрузку;

— регулирование загрузки;

— проверка браузера;

— фильтр MIME типов;

— аутентификация;

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

3) заполнить поле «Блокируемые IP-адреса (один в строке)». Не обязательное поле. Все запросы от перечисленных в данном поле IP-адресов будут заблокированы;

4) активировать чекбокс «Запретить доступ через встроенный прокси». Необходимо для включения функции полного запрета доступа к прокси-серверу;

5) активировать чекбокс «Запретить доступ через встроенный прокси к ЗЕЛЁНОЙ из других подсетей». Это 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 запрашивает доступ к веб-серверу из зеленой подсети, встроенный прокси-сервер найдет короткий путь между синим и зеленым интерфейсом, независимо от правил МЭ. Для защиты сервера, находящегося в зеленой подсети, рекомендуется включить эту функцию и использовать фильтр адресов или демилитаризованную зону при необходимости;

6) заполнить поле «Неограниченные MAC-адреса (один в строке)». Не обязательное поле. Это необходимо чтобы для всех MAC-адресов в данном списке действовали следующие ограничения:

— ограничение времени;

— предельные размеры для запросов на загрузку;

— регулирование загрузки;

— проверка браузера;

— фильтр MIME типов;

— аутентификация;

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

7) заполнить поле «Блокируемые MAC-адреса (один в строке)». Не обязательное поле. Предназначено для ввода MAC-адресов, все запросы от которых будут заблокированы;

8) перейти к настройке секции «Список URL фильтрации».

2.10.2.7. Настройка секции «Список URL фильтрации»

Настройка данной секции позволяет блокировать веб-запросы по ключевому слову в адресе с помощью задания «черных» и «белых» списков (см. рис. 31).

Секция «Список URL фильтрации»

Рис. 31

Для настройки секции «Список URL фильтрации» необходимо выполнить следующие действия:

1) заполнить поле «Пользовательский чёрный список». Это необходимо для ввода и создания «черного» списка;

2) заполнить поле «Пользовательский белый список». Это необходимо для ввода и создания «белого» списка;

3) активировать чекбокс «Включено». Это необходимо для включения функции URL фильтрации;

4) перейти к настройке секции «Ограничения по времени».

2.10.2.8. Настройка секции «Ограничения по времени»

Настройка данной секции позволяет (см. рис. 32) установить время активности веб-прокси. По умолчанию используется для обеспечения доступа 24 часа в сутки, 7 дней в неделю.

Секция «Ограничения по времени»

Рис. 32

Для настройки секции «Ограничения по времени» необходимо выполнить следующие действия:

1) в выпадающем списке «Доступ» выбрать «Разрешить» (для открытия веб-доступа) или «Запретить» (для блокировки веб-доступа в пределах выбранного периода времени);

2) выбрать чекбоксы («Пн», «Вт», «Ср», «Чт», «Пт», «Сб», «Вс») в соответствии с днями недели необходимыми для настройки выбранного правила ограничения по времени;

3) выбрать из выпадающих списков «с» и «по» время выбора начала и окончания ограничений по времени;

4) перейти к настройке секции «Фильтр MIME типов».

2.10.2.9. Настройка секции «Фильтр MIME типов»

Настройка данной секции позволяет (см. рис. 33) регулировать параметры фильтра MIME типов. Фильтр MIME включает фильтрацию по MIME типам и может быть настроен на блокирование содержимого в зависимости от его типа.

Секция «Фильтр MIME типов»

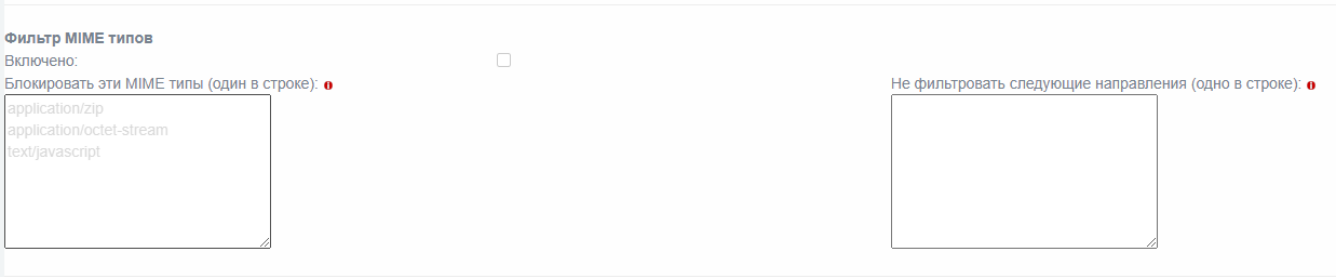


Рис. 33

Для настройки секции «Фильтр MIME типов» необходимо выполнить следующие действия:

1) активировать чекбокс «Включено» для включения фильтра MIME типов. Если фильтр включен, проверяются все входящие заголовки MIME типов;

2) заполнить поле «Блокировать эти MIME типы (один в строке)» (данное поле не обязательно к заполнению). Если запрошенный MIME тип будет заблокирован, доступ к нему будет запрещен. Таким образом, можно заблокировать контент, независимо от того, какой тип расширения имени файла используется. Например, следует добавить MIME типы в одной строке для блокировки скачивания файлов Word: `application/msword`. Также следует добавить MIME типы, каждый тип в отдельной строке, для блокировки скачивания MPEG и QuickTime видео файлов: `video/mpeg` и `video/quicktime`;

3) заполнить поле «Не фильтровать следующие направления (одно в строке)» (данное поле не обязательно к заполнению). 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;

Примеры настройки фильтрации:

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

4) перейти к настройке секции «Веб-браузер».

2.10.2.10. Настройка секции «Веб-браузер»

Настройка данной секции позволяет (см. рис. 34) настроить параметры проверки и разрешения использования веб-браузера.

Секция «Веб-браузер»

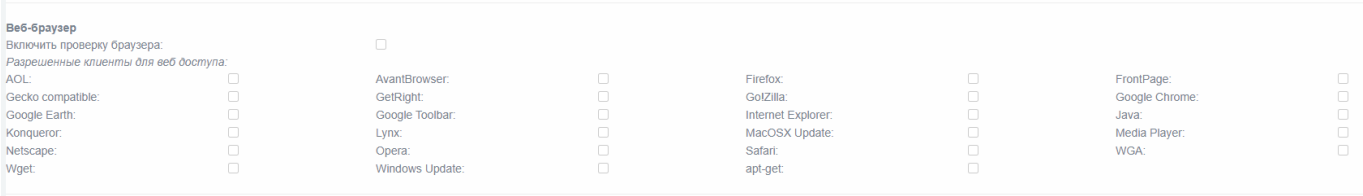


Рис. 34

Для настройки секции «Веб-браузер» необходимо выполнить следующие действия:

1) активировать чекбокс «Включить проверку браузера», если необходимо включить функцию проверки браузера;

2) из списка чекбоксов «Разрешенные клиенты для веб доступа» выбрать и активировать чекбоксы рядом с необходимыми названиями типов веб-браузеров для разрешения их к использованию;

3) перейти к настройке секции «Взаимодействие с сервером ICAP».

2.10.2.11. Настройка секции «Взаимодействие с сервером ICAP»

Настройка данной секции позволяет (см. рис. 35) настроить параметры взаимодействия с сервером ICAP.

Секция «Взаимодействие с сервером ICAP»

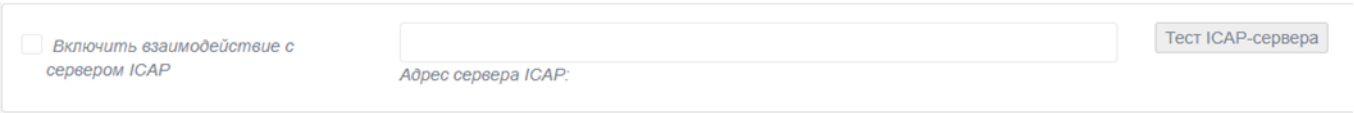


Рис. 35

Для настройки секции «Взаимодействие с сервером ICAP» необходимо выполнить следующие действия:

1) активировать чекбокс «Включить взаимодействие с сервером ICAP» для включения функции взаимодействия с сервером ICAP. Это позволит включить возможность подключения средства антивирусной защиты;

2) в поле «Адрес сервера ICAP» введите адрес СЗИ. Он будет использован при осуществлении функции прокси МЭ;

3) перейти к настройке секции «Фильтрация скриптов на дополнительном порту».

2.10.2.12. Настройка секции «Фильтрация скриптов на дополнительном порту»

Настройка данной секции позволяет (см. рис. 36) настроить параметры фильтрации скриптов (разрешения или блокирования скриптов в ответах HTTP-сервера).

Секция «Фильтрация скриптов на дополнительном порту»

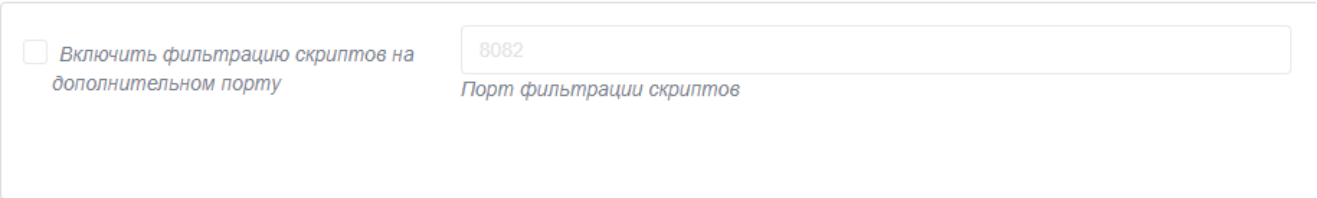


Рис. 36

Для настройки секции «Фильтрация скриптов на дополнительном порту» необходимо выполнить следующие действия:

1) активировать чекбокс «Включить фильтрацию скриптов на дополнительном порту» для включения поддержки фильтрации скриптов;

2) в поле «Порт фильтрации скриптов» ввести номер порта, к которому будет происходить обращение;

3) настроить (дополнительно при необходимости) остальные секции из представленных в подразделе «Прокси» раздела «Службы»;

4) нажать кнопку «Сохранить» внизу подраздела для сохранения и применения введенных настроек.

2.11. Создание виртуального интерфейса GRE-туннеля

Для настройки виртуального интерфейса GRE-туннеля необходимо выполнить следующие действия:

1) перейти в подраздел «GRE» раздела «VPN» (см. рис. 37);

Подраздел «GRE»

Рис. 37

2) в поле «Имя» ввести имя нового GRE-туннеля. Допускается имя, состоящее из латинских букв верхнего и нижнего регистра и цифр от 0 до 9;

3) в поле «IP-адрес локального интерфейса» ввести IP-адрес удаленного устройства, с которым будет устанавливаться GRE-туннель;

4) в поле «IP-адрес удаленного интерфейса» ввести IP-адрес удаленного устройства, с которым будет устанавливаться GRE-туннель;

5) в поле «IP-адрес локального интерфейса GRE» ввести виртуальный локальный IP-адрес GRE-туннеля;

6) в поле «Маска сети локального интерфейса GRE» ввести IP-маски для GRE-туннеля. Допустима корректная IP-маска в формате десятичной записи четырех байт маски, разделенных точками;

7) в поле «MTU» ввести максимальный размер пакета для GRE-туннеля;

8) нажать кнопку «Сохранить» для сохранения введенных настроек;

9) проверить добавление нового GRE-туннеля в информационную таблицу «Список GRE туннелей».

Добавленный GRE-туннель будет так же отображаться в подразделе «Состояние сети» раздела «Состояние» (см. рис. 38).

