



Программный комплекс INFOWATCH ARMA INDUSTRIAL FIREWALL

Промышленный межсетевой экран
нового поколения



Руководство пользователя по эксплуатации

версия 63 ред. от 25.01.2021

Листов 365

СОДЕРЖАНИЕ

Аннотация.....	17
1 Назначение программы	18
1.1 Запуск и авторизация	18
1.2 Описание графического интерфейса	19
1.2.1 Логотип и ссылка на «Инструментальную панель»	19
1.2.2 Область меню	20
1.2.3 Область быстрой навигации	21
1.2.4 Имя пользователя и доменное имя	21
1.2.5 Справочная информация	22
1.2.6 Расширенный режим	22
1.2.7 Подсказки	22
1.2.8 Вкладки	23
1.2.9 Выпадающие списки	23
1.3 Описание основных разделов графического интерфейса	23
1.3.1 Инструментальная панель	23
1.3.2 Создание отчетов	24
1.3.3 Межсетевой экран	24
1.3.4 Обнаружение вторжений	24
1.3.5 Система	25
1.3.6 Интерфейсы	26
1.3.7 Сеть	26
1.3.8 Маршрутизация	26
1.3.9 Службы	26
1.3.10 VPN	27
1.4 Журналирование	27
2 Раздел «Инструментальная панель»	33
2.1 Виджет «Система информации»	33
2.2 Виджет «Службы»	34
2.3 Виджет «Шлюзы»	35
2.4 Виджет «Интерфейсы»	35
2.5 Виджет «Использование ЦП»	36
2.6 Виджет «Журнал Syslog»	36
2.7 Виджет «CARP»	37
2.8 Виджет «Статистика интерфейса»	37

2.9 Виджет «Журнал межсетевого экрана»	38
2.10 Виджет «Monit»	38
2.11 Виджет «Сетевое время»	39
2.12 Виджет «Тепловые датчики»	39
2.13 Виджет «Графики трафика»	40
2.14 Виджет «OpenVPN»	41
2.15 Виджет «IPsec»	41
2.16 Виджет «Информация о лицензии»	41
3 Раздел «Создание отчетов»	42
3.1 Подраздел «Состояние»	42
3.1.1 Скрытие области «Параметры»	42
3.1.2 Выбор категорий	42
3.1.3 Выбор уровня приближения	44
3.1.4 Функция «Обратный порядок»	44
3.1.5 Разрешение графика	44
3.1.6 Функция «Показать таблицы»	45
3.1.7 Название графика	45
3.1.8 Фильтр меток.....	45
3.1.9 Область графика	45
3.1.10 Область масштабирования	45
3.1.11 Текущий вид – Общий	46
3.1.12 Текущий вид – Подробный	46
3.2 Подраздел «Анализ»	47
3.2.1 Категория «Всего»	47
3.2.2 Категория «Подробности»	49
3.2.3 Категория «Экспорт»	49
3.3 Подраздел «Netflow».....	50
3.3.1 Категория «Захват»	50
3.3.2 Категория «Кэш»	51
3.4 Подраздел «Настройки»	51
3.5 Подраздел «Трафик»	52
4 Раздел «Межсетевой экран»	54
4.1 Подраздел «Псевдонимы»	54
4.1.1 Типы псевдонимов	54
4.1.2 Таблица псевдонимов.....	55