Отображение информации о созданном GRE-туннеле

```
gre: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 1500
        inet 192.168.100.1  netmask 255.255.255.0  destination 192.168.100.1
        unspec C0-A8-04-01-FF-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Рис. 38

2.12. Создание туннеля GRE с использованием созданного интерфейса GRE

Для создания туннеля GRE с использованием созданного интерфейса GRE необходимо выполнить следующие действия:

1) обеспечить связь с двумя устройствами, между которыми необходимо создать GRE-туннель;

2) обеспечить прохождение пакетов протокола GRE от удаленного узла к локальному по указанным IP-адресам;

3) добавить правило МЭ, разрешающее прием изделием пакетов протокола GRE от удаленного узла на локальный по указанным IP-адресам, для этого необходимо:

— перейти в подраздел «Службы» раздела «Межсетевой экран» и добавить соответствующую службу с используемым протоколом GRE (см. рис. 39);

Добавление службы с используемым протоколом GRE

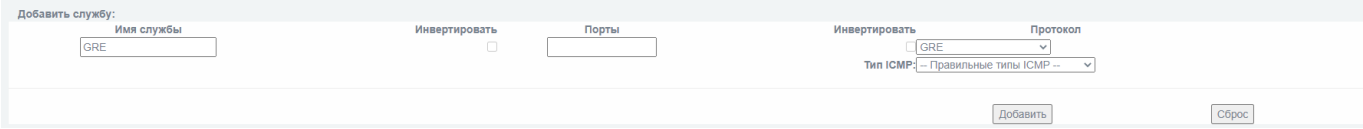


Рис. 39

— после нажатия кнопки «Добавить» служба, с используемым протоколом GRE, будет внесена в информационную таблицу «Свои сервисы» (см. рис. 40) и станет доступной для использования МЭ;

Отображение добавленной службы GRE

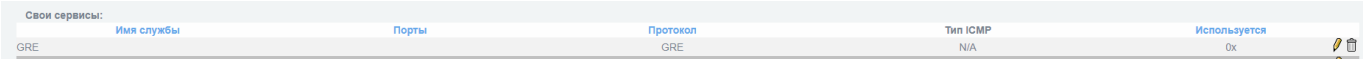


Рис. 40

— перейти на страницу «Доступ к устройству Рубикон» («Межсетевой экран» → «Правила межсетевого экрана» → нажать кнопку «Доступ к устройству Рубикон»);

— на странице «Доступ к устройству Рубикон» необходимо добавить правило, разрешающее прохождение пакетов протокола GRE от IP-адреса удаленного узла к IP-адресу локального интерфейса с использованием добавленной ранее службы GRE (см. рис. 41, 42, 43);

— по завершению настройки нажать кнопку «Сохранить» для добавления нового правила МЭ;

Добавление правила для GRE. Вкладка «Источник»

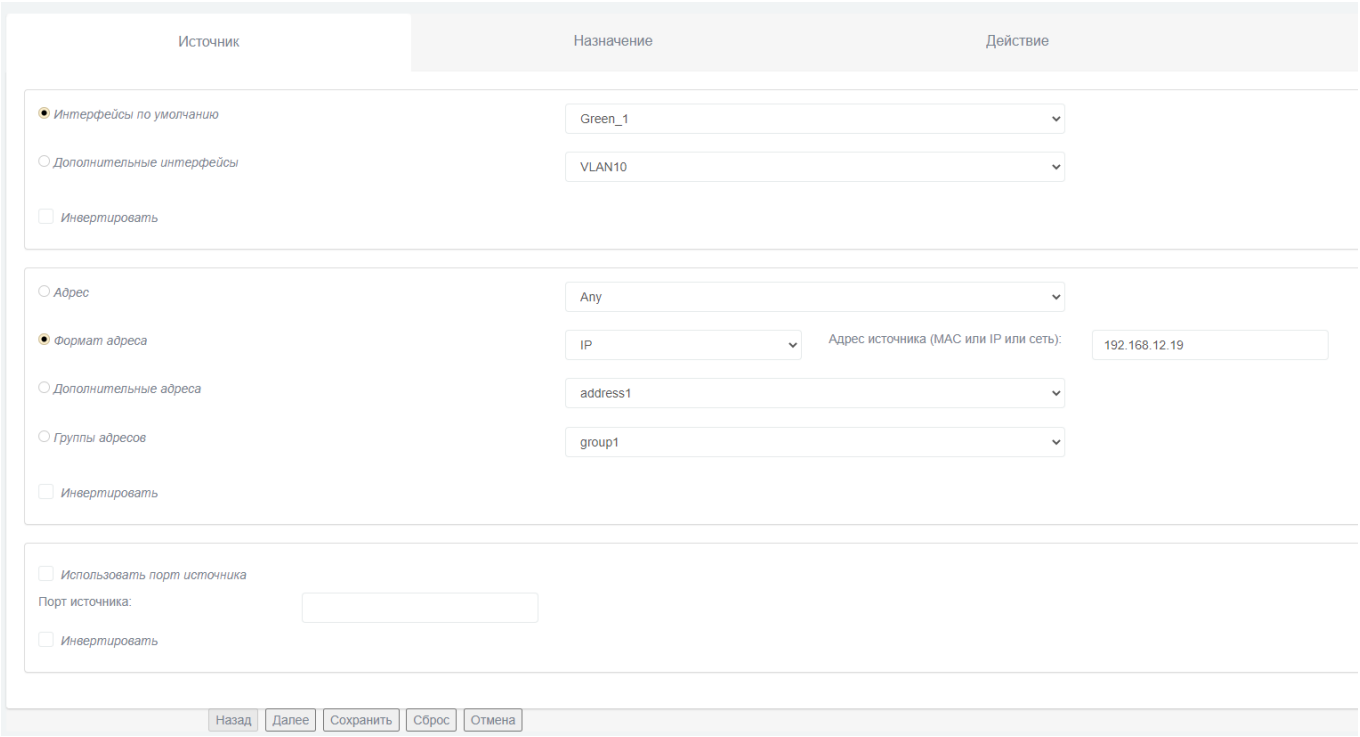


Рис. 41

Добавление правила для GRE. Вкладка «Назначение»

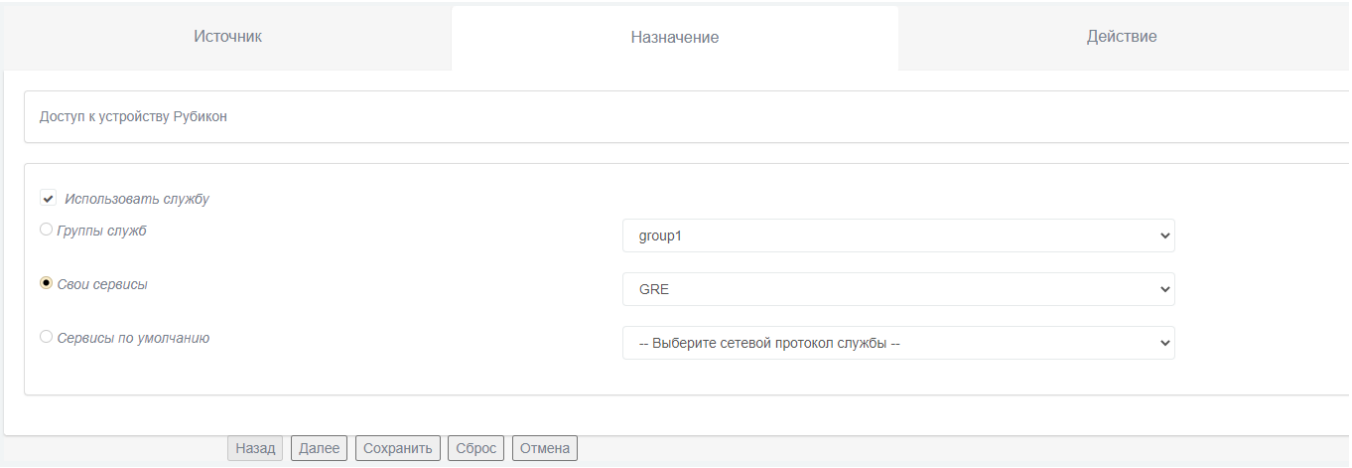


Рис. 42

Добавление правила для GRE. Вкладка «Действие»

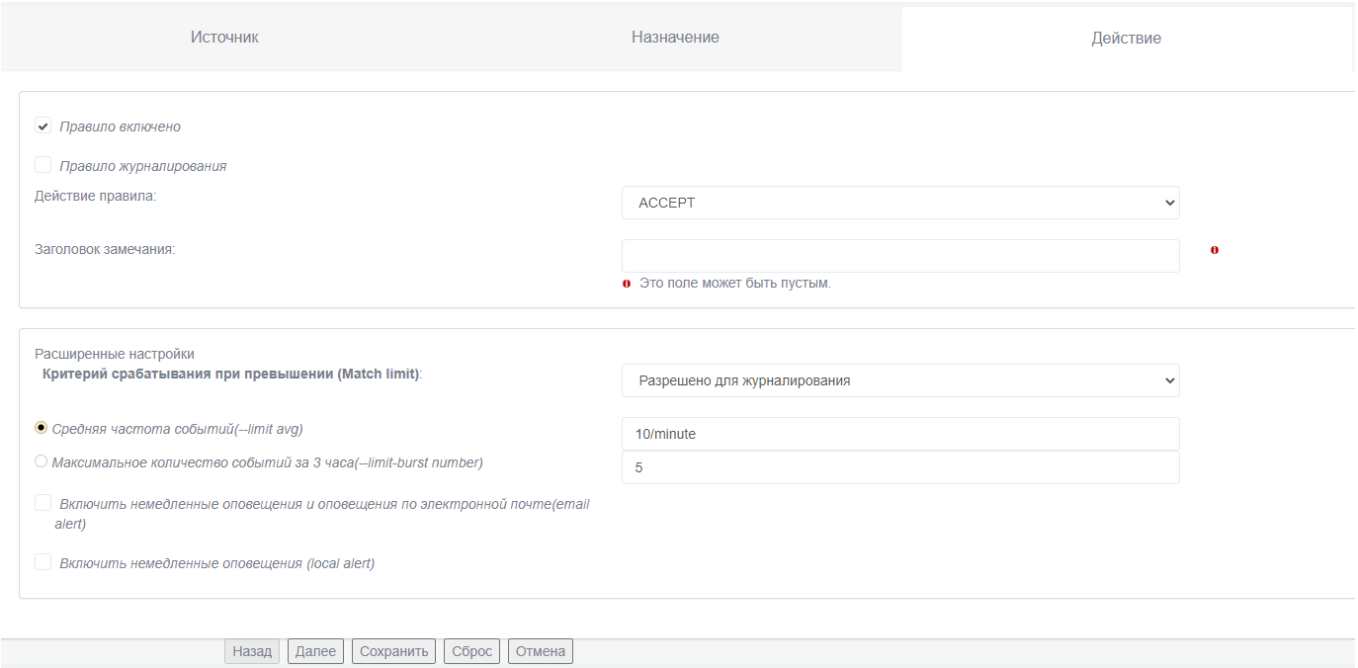


Рис. 43

— после добавления нового правила МЭ необходимо проверить, что данное правило добавилось (см. рис. 44) в информационную таблицу «Доступ к устройству Рубикон» блока «Текущие правила» («Межсетевой экран» → «Правила межсетевого экрана»);

Отображение нового правила в блоке «Текущие правила»

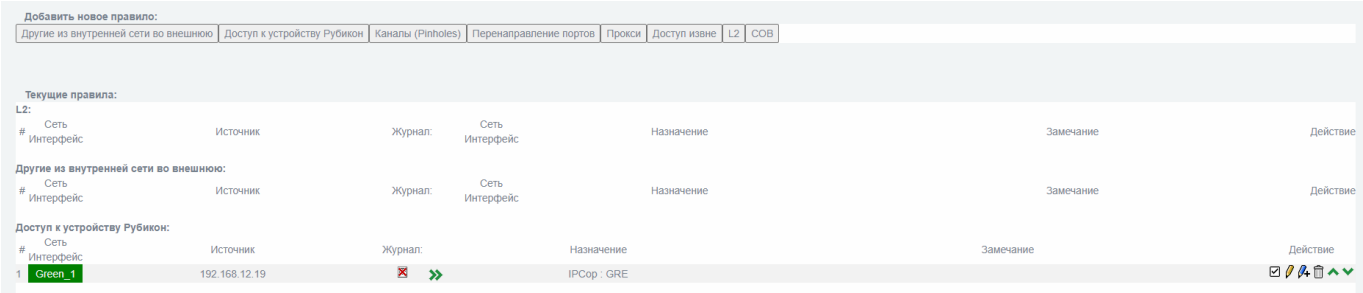


Рис. 44

4) Далее для создания дополнительных правил МЭ для GRE интерфейса необходимо выполнить следующее:

— добавить правила фильтрации на интерфейсе GRE трафика в соответствии с заданной политикой. Для этого необходимо перейти в подраздел «Настройки межсетевого экрана» раздела «Межсетевой экран» и установить расширенный режим настройки (см. рис. 45), активировав чекбокс «Включено» напротив функции «Расширенный режим». После нажать кнопку «Сохранить» для применения настройки;

Установка расширенного режима настройки

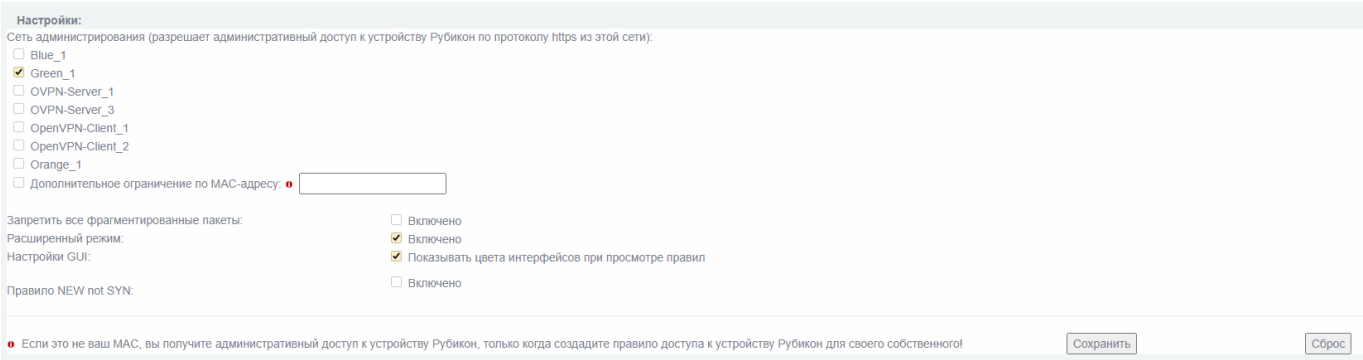


Рис. 45

— перейти в подраздел «Интерфейсы по умолчанию» раздела «Межсетевой экран» и внести созданный интерфейс GRE в список интерфейсов МЭ (см. рис. 46);

Внесение созданного интерфейса GRE в список интерфейсов МЭ

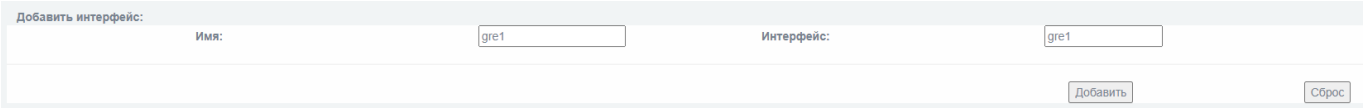


Рис. 46

— нажать кнопку «Добавить» чтобы сохранить настройки и добавить новый интерфейс;

— после добавления нового интерфейса GRE необходимо проверить, что данный интерфейс добавился (см. рис. 47) в информационную таблицу «Дополнительные интерфейсы» («Межсетевой экран» → «Интерфейсы по умолчанию»);

Отображение добавленного интерфейса в информационной таблице «Дополнительные интерфейсы»

Рис. 47

5) Далее следует создать правила в соответствии с политикой фильтрации пакетов с использованием созданного ранее интерфейса.

2.13. Настройка системы обнаружения вторжений

2.13.1. 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 подразделе «Обнаружение атак» раздела «Система обнаружения вторжений» (блок «Интерфейсы»).

Подраздел «Обнаружение атак» раздела «Система обнаружения вторжений» представлен на рисунке 48.

Подраздел «Обнаружение атак» раздела «Система обнаружения вторжений»

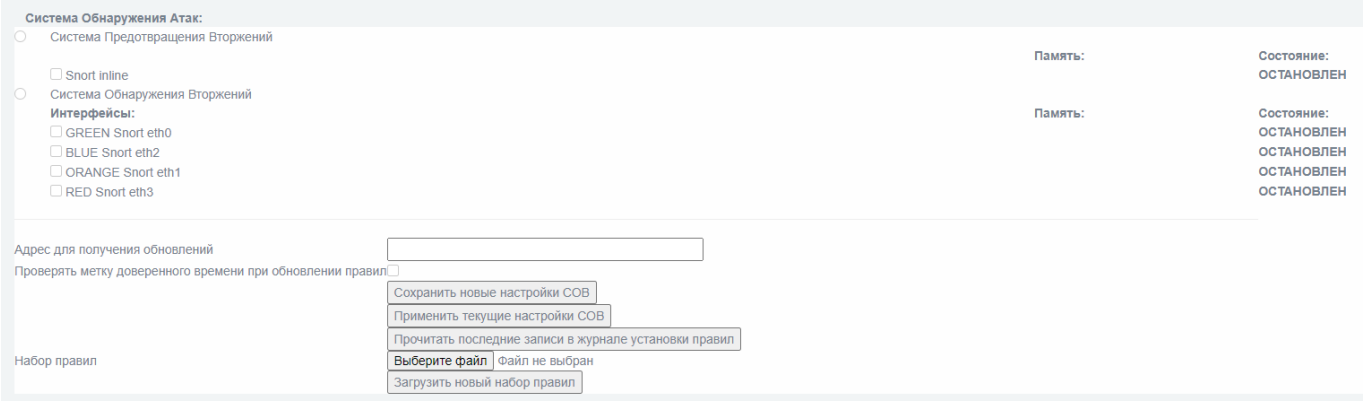


Рис. 48

2.13.2. Запуск на физическом интерфейсе

Для того чтобы подключить СОВ к одному из физических интерфейсов, необходимо активировать чекбокс с именем интерфейса в подразделе «Обнаружение атак» раздела «Система обнаружения вторжений», блок «Интерфейсы» (см. рис. 48).

После того как необходимый чекбокс активирован, следует сохранить изменения, нажав кнопку «Сохранить». Далее появится надпись с дальнейшими указаниями. Чтобы применить сохраненные изменения, следует нажать кнопку «Применить». Теперь СОВ запущена на выбранном интерфейсе (см. рис. 49).

Запуск СОВ на физическом интерфейсе

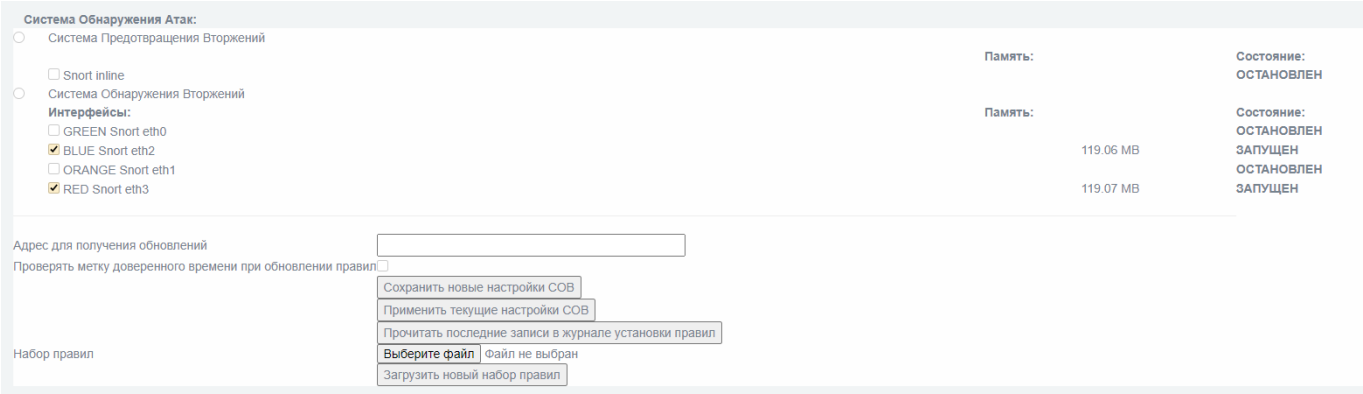


Рис. 49

2.13.3. Режимы обнаружения

Предусмотрено два режима обнаружения вторжений:

1) «Сигнатурный анализ»;

2) «Эвристический анализ».

2.13.3.1. Режим «Сигнатурный анализ»

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

Система обнаружения вторжений (атак) в режиме сигнатурного анализа может использоваться в двух режимах:

1) «Система предотвращения вторжений», при котором трафик, проходящий через изделие, может блокироваться при обнаружении атаки, совпадающей с какой-либо из загруженных сигнатур;

2) «Система обнаружения вторжений», при котором происходит сигнализация (в журнале или в оповещении в веб-интерфейсе) об обнаруженной атаке, совпадающей с какой-либо из загруженных сигнатур.

2.13.3.1.1. Система предотвращения вторжений

Режим «Система предотвращения вторжений» включается чекбоксом «Система Предотвращения Вторжений» в подразделе «Обнаружение Атак» раздела «Система предотвращения вторжений», а также активацией чекбокса «Snort inline» (см. рис. 50).

После совершенных изменений необходимо сохранить изменения (нажать кнопку «Сохранить новые настройки СОВ») и применить их (нажать кнопку «Применить текущие настройки СОВ»).

Включение режима «Система предотвращения вторжений»

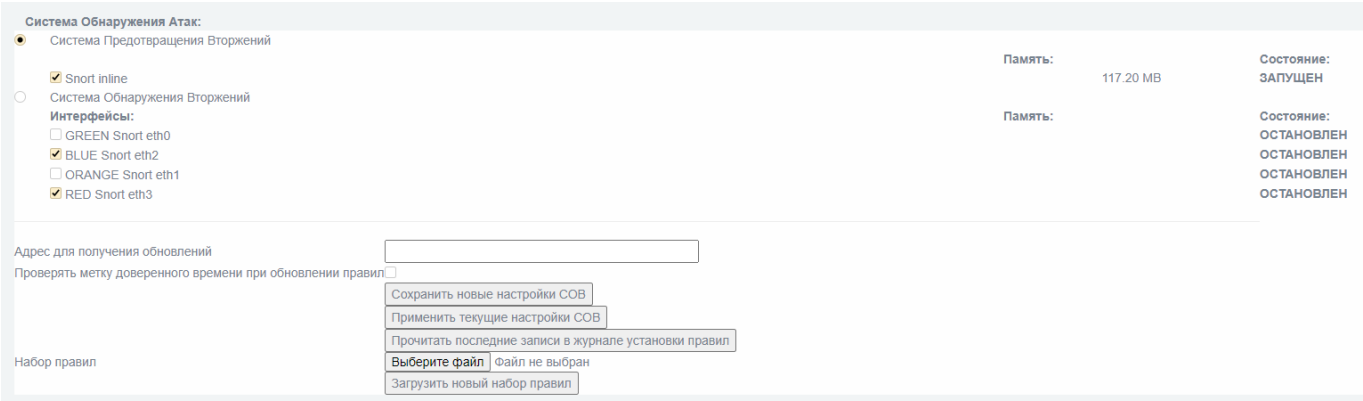


Рис. 50

Предотвращение вторжений осуществляется над трафиком, который специальным образом перенаправляется в СОВ через настройку правил МЭ.

В расширенном режиме МЭ необходимо:

1) перейти в подраздел «Правила межсетевого экрана» раздела «Межсетевой экран» и нажать на кнопку «Другие из внутренней сети во внешнюю»;

2) далее перейти на вкладку «Действие»;

3) выбрать в выпадающем списке «Действие правила» – параметр «Система Обнаружения Вторжений»;

4) сохранить изменения, нажав кнопку «Сохранить».

Трафик МЭ, который определяется данным правилом, будет передан на анализ в СОВ и, по результатам анализа, либо будет отброшен, либо пропущен.

Трафик, который не был передан из МЭ, система обнаружения вторжений в режиме предотвращения вторжений не рассматривает.

Примечание – Правила «L2» **не имеют** возможности передачи трафика на анализ в режиме предотвращения вторжений (можно использовать только возможности по обнаружению).

2.13.3.1.2. Система обнаружения вторжений

Режим «Система обнаружения вторжений» включается чекбоксом «Система Обнаружения Вторжений» в подразделе «Обнаружение Атак» раздела «Система предотвращения вторжений», а также активацией чекбоксов с необходимыми именами интерфейсов, на которых предполагается осуществление проверки трафика по сигнатурам (см. рис. 51).

После совершенных изменений необходимо сохранить изменения (нажать кнопку «Сохранить новые настройки СОВ») и применить их (нажать кнопку «Применить текущие настройки СОВ»).

Включение режима «Система обнаружения вторжений»

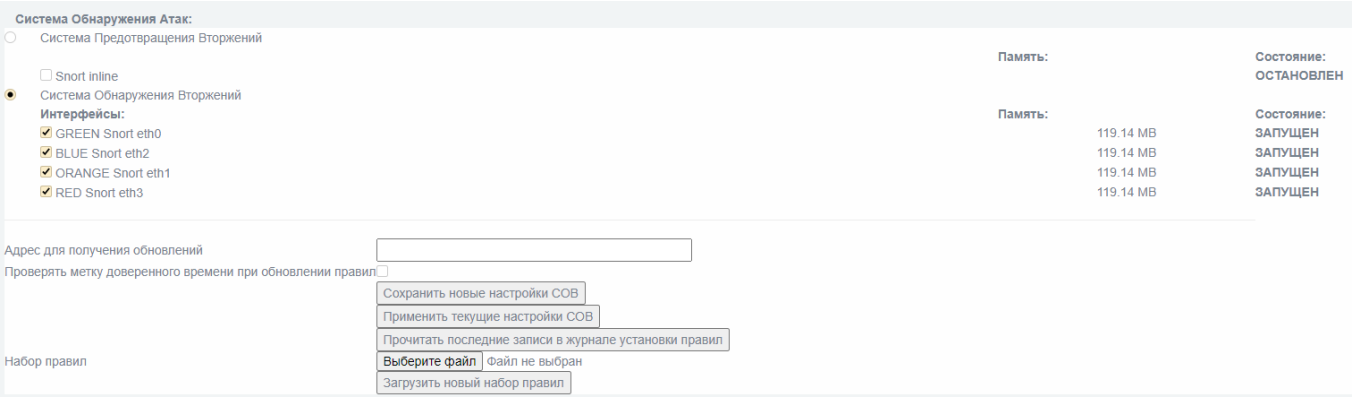


Рис. 51

В режиме «Система обнаружения вторжений» рассматривается весь трафик, поступающий на выбранный интерфейс.

Для обнаружения атак на интерфейсе **моста** необходимо создать мост например с именем «**idsbr**». После создания он отобразится в списке как «BRIDGE Snort **idsbr**» (см. рис. 52) и станет доступен для включения на нем системы обнаружения вторжений».

Настройка СОВ для моста

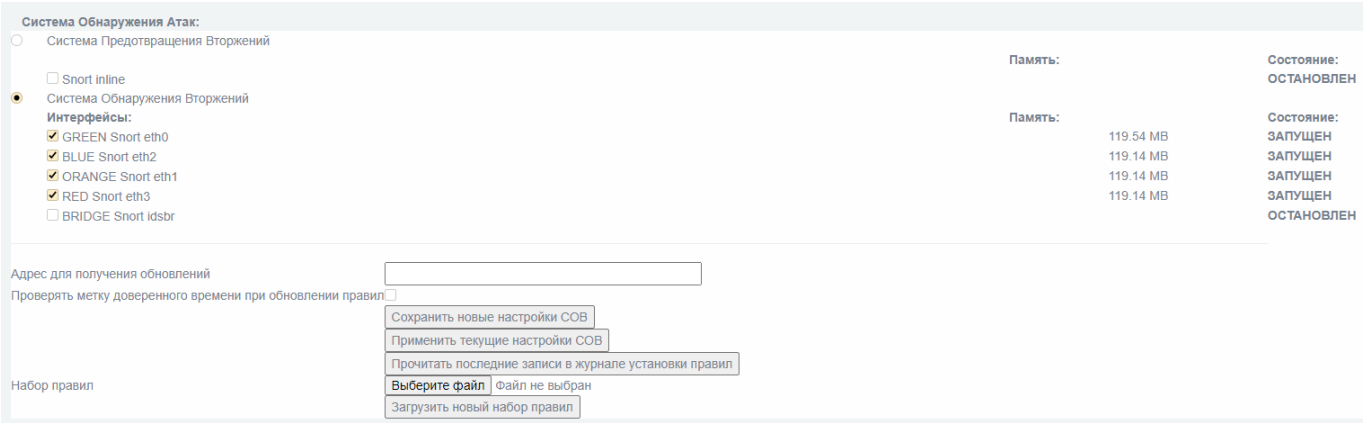


Рис. 52

2.13.3.2. Режим «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 подраздел «Настройка обнаружения сканирования» раздела «Система обнаружения вторжения».

В подразделе представлено несколько элементов управления (см. рис. 53):

1) чекбокс «Включено» – включает и отключает систему обнаружения сканирования;

2) выпадающий список «Протокол» – определяет те сетевые пакеты, которые будут анализироваться;

3) выпадающий список «Уровень срабатывания» – определяет предполагаемую интенсивность сканирования злоумышленником.

Настройка эвристического анализа

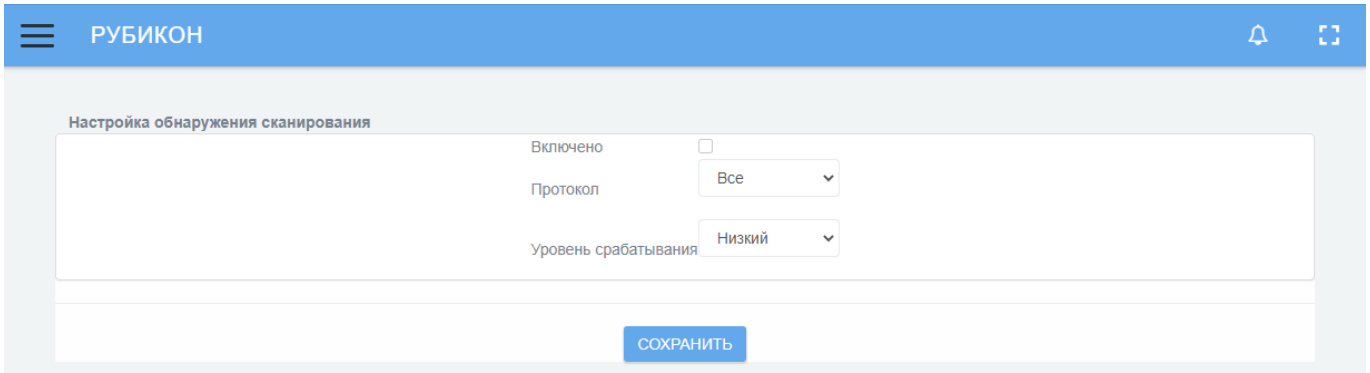


Рис. 53

2.14. Трансляция сетевых адресов

Трансляция сетевых адресов осуществляется с использованием технологии DNAT **автоматически** на красном интерфейсе. Адрес источника пакета заменяется адресом красного интерфейса изделия и наоборот.

Ручная настройка трансляции сетевых адресов **не предусмотрена**.

2.15. 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 выполнить следующие действия:

1) настроить сетевые адреса красного и оранжевого или зеленого интерфейса;

2) для настройки правил фильтрации перейти в подраздел «Правила межсетевого экрана» раздела «Межсетевой экран»;

3) нажать кнопку «Перенаправление портов» и перейти на страницу «Перенаправление портов»;

4) далее следует настроить правило фильтрации – во вкладке «Источник» внести информацию о параметрах источника пакета: адрес, порт и сервис, который изделие предоставляет в красную подсеть для доступа к требуемому узлу внутренней подсети (см. рис. 54);

Настройка вкладки «Источник» страницы «Перенаправление портов»

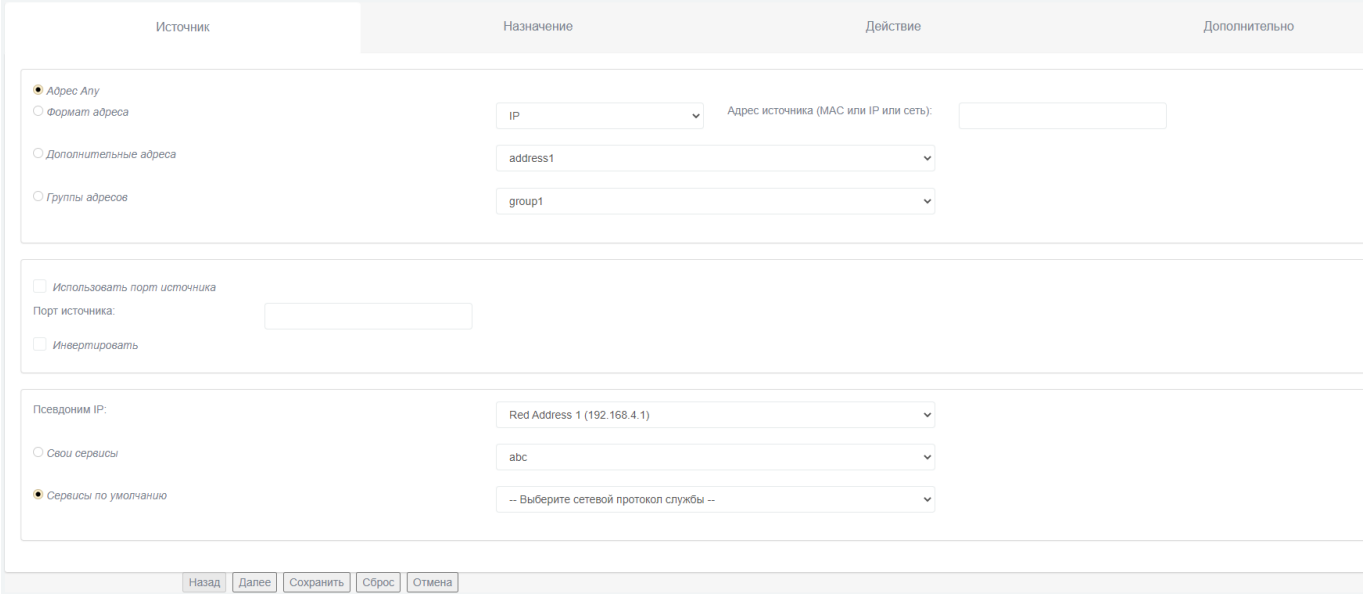


Рис. 54

5) во вкладке «Назначение» внести информацию о месте назначения (интерфейс, адрес, порт, предоставляемый конкретным узлом) (см. рис. 36);

Настройка вкладки «Назначение» страницы «Перенаправление портов»

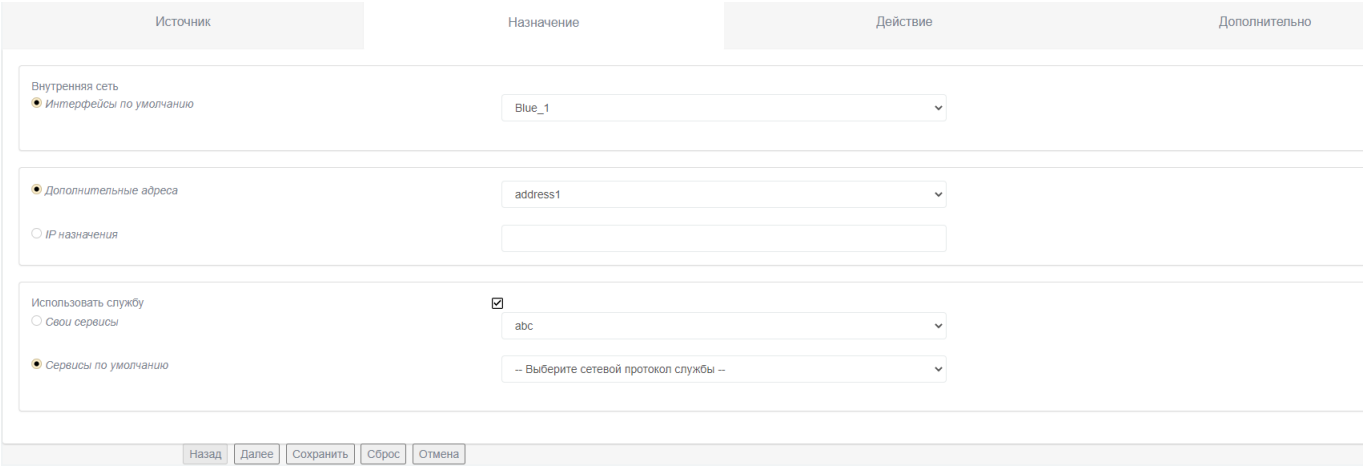


Рис. 55

6) во вкладке «Действие» внести информацию о параметрах фильтрации (см. рис. 56);

Настройка вкладки «Действие» страницы «Перенаправление портов»

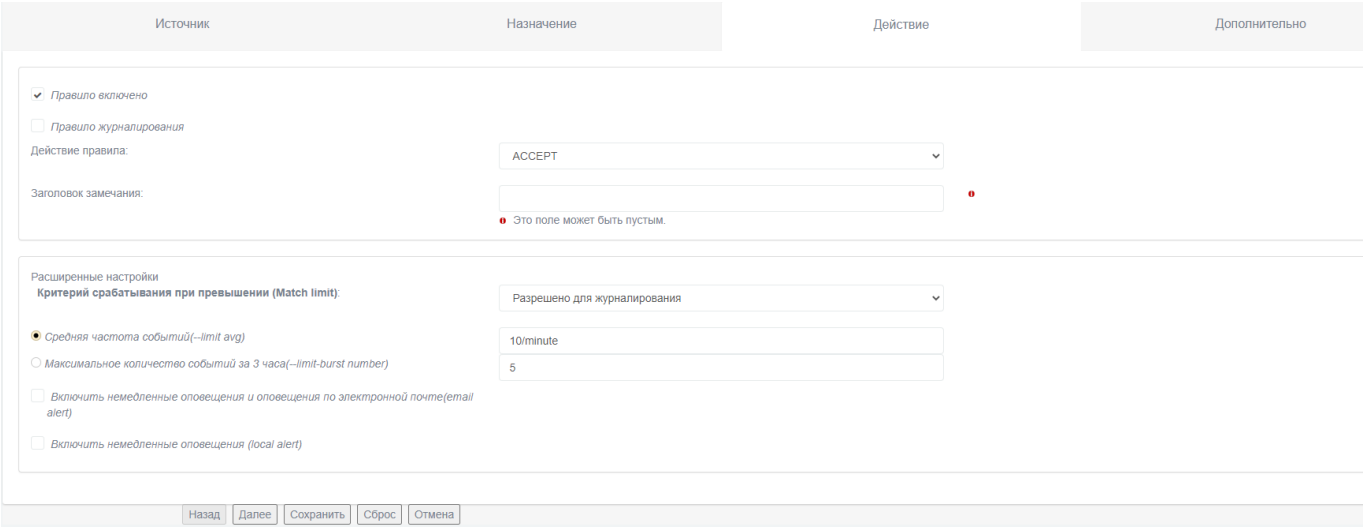


Рис. 56

7) выбрать необходимое действие для завершения операции по изменению текущего правила. На выбор предлагаются три возможных варианта:

— сохранить правило и вернуться к интерфейсу выбора необходимых действий по настройке правил нажатием кнопки «Сохранить»;

— сбросить установленные параметры фильтрации нажатием кнопки «Сброс»;

— выйти из интерфейса изменения правил без сохранения нажатием кнопки «Отмена».

2.16. Маскирование

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

1) переназначить цвет маскируемого интерфейса на **красный**;

2) перейти в подраздел «Интерфейсы» раздела «Система» (см. рис. 57). В настройках красного интерфейса появится новое поле «адрес подмены»;

Подраздел «Интерфейсы» раздела «Система»

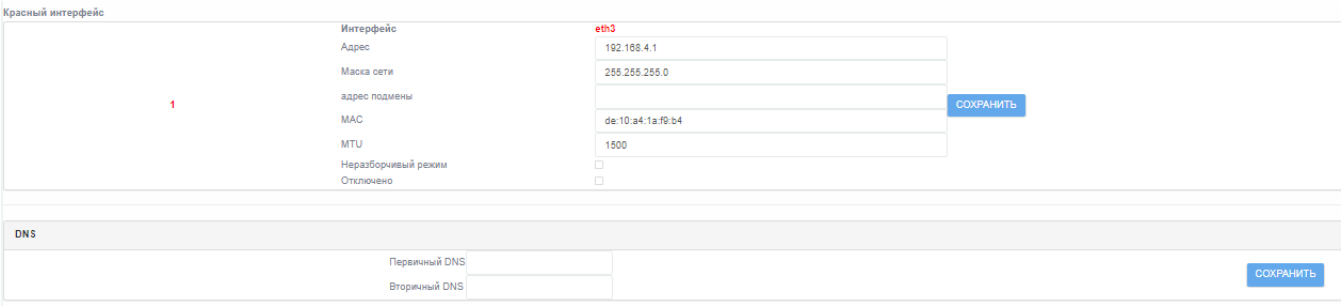


Рис. 57

3) ввести маскирующий адрес в поле «адрес подмены» красного интерфейса;

4) нажать кнопку «Сохранить» рядом с настраиваемым интерфейсом для сохранения изменений.

2.17. Таблицы состояний

Таблицы состояний отображают информацию об активных соединениях.

Для просмотра таблиц состояний необходимо выполнить следующие действия:

1) перейти в подраздел «Соединения» раздела «Состояние»;

2) в выпадающем списке «Отображать» выбрать значение «Состояние» или «Трафик»;

3) нажать кнопку «Сохранить».

Таблица «Трафик» (см. рис. 58) подсчитывает количество переданных пакетов в действующих соединениях.

Таблица «Трафик»

Протокол	Исходный IP-адрес:Порт источника	Исходный IP-адрес:Порт назначения	Пакеты / Байты	Ответ IP-адрес:Порт источника	Ответ IP-адрес:Порт назначения	Пакеты / Байты
tcp	192.168.56.101 :36828	192.168.56.1 :8443	14 / 2504	192.168.56.1 :8443	192.168.56.101 :36828	9 / 1678
tcp	192.168.56.101 :36852	192.168.56.1 :8443	12 / 1740	192.168.56.1 :8443	192.168.56.101 :36852	9 / 1045
tcp	192.168.56.101 :36838	192.168.56.1 :8443	11 / 1691	192.168.56.1 :8443	192.168.56.101 :36838	10 / 1097
tcp	192.168.56.101 :36866	192.168.56.1 :8443	13 / 2450	192.168.56.1 :8443	192.168.56.101 :36866	9 / 1678
tcp	192.168.56.101 :36884	192.168.56.1 :8443	9 / 2389	192.168.56.1 :8443	192.168.56.101 :36884	7 / 917
tcp	192.168.56.101 :36872	192.168.56.1 :8443	13 / 2454	192.168.56.1 :8443	192.168.56.101 :36872	9 / 1678
tcp	192.168.56.101 :36826	192.168.56.1 :8443	13 / 2452	192.168.56.1 :8443	192.168.56.101 :36826	9 / 1678
tcp	192.168.56.101 :36874	192.168.56.1 :8443	14 / 2502	192.168.56.1 :8443	192.168.56.101 :36874	9 / 1678
tcp	192.168.56.101 :36836	192.168.56.1 :8443	12 / 1743	192.168.56.1 :8443	192.168.56.101 :36836	8 / 993
tcp	192.168.56.101 :36830	192.168.56.1 :8443	12 / 1743	192.168.56.1 :8443	192.168.56.101 :36830	8 / 993
tcp	192.168.56.101 :36864	192.168.56.1 :8443	13 / 2454	192.168.56.1 :8443	192.168.56.101 :36864	9 / 1678
tcp	192.168.56.101 :36882	192.168.56.1 :8443	14 / 2502	192.168.56.1 :8443	192.168.56.101 :36882	8 / 1626

Легенда: ЛВС | ИНТЕРНЕТ | Беспроводная сеть | Демилитаризованная Зона (DMZ) | IPCop | IPsec | OpenVPN

Рис. 58

Таблица «Состояние» (см. рис. 59) отображает актуальное состояние действующих соединений.

Таблица «Состояние»

Протокол	Запрос IP-адрес:Порт источника	Запрос IP-адрес:Порт назначения	Ответ IP-адрес:Порт источника	Ответ IP-адрес:Порт назначения	Истекает (Секунды)	Состояние	Выделенный	Использовано
tcp	192.168.56.101 :36860	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36860	5	CLOSE	0	1
tcp	192.168.56.101 :36828	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36828	51	TIME_WAIT	0	1
tcp	192.168.56.101 :36826	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36826	51	TIME_WAIT	0	1
tcp	192.168.56.101 :36836	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36836	70	TIME_WAIT	0	1
tcp	192.168.56.101 :36818	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36818	19	TIME_WAIT	0	1
tcp	192.168.56.101 :36858	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36858	5	CLOSE	0	1
tcp	192.168.56.101 :36838	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36838	76	TIME_WAIT	0	1
tcp	192.168.56.101 :36862	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36862	431999	ESTABLISHED	0	1
tcp	192.168.56.101 :36830	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36830	58	TIME_WAIT	0	1
tcp	192.168.56.101 :36852	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36852	93	TIME_WAIT	0	1
tcp	192.168.56.101 :36820	192.168.56.1 :8443	192.168.56.1 :8443	192.168.56.101 :36820	25	TIME_WAIT	0	1

Легенда: ЛВС | ИНТЕРНЕТ | Беспроводная сеть | Демилитаризованная Зона (DMZ) | IPCop | IPsec | OpenVPN

Рис. 59

2.18. Настройка резервирования

2.18.1. Горячее резервирование

Функция горячего резервирования устройства «Рубикон» настраивается в меню «Сеть» → «Горячее резервирование CARP» и обеспечивает бесперебойную реализацию функций межсетевого экрана и СОВ в случае возможного выхода из строя устройства «Рубикон».

Горячее резервирование реализуется посредством двух идентично настроенных устройств «Рубикон», подключенными к одним и тем же сегментам сети одноименными интерфейсами. При этом один из комплексов назначается главным, а другой – резервным. Главное устройство при этом полноценно работает и выполняет функции МЭ и СОВ, а резервное находится в режиме ожидания и получает от главного пакеты о работоспособности. На каждом из одноименных сетевых интерфейсов главного и резервного устройств назначается одинаковый виртуальный IP-адрес, так, чтобы при выходе из строя главного устройства резервное сохраняло конфигурацию сети. Таким образом, **пара устройств «Рубикон»** представляется в сети как **одиночное устройство «Рубикон»**, сетевые адреса которого совпадают с настроенными виртуальными адресами.

При выходе из строя главного устройства резервное перестает получать по сети извещения о работоспособности главного устройства, и, через определенный (администратором в поле «задержка») промежуток времени, принимает на себя функции главного устройства: активирует функции приема, передачи и обработки сетевых пакетов на виртуальных адресах.

В случае восстановления функций главного устройства в сети оно рассылает сетевые пакеты о своей работоспособности. Резервное, получая указанные пакеты, возвращается в режим ожидания и перестает обрабатывать сетевые пакеты на виртуальных адресах.

Адрес дублирующего устройства определяется конкретным подключением к дублирующему устройству. На практике, обычно, устройства связывают по отдельным сетевым интерфейсам патч-кордом напрямую. Соответствующие интерфейсы, в этом случае (в которые подключен патч-корд), **должны быть из одной подсети** и не совпадать или пересекаться с другими подсетями. Поэтому, адрес дублирующего устройства должен быть адресом связанного патч-кордом интерфейса дублирующего устройства.

Пример резервирования устройств при организации взаимодействия «зеленой» и «красной» сети представлен на рисунке 60.

Резервирование устройств при организации взаимодействия «зеленой» и «красной» сети

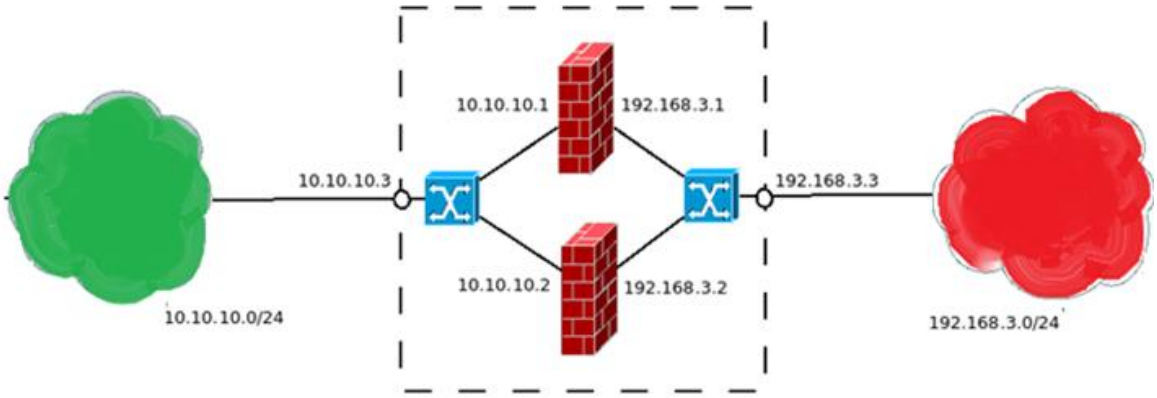


Рис. 60

В представленной схеме верхнее устройство «Рубикон» настроено в качестве главного, нижнее устройство «Рубикон» настроено в качестве резервного.

Адреса «зеленой» сети принадлежат диапазону 10.10.10.0/24, главному устройству «Рубикон» присвоен адрес в этой сети: 10.10.10.1, резервному устройству: 10.10.10.2. Виртуальный адрес резервирования в «зеленой» сети: 10.10.10.3. Адреса «красной» сети принадлежат диапазону 192.168.3.0/24, главному устройству присвоен адрес в этой сети: 192.168.3.1, резервному: 192.168.3.2. Виртуальный адрес резервирования в «красной» сети: 192.168.3.3.

Для настройки функции горячего резервирования необходимо:

1) настроить виртуальный адрес «зеленого» интерфейса. Для этого следует в подразделе «Горячее резервирование CARP (VRRP)» раздела «Сеть» – нажать кнопку « » редактирования интерфейса (GREEN_2) (см. рис. 61);

Подраздел «Горячее резервирование CARP (VRRP)» раздела «Сеть»

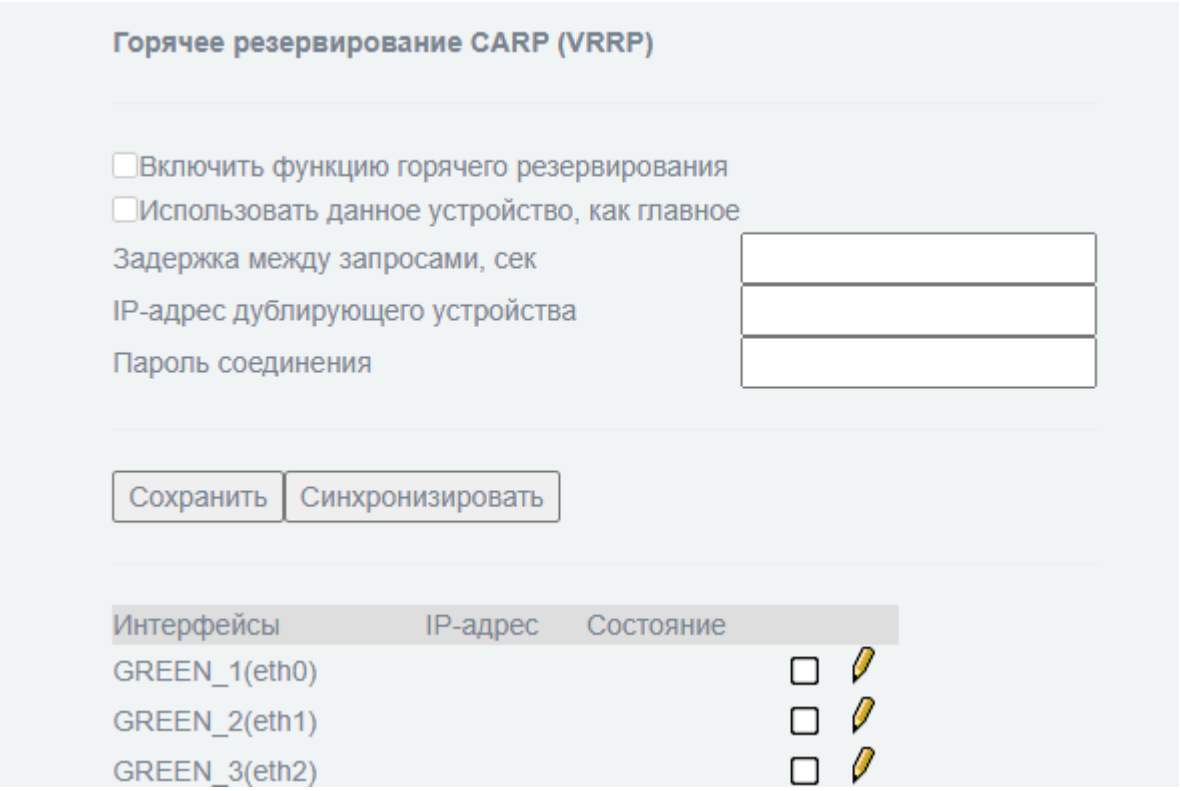


Рис. 61

2) в отобразившемся окне редактирования указать общий виртуальный IP-адрес и нажать кнопку «Сохранить» (см. рис. 62);

Общий виртуальный IP-адрес для «зеленого» интерфейса

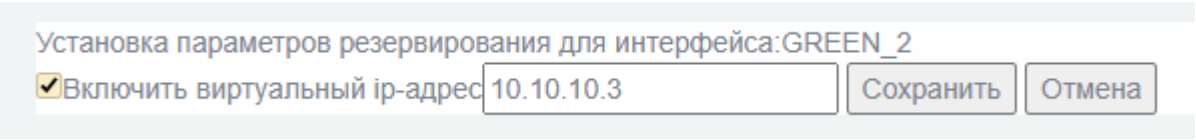


Рис. 62

3) настроить виртуальный адрес «красного» интерфейса. Для этого в подразделе «Горячее резервирование CARP (VRRP)» раздела «Сеть» нажать кнопку редактирования интерфейса (RED_1);

4) в отобразившемся окне редактирования указать общий виртуальный IP-адрес и нажать кнопку «Сохранить» (см. рис. 63);

Общий виртуальный IP-адрес для «красного» интерфейса

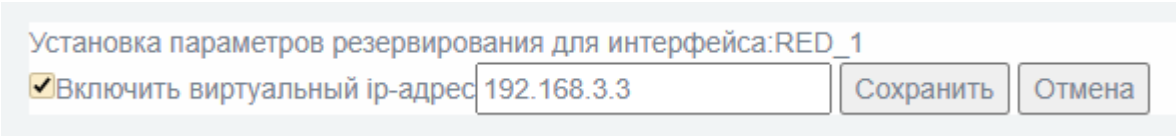


Рис. 63

5) для главного устройства установить элемент управления «Использовать данное устройство, как главное» (см. рис. 64);

Настройка главного устройства «Рубикон»

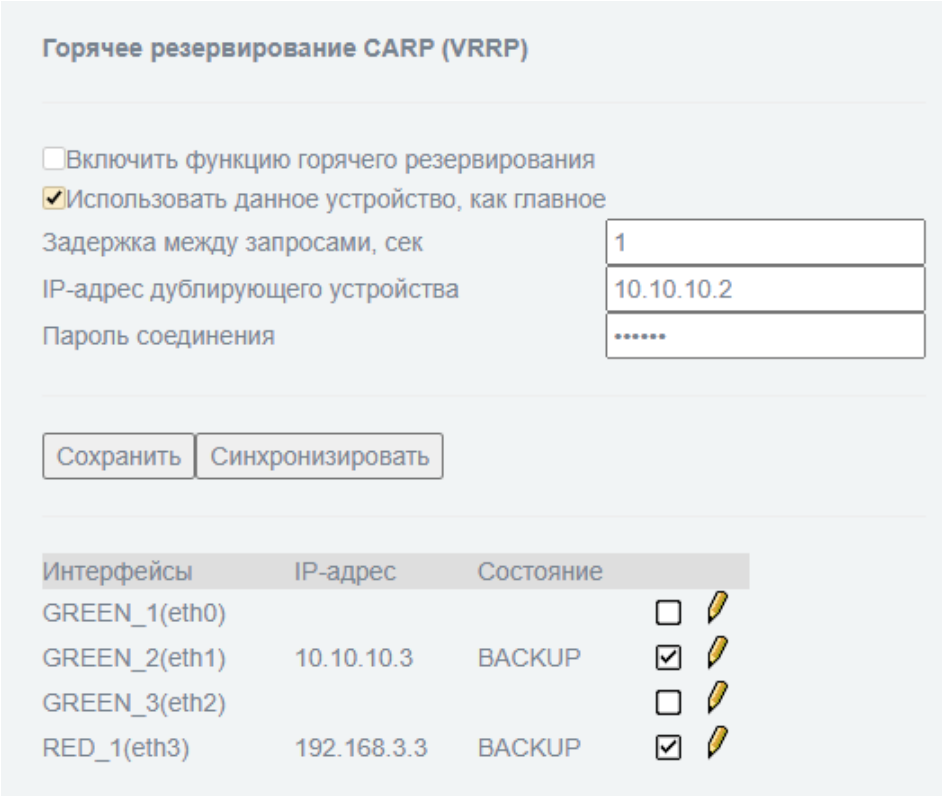


Рис. 64

6) для главного и резервного устройств заполнить поля «Задержка», «IP-адрес дублирующего устройства» и «Пароль соединения» следующими значениями:

— задержки между запросами;

— IP-адресом дублирующего устройства (если настраивается главное, то указывается IP-адрес резервного и наоборот);

— паролем для протокола обмена (пароли, заданные на главном и резервном устройстве, должны совпадать).

7) для главного и резервного устройств установить элемент управления «Включить функцию горячего резервирования» (см. рис. 65);

Включение функции горячего резервирования

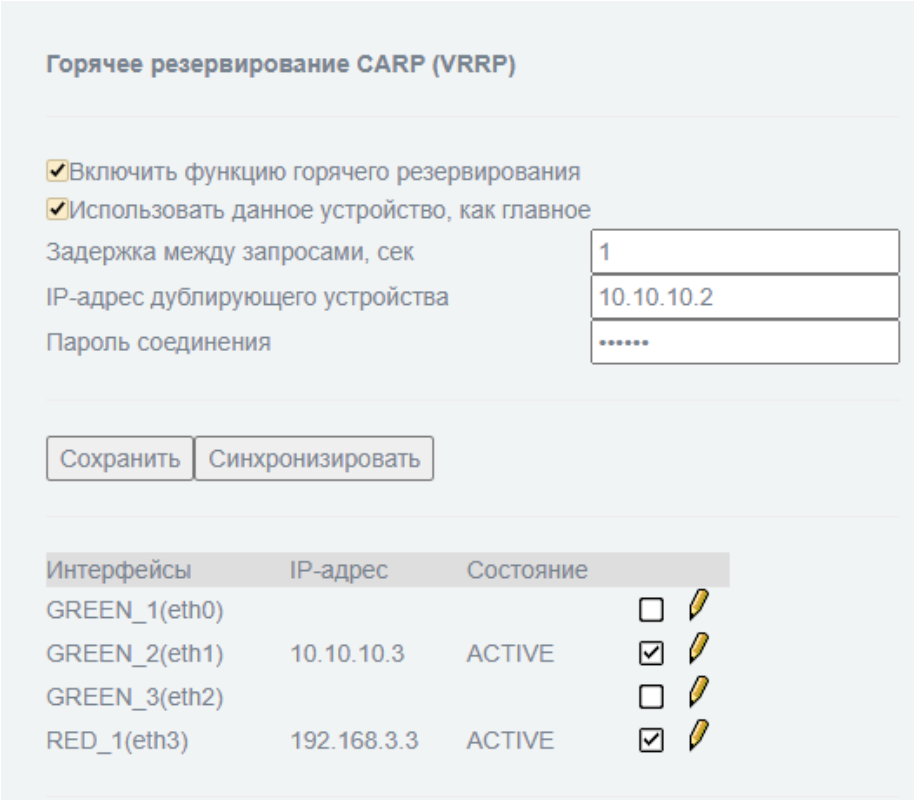


Рис. 65

8) для проверки правильности настройки горячего резервирования необходимо выполнить команду `ping` с адресом виртуального интерфейса: `$ ping 10.10.10.3`.

2.19. Работа с журналами событий

2.19.1. Общие положения

В «Рубикон» предусмотрены следующие журналы:

1) журнал МЭ;

2) журнал обнаружения атак (вторжений);

3) системный протокол.

Системный протокол содержит информацию обо всех действиях, производимых в «Рубикон».

Регистрируемые события:

1) запуск выполнения функций аудита;

2) попытка авторизации;

3) успешная авторизация;

4) неудачная авторизация;

5) действия, предпринимаемые в ответ на возможные нарушения безопасности;

6) чтение информации из записей аудита;

7) параметры, используемые при просмотре;

8) все модификации конфигурации аудита, происходящие во время сбора данных аудита;

9) разрешения на запрашиваемые информационные потоки;

10) все попытки импортировать данные пользователя;

11) все попытки экспортировать информацию;

12) все модификации режима выполнения функций;

13) все модификации значений данных;

14) использование функций управления;

15) модификация группы пользователей – исполнителей роли;

16) каждое использование прав, представленных ролью;

17) все модификации значений атрибутов безопасности;

18) обнаружение сбоя функций безопасности, если аудит возможен;

19) факт возникновения сбоя или прерывания обслуживания;

20) возобновление нормальной работы;

21) тип сбоя или прерывания обслуживания;

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

23) изменения внутреннего представления времени;

24) предоставление меток времени;

25) выполнение тестирования внешних сущностей и протоколирование результатов тестирования;

26) выполнение и результаты самотестирования функций безопасности;

27) успешное использование механизмов согласования данных функций безопасности;

28) использование механизмов согласования данных функций безопасности;

29) идентификация функций безопасности, данные которых интерпретируются;

30) обнаружение модифицированных данных функций безопасности;

31) любой сбой, обнаруженный функциями безопасности;

32) завершение выполнения функций аудита.

Журналы можно хранить локально или отправлять на удаленный сервер.

2.19.2. Настройка параметров отображения и ведения журналов

Для настройки параметров отображения и ведения журналов необходимо перейти в подраздел «Настройки журналирования» раздела «Журналы» (см. рис. 66).

Страница настройки параметров отображения журналов

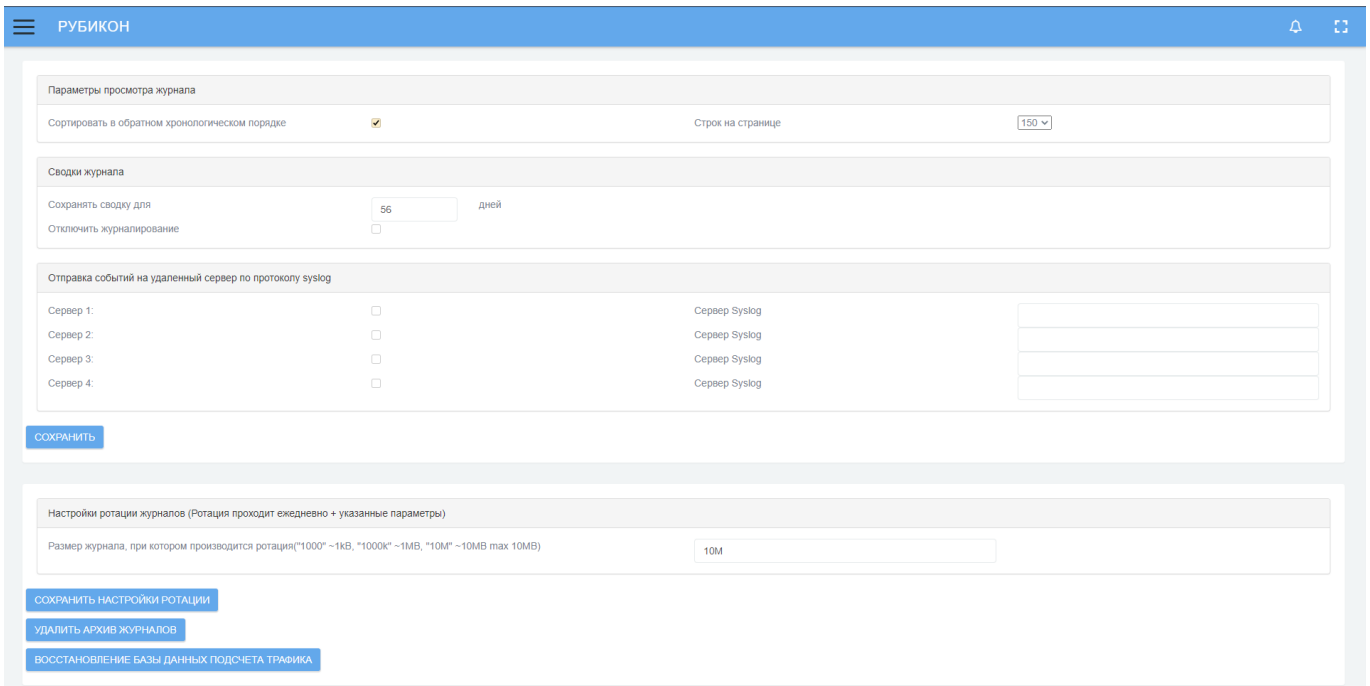


Рис. 66

Для настройки администратору доступны следующие поля:

1) «Параметры просмотра журнала»;

2) «Сводки журнала»;

3) «Запись удаленных событий»;

4) «Настройки ротации журнала».

2.19.2.1. Параметры просмотра журнала