4.1.3 Редактирование/создание псевдонима.....	56
4.1.4 Настройки GeoIP.....	56
4.2 Подраздел «Правила»	56
4.2.1 Категория «Общие»	57
4.2.2 Категория «[Название интерфейса]».....	61
4.3 Подраздел «NAT».....	62
4.3.1 Категория «Переадресация портов».....	62
4.3.2 Категория «Один к одному».....	65
4.3.3 Категория «Исходящий»	67
4.3.4 Категория «NPTv6»	70
4.4 Подраздел «Ограничение трафика»	72
4.4.1 Категория «Каналы»	72
4.4.2 Категория «Очереди».....	74
4.4.3 Категория «Правила»	76
4.4.4 Категория «Статус»	78
4.5 Подраздел «Группы интерфейсов»	79
4.6 Подраздел «Виртуальные IP-адреса»	80
4.6.1 Категория «Настройка»	80
4.6.2 Категория «Статус»	81
4.7 Подраздел «Настройки»	81
4.7.1 Категория «Дополнительно»	82
4.7.2 Категория «Нормализация»	86
4.7.3 Категория «Расписания»	89
4.8 Подраздел «Журналы»	90
4.8.1 Категория «В реальном времени»	90
4.8.2 Категория «Обзор»	91
4.8.3 Категория «Открытый вид»	95
4.9 Подраздел «Диагностика»	96
4.9.1 Категория «pfinfo»	96
4.9.2 Категория «pfTop».....	99
4.9.3 Категория «pfTables»	99
4.9.4 Категория «Снимок состояний»	100
4.9.5 Категория «Сброс состояний».....	100
4.9.6 Категория «Сводка состояний».....	101
5 Раздел «Обнаружение вторжений»	103
5.1 Подраздел «Администрирование»	103

5.1.1 Категория «Настройки»	103
5.1.2 Категория «Сохранение»	104
5.1.3 Категория «Правила»	106
5.1.4 Категория «Предупреждения»	106
5.2 Подраздел «Контроль уровня приложений»	107
5.2.1 Шаблон протокола Modbus	113
5.2.2 Шаблон протокола IEC 104	115
5.2.3 Шаблон протокола S7comm	120
5.2.4 Шаблон протокола OPC UA	125
5.2.5 Шаблон протокола OPC DA	130
5.2.6 Шаблон протокола UMAS	132
5.2.7 Шаблон протокола MMS	138
5.2.8 Шаблон протокола GOOSE	142
5.2.9 Шаблон «Настроенное пользователем»	144
5.3 Подраздел «Журнал»	145
5.4 Подраздел «Настройки импорта правил»	146
6 Раздел «Система»	149
6.1 Подраздел «Доступ»	149
6.1.1 Категория «Пользователи»	149
6.1.2 Категория «Группы»	149
6.1.3 Категория «Серверы»	149
6.1.4 Категория «Средство проверки»	149
6.2 Подраздел «Прошивка»	149
6.2.1 Категория «Обновления»	149
6.2.2 Категория «Контроль целостности»	150
6.3 Подраздел «Настройки»	151
6.3.1 Категория «Экспорт событий»	151
6.3.2 Категория «Общие настройки»	153
6.3.3 Категория «Администрирование»	154
6.3.4 Категория «Пароль»	157
6.3.5 Категория «Журналирование»	158
6.3.6 Категория «SNMP»	159
6.3.7 Категория «Прочее»	161
6.3.8 Категория «Параметры»	164
6.3.9 Категория «Планировщик задач Cron»	165
6.4 Подраздел «Шлюзы»	166

6.4.1 Категория «Единичный».....	166
6.4.2 Категория «Группа».....	169
6.4.3 Категория «Журнал»	170
6.5 Подраздел «Маршруты».....	170
6.5.1 Категория «Конфигурация»	170
6.5.2 Категория «Статус»	171
6.5.3 Категория «Журнал»	172
6.6 Подраздел «Высокий уровень доступности».....	173
6.6.1 Категория «Настройки»	173
6.6.2 Категория «Статус»	177
6.7 Подраздел «Диагностика»	178
6.7.1 Категория «Активность».....	178
6.7.2 Категория «Службы».....	179
6.8 Подраздел «Конфигурация»	179
6.8.1 Категория «Резервные копии».....	180
6.8.2 Категория «Значения по умолчанию»	180
6.8.3 Категория «История изменений»	181
6.8.4 Категория «Настройки экспорта»	182
6.9 Подраздел «Доверенные сертификаты».....	182
6.9.1 Категория «Полномочия»	182
6.9.2 Категория «Сертификаты».....	186
6.9.3 Категория «Отзыв сертификатов»	191
6.10 Подраздел «Мастер».....	193
6.10.1 Мастер: шаг 1.....	193
6.10.2 Мастер: шаг 2.....	193
6.10.3 Мастер: шаг 3.....	194
6.10.4 Мастер: шаг 4.....	194
6.10.5 Мастер: шаг 5.....	194
6.10.6 Мастер: шаг 6.....	194
6.11 Подраздел «Журналы».....	195
6.11.1 Категория «Журнал Syslog»	195
6.11.2 Категория «Backend журнал»	195
6.11.3 Категория «Журнал веб-интерфейса».....	196
6.11.4 Категория «Журнал событий безопасности».....	196
6.11.5 Категория «Журнал системных событий»	198
6.11.6 Категория «Журнал действий пользователей»	199

6.12 Подраздел «Питание»	200
6.12.1 Категория «Перезагрузка».....	200
6.12.2 Категория «Выключение»	201
6.12.3 Категория «Выход».....	201
7 Раздел «Интерфейсы»	202
7.1 Подраздел «[Название интерфейса]»	202
7.2 Подраздел «Назначение портов»	211
7.3 Подраздел «Обзор»	212
7.4 Подраздел «Настройки»	213
7.5 Подраздел «Другие типы»	214
7.5.1 Категория «Сетевой мост»	214
7.5.2 Категория «LAGG»	217
7.5.3 Категория «Loopback».....	219
7.5.4 Категория «VLAN»	219
7.5.5 Категория «VXLAN»	220
7.6 Подраздел «Диагностика»	222
7.6.1 Категория «ARP-таблица»	222
7.6.2 Категория «Просмотр DNS-записей»	222
7.6.3 Категория «NDP-таблица»	223
7.6.4 Категория «Netstat».....	223
7.6.5 Категория «Захват пакетов»	224
7.6.6 Категория «Ping»	226
7.6.7 Категория «Проверка порта»	227
7.6.8 Категория «Маршрут трассировки»	228
8 Раздел «Сеть»	230
8.1 Подраздел «Обнаружение устройств»	230
8.1.1 Категория «Общие настройки»	230
8.1.2 Категория «Хосты».....	230
8.2 Подраздел «Анализ трафика»	231
8.2.1 Категория «Журналирование»	231
9 Раздел «Маршрутизация».....	233
9.1 Подраздел «Общие настройки».....	233
9.2 Подраздел «RIP».....	233
9.3 Подраздел «OSPF».....	234
9.3.1 Категория «Общие настройки»	234

9.3.2 Категория «Сети».....	235
9.3.3 Категория «Интерфейсы»	236
9.3.4 Категория «Список префиксов»	238
9.3.5 Категория «Карты маршрутизации»	239
9.4 Подраздел «Диагностика»	240
9.4.1 Категория «Общие настройки»	240
9.4.3 Категория «Журналирование»	244
10 Раздел «Службы».....	246
10.1 Подраздел «Портал авторизации».....	246
10.1.1 Категория «Администрирование»	246
10.1.2 Категория «Сессии»	249
10.1.3 Категория «Ваучеры»	250
10.1.4 Категория «Журнал».....	251
10.2 Подраздел «DHCPv4».....	251
10.2.1 Категория «[Название интерфейса]»	251
10.2.2 Категория «Ретрансляция»	256
10.2.3 Категория «Аренда адресов»	256
10.2.4 Категория «Журнал»	257
10.3 Подраздел «DHCPv6».....	257
10.3.1 Категория «[Название интерфейса]»	257
10.4 Подраздел «Monit»	258
10.4.1 Категория «Настройки»	258
10.4.2 Категория «Статус».....	263
10.5 Подраздел «Сетевое время»	264
10.5.1 Категория «Общие настройки»	264
10.5.2 Категория «GPS-приемник»	265
10.5.3 Категория «PPS»	266
10.5.4 Категория «Статус».....	267
10.5.5 Категория «Журнал»	268
10.6 Подраздел «Веб-прокси».....	268
10.6.1 Категория «Администрирование»	269
10.6.2 Категория «Журнал кэша»	283
10.6.3 Категория «Журнал доступа»	283
10.6.4 Категория «Журнал хранения»	283
11 Раздел VPN	285
11.1 Подраздел «IPsec».....	285