Параметр «Сортировать 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.

2.19.2.2. Сводки журнала

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

Отметка напротив поля «Отключить журналирование» позволяет отключить запись всех системных событий и обнаруженных атак, а также отправку записей на удаленный сервер (если эта опция была включена ранее).

2.19.2.3. Запись удаленных событий

Параметр «Включено» предназначен для включения возможности журналирования событий на удаленном сервере.

Поле «Сервер Syslog» предназначено для указания адреса удаленного syslog-сервера.

2.19.2.4. Настройки ротации журналов

Для настройки ротации журналов необходимо выполнить следующие действия:

1) задать значение параметра «Количество файлов старых журналов, которые необходимо сохранить на устройстве» в текстовом поле;

2) задать значение параметра «Размер журнала, при котором производится ротация («1000» ~1kB, «1000k» ~1MB, «10M» ~10MB, max 10MB)» в текстовом поле;

3) перейти по ссылке «Посмотреть статистику ротированных журналов» для просмотра статистики;

4) для сохранения внесенных изменений в настройки параметров отображения и ведения журналов нажать кнопку «Сохранить».

2.19.3. Сервер времени

Для настройки сервера времени необходимо перейти в подраздел «Сервер времени» раздела «Службы» (см. рис. 67).

Подраздел «Сервер времени» раздела «Службы»

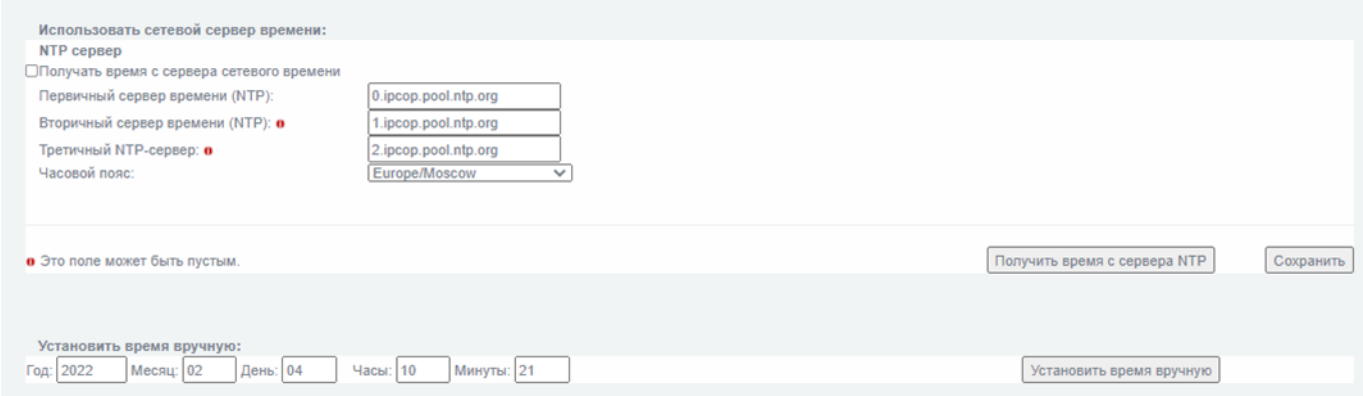


Рис. 67

В разделе следует указать сервер, который будет передавать временные метки для журналирования, для этого необходимо выполнить следующие действия:

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

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

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

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

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

6) нажать кнопку «Сохранить».

Для установки времени вручную необходимо перейти в секцию «Установить время вручную» (см. рис. 67).

2.19.4. Журнал межсетевого экрана

Для работы с журналом межсетевого экрана следует перейти в подраздел «Журнал межсетевого экрана» раздела «Журналы (см.рис. 68).

Подраздел «Журнал межсетевого экрана» раздел «Журналы»

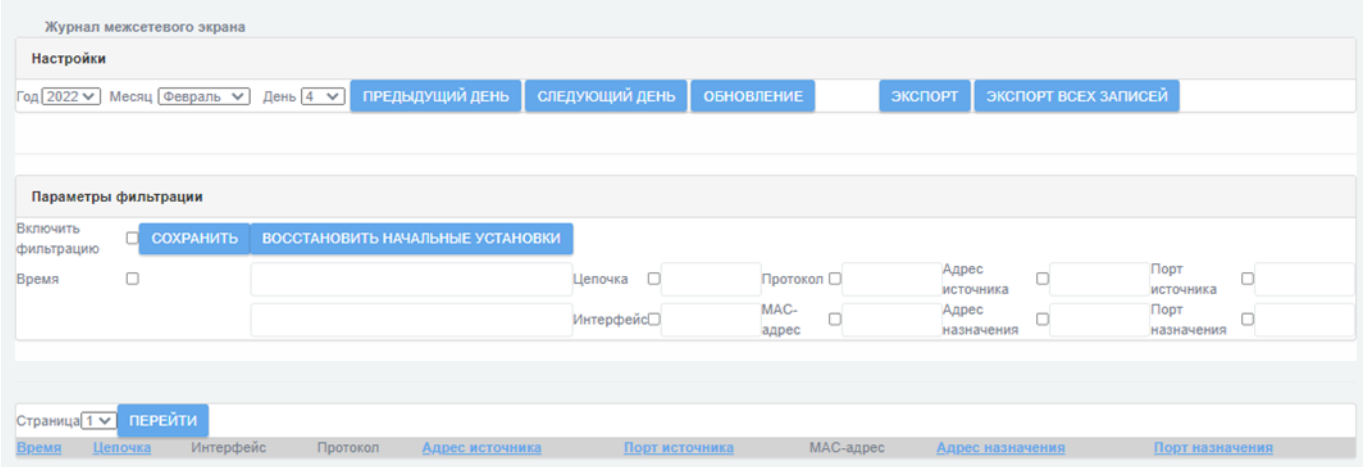


Рис. 68

На странице журнала МЭ предусмотрена возможность выборочного просмотра записей. Для просмотра информации журнала, отсортированной по какому-либо параметру, необходимо включить фильтрацию. Для этого следует отметить соответствующие пункты и нажать кнопку «Сохранить».

Загрузить события из журнала можно за период, равный одним суткам. Для этого необходимо указать день и месяц текущего года (см. рис. 68).

Имеется возможность ограничить промежуток времени, за который будут отображены события выбранных суток, путем выставления конкретных временных рамок (см. рис. 68).

Назначение кнопок на странице журнала межсетевого экрана представлены в таблице 8.

Таблица 8 – Назначение кнопок на странице журнала межсетевого экрана

Внешний вид кнопки	Описание назначения кнопки
СЛЕДУЮЩИЙ ДЕНЬ	предназначена для перехода к странице информации на один день раньше
ПРЕДЫДУЩИЙ ДЕНЬ	предназначена для перехода к странице информации на один день позже
ОБНОВЛЕНИЕ	предназначена для обновления информации для выбранного периода времени
ЭКСПОРТ	предназначена для экспорта отсортированных данных в текстовом виде
ЭКСПОРТ ВСЕХ ЗАПИСЕЙ	предназначена для экспорта всех данных в виде архива
ВОССТАНОВИТЬ НАЧАЛЬНЫЕ УСТАНОВКИ	предназначена для сброса всех параметров фильтров

Доступны следующие параметры для настройки фильтрации журнала МЭ:

1) время;

2) цепочка;

3) интерфейс;

4) протокол;

5) адрес источника;

6) порт источника;

7) MAC-адрес;

8) адрес назначения;

9) порт назначения.

Журналы МЭ сортируются по адресу источника, порту источника и MAC-адресу.

2.19.5. Журнал обнаружения атак

Для просмотра журнала обнаружения атак СОВ необходимо перейти в подраздел «Журнал обнаружения атак» раздела «Журналы» (см. рис. 69).

Подраздел «Журнал обнаружения атак» раздела «Журналы»

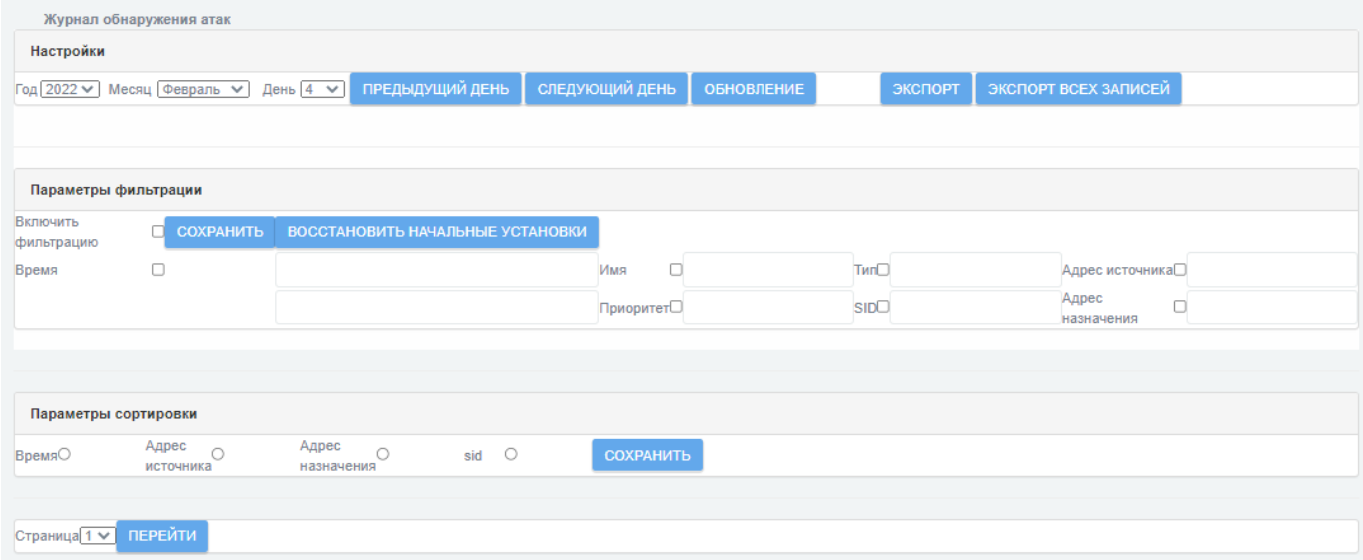


Рис. 69

На странице журнала обнаружения атак предусмотрена возможность выборочного просмотра записей. Для просмотра записей журнала, отсортированных по какому-либо параметру, необходимо включить сортировку. Для этого необходимо выбрать соответствующий параметр в поле «Параметры сортировки» и нажать кнопку «Сохранить».

Загрузить события из журнала можно по умолчанию за период, равный одним суткам. Для этого необходимо указать день и месяц текущего года (см. рис. 69).

Есть возможность выбрать промежуток времени, за который будут отображены события выбранных суток, путем выставления конкретных временных рамок (см. рис. 69).

Назначение кнопок на странице журнала обнаружения атак аналогичны представленным в таблице 8.

Доступны следующие параметры для настройки фильтрации журнала обнаружения атак:

1) имя;

2) приоритет;

3) тип;

4) SID (Security Identifier);

5) адрес источника;

6) адрес назначения.

2.19.6. Системный протокол

Для просмотра системного протокола необходимо перейти в подраздел «Системный протокол» раздела «Журналы» (см. рис. 70).

Подраздел «Системный протокол» раздела «Журналы»

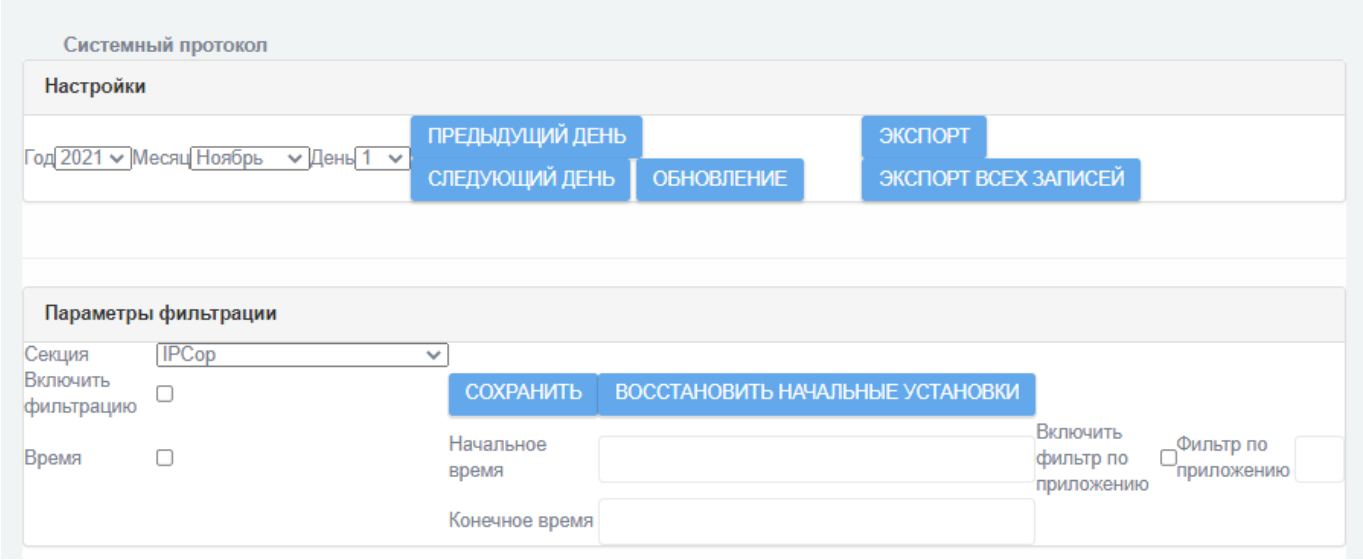


Рис. 70

Параметры, доступные для настройки фильтрации системного протокола представлены в таблице 9.

Таблица 9 – Параметры настройки фильтрации системного протокола

Параметр	Вид
Дата	Год 2021 Месяц Ноябрь День 1
Время	Начальное время Конечное время
Секция	Секция IPCop Включить фильтрацию Время IPCop Красный интерфейс DNS Сервер DHCP Cron Изменение конфигурации NTP Вход/Выход Ядро Настройка IPSec Доступ к устройству Ошибки чтения журналов Обновление копии Журнал изменения правил Журнал обращений к прокси Журнал запуска приложений Настройка правил СОВ Запись в журнал Страница 1 Время Секция 12:01:01 ipcop 12:01:01 ipcop 12:01:01 ipcop 12:01:01 ipcop 12:01:01 ipcop 12:01:01 ipcop 12:00:05 ipcop
Приложение	Включить фильтр по приложению ☐Фильтр по приложению

Для перехода к выбранной из выпадающего списка странице журнала также присутствует кнопка «Перейти».

Для применения фильтров по времени и по приложению, необходимо активировать соответствующие чекбоксы « ☑ » в них, а также в параметре «Включить фильтрацию». После выполнения данных действий следует подтвердить и сохранить новые настройки нажатием кнопки «Сохранить».

На рисунках 71 и 72 приведены примеры фильтрации системного протокола по секции «IPCop» и к секции «Доступ к устройству».

Пример фильтрации системного протокола по секции «IPCop»

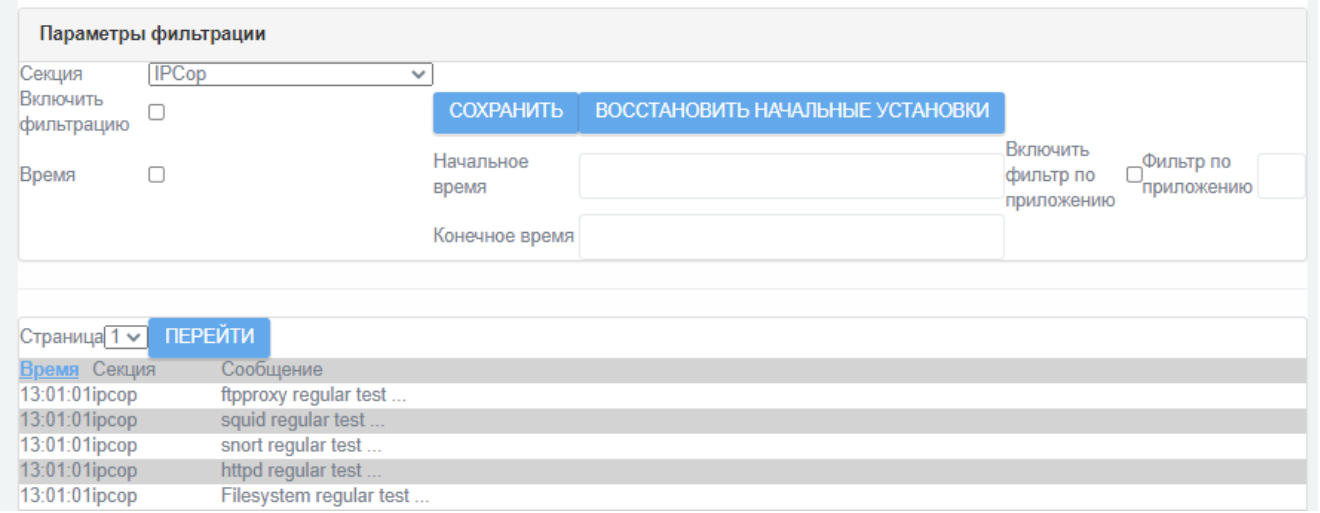


Рис. 71

Пример фильтрации системного протокола по секции «Доступ к устройству»

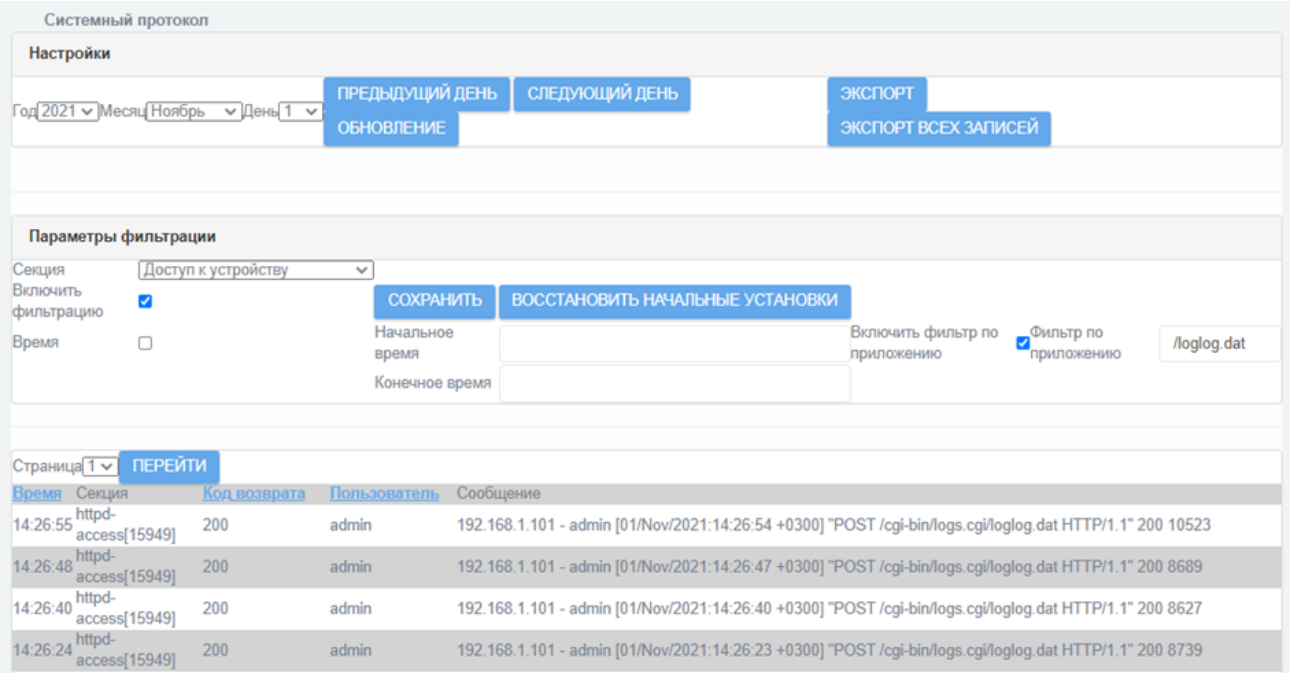


Рис. 72

2.19.7. Работа с уведомлениями

В случае попыток нарушения правил и при обнаружении критичных событий безопасности в шапке веб-интерфейса отображается соответствующее сообщение.

При нажатии на кнопку уведомлений «» выводится развернутая информация о возникшей проблеме в форме всплывающего окна (см. рис. 73).

Новые уведомления «Рубикон»

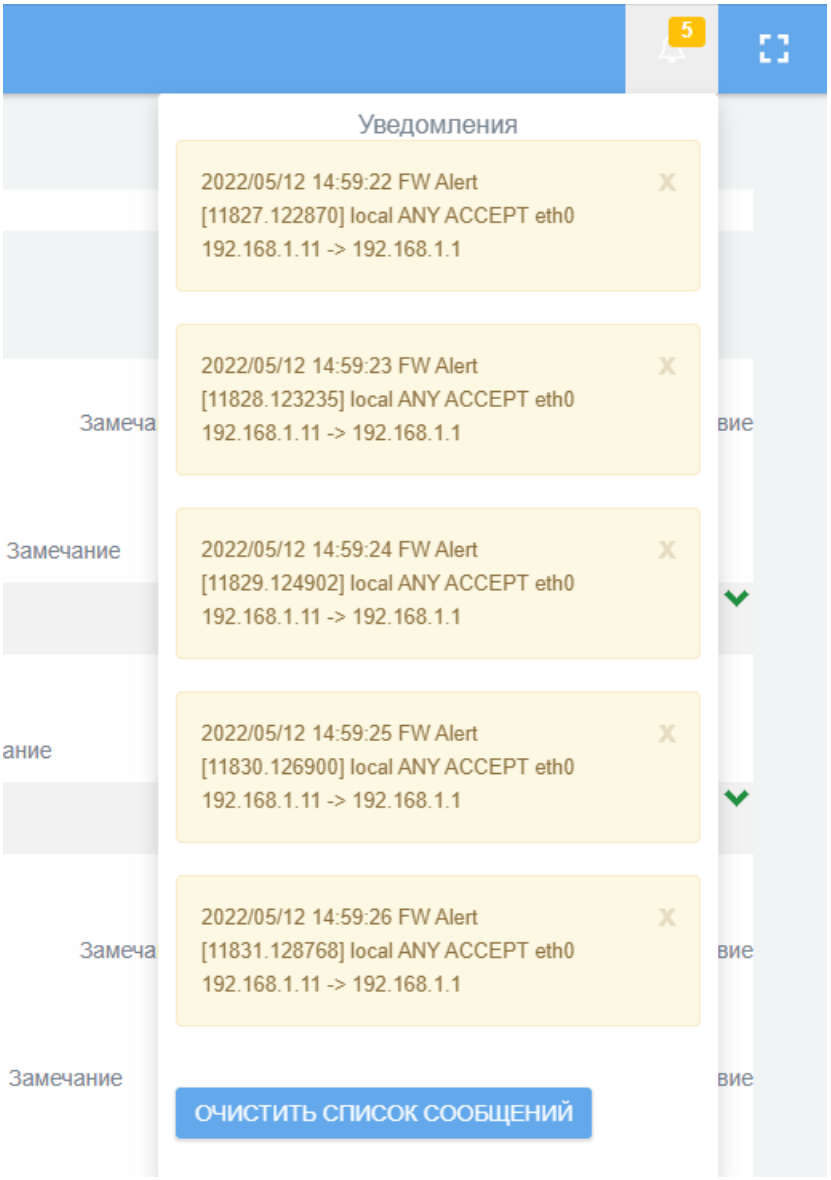


Рис. 73

Также «Рубикон» позволяет настроить уведомление администратора об обнаруженных атаках и нарушениях правил МЭ по электронной почте.

Для настройки уведомлений по электронной почте необходимо перейти в подраздел «Почта» раздела «Система» (см. рис. 74).

Подраздел «Почта» раздела «Система»

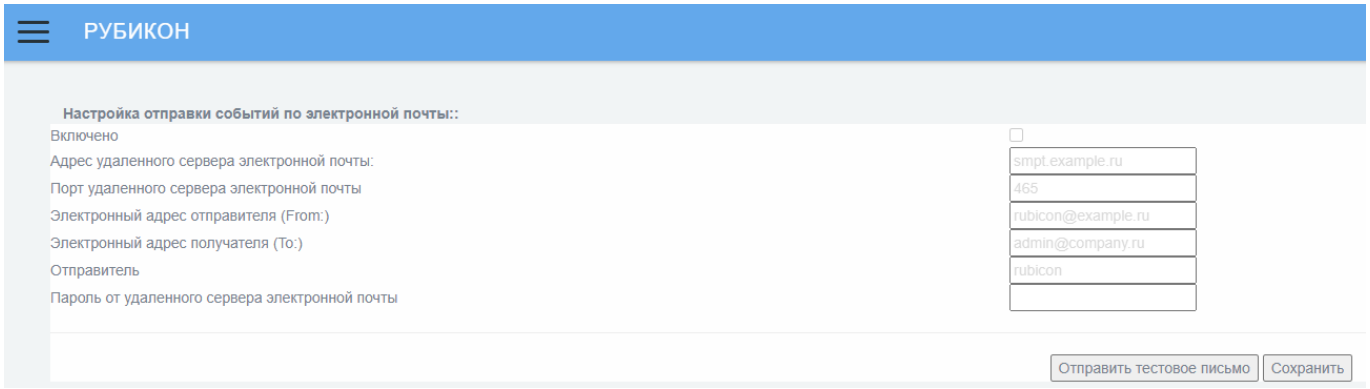


Рис. 74

Для получения оповещения на электронную почту также необходимо включить параметр «email alert» в правиле МЭ (см. рис. 75).

Поле включения параметра «email alert»

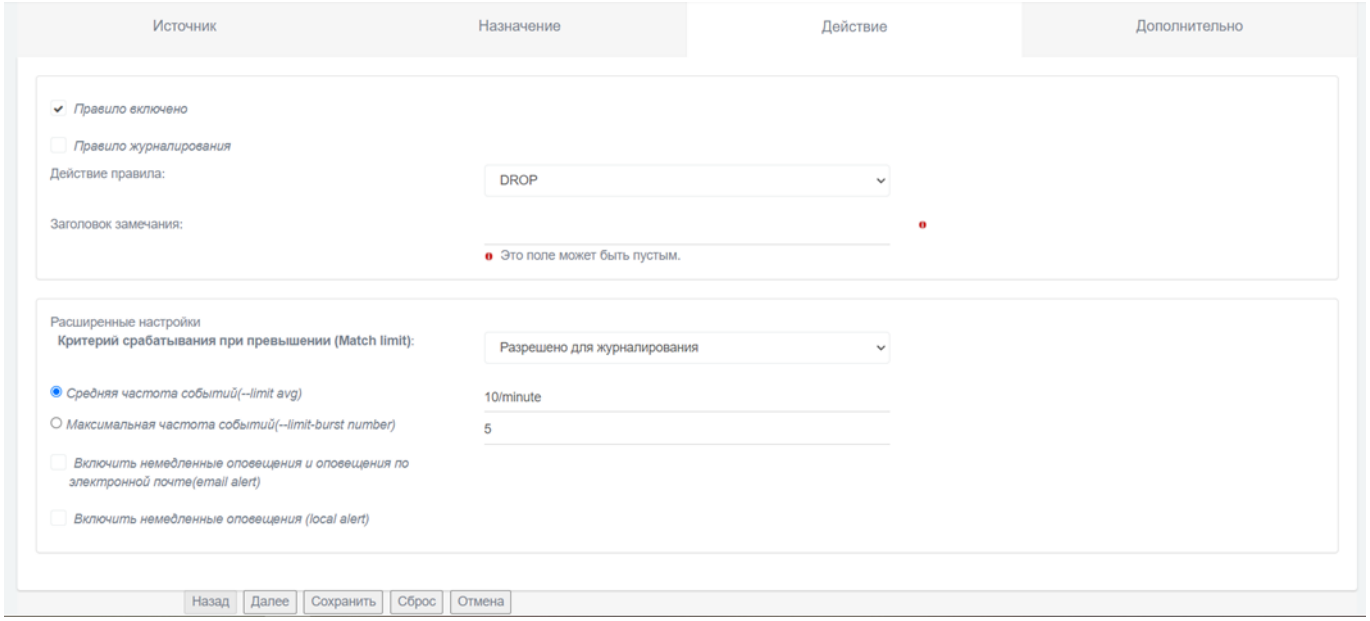


Рис. 75

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

2.20. Настройка автоматического восстановления

2.20.1. Действия системы в случае сбоя

Перейдите в подраздел «Автоматическое восстановление» раздел «Система» (см. рис. 76).

Подраздел «Автоматическое восстановление» раздела «Система»

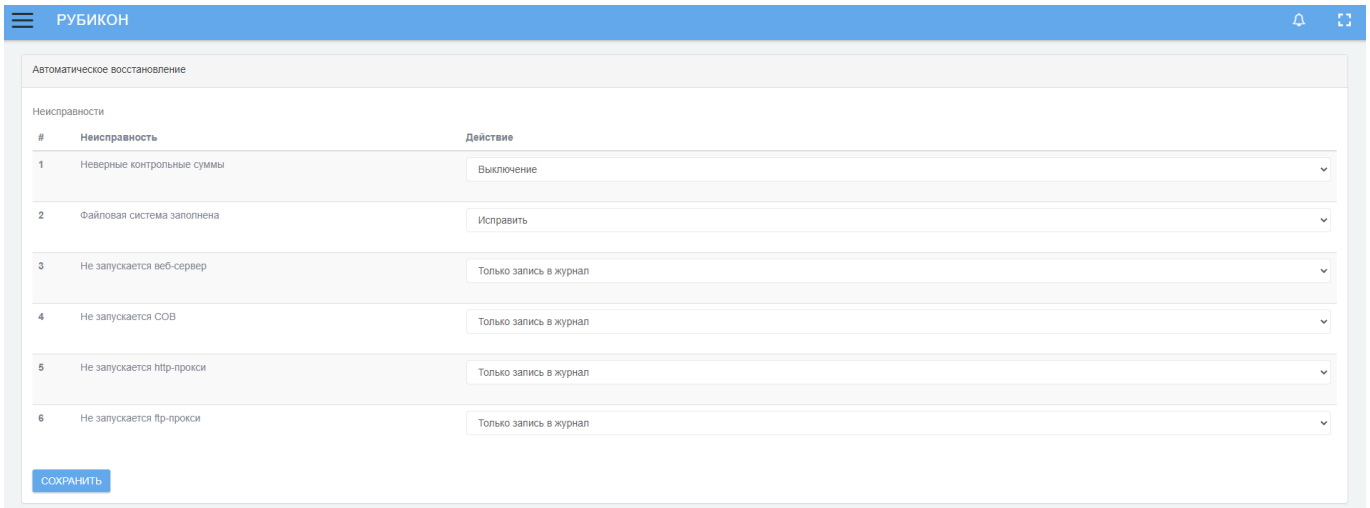


Рис. 76

В разделе представлено 6 типов сбоев, а 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:

— 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, если требуется изменить предлагаемые по умолчанию действия, то после внесения изменений необходимо нажать кнопку «Сохранить».

В случае сбоя в журнале аудита регистрируются соответствующие события:

1) «файл конфигурации системы автоматического восстановления не найден» – данная запись появляется при ошибке чтения файла конфигурации механизма автоматического восстановления;

2) «неверные контрольные суммы» – индикация ошибки;

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

4) «не удалось выключить Рубикон» – запись появляется при ошибке выключения «Рубикон»;

5) «критически мало места на жестком диске» – индикация ошибки, когда жесткий диск заполнен на 90 %;

6) «не удалось очистить /var/log/archives» – запись появляется в случае ошибки действия «Исправить» при неисправности «критически мало места на жестком диске»;

7) «директория /var/log/archive очищена, но места на жестком диске недостаточно для стабильной работы» – запись появляется в случае, если какой-то причине очистка не произошла и / или недостаточна и диск продолжает быть заполнен более чем на 90 %;

8) «не удалось перезапустить веб-сервер» – запись 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» – индикация ошибки;

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

14) «не удалось перезапустить ftp-прокси» – индикация ошибки.

Пример записи в журнале от механизма восстановления представлен на рисунке 77.

Запись в журнале от механизма восстановления

Страница 1 ПЕРЕЙТИ

Время	Секция	Сообщение
16:11:07	ipcop	checking checksum Контрольные суммы NOT OK
16:11:07	ipcop	Wrong checksum: //usr/lib/ipcop/modules/LogConfigPageClass.pm
16:10:54	ipcop	restartpingmonitor.pl:: stop
16:10:54	ipcop	rc.snort: barnyard2 command: /usr/bin/restartbarnyard2 eth0 eth1 eth2 eth3
16:01:03	ipcop	restartpingmonitor.pl:: stop
16:01:02	ipcop	rc.snort: barnyard2 command: /usr/bin/restartbarnyard2 eth0 eth1 eth2 eth3
16:01:01	ipcop	ftpproxy regular test ...
16:01:01	ipcop	squid regular test ...
16:01:01	ipcop	СОВ не запущена для интерфейса GREEN_2
16:01:01	ipcop	snort regular test ...
16:01:01	ipcop	Веб-сервер выключен
16:01:01	ipcop	httpd regular test ...
16:01:01	ipcop	Filesystem regular test ...

Рис. 77

2.20.2. Консоль восстановления

Консоль восстановления представляет из себя терминальный интерфейс взаимодействия с пользователем и предназначена для возможности восстановления функционирования «Рубикон» в случае неработоспособности или отсутствия доступа к веб-интерфейсу.

Для того чтобы запустить консоль восстановления выполните следующие действия:

1) установить связь с изделием при помощи консольного порта для подключения терминального оборудования или через видеовыход VGA с использованием клавиатуры, подключенной к разъему USB;

2) в открывшемся терминале ввести логин «**rescue**» (по умолчанию) и пароль пользователя «**rescue**» (по умолчанию).

После выполнения указанных шагов отобразятся строки, представленные на рисунке 78.

Вход в консоль «Рубикон»