11.1.1 Категория «Настройки туннеля»	285
11.1.2 Категория «Мобильные клиенты»	288
11.1.3 Категория «Предварительно выданные ключи»	290
11.1.4 Категория «Пары ключей RSA»	290
11.1.5 Категория «Дополнительные настройки»	291
11.1.6 Категория «Информация о статусе»	292
11.1.7 Категория «Статус аренды адресов»	292
11.1.8 Категория «База данных безопасных ассоциаций (SAD)»	293
11.1.9 Категория «База данных политик безопасности (SPD)»	293
11.1.10 Категория «Журнал»	293
11.2 Подраздел «OpenVPN»	294
11.2.1 Категория «Серверы»	294
11.2.2 Категория «Клиенты»	299
11.2.3 Категория «Переопределение значений для конкретного клиента» ...	303
11.2.4 Категория «Экспорт настроек клиента»	305
11.2.5 Категория «Статус соединения»	306
11.2.6 Категория «Журнал»	306
12 Пользовательские сценарии	308
12.1 Настройка Netflow	308
12.2 Кэширующий прокси (Squid)	309
12.2.1 Кэширующий прокси: установка	309
12.2.2 Настройка веб-фильтрации	313
12.3 Встроенная система предотвращения вторжений	315
12.3.1 Настройка системы обнаружения вторжений в режиме IDS	315
12.3.2 Настройка системы предотвращения вторжений в режиме IPS	316
12.4 Задание и синхронизация времени по протоколу NTP	317
12.5 Настройки экспорта событий по SYSLOG (интеграция с SIEM-системами) ...	318
12.6 Изменение возможностей (прав) пользователей	318
12.7 Создание нового пользователя	319
12.8 Выбор совокупности регистрируемых событий	320
12.9 Фильтрация промышленных протоколов АСУ ТП	322
12.9.1 Настройка протокола Modbus	322
12.9.2 Настройка протокола IEC 104	322
12.9.3 Настройка протокола S7comm	322
12.9.4 Настройка протокола OPC UA	322
12.9.5 Настройка протокола OPC DA	322

12.9.6 Настройка протокола UMAS.....	322
12.9.7 Настройка протокола MMS.....	322
12.9.8 Настройка протокола GOOSE.....	323
12.10 Импорт пользовательских решающих правил в формате Snort	323
12.11 Экспорт пользовательских решающих правил.....	323
12.12 Динамическая маршрутизация	324
12.13 Настройки для работы на уровне L2	329
12.13.1 Отключение исходящего NAT	329
12.13.2 Изменение системных параметров	329
12.13.3 Создание моста	330
12.13.4 Назначение управляющего интерфейса	330
12.13.5 Отключение частных сетей и Bogon.....	331
12.13.6 Отключение DHCP сервера на LAN	331
12.13.7 Отключение интерфейсов LAN и WAN	331
12.14 Настройки режима отказоустойчивого кластера (высокой доступности) ..	331
12.14.1 Установка интерфейсов и основные правила межсетевого экрана ..	332
12.14.2 Настройка виртуальных IP-адресов.....	333
12.14.3 Настройка исходящего NAT	333
12.14.4 Настройка синхронизации XMLRPC SYNC	333
12.14.5 Настройка тестирования.....	334
12.15 Создание правил МЭ.....	334
12.15.1 Создание правил МЭ для всех сетевых интерфейсов	334
12.15.2 Создание правил МЭ для определенного сетевого интерфейса.....	334
12.16 Создание правил NAT	335
12.17 Настройка прокси-сервера для взаимодействия с внешним антивирусом на удаленном хосте по протоколу ICAP	335
12.17.1 Настройка HTTP-прокси.....	335
12.17.2 Настройка HTTPS-прокси	337
12.17.3 Настройка внешнего антивируса.....	342
12.17.4 Настройка ПК «InfoWatch ARMA Industrial Firewall» для взаимодействия с внешним антивирусом	343
12.18 Настройка портала авторизации.....	343
12.19 Создание Custom правил COB	346
12.20 Настройка записи дампов трафика	346
12.21 Настройка Active Directory сервера аутентификации (импорт пользователей).....	346