```
Debian GNU/Linux 10 rubicon tty1

rubicon login: rescue
Password:
Last login: Tue Apr 19 10:18:18 MSK 2022 on tty1

########## Welcome to the Rubicon Rescue! ##########
#                                                  #
#       To continue enter the command: help        #
#                                                  #
####################################################
rescue@rubicon:~$
```

Рис. 78

Следует ввести команду `help` для того, чтобы посмотреть список команд с описанием (см. рис. 79).

Список консольных команд с описанием

```
rescue@rubicon:~$ help
cls             ->      clear screen
exit            ->      exit shell
help            ->      show this help message
readfile        ->      read file, see "readfile -h"
ifshow          ->      show interface info
listdir         ->      show contens of directory, see "listdir -h"
chpass          ->      change password to rescue console
ping            ->      default ping utility
powercontrol    ->      reboot or shutdown see powercontrol -h
restore_cfg     ->      restore backup configuration
                        use "listdir rescue backup" to get backups
rs_web_passwd   ->      reset WEB GUI login:password to defaults
traceroute      ->      default traceroute utility
identeth        ->      identify interfaces with LED blinking, see "identeth -h"
snortctl        ->      Turn on/off snort and download updates from preconfigured URL
tcpdump         ->      Confined tcpdump utility, see "tcpdump -h"
rescue@rubicon:~$ _
```

Рис. 79

Команда `cls` – команда очистки экрана.

Команда `exit` – выход из оболочки консоли восстановления.

Команда `help` – выводит список команд с описанием.

Утилита «readfile» – утилита просмотра файлов.

Для получения списка доступных файлов необходимо использовать команду `readfile -h`.

Команда `ifshow` – вывод списка подключенных к системе сетевых интерфейсов и их характеристик.

Команда `listdir` – вывод списка файлов выбранной директории, в том числе скрытые.

Для вывода списка доступных директорий необходимо использовать команду `listdir -h` (см. рис. 80).

Вывод списка доступных директорий

```
rescue@rubicon:~$ listdir -h
Usage:

listdir TYPE ALIAS
listdir -h
type: log alias: all path: /var/log
type: log alias: archives path: /var/log/archives
type: log alias: archives-db path: /var/log/archives/db
type: log alias: ntpstats path: /var/log/ntpstats
type: log alias: snort path: /var/log/snort
type: log alias: apache2 path: /var/log/apache2
type: log alias: apt path: /var/log/apt
type: log alias: cache path: /var/log/cache
type: log alias: squidguard path: /var/log/squidguard
type: log alias: httpd path: /var/log/httpd
type: log alias: dyndns path: /var/log/dyndns
type: log alias: installer path: /var/log/installer
type: log alias: installer-cdebconf path: /var/log/installer/cdebconf
type: log alias: suricata path: /var/log/suricata
type: log alias: quagga path: /var/log/quagga
type: log alias: updates path: /var/log/updates
type: log alias: tmp path: /var/log/tmp
```

Рис. 80

Команда `chpass` – команда для изменения пароля консоли восстановления.

Утилита «ping» – утилита «ping» по умолчанию

Утилита «powercontrol» – утилита управления выключением и перезагрузкой изделия. Параметры утилиты выводятся на экран (см. рис. 81) с помощью команды `powercontrol -h`.

Параметры утилиты «powercontrol»

```
rescue@rubicon:~$ powercontrol -h
Usage: powercontrol [OPTION] [warning message]

Options:
  --boot                reboot after shutdown
  --bootfs              reboot after shutdown and force fsck
  --down                halt or power off after shutdown
  -v, --verbose         be verbose
  --help                display this help and exit
rescue@rubicon:~$
```

Рис. 81

Утилита «restore_cfg» – позволяет восстановить конфигурацию «Рубикон». Сохраненные файлы конфигурации в формате «*.dat» можно найти с помощью команды `listdir rescue backup`.

Утилита «rs_web_passwd» – позволяет сбросить пароль администратора для web-интерфейса «Рубикон». Пароль по умолчанию: **radmin**.

Утилита «traceroute» – утилита определения маршрута до сетевого узла.

Утилита «identeth» – утилита идентификации сетевого адаптера. Отправляет команду мигания светодиода выбранного сетевого адаптера.

Утилита «snortctl» – утилита для включения / выключения СОВ и загрузки обновлений с предварительно настроенным URL источника обновлений.

Утилита «tcpdump» – позволяет перехватывать и анализировать сетевой трафик, проходящий через «Рубикон».

Основные назначения «tcpdump»:

1) отладка сетевых приложений;

2) отладка сети и сетевой конфигурации в целом.

Параметры утилиты выводятся на экран с помощью команды `tcpdump -h` (см. рис. 82).

Параметры утилиты «tcpdump»