12.22	Добавление правил МЭ и COB для пользователей сервера аутентификации Active Directory	346
12.23	Ограничение пропускной способности для пользователей сервера аутентификации Active Directory	349
12.24	Импорт правил COB по SMB	350
12.24.1	Импорт правил COB по SMB по запросу пользователя	350
12.24.2	Импорт правил COB по SMB по расписанию	351
12.25	Импорт правил COB по FTP	352
12.25.1	Импорт правил COB по FTP по запросу пользователя	352
12.25.2	Импорт правил COB по FTP по расписанию	353
12.26	Экспорт конфигурации по SMB	354
12.26.1	Экспорт конфигурации по SMB запросу пользователя	354
12.26.2	Экспорт конфигурации по SMB по расписанию	354
12.27	Экспорт конфигурации по FTP	354
12.27.1	Экспорт конфигурации по FTP по запросу пользователя	354
12.27.2	Экспорт конфигурации по FTP по расписанию	354
12.28	Настройка DHCP-сервера	354
12.29	Настройка DHCP клиента	354
12.30	Настройка динамической маршрутизации RIP	355
12.31	Настройка динамической маршрутизации OSPF	355
12.32	Настройка блокирования сеанса доступа пользователя при неактивности	355
12.33	Просмотр и фильтрация пакетов, прошедших через ПК «InfoWath ARMA Industrial Firewall»	355
12.34	Настройка мониторинга по SNMP (v1, v2)	356
12.35	Настройка мониторинга по SNMPv3	356
12.36	Создание сертификата	356
12.37	Настройка статической маршрутизации	357
12.38	Настройка OpenVPN в режиме «сеть – сеть»	357
12.38.1	Настройка VPN на маршрутизаторе ARMA_IF_1	359
12.38.2	Копирование ключа	360
12.38.3	Настройка VPN на маршрутизаторе ARMA_IF_2	360
12.38.4	Создание правил межсетевого экрана	361
13	Сообщения пользователю	364
13.1	Неправильный ввод в системе	364

13.2 Предупреждение об удалении	364
13.3 Неправильный ввод в поле	364
13.4 Предупреждение при применении настроек	364
13.5 Импорт файла с некорректными правилами	365

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АСУ	–	автоматизированная система управления
АСУ ТП	–	автоматизированная система управления технологическим процессом
МП	–	материнская плата
МЭ	–	межсетевой экран
МЭК	–	международная электротехническая комиссия
ОС	–	операционная система
ПК	–	программный комплекс
ПЛК	–	программируемый логический контроллер
ПО	–	программное обеспечение
СЗИ	–	средство защиты информации
СОВ	–	система обнаружения вторжений
СПВ	–	средство предотвращения вторжений
ЦПУ	–	центральное процессорное устройство
ACK	–	(англ. Acknowledge) – подтверждение
ACL	–	(англ. Access Control List) – список управления доступом
APCI	–	(англ. Advanced Configuration and Power Interface) – усовершенствованный интерфейс управления конфигурацией и питанием
APDU	–	(англ. Application Protocol Data Unit) – протокольный блок данных прикладного уровня
API	–	(англ. Application Programming Interface) – программный интерфейс приложения
ARP	–	(англ. Address Resolution Protocol) – протокол определения адреса
AS	–	(англ. Autonomous System) – автономная система
C2	–	(англ. Command and Control) – командование и управление
CARP	–	(англ. Common Address Redundancy Protocol) – протокол дубликации общего адреса
CDN	–	(англ. Content Delivery Networks) – сеть доставки содержимого
CIDR	–	(англ. Classless Inter-Domain Routing) – бесклассовая адресация
CIP	–	(англ. Common Industrial Protocol) – общий промышленный протокол
CLI	–	(англ. Command Line Interface) – командная строка
COT	–	(англ. Cause Of Transfer) – причина передачи
CPU	–	(англ. Central Processing Unit) – центральное процессорное устройство
CRC	–	(англ. Cyclic Redundancy Check) – циклический избыточный код
CSV	–	(англ. Comma-Separated Values) – значения, разделенные