```
rescue@rubicon:~$ tcpdump -h
Usage:
        tcpdump <OPTION1> <OPTION2> [OPTION3]
        OPTION1:
                -    - No argument (default).
                -q   - Print minimum information.
                -eq  - Displays MAC addresses + minimum info.
                -A   - Output the contents of the network packet in ASCII.
                -XX  - Output the contents of the network packet in HEX and ASCII.
                -v   - Displays detailed information (TTL; ID; total length of the header,
                       as well as its parameters; checksums of IP and ICMP headers).
                -vv  - Output even more complete information, mainly for NFS and SMB.
                -vvv - Display as detailed information as possible.
        OPTION2:
                interface - example: eth1.
        OPTION3:
                ip|arp|tcp|udp|icmp - Checks if a packet belongs to one of the specified
                                      protocols.
                host <IP>           - True if either the IPv4/v6 source or destination
                                      of the packet is host.
                port <PORT>         - True if either the source or destination port of
                                      the packet is port.
                shost <IP>          - Checks if the source address of an IP packet matches
                                      the specified value.
                sport <PORT>        - Checks if the source port of an port packet matches
                                      the specified value.
                dhost <IP>          - Checks if the destination address of an IP packet matches
                                      the specified value.
                dport <PORT>        - Checks if the destination port of an port packet matches
                                      the specified value.
rescue@rubicon:~$
```

Рис. 82

Утилита «tcpdump» использует три параметра:

1) OPTION1 – отвечает за полноту вывода информации;

2) OPTION2 – интерфейс (список интерфейсов отображается утилитой «ifshow»);

3) OPTION3 – отвечает за отображение сетевого трафика согласно настройкам пользователя.

Параметр «OPTION1» утилиты «tcpdump» представлен в таблице 10.

Таблица 10 – Параметр «OPTION1» утилиты «tcpdump»

Параметр	Значение
–	Без значения (по умолчанию)
-q	Выводит минимум информации. Имя протокола, указание источника и назначения сетевого пакета, порты и количество переданных данных
-eq	Отображение MAC-адресов + минимальной информации (см. опцию -q)

Параметр	Значение
-A	Вывод содержимого сетевых пакетов в кодировке ASCII
-XX	Вывод содержимого сетевых пакетов в HEX – формате и кодировке ASCII
-v	Вывод подробной информации (TTL; ID; общая длина заголовка, а также его параметры; отображает контрольные суммы IP и ICMP-заголовков)
-vv	Вывод еще более полной информации, в основном касается NFS и SMB
-vvv	Вывод максимально подробной информации

Параметр «OPTION3» утилиты «tcpdump» представлен в таблице 11.

Таблица 11 – Параметр «OPTION3» утилиты «tcpdump»

Параметр	Значение
ip|arp|tcp|udp|icmp	Позволяет отображать сетевой трафик для выбранного протокола передачи пакетов (один из перечисленных)
host <IP>	Позволяет отображать сетевой трафик, если поле «источник» пакета – host
port <PORT>	Позволяет отображать сетевой трафик, если пакет имеет порт-источник – port
shost <IP>	Позволяет отображать сетевой трафик, если IP-адрес источника пакета соответствует указанному значению
sport <PORT>	Позволяет отображать сетевой трафик, если порт источника пакета соответствует указанному значению
dhost <IP>	Позволяет отображать сетевой трафик, если IP-адрес назначения пакета соответствует указанному значению
dport <PORT>	Позволяет отображать сетевой трафик, если порт назначения пакета соответствует указанному значению

Для остановки работы утилиты нажмите сочетание клавиш «Ctrl» + «C».

2.21. Проверка целостности программного обеспечения

2.21.1. Контроль целостности исполняемых файлов и файлов конфигурации

Для контроля целостности исполняемых файлов и файлов конфигурации необходимо зайти в подраздел «Контрольные суммы» раздела «Состояние» и нажать кнопку «Проверить контрольные суммы».

При наличии ошибок контрольных сумм исполняемых файлов и файлов конфигурации, результаты проверки будут отображены в поле «Ошибки» (см. рис. 83).

Результаты верификации контрольных сумм файлов

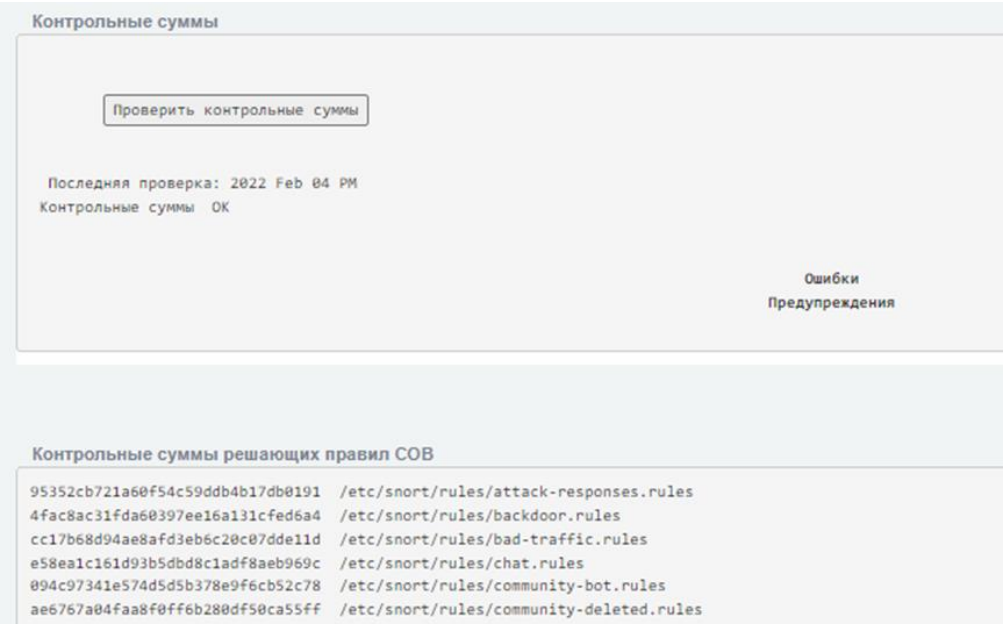


Рис. 83

2.22. Тестирование САВЗ

Тестирование САВЗ выполняется следующим образом:

1) перейти в подраздел «Прокси» раздела «Службы» (см. рис. 84);

2) активировать чекбокс «Включить взаимодействие с сервером ICAP»;

3) задать параметр «Адрес сервера ICAP». В текстовом поле необходимо ввести адрес средства антивирусной защиты. Он будет использован при осуществлении функции прокси;

4) нажать на кнопку «Тест ICAP-сервера».

После перехода по ссылке, будет выполнено тестирование САВЗ.

Тестирование САВЗ

Рис. 84

2.23. Процедуры обновления изделия

2.23.1. Общий порядок поставки обновлений

Доставка обновлений ПО «Рубикон-А» осуществляется с использованием сетевых протоколов передачи данных (загрузка с сервера предприятия-изготовителя «Рубикон» – АО «Научно-производственное объединение «Эшелон» (далее – «Разработчик»)).

Процедура выпуска обновлений ПО «Рубикон-А» состоит из следующих мероприятий:

1) анализ сообщений о недостатках и потребностей пользователей;

2) проектирование и разработка обновления продукта с учетом проведенного анализа;

3) тестирование обновленного ПО «Рубикон-А»;

4) оценка влияния обновлений ПО «Рубикон-А» на функции безопасности изделия «Рубикон»;

5) выпуск документа «Release Notes», содержащего информацию об обновлении, процедур его получения, установки и верификации;

6) при необходимости выпуск новой версии эксплуатационной документации;

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

8) отгрузка файлов на сервер обновлений;

9) предоставление обновлений пользователям для загрузки.

2.23.2. Процедуры и меры безопасности при доставке обновлений ПО «Рубикон-А»

Разработчик ведет учет пользователей изделий «Рубикон». Выполняется регистрация следующей информации: наименование организации, адрес организации, номер знака соответствия, контактная информация (содержит электронный почтовый адрес специалиста, обеспечивающего администрирование изделий «Рубикон»).

Уведомление пользователей о выпуске обновления ПО «Рубикон-А» 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.

2.23.2.1. Доставка и контроль целостности обновлений ПО

Обновления ПО «Рубикон-А» публикуются в закрытой части сервера разработчика. Доступ пользователей к закрытой части сервера осуществляется с использованием учетной записи и пароля, указанного в электронном почтовом сообщении, уведомляющем о наличии обновления. При публикации обновлений ПО «Рубикон-А» также публикуется файл сертификата его подписи. После получения обновления пользователь имеет возможность выполнить проверку его легитимности.

2.23.2.2. Установка и контроль правильности установки обновления

Для установки обновления ПО необходимо в основном меню зайти в раздел «Система» подраздел «Пакеты» (см. рис. 85).

Вход в раздел установки обновления ПО

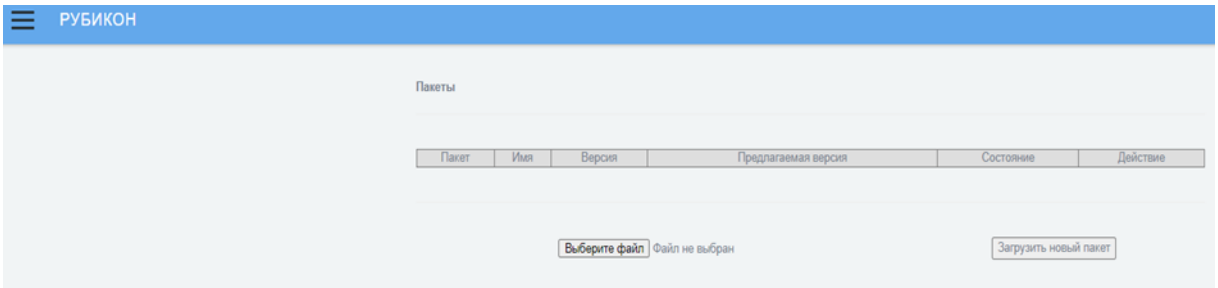


Рис. 85

С помощью кнопки «Выберите файл» добавить скачанный файл с обновленным ПО и нажать кнопку «Загрузить новый пакет» (см. рис. 86).

Загрузка пакета с обновлением ПО

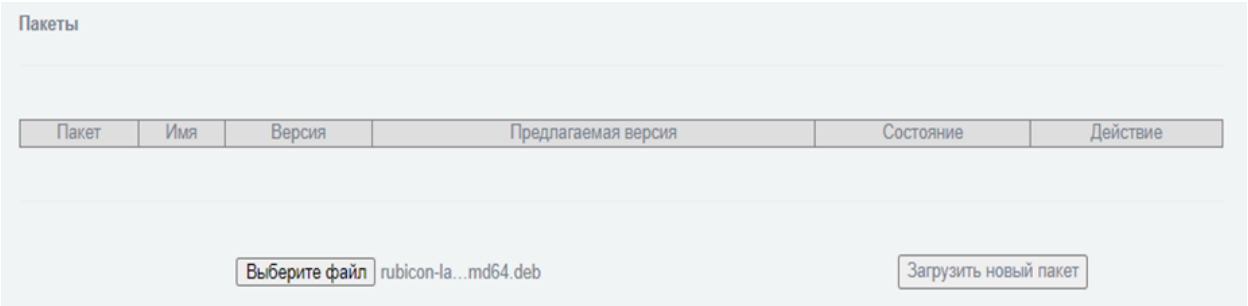


Рис. 86

Нажмите на кнопку «✔» в окне «Действие» для установки выбранного обновления ПО (см. рис. 87).

Установка обновления ПО

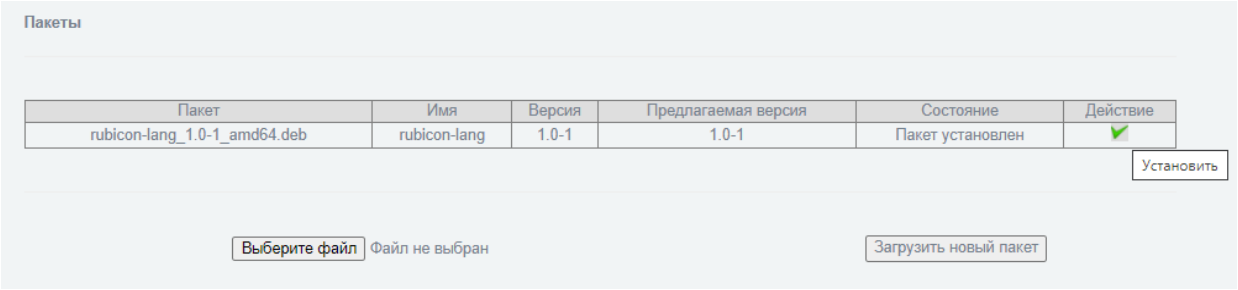


Рис. 87

Критерием правильности установки обновления ПО является доступность веб-интерфейса «Рубикон» и отображение информации об установленном обновлении ПО в окне «Состояние» подраздела «Пакеты» (см. рис. 88).

Примечание – Окно «Действие» при этом перестанет быть активным и отобразит символ «–», означающий что действия с данным пакетом не требуются.

Отображение информации об обновлении ПО

Пакеты

Пакет	Имя	Версия	Предлагаемая версия	Состояние	Действие
rubicon-lang_1.0-1_amd64.deb	rubicon-lang	1.0-1	1.0-1	Пакет установлен	-

Выберите файл Файл не выбран Загрузить новый пакет

Рис. 88

2.24. Настройки базы решающих правил

2.24.1. Загрузка новой базы решающих правил

Для настройки новой БРП необходимо загрузить в подразделе «Обнаружение атак» раздела «Система обнаружения вторжений» (см. рис. 89) непосредственно набор правил, полученный от разработчика через доверенный источник, предварительно проверив приложенный к нему файл сертификата подписи.

Настройка БРП. Импорт файлов в систему

Адрес для получения обновлений

Проверять метку доверенного времени при обновлении правил

Сохранить новые настройки СОВ

Применить текущие настройки СОВ

Прочитать последние записи в журнале установки правил

Набор правил Выберите файл Файл не выбран

Загрузить новый набор правил

Рис. 89

Процедуры обновления БРП указаны в разделе «Общий порядок поставки БРП» настоящего документа.

Опционально (по запросу пользователя) производитель может дополнительно к набору правил сгенерировать метку времени (см. рис. 90).

Настройка БРП. Импорт файлов с меткой времени в систему

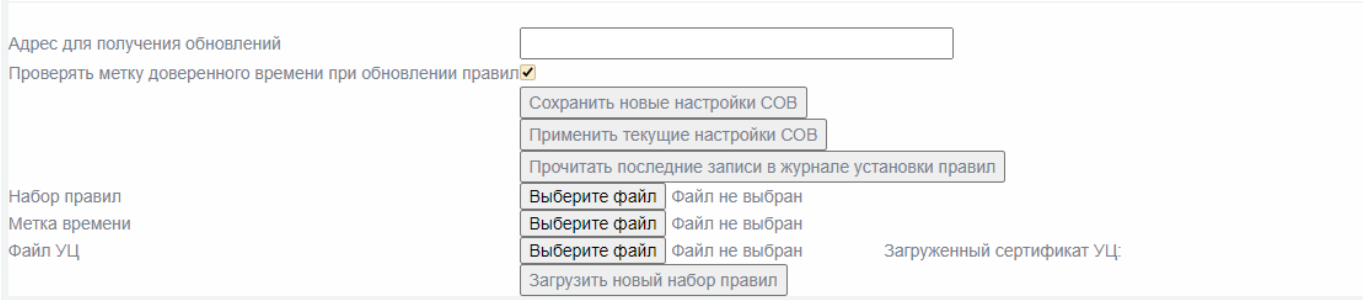


Рис. 90

В этом случае для загрузки БРП необходимо проставить чекбокс «Проверять метку доверенного времени при обновлении правил» и загрузить следующие файлы:

1) метку времени в формате tsr, полученную от сервера 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.

2) непосредственно набор правил;

3) файл УЦ: сертификат, выданный УЦ серверу доверенного времени.

После того как все файлы выбраны, следует нажать кнопку «Загрузить новый набор правил». Если хотя бы один из требуемых файлов не был загружен, после нажатия кнопки «Загрузить новый набор правил» администратор увидит сообщение об ошибке (см. рис. 91).

Сообщение об ошибке

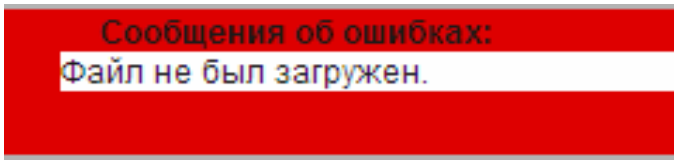


Рис. 91

После загрузки происходит проверка:

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

2) актуальности сертификата сервера доверенного времени, извлекаемого из метки времени.

В случае успешного прохождения проверки с помощью сертификата сервера доверенного времени проверяется электронная подпись метки времени. Если подпись верна, происходит загрузка правил в хранилище СОВ и удаление временных файлов.

Пользователю выводится сообщение: «Предупреждение: Используйте кнопку «Применить сейчас», чтобы сохранить изменения в настройках» (см. рис. 92).

Следует нажать кнопку «Применить сейчас», это позволит обновить правила и перезапустится СОВ на выбранных интерфейсах.

Сообщение «Предупреждение»

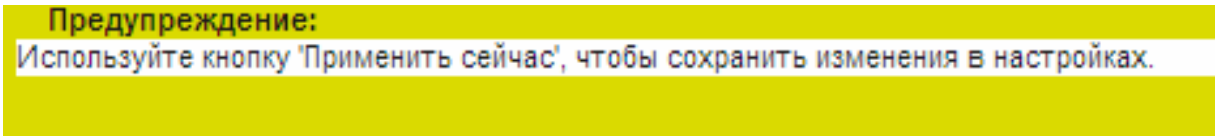


Рис. 92

После успешного перезапуска, а также по нажатию кнопки «Прочитать последние записи в журнале установки правил», отображается информация, представленная на рисунке 93.

Информация об установленных обновлениях

Рис. 93

Результат проверки «done» означает успешное прохождение проверки. Можно также увидеть сведения о загружаемом наборе правил.

Справа от кнопки «Применить» отображается дата последнего изменения правил. Также отображаются сведения о результатах проверки метки времени.

При неуспешной проверке будет выведено сообщение об ошибке (см. рис. 94).

Сообщение об ошибке при неуспешной проверке

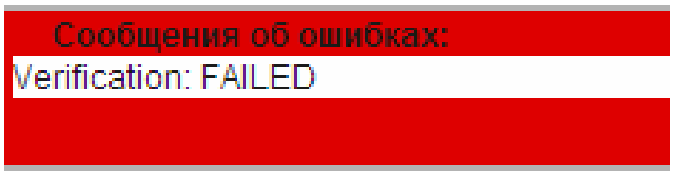


Рис. 94

Данное сообщение может означать, что:

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

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

3) сертификат сервера доверенного времени неактуален.

2.24.2. Настройка решающих правил

2.24.2.1. Включение/отключение решающих правил

Для включения (отключения) выбранного правила с помощью межсетевого экрана активируйте чекбокс для включения (деактивируйте для отключения) напротив названия правила в блоке «Список правил СОВ» подраздела «Настройка правил СОВ» раздела «Система Обнаружения Вторжений» (см. рис. 95).

Блок «Список правил СОВ» подраздела «Настройка правил СОВ»

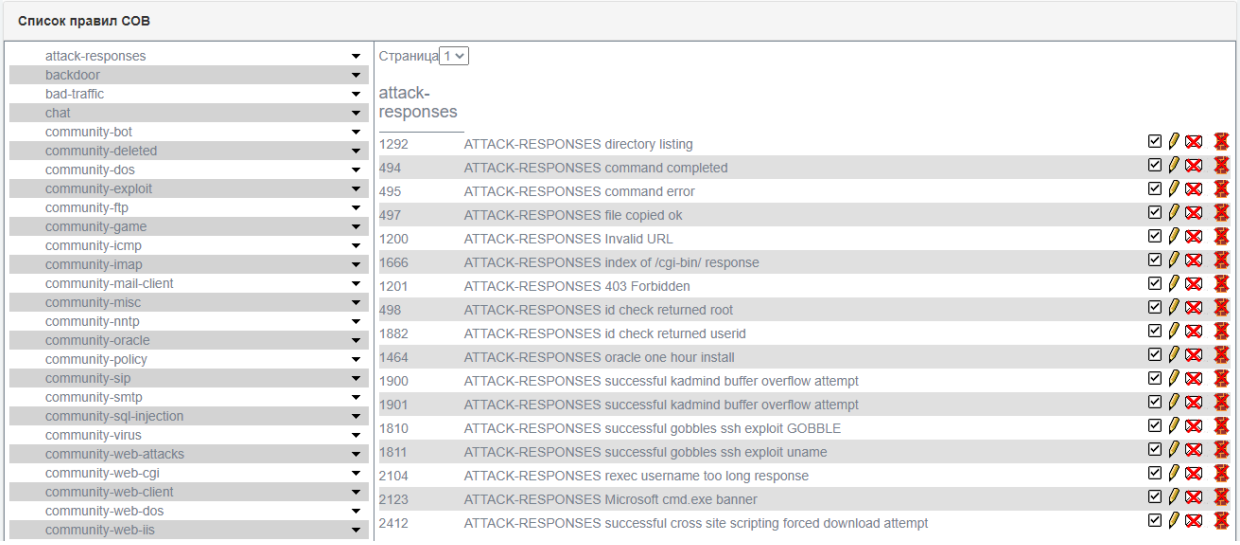


Рис. 95

В левом информационном поле содержится информация о группах правил СОВ. Пользовательские правила СОВ будут находиться в группе с названием «rubicon».

Под блоком «Список правил СОВ» представлена легенда (см. рис. 96) всех возможных действий с правилами в подразделе «Настройка правил СОВ».

Легенда подраздела «Настройка правил СОВ»

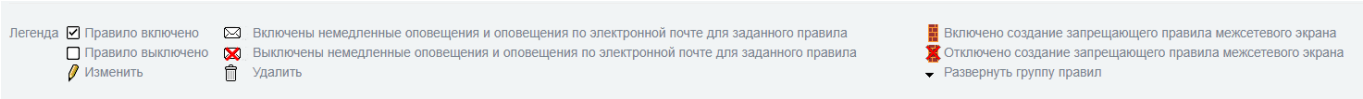


Рис. 96

2.24.2.2. Включение/отключение уведомления по электронной почте для каждого правила

Для включения (отключения) уведомления администратора по электронной почте о срабатывании определенного решающего правила нажмите кнопку « » для включения (нажмите кнопку « » для отключения) напротив названия правила в блоке «Список правил СОВ» подраздела «Настройка правил СОВ» раздела «Система Обнаружения Вторжений».

Например, на рисунке 95 отключены уведомления по электронной почте для всех правил.

2.24.2.3. Включение/отключение блокирования атакующего IP-адреса с помощью межсетевого экрана

Для включения (отключения) блокирования атакующего IP-адреса с помощью МЭ нажмите кнопку « » для включения (нажмите кнопку « » для отключения) напротив названия правила в блоке «Список правил СОВ» подраздела «Настройка правил СОВ» раздела «Система Обнаружения Вторжений».

В случае включенной возможности блокирования атакующего IP-адреса с помощью МЭ и обнаружения выбранной атаки в сетевом пакете, в МЭ будет создано правило блокирования соединений с IP-адресом источника и назначения, совпадающим с IP-адресом источника и назначения пакета, в котором обнаружена сигнатура атаки.

2.24.2.4. Включение/отключение блокирования атаки с помощью межсетевого экрана

Для включения (отключения) блокирования атаки с помощью межсетевого экрана необходимо выполнить следующие действия:

1) в подразделе «Правила межсетевого экрана» раздела «Межсетевой экран» необходимо создать правило МЭ для отправки сетевого пакета в СОВ;

2) созданное правило МЭ (см. рис. 97) необходимо проверить в подразделе «NFTables» раздела «Состояние» (см. рис. 98);

3) далее включить СОВ в режиме предотвращение атак в подразделе «Обнаружение атак» раздела «Система Обнаружения Вторжений» (см. рис. 99).

Созданное правило МЭ

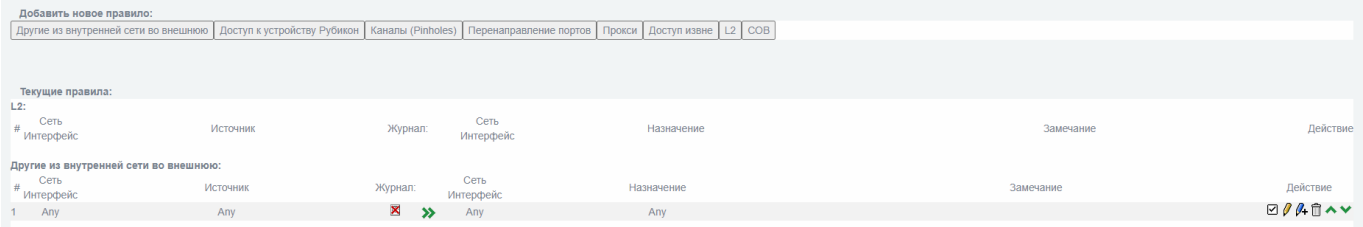


Рис. 97

Проверка созданного правила МЭ в подразделе «NFTables» раздела «Состояние»

Рис. 98

Включение СОВ в режиме предотвращение атак

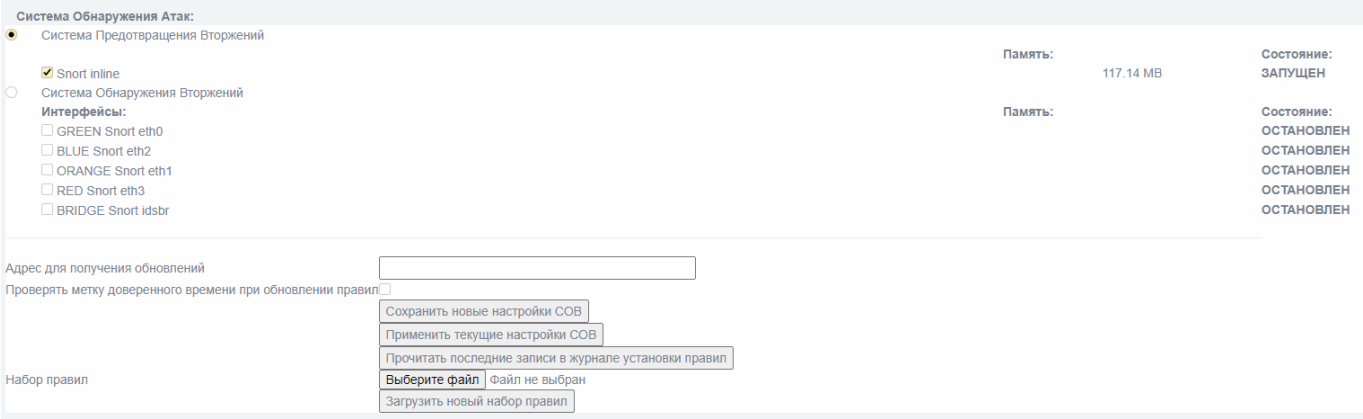


Рис. 99

2.25. Процедуры обновления БРП

2.25.1. 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_a_rules.tar.gz.

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

2.25.2. Локализация и противодействие новому типу вторжения (атаки)

2.25.2.1. Фиксация появления нового типа вторжения

Обновление БРП является важным аспектом эффективного функционирования системы обнаружения вторжения.

Поставщик БРП осуществляет 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.

2.25.2.2. Предоставление обновления покупателям

Процедура предоставления покупателям обновлений БРП в общем случае выполняется 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:

— формирование архива с БРП;

— формирование файла сертификата подписи.

7) отгрузка файлов на сервер обновлений;

8) предоставление обновлений БРП клиентам для загрузки.

2.25.3. Процедуры и меры безопасности при доставке обновлений БРП

2.25.3.1. Оповещение пользователей изделия «Рубикон» об обновлении БРП

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.

2.25.3.2. Доставка и контроль целостности БРП на стороне пользователя изделия «Рубикон»

Обновления БРП, успешно прошедшие контроль влияния на безопасность изделия «Рубикон», публикуются в закрытой части сервера разработчика. Доступ пользователей к закрытой части сервера осуществляется с использованием учетной записи и пароля, указанного в электронном почтовом сообщении, уведомляющем о наличии обновления. При публикации обновления БРП публикуется файл подписи. После получение обновления БРП пользователь имеет возможность выполнить контроль его легитимности.

2.25.4. Установка и контроль правильности установки обновления БРП

Для установки обновлений БРП зайдите в раздел «Система Обнаружения Вторжений» подраздел «Обнаружение Атак».

Далее нажмите кнопку «Выберите файл» и укажите скачанный файл с обновлениями БРП. Название файла появится справа от кнопки (см. рис. 100).

Нажмите кнопку «Загрузить новый набор правил».

Загрузка файла с обновлениями БРП

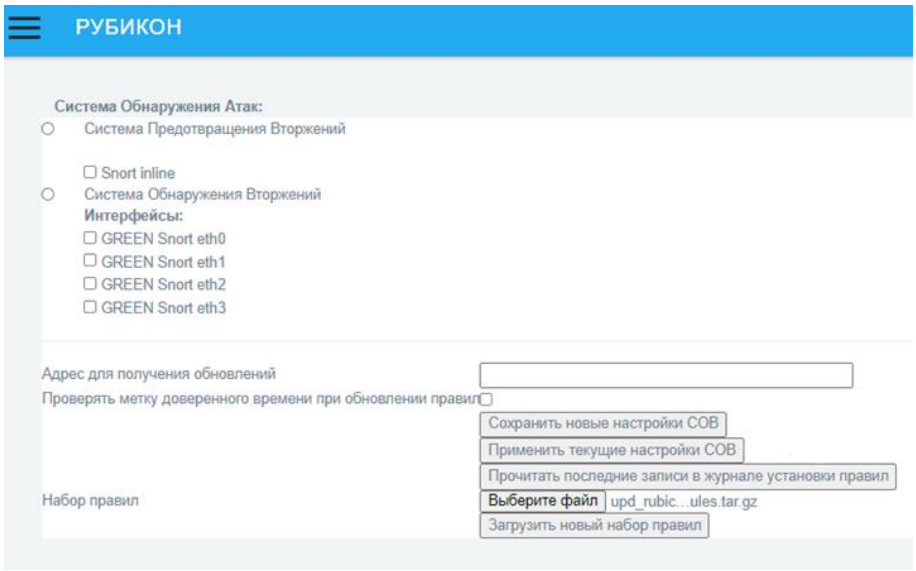


Рис. 100

Нажмите кнопку «Применить текущие настройки СОВ» для выполнения обновления БРП. После выполнения обновления справа от этой кнопки появится дата и время выполнения обновления БРП и откроется окно журнала с записью о выполнении обновления БРП (см. рис. 101).

Отчет о выполнении обновления БРП

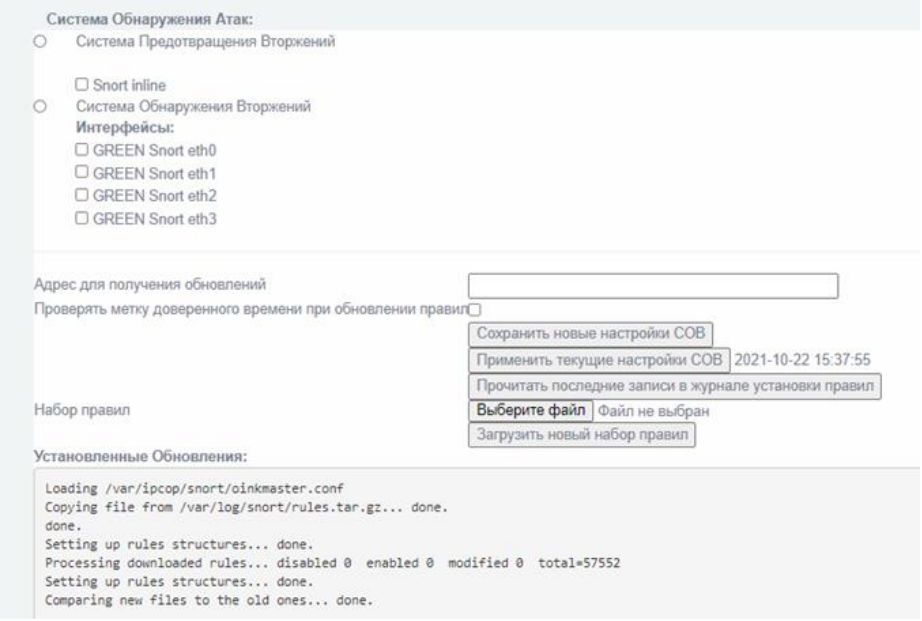


Рис. 101

Правильность обновления БРП контролируется по записям журнала установки правил. Вы можете их посмотреть в любой момент, нажав соответствующую кнопку в интерфейсе.

2.26. Процедура переустановки ПО

В случае невозможности решить проблемы с работоспособностью изделия с помощью консоли восстановления или функции резервного копирования, необходимо выполнить полную переустановку ПО «Рубикон-А». При этом вся информация, накопленная за время работы ПО, будет безвозвратно уничтожена.

Для переустановки ПО «Рубикон-А» выполните следующие шаги:

1) при наличии на аппаратной платформе видеовыхода (VGA, DVI, HDMI и так далее) подключите устройство отображения видеоинформации к соответствующему разъему. При его отсутствии, вывод псевдографики осуществляется через COM-порт и терминальную программу;

2) подключите к аппаратной платформе алфавитно-цифровую клавиатуру;

3) подключите к разъему накопитель данных с установочным дистрибутивом ПО «Рубикон-А» из состава комплекта поставки;

4) подайте электропитание на аппаратную платформу;

5) при включении аппаратной платформы зайдите в меню выбора загрузочного устройства и выберите загрузку с накопителя данных;

6) далее установка ПО «Рубикон-А» начнется в автоматическом режиме;

7) по окончании установки аппаратная платформа перезагрузится;

Примечание – В момент перезагрузки аппаратной платформы необходимо извлечь накопитель данных из аппаратной платформы до запуска ПО «Рубикон-А (в момент инициализации BIOS)».

8) дождаться полной загрузки аппаратной платформы.

После успешного запуска необходимо заново произвести первичную настройку ПО «Рубикон-А».

3. ТЕКСТОВЫЕ СООБЩЕНИЯ

В настоящем разделе описываются типовые сообщения при возникновении аварийных ситуаций.

Большинство аварийных ситуаций можно разделить на две группы:

1) ситуации, связанные с ошибками конфигурации:

— некорректные сетевые настройки;

— некорректные настройки фильтрации пакетов;

— некорректные правила СОВ.

2) ситуации, связанные с ошибками оборудования:

— выход из строя сетевых контроллеров;

— выход из строя дисковых накопителей.

При некорректном заполнении полей «Рубикон» отобразит сообщение об ошибке, как представлено на рисунке 102.

Сообщение об ошибке появляется в верхней части экрана и содержит в себе текст описания возникшей проблемы.

Сообщение об ошибке

Рис. 102

В большинстве случаев неполадки устраняются переконфигурированием изделия, восстановлением из ранее сделанной резервной копии или переустановкой ПО с использованием установочного дистрибутива.

Возникающие в процессе работы сообщения об ошибках будут записаны в журнале событий «Системный протокол».

Пример отображения возникшего сообщения об ошибке (см. рис. 103) в журнале событий «Системный протокол» представлен на рисунке 104.

Пример возникшего сообщения об ошибке

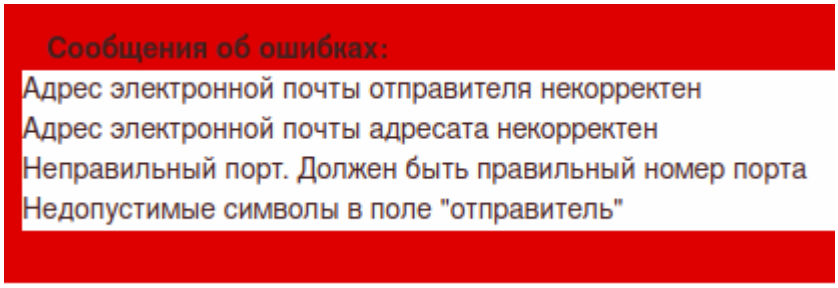


Рис. 103

Пример записи в журнале событий «Системный протокол»

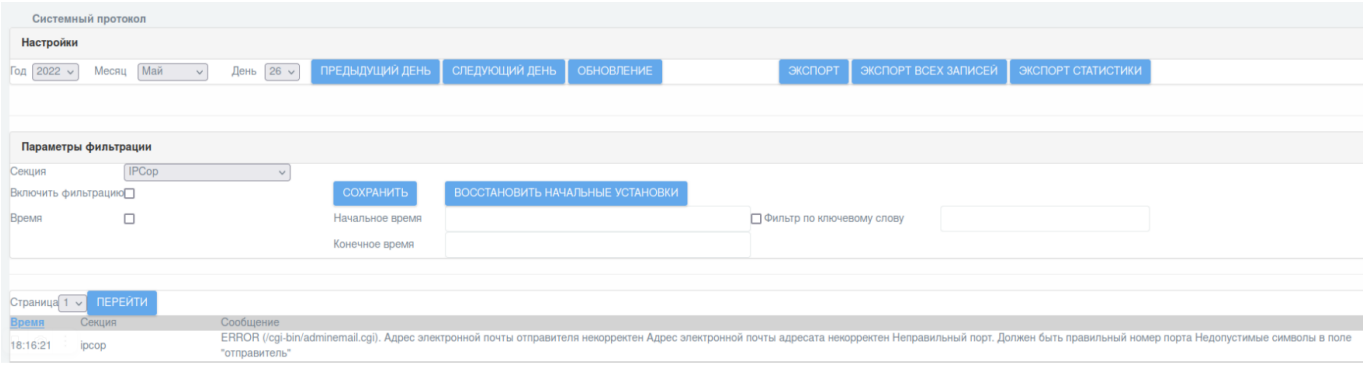


Рис. 104

Описание всех возвращаемых сообщений об ошибках и предупреждений в интерфейсе ПО «Рубикон-А» представлены в приложении 2.

ПРИЛОЖЕНИЕ 1.

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

DHCP	–	(*англ. Dynamic Host Configuration Protocol*) – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
DMZ	–	демилитаризованная зона. Сегмент сети, предназначенный для размещения сетевых устройств, взаимодействующих с внешними сетями
ICMP	–	(*англ. Internet Control Message Protocol* – протокол межсетевых управляющих сообщений) – сетевой протокол, входящий в стек протоколов TCP/IP
IP	–	*(англ. Internet Protocol Address)* – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP
SID	–	*(англ. Security Identifier)* – структура данных переменной длины, которая идентифицирует учетную запись пользователя, группы, службы, домена или компьютера (в Windows на базе технологии NT (NT4, 2000, XP, 2003, Vista,7,8,10)
VPN	–	*(англ. Virtual Private Network – виртуальная частная сеть)* – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет)
АРМ	–	автоматизированное рабочее место
БРП	–	база решающих правил
ИС	–	информационная система
МЭ	–	межсетевой экран
ОС	–	операционная система
ПО	–	программное обеспечение
САВЗ	–	средства антивирусной защиты
СЗИ	–	средство защиты информации
СОВ	–	система обнаружения вторжений
ЭВМ	–	электронно-вычислительная машина

ПРИЛОЖЕНИЕ 2.

ПЕРЕЧЕНЬ СООБЩЕНИЙ ОБ ОШИБКАХ И ПРЕДУПРЕЖДЕНИЙ

Описание всех возвращаемых сообщений об ошибках и предупреждений в интерфейсе ПО «Рубикон-А» представлены в таблице П2. 1.

Таблица П2. 1 – Перечень сообщений об ошибках и предупреждений

Страница	Тип	Текст сообщения	Примечание
Адреса	Ошибка	Не введено имя сети	Нужно присвоить задаваемой сети произвольное имя
		Имя может содержать только английские буквы и цифры	В данное поле нужно вводить только английские буквы и цифры
		Неправильный IP-адрес	Нужно ввести корректный IP-адрес
		Некорректная маска	Нужно ввести корректную маску подсети
		Этот адрес используется в правилах перенаправления портов	Само по себе не является ошибкой, обратить внимание на уточнение
		В качестве пункта назначения в правилах для переадресации портов разрешены только IP-адреса узла (а не IP-адреса подсетей)	Нужно задать IP-адрес узла, а не подсети
		Неверный MAC-адрес	Нужно ввести корректный MAC-адрес
		Этот адрес используется как направление в правилах межсетевого экрана	Само по себе не является ошибкой, обратить внимание на уточнение
		MAC-адрес не может использоваться как адрес назначения	MAC-адрес нельзя использовать в качестве адреса назначения
		Не выбран тип адреса. Выберите тип адреса	Нужно выбрать тип адреса
		Это имя уже используется, пожалуйста, выберите другое	Задайте другое имя
Группы адресов	Ошибка	Хотя бы один адрес должен быть разрешен в группе	Нужно разрешить в группе хотя бы один адрес
		Имя группы адресов уже существует	Нужно указать другое имя

Страница	Тип	Текст сообщения	Примечание
Группы адресов	Ошибка	Имя группы адресов не может быть пустым	Нужно ввести произвольное имя
		Имя может содержать только английские буквы и цифры	В данное поле нужно вводить только английские буквы и цифры
		Не выбрана группа адресов, пожалуйста, выберите	Нужно выбрать группу адресов
		Не выбран тип Группы адресов, пожалуйста, выберите	Нужно выбрать тип группы адресов
		Такого дополнительного адреса не существует	Укажите существующий дополнительный адрес
		Такого дефолтного адреса не существует	Укажите существующий дефолтный адрес
		Неверный адрес	Нужно указать корректный адрес
		Выбранный адрес уже входит в выбранную группу	Нужно выбрать другой адрес
		Не выбран тип адреса. Выберите тип адреса	Нужно выбрать тип адреса
Почта	Ошибка	Адрес электронной почты отправителя некорректен	Нужно указать корректный адрес электронной почты
		Адрес электронной почты адресата некорректен	Нужно указать корректный адрес электронной почты
		Неправильный порт. Должен быть правильный номер порта	Нужно указать корректный номер порта
		Недопустимые символы в поле \""отправитель\""	Значение поля отправителя должно содержать только символы из множества [-_a-zA-Z0-9 @.]
		Невозможно отправить тестовое письмо	Произошла ошибка при отправке тестового письма
	Предупреждение	Тестовое письмо успешно отправлено	Тестовое письмо успешно отправлено
Псевдонимы	Ошибка	Некорректное имя псевдонима	Неизвестная ошибка
		Неправильный IP-адрес	Нужно ввести корректный IP-адрес
		Неверная маска	Нужно ввести корректную маску подсети

Страница	Тип	Текст сообщения	Примечание
Псевдонимы	Ошибка	Неверные параметры	В переданных параметрах присутствует ошибка. Измените параметры и попробуйте снова
		Некорректное имя интерфейса	Нужно указать корректное имя интерфейса
		Неверное имя	Нужно указать корректное значение имени
		Такой IP-адрес уже существует (красный интерфейс)	Нужно указать другой IP-адрес, не дублирующий IP-адрес красного интерфейса
		Такой IP-адрес уже существует	Нужно указать другой IP-адрес
		Это имя уже используется, пожалуйста, выберите другое	Нужно выбрать другое имя
Конфигурация ARP	Ошибка	Неверный ввод	Нужно ввести корректное значение
		Неправильный IP-адрес	Нужно ввести корректный IP-адрес
		Неверный MAC адрес	Нужно ввести корректный MAC-адрес
		Невозможно создать запись «ARP»	Произошла ошибка при создании записи «ARP»
Резервное копирование	Ошибка	Ошибка создания файла ключа	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка добавления файлов в архив	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка сжатия архива	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка шифрования архива	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Неверный пароль	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования

Страница	Тип	Текст сообщения	Примечание
Резервное копирование	Ошибка	Ошибка создания архива	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка при расшифровке архива	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Поврежденный зашифрованный архив	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка при распаковке архива	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Зашифрованный архив не найден	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка при восстановлении архива	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Пароль не установлен	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Пароль содержит запрещенные символы	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Пароли должны быть хотя бы 6 символов в длину	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Описание разрешено максимум 80 символов	Нужно добавить описание максимум на 80 символов
		Недопустимые символы в --Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Данные не были загружены	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования

Страница	Тип	Текст сообщения	Примечание
Резервное копирование	Ошибка	Ошибка сохранения	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка в имени бэкапа	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка исходной версии конвертора	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка выходной версии конвертора	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка количества параметров файла конфигурации замены	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка исходного параметра файла конфигурации замены	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка выходного параметра файла конфигурации замены	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка директории файла конфигурации замены	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка ключа файла конфигурации замены	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка количества параметров файла конфигурации добавления	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка исходного параметра файла конфигурации добавления	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка директории файла конфигурации добавления	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования

Страница	Тип	Текст сообщения	Примечание
Резервное копирование	Ошибка	Ошибка директории файла конфигурации исключений	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка при распаковке архива	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Ошибка конвертора	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
		Требуется ключ резервной копии для восстановления	Внутренняя ошибка. Ошибка в процедуре работы с файлами резервного копирования
	Предупреждение	После восстановления архива конфигурации требуется перезагрузка	Для применения параметров нужно выполнить перезагрузку
BGP	Ошибка	Ошибка в передаваемых CGI параметрах	Один или несколько переданных параметров некорректны
		Неверный идентификатор маршрутизатора	В качестве идентификатора следует использовать IP-адрес
		Неверная область	Нужно указать целое положительное число
		Неправильный параметр сети	Нужно ввести корректный параметр сети
		Неверный идентификатор соседа	В качестве идентификатора следует использовать IP-адрес
		Неверная удаленная автономная система	Нужно указать целое положительное число
		Неверный вес	Укажите корректный вес в виде целого числа
		Неверный идентификатор соседа	В качестве идентификатора следует использовать IP-адрес
Объединение интерфейсов	Ошибка	Имя интерфейса уже существует	Нужно указать отличное от существующих имя
		Невозможно добавить административный интерфейс	Не следует использовать административный интерфейс
		Неправильный IP-адрес	Укажите корректный IP-адрес
		Неверная маска	Укажите корректную маску

Страница	Тип	Текст сообщения	Примечание
Объединение интерфейсов	Ошибка	Неверная частота мониторинга ARP канала	Нужно указать целое положительное число
		Неверный IP-адрес для ARP мониторинга	Нужно указать корректный IP-адрес
		Неверная частота мониторинга канала МП	Нужно указать целое положительное число
		Неверная задержка перед отключением интерфейса	Нужно указать целое положительное число
		Неверная задержка перед включением интерфейса	Нужно указать целое положительное число
		Неверный режим объединения	Нужно указать целое число от 0 до 6
		Ошибка отображения страницы	Внутренняя ошибка
Мосты	Ошибка	--Сообщение, определяемое во время выполнения--	Список порядковых номеров всех отображаемых на странице интерфейсов
		Такое имя VLAN или моста уже используется	Нужно указать отличное от существующих имя
		Невозможно добавить административный интерфейс	Не следует использовать административный интерфейс
		Неправильный IP-адрес	Укажите корректный IP-адрес
		Неверная сетевая маска	Укажите корректную маску
		Неверное имя	Укажите корректное имя
		Имя может содержать только английские буквы и цифры	В данное поле нужно вводить только английские буквы и цифры
		Такое имя VLAN или моста уже используется	Нужно указать отличное от существующих имя
		Мост с таким именем уже существует	Такой мост уже существует
		Неправильный IP-адрес	Нужно ввести корректный IP-адрес
		Выключите СОВ на интерфейсе моста «idsbr», для его изменения	Для применения настройки сначала нужно выключить СОВ
Выпуск сертификатов	Ошибка	Корневой сертификат уже существует	Можно создать только один корневой сертификат
		Неправильный ввод имени хоста	Нужно указать корректное имя хоста
		Имя узла не может быть пустым	Нужно указать корректное имя хоста

Страница	Тип	Текст сообщения	Примечание
Выпуск сертификатов	Ошибка	Название организации не может быть пустым	Нужно указать название организации
		Название организации слишком длинное; оно не должно превышать 60 символов	Нужно указать название организации не длиннее 60 символов
		Неправильный ввод организации	Нужно указать корректное название организации
		Неправильный ввод почтового адреса	Нужно указать корректный адрес электронной почты
		Почтовый адрес слишком длинный, он должен быть не длиннее 40 символов	Нужно указать корректный адрес электронной почты не длиннее 40 символов
		Неправильный ввод департамента	Нужно указать корректное название департамента
		Неправильный ввод города	Нужно указать корректное название города
		Неправильный ввод области или района	Нужно указать корректное название области или района
		Неправильный ввод страны	Нужно указать корректное название страны
		«OpenSSL» вызвал ошибку	Внутренняя ошибка в «OpenSSL»
		Не найден файл сертификата	Для данного действия нужен файл сертификата
		Отсутствует файл «CRL»	Для данного действия нужен файл запроса на сертификат
		Файл не был загружен	Нужно повторить загрузку файла
		Файл некорректного формата	Формат файла для данного действия не является корректным
		Файл уже существует	В данной настройке можно загрузить только один файл
		Не удалось переместить файл сертификата	Внутренняя ошибка
		Отсутствует файл сертификата	Для данного действия нужен файл сертификата

Страница	Тип	Текст сообщения	Примечание
Выпуск сертификатов	Предупреждение	Все выпущенные сертификаты будут отозваны	В результате данного действия будут отозваны весе выпущенные сертификаты
		Корневой сертификат удален, все выданные сертификаты отозваны. Не забудьте скачать обновленный «CRL» и разослать его клиентам	Отозваны все выпущенные сертификаты
Страница «Рубикон: Подключения», открываемая вручную (https://<IP-адрес>:8443/cgi-bin/connect.cgi)	Ошибка	С этого IP пользователь уже был подключен	Пользователь может подключиться с одного IP только один раз
Настройка VPN	Ошибка	Порт зарезервирован только для использования комплексом «Рубикон»	Нужно выбрать другой порт
		Неверный MTU	Нужно указать целое положительное число не менее 1000
		Неправильно задан локальный порт	Нужно указать корректный номер порта
		Неверный ввод «Keepalive ping»	Нужно указать целое неотрицательное число
		Неверный ввод «Keepalive ping-restart»	Нужно указать целое неотрицательное число
		Неверный ввод «Keepalive», по меньшей мере используйте соотношение 1:2	«Keepalive ping-restart» должен быть больше или равен удвоенного «Keepalive ping»
		Неправильно заданная подсеть VPN	Нужно задать корректную подсеть
		Файл не был загружен	Нужно повторить загрузку файла
		Не удалось переместить файл сертификата	Внутренняя ошибка
		Неправильное имя хоста	Имя хоста должно быть не длиннее 63 символов, состоять только из символов [a-zA-Z0-9-], а первый и последний символ должны быть [a-zA-Z0-9]
		Неверный адрес	Нужно указать корректный адрес

Страница	Тип	Текст сообщения	Примечание
Настройка VPN	Ошибка	Ошибка генерации запроса на сертификат	Внутренняя ошибка
		Неправильный сертификат	Нужен корректный сертификат
		Неправильный сертификат удостоверяющего центра.	Нужен корректный сертификат удостоверяющего центра
		Не удалось переместить файл	Внутренняя ошибка
		Неправильный IP-адрес	Нужно ввести корректный IP-адрес
		Неправильный порт. Должен быть правильный номер порта	Нужно указать корректный номер порта
	Предупреждение	Изменения вступят в силу после перезапуска сервиса	Нужно перезагрузить систему
		Для интерфейсов, включенных в мост, игнорируются правила МЭ	Не ошибка
Сервер DHCP	Ошибка	DHCP on --имя интерфейса--: Неправильный начальный адрес	Нужно задать корректный начальный IP-адрес
		DHCP on --имя интерфейса--: Неправильный конечный адрес	Нужно задать корректный конечный IP-адрес
		DHCP on --имя интерфейса--: Неверное время аренды по умолчанию. --настройка--	Нужно задать неотрицательное целое число
		DHCP on --имя интерфейса--: Неверный первичный DNS	Нужно задать корректный IP-адрес первичного DNS
		DHCP on --имя интерфейса--: Неверный вторичный DNS	Нужно задать корректный IP-адрес вторичного DNS
		DHCP on --имя интерфейса--: Нельзя задать вторичный DNS без указания первичного	Нужно задать первичный адрес DNS
		DHCP on --имя интерфейса--: Неверный адрес WINS сервера	Нужно задать корректный IP-адрес WINS сервера
		DHCP on --имя интерфейса--: Нельзя задать вторичный WINS без задания первичного	Нужно задать первичный адрес WINS сервера
		DHCP on --имя интерфейса--: Неверный адрес первичного NTP-сервера	Нужно задать корректный IP-адрес первичного NTP-сервера
		DHCP on --имя интерфейса--: Неверный адрес вторичного NTP-сервера	Нужно задать корректный IP-адрес вторичного NTP-сервера

Страница	Тип	Текст сообщения	Примечание
Сервер DHCP	Ошибка	DHCP on --имя интерфейса--: Нельзя задать вторичный NTP без указания первичного	Нужно задать первичный адрес NTP-сервера
		Неправильный фиксированный MAC-адрес	Нужно указать корректный MAC-адрес
		Неправильный фиксированный IP адрес	Нужно указать корректный IP-адрес
	Предупреждение	DHCP on --имя интерфейса--: Локальный NTP-сервер указан, но не включен	Не ошибка
Конфигурация DMZ	Ошибка	Неверный ввод	Нужно ввести корректное значение
		Неправильный IP-адрес или адрес сети	Нужно указать корректный IP-адрес
		Порт назначения должен быть правильным номером порта или диапазоном портов	Нужно указать корректный номер порта или диапазон портов через символ [:]
		Начальное значение порта назначения в интервале больше или равно конечному	Начальное значение порта должно быть меньше конечного
		Неправильный IP назначения	Нужно указать корректный IP-адрес назначения
		Нет необходимости задавать DMZ «Pinholes» для той же сети. Выберите другую исходную сеть или сеть назначения	Нужно указать другую исходную сеть или сеть назначения
		Выберите сеть источника. Если у вас не настроена Оранжевая или Синяя сети, вам не нужны каналы к DMZ	Нужно указать сеть источника
		Выберите сеть назначения	Нужно указать сеть назначения
Настройка адаптеров	Ошибка	Невозможно изменить цвет административного интерфейса	Нужно выбрать другой интерфейс или отключить на данном интерфейсе администрирование
		Ошибка цвета интерфейса	Не удается распознать указанный цвет, нужно выбрать цвет GREEN, RED, BLUE, ORANGE
		Имя интерфейса уже существует	Нужно задать другое имя

Страница	Тип	Текст сообщения	Примечание
Настройка адаптеров	Ошибка	На интерфейсе установлены правила	Нужно удалить правила на интерфейсе перед выполнением настройки
		Недопустимые символы в имени интерфейса. Разрешены следующие: -_a-zA-Z0-9	Нужно задать имя, содержащее только символы -_a-zA-Z0-9
		превышение длины имени интерфейса	Имя интерфейса должно быть менее 15 символов
	Предупреждение	Необходимо сделать резервную копию	Нужно сделать резервную копию
		Изменения вступят в силу после перезапуска сервиса	Нужно выполнить перезагрузку
FTP посредник	Ошибка	Ошибка в последовательности FTP команд	Нужно задать корректную последовательность названий FTP команд через пробел
		Неправильный порт. Должен быть правильный номер порта	Нужно задать корректный номер порта
		Ошибка в передаваемых CGI параметрах	Один или несколько переданных параметров содержат ошибку
Правила межсетевого экрана	Ошибка	Файл настроек поврежден	Внутренняя ошибка
		Неправильный IP-адрес или адрес сети	Нужно указать корректный IP-адрес
		Перенаправление портов. Некорректное значение «Сервисы по умолчанию»	Нужно задать корректное значение для сервисов по умолчанию
		Перенаправление портов. Некорректное значение «Псевдоним IP»	Нужно задать корректное значение для псевдонима IP
		Перенаправление портов. Некорректное значение типа сервисов	Нужно задать корректное значение для типа сервисов
		Неверная сеть	Нужно указать корректную сеть (Интерфейс)
		Некорректное значение дополнительного адреса источника	Нужно задать корректное значение Дополнительного адреса Источника
		Некорректное значение состояния	Нужно задать корректное значение состояния
		Некорректный формат примечания	Нужно задать корректное значение примечания

Страница	Тип	Текст сообщения	Примечание
Правила межсетевого экрана	Ошибка	Ошибка ввода «Действие»	Нужно указать корректное действие
		Неверный IP-адрес	Нужно указать корректный IP-адрес
		Ошибка в передаваемых CGI параметрах	Один или несколько переданных параметров содержат ошибку
		Не выбран тип адреса. Выберите тип адреса	Нужно выбрать тип адреса
		Некорректное значение смещения в пакете	Нужно задать корректное смещение в пакете (можно использовать как десятичное, так и шестнадцатеричное представление с префиксом 0x)
		Некорректное значение маски поиска во фрагменте пакета	Нужно задать корректную маску поиска в пакете (можно использовать как десятичное, так и шестнадцатеричное представление с префиксом 0x)
		Некорректное наименьшее значение величины фрагмента в пакете	Нужно задать корректное наименьшее значение величины фрагмента в пакете (можно использовать как десятичное, так и шестнадцатеричное представление с префиксом 0x)
		Некорректное наибольшее значение величины фрагмента в пакете	Нужно задать корректное наибольшее значение величины фрагмента в пакете (можно использовать как десятичное, так и шестнадцатеричное представление с префиксом 0x)
		Не выбран тип интерфейса, выберите тип	Нужно указать корректный тип интерфейса
		Неправильно задан уровень мандатных меток. Поддерживаются значения 0-255	Нужно задать корректное значение уровня мандатной метки в интервале от 0 до 255

Страница	Тип	Текст сообщения	Примечание
Правила межсетевого экрана	Ошибка	Неправильно задана категория мандатных меток. Поддерживаются двоичные значения до 64 бит	Нужно задать корректное значение категории мандатной метки двоичным числом без префикса до 64 разрядов
		Инвертирование порта не допускается для произвольных служб в правилах перенаправления портов	Нужно сбросить флаг инверсии при использовании данной опции
		Инвертирование протокола не допускается для произвольных служб в правилах перенаправления портов	Нужно сбросить флаг инверсии при использовании данной опции
		При использовании диапазона портов в перенаправлении, указанный диапазон должен быть идентичным при задании служб «Внешний адрес приемника» и «Внутренний адрес приемника»	Нужно настроить одинаковые диапазоны портов при перенаправлении портов для внешнего и внутреннего адресов
		Протокол для службы Внешнего адреса назначения и службы Внутреннего адреса назначения должен совпадать	Нужно настроить одинаковые протоколы при перенаправлении портов для внешнего и внутреннего адресов
		Доступ к устройству возможен только от Зеленого, Синего интерфейса и VPN	Для данной настройки нужно использовать Зеленый, Синий интерфейсы или VPN
		Для источника нельзя инвертировать «Any» интерфейсы	Нужно сбросить флаг инверсии для данной настройки
		Можно добавить только красный сетевой интерфейс	Для данного типа правил можно использовать только красный сетевой интерфейс
		Неверный интерфейс	Нужно указать корректный интерфейс
		Неверный IP-адрес	Нужно указать корректный IP-адрес
		Неверный MAC-адрес	Нужно указать корректный MAC-адрес

Страница	Тип	Текст сообщения	Примечание
Правила межсетевого экрана	Ошибка	Неверный формат адреса	Нужно указать корректный формат адреса
		Неверная сеть	Нужно указать корректную сеть
		Неверный адрес	Нужно указать корректный адрес
		Неверная группа адресов	Нужно указать корректную группу адресов
		Некорректный ввод пользователя	Нужно задать корректное имя пользователя
		Не выбран тип адреса. Выберите тип адреса	Нужно задать корректный тип адреса
		Порт источника должен быть допустимым номером порта или диапазоном портов	Нужно задать корректный порт или диапазон портов
		Первая величина диапазона портов источника больше или равна второй величине	Нужно задать диапазон портов, в котором первая величина должна быть меньше второй
		Нельзя выбрать «email alert» и «local alert» одновременно	Нужно выбрать или «email alert» или «local alert»
		Неверное назначение	Нужно выбрать один из корректных типов правила МЭ
		Неверный красный адрес устройства Рубикон	Нужно указать корректный адрес красного интерфейса Рубикон
		Неверная служба	Нужно указать корректную службу
		Не выбран тип службы, выберите тип	Нужно указать корректный тип службы
		Для создания правила требуется наличие красного интерфейса	Для создания данного правила предварительно нужно настроить красный интерфейс
		Для назначения нельзя инвертировать «Any» интерфейсы	Нужно сбросить флаг инверсии для данной настройки
		Некорректный цвет интерфейса	Нужно выбрать корректный цвет интерфейса GREEN (зеленый), RED (красный), BLUE (синий), ORANGE (оранжевый)

Страница	Тип	Текст сообщения	Примечание
Правила межсетевого экрана	Ошибка	Не выбран тип интерфейса, выберите тип	Нужно указать корректный тип интерфейса
		MAC-адрес не может использоваться как адрес назначения	Для данной настройки нельзя использовать MAC-адрес
		В качестве пункта назначения в правилах для переадресации портов разрешены только IP-адреса узла (а не IP-адреса подсетей)	Нужно использовать IP-адрес хоста, а не адрес подсети
		Нельзя использовать порт источника, при выбранной службе «Ping»	Порт источника не применим при использовании службы «Ping»
		Интерфейсы источника и приемника не могут быть одинаковыми	Нужно выбрать различные интерфейсы источника и назначения
		Адреса источника и приемника не могут быть одинаковыми	Нужно выбрать различные адреса источника и назначения
		Неверный IP-адрес	Нужно указать корректный IP-адрес
		Необходимо выбрать позицию правила	Нужно указать корректную позицию правила
		Неверное значение лимита "Средняя частота событий (--limit avg)": Значение по умолчанию 10/minute. Величина выражается в пакетах/секунду, если явно не заданы постфиксы /sec /minute /hour /day	Нужно указать целое неотрицательное значение ограничителя журналирования и опционально один из постфиксов /sec /minute /hour /day. Отсутствие постфикса эквивалентно постфиксу /sec
		Неверное значение лимита "Максимальное количество событий за 3 часа (--limit-burst number)": Значение по умолчанию 5	Нужно указать целое неотрицательное значение ограничителя журналирования
		Не выбран тип ограничения, выберите тип	Нужно выбрать тип ограничителя журналирования
		Выберите доступна или нет возможность задания ограничений	Нужно выбрать одну из настроек ограничителя или отключить его

Страница	Тип	Текст сообщения	Примечание
Правила межсетевого экрана	Ошибка	Неверный начальный день	Нужно указать целое число от 1 до 31
		Неверный конечный день	Нужно указать целое число от 1 до 31
		Хотя бы один день должен быть разрешен	Нужно установить флаг разрешения напротив хотя бы одного дня
		Не выбран тип дня. Выберите тип дня	Нужно выбрать корректный тип дня
		Неверный начальный час	Нужно указать целое число от 0 до 23
		Неверный конечный час	Нужно указать целое число от 0 до 23
		Неверная начальная минута	Нужно указать целое число от 0 до 59
		Неверная конечная минута	Нужно указать целое число от 0 до 59
		Некорректное значение смещения в пакете	Нужно задать корректное смещение в пакете (можно использовать как десятичное, так и шестнадцатеричное представление с префиксом 0x)
		Некорректное значение маски поиска во фрагменте пакета	Нужно задать корректную маску поиска в пакете (можно использовать как десятичное, так и шестнадцатеричное представление с префиксом 0x)
		Некорректное наименьшее значение величины фрагмента в пакете	Нужно задать корректное наименьшее значение величины фрагмента в пакете (можно использовать как десятичное, так и шестнадцатеричное представление с префиксом 0x)

Страница	Тип	Текст сообщения	Примечание
Правила межсетевого экрана	Ошибка	Некорректное наибольшее значение величины фрагмента в пакете	Нужно задать корректное наибольшее значение величины фрагмента в пакете (можно использовать как десятичное, так и шестнадцатеричное представление с префиксом 0x)
		Неправильно задан уровень мандатных меток. Поддерживаются значения 0-255	Нужно задать корректное значение уровня мандатной метки в интервале от 0 до 255
		Неправильно задана категория мандатных меток. Поддерживаются двоичные значения до 64 бит	Нужно задать корректное значение категории мандатной метки двоичным числом без префикса до 64 разрядов
		Неправильно задано значение метки	Метка может использоваться только в правилах "Из внутренней сети во внешнюю" и должна быть целым числом больше 1000 и меньше 4294967296
		Правило уже существует	Нужно поменять один или несколько параметров
	Предупреждение	Это правило открывает Ваш Межсетевой экран	Нужно обратить внимание на широту разрешающих действий созданного правила
		Это правило может открыть Ваш межсетевой экран	Нужно обратить внимание на широту разрешающих действий созданного правила
Настройки межсетевого экрана	Ошибка	Неверный интерфейс	Нужно указать корректный интерфейс
		Неверная политика	Нужно указать корректное значение политики
		Неверное действие	Нужно указать корректное действие
		Ошибка в передаваемых CGI параметрах	Один или несколько переданных параметров содержат ошибку
		Не существует такого сетевого интерфейса	Нужно указать существующий интерфейс

Страница	Тип	Текст сообщения	Примечание
Настройки межсетевого экрана	Ошибка	Неверное действие по умолчанию	Нужно указать корректное действие по умолчанию
		При указанных параметрах администрирование Рубикона невозможно. Для администрирования должен быть настроен по крайней мере один физический интерфейс	Нужно включить администрирование хотя бы на одном физическом интерфейсе для управления изделием
		Неверный MAC-адрес	Нужно указать корректный MAC-адрес
GRE	Ошибка	Невозможный удаленный IP	Нужно указать корректный IP-адрес
		Невозможный локальный IP	Нужно указать корректный IP-адрес
		Неправильный GRE IP	Нужно указать корректный IP-адрес
		Неверная маска	Укажите корректную маску
		Неверный MTU	Нужно указать целое число от 68 до 65535
		Имя может содержать только английские буквы и цифры	В данное поле нужно вводить только английские буквы и цифры
		Это имя уже используется, пожалуйста, выберите другое	Нужно указать другое имя
		Неверный IP-адрес или маска сети	Нужно указать другой IP-адрес или маску подсети
		Имя может содержать только английские буквы и цифры (hidden param)	В данное поле нужно вводить только английские буквы и цифры
		Не существует такой GRE туннель	Нужно указать существующий GRE туннель
		Нельзя изменить имя существующего GRE туннеля	Можно создать другой GRE туннель с другим именем
Задать имена хостов	Ошибка	Комбинация Имя узла/Доменное имя уже присутствует	Комбинации Имя узла/Доменное имя должны быть уникальны
		Неправильный фиксированный IP-адрес	Нужно указать корректный IP-адрес

Страница	Тип	Текст сообщения	Примечание
Задать имена хостов	Ошибка	Неправильное имя хоста	Имя хоста должно быть не длиннее 63 символов, состоять только из символов [a-zA-Z0-9-], а первый и последний символ должны быть [a-zA-Z0-9]
		Неправильное доменное имя	Корректное имя домена состоит из символов [A-Za-z_0-9-]
Обнаружение Атак	Ошибка	Не задан адрес удаленного сервера	Нужно указать адрес удаленного сервера обновлений
		Не удалось загрузить обновления БРП СОВ с удаленного сервера в ручном режиме	Внутренняя ошибка при загрузке обновлений
		--Сообщение, определяемое во время выполнения--	Произошла ошибка при загрузке архива обновлений СОВ или вспомогательных файлов (при наличии)
		Файл не был загружен	Нужно повторить загрузку файла
		--Сообщение, определяемое во время выполнения--	Произошла ошибка при верификации архива обновлений правил СОВ
		Неправильное имя хоста	Имя хоста должно быть не длиннее 63 символов, состоять только из символов [a-zA-Z0-9-], а первый и последний символ должны быть [a-zA-Z0-9]
		--Сообщение, определяемое во время выполнения-- Не удалось запустить сервис «Snort»	Внутренняя ошибка. Произошла ошибка с указанным кодом возврата при запуске сервиса СОВ
		--Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка при обработке архива обновлений СОВ
		Невозможно открыть файл --Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Ошибка открытия журнала обновления правил СОВ

Страница	Тип	Текст сообщения	Примечание
Обнаружение Атак	Предупреждение	Обновления БРП СОВ успешно загружены с удаленного сервера	Не ошибка
		Используйте кнопку «Применить сейчас», чтобы сохранить изменения в настройках	Для применения настроек нужно использовать кнопку «Применить сейчас»
		Система пытается использовать область подкачки и обладает малым количеством свободной памяти. Это может нарушить стабильность вашей системы. СОВ использует слишком много памяти. Прокси сервер использует память пропорционально размеру кэш-памяти. Уменьшите количество используемых служб или добавьте больше памяти. Информация состояния	Можно уменьшить потребление памяти отключив вспомогательные службы (напр. Прокси) или выключить СОВ на тех интерфейсах, где он не нужен
Настройка правил СОВ	Ошибка	Внутренняя ошибка	Внутренняя ошибка
		Невозможно открыть файл	Внутренняя ошибка
	Ошибка	Невозможно открыть файл	Внутренняя ошибка
	Ошибка	Внутренняя ошибка	Внутренняя ошибка
	Предупреждение	Решающие правила СОВ для данной группы отсутствуют	Не ошибка
Переменные СОВ	Ошибка	Имя и значение переменной не могут быть пустыми	Нужно задать корректные имя и значение переменной
		Переменная уже существует: --имя переменной--	Нужно выбрать другое имя
		Попытка отредактировать внутреннюю системную переменную: --имя переменной--	Нужно выбрать другое имя
		Имя переменной содержит недопустимые символы	Нужно использовать символы [a-zA-Z0-9_-]
		Значение переменной содержит недопустимые символы	Нужно использовать символы [\$\[\]\!\.,0-9a-zA-Z_\/:]

Страница	Тип	Текст сообщения	Примечание
Переменные СОВ	Ошибка	«После символа \""$\"" ожидается имя уже определенной переменной»	Нужно или изменить вводимое значение на имя уже существующей переменной для ссылки на нее или удалить символ $
		Нельзя удалить переменную, которая используется где-то еще: --имя переменной--	Нужно сначала убедиться, что удаляемая переменная не используется в других переменных или в правилах СОВ
		Внутренняя ошибка: --код ошибки--	Внутренняя ошибка
Интерфейсы по умолчанию	Ошибка	Не введено имя интерфейса	Нужно задать произвольное имя для интерфейса, которое будет доступно в web-интерфейсе
		Не введен интерфейс	Нужно задать корректный интерфейс
		Только буквы, цифры и: (для псевдонимов) разрешены при вводе интерфейса	Нужно задать значение, содержащее только буквы, цифры и символ «:»