DCE-RPC	–	запятыми, формат файла (англ. Distributed Computing Environment / Remote Procedure Calls) – распределенная вычислительная среда/удаленные вызовы процедур
DH	–	(англ. Diffie–Hellman) – протокол Диффи-Хеллмана
DHCP	–	(англ. Dynamic Host Configuration Protocol) – протокол динамической настройки узла
DNS	–	(англ. Domain Name System) – система доменных имён
DOS	–	(англ. Denial of Service) – отказ в обслуживании
DSCP	–	(англ. Differentiated Services Code Point) – точка кода дифференцированных услуг
ECN	–	(англ. Explicit Congestion Notification) – явное уведомление о перегруженности
ENIP	–	(англ. EtherNet IP) – промышленный протокол Ethernet
FQDN	–	(англ. Fully Qualified Domain Name) – полностью определенное имя домена
GOOSE	–	(англ. Generic Object-Oriented Substation Event) – общее объектно-ориентированное событие на подстанции
FTP	–	(англ. File Transfer Protocol) – протокол передачи файлов по сети
HTTP	–	(англ. HyperText Transfer Protocol) – протокол передачи гипертекста
HTTPS	–	(англ. HyperText Transfer Protocol Secure) – расширенный протокол HTTP
IANA	–	(англ. Internet Assigned Numbers Authority) – администрация адресного пространства Интернета
ICAP	–	(англ. Internet Content Adaptation Protocol) – протокол адаптации контента Интернета
ICMP	–	(англ. Internet Control Message Protocol) – протокол межсетевых управляющих сообщений
ID	–	идентификатор
IDS	–	(англ. Intrusion Detection System) – система обнаружения вторжений
IEC	–	(англ. International Electrotechnical Commission) – международная электротехническая комиссия
IOA	–	(англ. Information Object Address) – адрес объекта информации
IP	–	(англ. Internet Protocol) – межсетевой протокол
IPS	–	(англ. Intrusion Prevention System) – система предотвращения вторжений
L2TP	–	(англ. Layer 2 Tunneling Protocol) – протокол туннелирования второго уровня
LAN	–	(англ. Local Area Network) – локальная вычислительная сеть
LDAP	–	(англ. Lightweight Directory Access Protocol) – облегчённый протокол доступа к каталогам

LRO	–	(англ. Large receive offload) – дефрагментация принимаемых пакетов
MAC	–	(англ. Media Access Control) – управление доступом к среде
MMS	–	(англ. Manufacturing Message Specification) – протокол передачи данных по технологии «клиент-сервер»
NAT	–	(англ. Network Address Translation) – преобразование сетевых адресов
NPT	–	(англ. Network Prefix Translation) – протокол трансляции сетевых префиксов
NTP	–	(англ. Network Time Protocol) – протокол сетевого времени
OPC	–	(англ. Open Platform Communications) – семейство технологий управления объектами автоматизации
OSI	–	(англ. Open Systems Interconnection) – модель взаимодействия открытых систем
OSPF	–	(англ. Open Shortest Path First) – протокол динамической маршрутизации
PAT	–	(англ. Port Address Translation) – трансляция порт-адрес
pf	–	(англ. Packet Filter) – межсетевой экран операционной системы FreeBSD
PID	–	(англ. Process Identifier) – идентификатор процесса
PPP	–	(англ. Point-to-Point Protocol) – двухточечный протокол канального уровня
PPPoE	–	(англ. Point-to-Point Protocol Over Ethernet) – сетевой протокол канального уровня передачи кадров PPP через Ethernet
PPTP	–	(англ. Point-to-Point Tunneling Protocol) – туннельный протокол типа точка-точка
RAM	–	(англ. Random Access Memory) – оперативная память
RFC	–	(англ. Request for Comments) – рабочее предложение
RIP	–	(англ. Routing Information Protocol) – протокол маршрутной информации
RRD	–	(англ. Round-Robin Database) – циклическая база данных
RTT	–	(англ. Round-Trip Time) – время приема-передачи
SCADA	–	(англ. Supervisory Control And Data Acquisition) – диспетчерское управление и сбор данных
SMB	–	(англ. Server Message Block) – сетевой протокол прикладного уровня для удаленного доступа к файлам
SNMP	–	(англ. Simple Network Management Protocol) – простой протокол сетевого управления
SPAN	–	(англ. Switch Port Analyzer) – анализатор коммутируемых портов
SSH	–	(англ. Secure Shell) – безопасная оболочка
SSL	–	(англ. Secure Sockets Layer) – уровень защищенных сокетов
SSLBL	–	(англ. Black List SSL) – черный список SSL
TCP	–	(англ. Transmission Control Protocol) – протокол управления