		Имя интерфейса уже существует	Нужно ввести другое имя
		Неверный интерфейс	Значение поля «Имя» должно состоять из символов [-_a-zA-Z0-9]
		Имя интерфейса не может использовать имя физического интерфейса	Нужно ввести произвольное имя, не являющееся именем физического интерфейса
		Физические интерфейсы не могут быть использованы в качестве интерфейса по умолчанию	Нужно задать интерфейс, не являющийся физическим. Данное настройка предназначена для задания видимых имен не физическим интерфейсам
	Предупреждение	Вы можете задать дополнительные интерфейсы только в «Расширенном режиме»	Для выполнения настройки нужно включить «Расширенный режим»
Настройка IPSec	Ошибка	Не удалось переместить файл сертификата: --Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка при загрузке сертификата

Страница	Тип	Текст сообщения	Примечание
Настройка IPSec	Ошибка	--Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка при обработке файла сертификата/запроса/ключа
		--Сообщение, определяемое во время выполнения-- Неправильный сертификат удостоверяющего центра	Нужен корректный сертификат удостоверяющего центра
		CA сертификат с таким именем уже существует	Имя сертификата удостоверяющего центра должно быть уникально
		Соединение с таким именем уже существует	Нужно задать другое имя
		Невозможно сменить сертификаты	Внутренняя ошибка
		Сертификат не имеет действительного УЦ	Нужно использовать сертификат, с которым ассоциирован действительный УЦ
		Тип соединения неверен	Нужно указать корректный тип соединения
		Невозможно извлечь общее имя из сертификата	Внутренняя ошибка при обработке сертификата
		Почтовый адрес слишком длинный, он должен быть не длиннее 40 символов	Нужно указать почтовый адрес не длиннее 40 символов
		«ESP Время жизни» должно быть от 1 до 24 часов	Нужно указать значение «ESP Время жизни» от 1 до 24 часов
		Имя узла не может быть пустым	Нужно указать имя узла
		«Время жизни IKE» должно быть от 1 до 8 часов.	Нужно указать значение «Время жизни IKE» от 1 до 8 часов
		Недопустимые символы в pre-shared ключе	Нужно задать pre-shared ключ, не содержащий символа « ' »
		Неправильный ввод метода аутентификации	Нужно указать корректный метод аутентификации
		Неправильный ввод города	Нужно указать значение, состоящее из символов [a-zA-Z0-9 ,\.\-_]
		Неправильный ввод страны	Нужно указать значение, состоящее из символов [A-Z]

Страница	Тип	Текст сообщения	Примечание
Настройка IPSec	Ошибка	Неправильный ввод департамента	Нужно указать значение, состоящее из символов [a-zA-Z0-9 ,\.\-_]
		Некорректное значение задержки при обнаружении нерабочего узла	Нужно указать целое неотрицательное число
		Некорректное значение таймаута при обнаружении нерабочего узла	Нужно указать целое неотрицательное число
		Неправильный ввод почтового адреса	Нужно указать корректный e-mail адрес
		Неправильный ввод «ESP Keylife»	Нужно указать целое неотрицательное число
		Неправильный ввод имени хоста	Нужно задать значение имени хоста в виде корректного IP-адреса или в виде FQDN
		Неправильный ввод «IKE lifetime»	Нужно указать целое неотрицательное число
		Некорректное значение таймаута неактивности	Нужно указать целое неотрицательное число
		Неправильный ввод полного имени пользователя или имени хоста системы	Нужно указать значение, состоящее из символов [a-zA-Z0-9 ,\.\-_]
		Неправильный ввод организации	Нужно указать значение, состоящее из символов [a-zA-Z0-9 ,\.\-_]
		Неправильный ввод удаленного хоста/IP	Нужно задать или корректный IP-адрес или FQDN или ключевое слово "%any"
		Неправильный ввод области или района	Нужно указать значение, состоящее из символов [a-zA-Z0-9 ,\.\-_]
		Неверный ввод	Нужно ввести корректное значение
		Неверный ключ	Внутренняя ошибка
		При использовании внешнего и внутреннего идентификаторов, они не должны быть одинаковыми и должны начинаться со знака «@». Внешний и внутренний идентификаторы относительно соединения	–

Страница	Тип	Текст сообщения	Примечание
Настройка IPSec	Ошибка	Неправильный временной промежуток	Нужно указать количество секунд от 0 до 999
		Неверная локальная подсеть	Нужно указать корректный IP-адрес локальной подсети
		Неверное имя	Нужно указать корректное значение имени
		Имя должно содержать только символы.	Нужно указать значение, состоящее из символов [a-zA-Z0-9]
		Полное имя пользователя или имя узла слишком длинное	Нужно указать значение не длиннее 60 символов
		Неправильный сертификат удостоверяющего центра	Нужен корректный сертификат удостоверяющего центра
		Название организации не может быть пустым	Нужно указать название организации
		Название организации слишком длинное; оно не должно превышать 60 символов	Нужно указать название организации не длиннее 60 символов
		Пароль слишком короткий	Нужно указать значение длиной не менее 5 символов
		Пароли не совпадают	Нужно ввести одинаковые значения
		Предварительно распределенный ключ (Pre-shared key) слишком короткий	Нужно задать предварительно распределенный ключ
		Удаленная подсеть введена неправильно	Нужно указать корректный IP-адрес удаленной подсети
		Файл не был загружен	Нужно повторить загрузку файла
		Некорректный IP-адрес или маска в адресе подсети	Нужно задать корректный IP-адрес с указанием маски
		Корневой сертификат уже существует	Можно создать только один корневой сертификат

Страница	Тип	Текст сообщения	Примечание
Настройка IPSec	Ошибка	SubjectAltName - разделенный запятыми список email, dns, uri, rid и ip объектов. email: почтовый адрес. Синтаксис email: копия для использования получается из поля email сертификата. DNS: корректное доменное имя. URI: любой корректный uri. RID: зарегистрированный идентификатор объекта. IP: IP адрес. Замечание: кодировка ограничена и регистр имеет значение. Пример: email:youname@foo.org, email:copy, DNS:www.youname.ru, IP:127.0.0.1, URI:http://url/to/something	Нужно указать значение в корректном синтаксисе согласно рекомендациям и примеру в сообщении об ошибке
		Вы должны указать корректное отличительное имя (DN) для такой аутентификации	Для данного типа аутентификации нужно указать корректное отличительное имя (DN)
		Вы можете задать только одно соединение «Roadwarrior», когда используется аутентификация с pre-shared ключом. Вы уже имеете соединение «Roadwarrior» с аутентификацией с pre-shared ключом или пытаетесь добавить его сейчас	Нужно выбрать или другой тип аутентификации, или другой тип соединения (не «Roadwarrior»)
	Предупреждение	Проверка виртуальной частной сети --Сообщение, определяемое во время выполнения--. DNS проверка не пройдена	Обратить внимание, что заданное имя не удалось разрешить в IP-адрес
		Удаленная подсеть введена неправильно	Нужно указать корректный IP-адрес удаленной подсети
NFTables	Ошибка	Недопустимые символы в «Цепочка». Разрешенные символы: a-zA-Z0-9_-	Нужно задать значение, состоящее из символов a-zA-Z0-9_-

Страница	Тип	Текст сообщения	Примечание
NFTables	Ошибка	Недопустимые символы в «Таблица». Разрешенные символы: a-zA-Z0-9_-	Нужно задать значение, состоящее из символов a-zA-Z0-9_-
OSPF	Ошибка	Ошибка в передаваемых CGI параметрах	Один или несколько переданных параметров содержат ошибку
		Неправильный IP-адрес	Укажите корректный IP-адрес
		Неверный пароль	Нужно задать пароль длиной не менее 6 символов
		Неверный IP адрес или маска сети	Нужно указать другой IP-адрес или маску подсети
		Неверная область	Нужно указать корректный идентификатор зоны
		Не существует такого сетевого интерфейса	Нужно указать существующий интерфейс
		Некорректный приоритет (priority)	Нужно указать целое неотрицательное число
		Некорректная стоимость (cost)	Нужно указать целое неотрицательное число
		Неверный тип сети	Нужно указать корректный тип сети
		Неверный параметр аутентификации	Нужно указать ключ аутентификации
		Не задан ключ в режиме аутентификации с подписью	В данном режиме работы нужно задать ключ аутентификации
		Не задан ключ подписи сообщений в режиме аутентификации с подписью	В данном режиме работы нужно задать ключ подписи сообщений
		Задан ключ подписи сообщений в режиме аутентификации без подписи	В данном режиме работы не нужно задавать ключ подписи сообщений
Настройка VPN	Ошибка	Не удалось переместить файл сертификата: --Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка при загрузке сертификата
		Ошибка генерации запроса на сертификат	Внутренняя ошибка
		Не удалось переместить файл: --Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка при загрузке файла конфигурации

Страница	Тип	Текст сообщения	Примечание
Настройка VPN	Ошибка	Неправильный сертификат	Нужен корректный сертификат
		Имя клиента не может быть пустым	Нужно задать корректное имя клиента
		--Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка при обработке файла сертификата/запроса/ключа/конфигурации
		Имя пользователя не может быть пустым	Внутренняя ошибка
		Неверная группа адресов	Нужно указать корректную группу адресов
		Неверный адрес	Нужно указать корректный адрес
		Неправильное имя хоста	Имя хоста должно быть не длиннее 63 символов, состоять только из символов [a-zA-Z0-9-], а первый и последний символ должны быть [a-zA-Z0-9]
		Неправильный ввод имени хоста	Нужно задать значение имени хоста в виде корректного IP-адреса или в виде «FQDN»
		Некорректное значение диапазона IP-адресов для клиентов VPN	Значения диапазона IP-адресов для клиентов VPN должны быть корректными IP-адресами
		Неверный ввод «Keepalive ping»	Нужно указать целое неотрицательное число
		Неверный ввод «Keepalive», по меньшей мере используйте соотношение 1:2	«Keepalive ping-restart» должен быть больше или равен удвоенного «Keepalive ping»
		Неверный ввод «Keepalive ping-restart»	Нужно указать целое неотрицательное число
		Неверный ввод порта учета	Нужно указать корректный номер порта
		Неверный ввод: порт аутентификации и учета не могут быть одинаковыми	Нужно задать отличающиеся порты учета и аутентификации
		Неверный ввод порта аутентификации	Нужно указать корректный номер порта

Страница	Тип	Текст сообщения	Примечание
Настройка VPN	Ошибка	Неверный ввод имени хоста/IP «Radius»	Нужно задать значение имени хоста в виде корректного IP-адреса или в виде «FQDN»
		Неверный ввод максимума повторов	Нужно указать целое неотрицательное число
		Неверный ввод таймаута	Нужно указать целое неотрицательное число
		Некорректный ввод времени жизни соединения	Нужно указать целое неотрицательное число
		Неверный ключ	Внутренняя ошибка
		Неправильно задано максимально допустимое количество пользователей	Нужно указать целое неотрицательное число
		Неверный MTU	Нужно указать целое положительное число не менее 1000
		Неправильный порт. Должен быть правильный номер порта	Нужно указать корректный номер порта
		Заданы не все необходимые параметры	Нужно корректно задать все необходимые параметры
		Неправильный сертификат удостоверяющего центра	Нужен корректный сертификат удостоверяющего центра
		Неправильно заданная подсеть VPN	Нужно задать корректную подсеть
		Порт зарезервирован только для использования комплексом «Рубикон»	Нужно выбрать другой порт
		Файл не был загружен	Нужно повторить загрузку файла
		Уже существует запись с таким адресом	Нужно указать другой адрес
	Предупреждение	Изменения вступят в силу после перезапуска сервиса	Нужно перезагрузить систему
		Для интерфейсов, включенных в мост, игнорируются правила МЭ	Не ошибка
Пакеты	Ошибка	Ошибка при инсталляции пакета: --Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка с указанным кодом возврата при установке пакета
		Не удалось обновить контрольные суммы	Внутренняя ошибка

Страница	Тип	Текст сообщения	Примечание
Пакеты	Ошибка	Файл не был загружен	Нужно повторить загрузку файла
		--Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка при обработке файла пакета
		Некорректный файл пакета	Нужно загрузить корректный пакет формата Debian (deb-пакет) для архитектур «amd64"» или «all»
		Неподдерживаемый файл пакета	Нужно загрузить корректный пакет формата Debian (deb-пакет) для архитектур «amd64» или «all»
		Перемещение файла пакета не удалось: --Сообщение, определяемое во время выполнения--	Внутренняя ошибка. Произошла ошибка при загрузке пакета
Проверка доступности узлов	Ошибка	Неправильный IP-адрес	Укажите корректный IP-адрес
Настройка обнаружения сканирования	Ошибка	Ошибка в передаваемых CGI параметрах	Один или несколько переданных параметров содержат ошибку
		Тип протокола неверен	Нужно указать корректный тип протокола
		Невозможно открыть файл	Внутренняя ошибка
Прокси	Ошибка	Неверное значение для TTL кэша аутентификации	Нужно указать целое неотрицательное число
		Неверное количество процессов аутентификации	Нужно указать целое неотрицательное число от 1 до 255
		TTL кэша аутентификации не может быть 0, когда используются лимиты IP-адресов	При использовании настройки лимита IP-адресов нужно указать отличное от нуля значение TTL кэша аутентификации
		Неверное значение для TTL кэша пользователь/IP	Нужно указать целое неотрицательное число
		Неверное число процессов фильтра	Нужно указать целое неотрицательное число не менее 1
		Неверное значение размера HDD кэша (требуется мин 10 МБ)	Нужно указать целое неотрицательное число не менее 10 или ноль

Страница	Тип	Текст сообщения	Примечание
Прокси	Ошибка	Неверное время ожидания соединения протокола Ident	Нужно указать целое неотрицательное число не менее 1
		Неверное имя хоста резервного контроллера домена	В случае, если поле не пустое, нужно указать корректное имя хоста
		Неверное имя хоста первичного контроллера домена	Нужно указать корректное имя хоста
		Неверный порт прокси	Нужно указать корректный номер порта
		Неверные имя или пароль прокси верхнего уровня	Нужно указать имя пользователя и пароль прокси верхнего уровня, либо не указывать ни то ни другое
		Требуется базовый DN LDAP	При использовании данной настройки нужно указать базовый DN LDAP
		Требуются имя пользователя и пароль LDAP bind DN	При использовании данной настройки и типе Active Direcory или Novell eDirectory нужно указать имя пользователя и пароль LDAP bind DN
		Неверный номер порта LDAP сервера	Нужно указать корректный номер порта
		Неверный IP-адрес LDAP сервера	Нужно указать корректный IP-адрес
		Неверное количество IP-адресов на пользователя	Нужно указать целое неотрицательное число от 1 до 255 или не указывать ничего
		Неверное значение размера кэша в памяти	Нужно указать целое неотрицательное число
		Хотя бы один браузер или клиент должен быть выбран для веб доступа	При использовании данной настройки нужно разрешить хотя бы один браузер или клиент
		Имя пользователя не может быть пустым	Нужно указать имя пользователя
		Веб-прокси должен быть запущен в непрозрачном режиме для аутентификации	Нужно запустить прокси в непрозрачном режиме при использовании данной настройки

Страница	Тип	Текст сообщения	Примечание
Прокси	Ошибка	Требуется имя домена Windows	При использовании аутентификации Windows нужно указать имя домена Windows
		Требуется имя хоста первичного контроллера домена	При использовании аутентификации Windows нужно указать имя хоста первичного контроллера домена
		Пароль должен быть минимум--Сообщение, определяемое во время выполнения-- символов	Нужно задать длину пароля не менее текущего значения минимальной длины пароля
		Неверное значение длины пароля	Нужно указать целое неотрицательное число от 1 до 255
		Пароли не совпадают	Нужно указать совпадающие значения
		Неверный номер порта RADIUS-сервера	Нужно указать корректный номер порта
		Требуется общий секрет RADIUS	Нужно указать общий секрет RADIUS
		Неверный IP-адрес RADIUS-сервера	Нужно указать корректный IP-адрес
		Неверное ограничение по времени	Конечный момент времени должен быть позже начального
		Неверный ввод	Нужно ввести корректное значение
		Неверный максимальный входящий размер	Нужно указать целое неотрицательное число
		Неверный максимальный размер объекта	Нужно указать целое неотрицательное число
		Неверный максимальный исходящий размер	Нужно указать целое неотрицательное число
		Неверный минимальный размер объекта	Нужно указать целое неотрицательное число
		Для запуска фильтрации скриптов, запустите прокси	Для активации данной функции нужно включить прокси
		Неверный порт назначения	Нужно указать корректный номер порта или диапазон через символ «-»
		Список контроля доступа не может быть пустым	Нужно добавить в список хотя бы одно значение

Страница	Тип	Текст сообщения	Примечание
Прокси	Ошибка	Неверный IP-адрес или маска сети	Нужно указать другой IP-адрес или маску подсети
		Неверный MAC-адрес	Нужно ввести корректный MAC-адрес
	Предупреждение	Прокси-сервер будет перезапущен	Не ошибка. Перезапуск прокси-сервера
Горячее резервирование CARP (VRRP)	Ошибка	Пароль не должен быть пустым	Нужно задать значение пароля
		Некорректное значение задержки	Нужно указать целое неотрицательное число
		Неправильный IP-адрес	Укажите корректный IP-адрес
		Пароль содержит запрещенные символы	Нужно задать пароль без запрещенных символов
Автоматическое восстановление	Ошибка	Ошибка в передаваемых CGI параметрах	Один или несколько переданных параметров содержат ошибку
Маршруты	Ошибка	Некорректное имя интерфейса	Нужно указать существующий интерфейс
		Неправильный промежуточный адрес	Нужно указать корректный IP-адрес
		Ошибка согласования параметров	Указанные параметры не согласуются по смыслу
		Не существует такого сетевого интерфейса -- Сообщение, определяемое во время выполнения--	Нужно указать существующий интерфейс
		Не существует такого сетевого интерфейса	Нужно указать существующий интерфейс
		Неправильное устройство	Нужно указать существующий интерфейс
		Неправильный IP-адрес -- Сообщение, определяемое во время выполнения--	Нужно указать корректный IP-адрес
		Неверная сеть --Сообщение, определяемое во время выполнения--	Нужно указать корректную сеть
		Неверная сеть	Нужно указать корректную сеть
		Неверная сетевая маска	Укажите корректную маску

Страница	Тип	Текст сообщения	Примечание
Маршруты	Ошибка	Неверные параметры	В переданных параметрах присутствует ошибка. Измените параметры и попробуйте снова
		Неверный вес маршрута -- Сообщение, определяемое во время выполнения--	Нужно указать целое неотрицательное число
		Неправильный промежуточный адрес -- Сообщение, определяемое во время выполнения--	Нужно указать корректный IP-адрес
		Имя может содержать только английские буквы и цифры	В данное поле нужно вводить только английские буквы и цифры
		Такое имя службы уже используется	Нужно указать отличное от существующих имя
		Неверный вес маршрута	Нужно указать целое неотрицательное число или не указывать ничего
		Неправильно задано значение метки	Нужно указать целое неотрицательное число больше 1001 и меньше 2147483648 или не указывать ничего
Группы служб	Ошибка	Хотя бы одна служба должна быть разрешена в группе	Нужно разрешить хотя бы одну службу в группе
		Такой дополнительной службы не существует	Нужно использовать существующую службу
		Такой службы по умолчанию – не существует	Нужно использовать существующую службу
		Неверная служба	Нужно выбрать корректную службу
		Не выбран тип службы, выберите тип	Нужно выбрать тип службы
		Не выбран тип группы служб, выберите	Нужно выбрать тип группы службы
		Не выбрана группа служб, выберите	Нужно выбрать существующую группу служб
		Выбранные службы уже есть в выбранной группе	Нужно использовать другие службы или другую группу
		Такое имя группы служб уже существует	Нужно задать другое имя
		Имя группы служб не может быть пустым	Нужно задать имя новой группы служб

Страница	Тип	Текст сообщения	Примечание
Службы	Ошибка	Такое имя службы уже используется	Нужно задать другое имя
		ICMP выбран как протокол, но указан не ICMP тип	С протоколом ICMP нужно использовать ICMP тип
		Невозможное значение ICMP типа ((max-min)>1)	Нужно выбрать корректное значение ICMP типа
		Не введено имя службы	Нужно задать имя службы
		Ошибка ввода протокола	Нужно указать корректное название протокола. Нужно выбрать корректный протокол
		Порт источника должен быть допустимым номером порта или диапазоном портов	Нужно указать корректный порт или диапазон, разделенный символами: или «-», где начальное значение меньше конечного
		Первая величина диапазона портов источника больше или равна второй величине	Нужно задать первое значение в диапазоне меньше второго
Ограничение Трафика	Ошибка	Имя интерфейса уже существует	Нужно указать отличное от существующих имя
		Не существует такого сетевого интерфейса	Нужно указать существующий интерфейс
		Некорректная скорость исходящих соединений	Нужно указать хотя бы одно целое число (скорость исходящих соединений) в диапазоне от 1 до 104857600
		Неправильный IP-адрес	Укажите корректный IP-адрес
		Неправильный порт. Должен быть правильный номер порта	Нужно задать корректный номер порта
		Ошибка приоритета для заданной тройки интерфейс/адрес/служба	Заданная последовательность параметров дублирует существующую запись
		Ошибка ввода приоритета	Нужно выбрать корректное значение приоритета
		Тип протокола неверен	Нужно выбрать корректный тип протокола

Страница	Тип	Текст сообщения	Примечание
Ограничение Трафика	Ошибка	Некорректная скорость входящих соединений	Нужно указать хотя бы одно целое число (скорость входящих соединений) в диапазоне от 1 до 104857600
		Отсутствует ограничение трафика для выбранного интерфейса	Нужно настроить ограничение трафика на выбранном интерфейсе
Группы состояний	Ошибка	Ошибка создания группы состояния соединений	Заданная последовательность параметров дублирует существующую запись
		Некорректное значение состояния	Нужно выбрать корректное значение состояния
Интерфейсы	Ошибка	Для изменения IP-адреса на красном интерфейсе требуется перезагрузка	Нужно выполнить перезагрузку
		Неверный адрес	Нужно указать корректный адрес
		Мост должен включать не менее двух интерфейсов	Нужно включить в мост хотя бы два интерфейса
		Неправильный IP-адрес	Нужно ввести корректный IP-адрес
		Неверная сетевая маска	Укажите корректную сетевую маску
	Предупреждение	Для интерфейсов, включенных в мост, игнорируются правила МЭ	Не ошибка
Сервер времени	Ошибка	Невозможно включить NTP без указания первичного	Нужно указать первичный сервер времени
		Нельзя задать вторичный NTP без указания первичного	Нужно указать первичный сервер времени
		Нельзя задать третичный NTP-сервер без указания вторичного	Нужно указать вторичный сервер времени
		Дата введена неправильно	Нужно корректно задать дату
		Неверный адрес первичного NTP-сервера	Нужно задать корректный IP-адрес или FQDN
		Неверный адрес вторичного NTP-сервера	Нужно задать корректный IP-адрес или FQDN
		Неверный адрес третичного NTP-сервера	Нужно задать корректный IP-адрес или FQDN

Страница	Тип	Текст сообщения	Примечание
Сервер времени	Ошибка	Введено неправильное время	Нужно корректно задать время
Подсчет трафика	Ошибка	Неверный ввод	Нужно ввести корректное значение
Пользователи	Ошибка	Неверное значение длины пароля. Необходимо указать пароль длиной не менее 6 символов	Нужно указать пароль длиной не менее 6 символов
		Некорректный ввод пользователя	Нужно задать корректное имя пользователя
		Пароль содержит запрещенные символы	Нужно задать пароль без запрещенных символов
		Пароли не совпадают	Нужно ввести одинаковые значения
		Необходимо указать пароль длиной не менее 6 символов	Нужно указать пароль длиной не менее 6 символов
		Введите текущий пароль	Нужно ввести текущий пароль
		Неправильный пароль	Нужно ввести правильный пароль
		Ошибка валидации пароля 1	Внутренняя ошибка
		Ошибка валидации пароля 3	Нужно ввести корректный текущий пароль
		Ошибка валидации пароля 2	Внутренняя ошибка
		Пароли не совпадают	Нужно ввести одинаковые значения
		Ошибка ввода	Нужно ввести корректное непустое имя пользователя, не пересекающееся с существующими записями
		Ошибка отображения страницы	Внутренняя ошибка
VLANs	Ошибка	Заблокированные интерфейсы являются административными или используются	Нужно указать другой интерфейс
		Ошибка согласования параметров	Сетевые параметры VLAN (Адрес сети, маска, адрес) не согласованы между собой
		Неправильный IP-адрес	Укажите корректный IP-адрес
		Неверная маска	Укажите корректную маску

Страница	Тип	Текст сообщения	Примечание
VLANs	Ошибка	Неверное имя	Укажите корректное имя
		Неверная сеть	Нужно указать корректную сеть
		Неверный тэг VLAN	Нужно указать тэг, отличный от уже существующих
		Имя может содержать только английские буквы и цифры	В данное поле нужно вводить только английские буквы и цифры
		Такое имя VLAN или моста уже используется	Нужно указать отличное от существующих имя
		Невозможно добавить административный интерфейс	Не следует использовать административный интерфейс
		VLAN уже существует	Нужно создать VLAN, отличный от существующих
Доступ к Синему интерфейсу	Ошибка	Такой IP-адрес уже существует	Нужно указать другой IP-адрес
		Введен существующий MAC-адрес	Нужно указать другой MAC-адрес
		Неправильный фиксированный IP-адрес	Нужно указать корректный IP-адрес
		Неправильный фиксированный MAC-адрес	Нужно указать корректный MAC-адрес
Журнал межсетевого экрана	Ошибка	Ошибка ввода начального времени	Нужно указать корректное время
		Ошибка ввода конечного времени	Нужно указать корректное конечное время
		Ошибка ввода цепочки фильтра	Нужно указать корректное название цепочки
		Ошибка ввода интерфейса	Нужно указать корректное имя интерфейса
		Ошибка ввода протокола	Нужно указать корректное название протокола
		Ошибка ввода MAC-адреса	Нужно указать корректный MAC-адрес
		Ошибка ввода адреса источника	Нужно указать корректный IP-адрес источника
		Ошибка ввода адреса назначения	Нужно указать корректный IP-адрес назначения

Страница	Тип	Текст сообщения	Примечание
Журнал межсетевого экрана	Ошибка	Ошибка ввода порта источника	Нужно указать целое число от 1 до 65535
		Ошибка ввода порта назначения	Нужно указать целое число от 1 до 65535
Журнал обнаружения атак	Ошибка	Некорректное значение параметра сортировки	Нужно выбрать корректный параметр сортировки
		Ошибка ввода начального времени	Нужно указать корректное начальное время
		Ошибка ввода конечного времени	Нужно указать корректное конечное время
		Ошибка ввода имени	Нужно указать корректное имя
		Ошибка ввода приоритета	Нужно указать целое неотрицательное число
		Ошибка ввода типа	Нужно указать корректный тип
		Ошибка ввода «SID»	Нужно указать целое неотрицательное число
		Ошибка ввода адреса источника	Нужно указать корректный IP-адрес источника
		Ошибка ввода адреса назначения	Нужно указать корректный IP-адрес назначения
Системный протокол	Ошибка	Ошибка ввода начального времени	Нужно указать корректное начальное время
		Ошибка ввода конечного времени	Нужно указать корректное конечное время
		Ошибка ввода секции	Нужно указать корректное значение секции

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ докумен-та	Входящий № сопрово-дительно-го докум. и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					