	передачей
TFTP	– (англ. Trivial File Transfer Protocol) – простой протокол передачи файлов
TLS	– (англ. Transport Layer Security) – протокол защиты транспортного уровня
TOTP	– (англ. Time Based One Time Password) – алгоритм создания одноразовых паролей
TOS	– (англ. Type of Service) – тип обслуживания
TSO	– (англ. TCP Segmentation Offload) – разгрузка сегментированием на уровне TCP
TTL	– (англ. Time To Live) – время жизни пакета данных в протоколе IP
UDP	– (англ. User Datagram Protocol) – протокол пользовательских датаграмм
UEFI	– (англ. Unified Extensible Firmware Interface) – интерфейс расширяемой прошивки
URG	– (англ. Urgent pointer field is significant) – указатель важности
URI	– (англ. Uniform Resource Identifier) – унифицированный идентификатор ресурса
URL	– (англ. Uniform Resource Locator) – единый указатель ресурса
USB	– (англ. Universal Serial Bus) – универсальная последовательная шина
UTC	– (англ. Coordinated Universal Time) – всемирное координированное время
VHID	– (англ. Virtual Host ID) – виртуальный идентификатор хоста
VLAN	– (англ. Virtual Local Area Network) – виртуальная локальная сеть
WAN	– (англ. Wide Area Network) – глобальная вычислительная сеть
WCCP	– (англ. Web Cache Communication Protocol) – протокол перенаправления контента
WPAD	– (англ. Web Proxy Auto-Discovery Protocol) – протокол автоматической настройки прокси
WMI	– (англ. Windows Management Instrumentation) – инструментарий управления Windows
XML	– (англ. Extensible Markup Language) – расширяемый язык разметки
XMLRP	– (англ. Extensible Markup Language Remote Procedure Call) – XML-вызов удаленных процедур

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, которые выполняют конфигурирование и мониторинг работы ПК «InfoWatch ARMA Industrial Firewall» v.3.5.

Руководство пользователя по эксплуатации описывает принципы работы с ПК «InfoWatch ARMA Industrial Firewall», доступные функции, а также подробное описание их настройки и использования.

Пользователю ПК «InfoWatch ARMA Industrial Firewall» необходимо изучить настоящее руководство перед эксплуатацией.

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

ПК «InfoWatch ARMA Industrial Firewall» является межсетевым экраном с функцией обнаружения и предотвращения вторжений, который обеспечивает выполнение следующих задач:

- защита устройств и компьютеров сети АСУ ТП со стороны внешней сети;
- сокрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT);
- межсетевое экранирование на основе информации с транспортного, сетевого и прикладного уровней;
- обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровне;
- экспорт событий безопасности (syslog);
- статическая и динамическая маршрутизация;
- контроль доступа пользователей локальной сети к сети (Портал авторизации);
- контроль доступа пользователей локальной сети к ресурсам Internet (URL-фильтрация);
- статическая и динамическая маршрутизация;
- зеркалирование трафика с выбранного порта на отдельный порт;
- уведомление о событиях безопасности по электронной почте и syslog;
- сбор и разбор сетевого трафика;
- предотвращения задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом (QoS, Traffic Shaping);
- сбор статистики NetFlow;
- прокси-сервер;
- DHCP-сервер.

1.1 Запуск и авторизация

Для доступа к веб-интерфейсу управления ПК «InfoWatch ARMA Industrial Firewall» необходимо:

- открыть веб-браузер (требования к веб-браузерам приведены в Руководстве администратора в разделе 1.1)
- ввести адрес LAN интерфейса, указанный в консольном интерфейсе, в формате: `http(s)://[IP-адрес LAN интерфейса]` (по умолчанию используется подключение через протокол https), например, «`https://192.168.1.1`».

Более подробная информация о настройке системы описана в Руководстве администратора в разделе 2.

Для начала работы с системой необходимо авторизоваться (Рисунок 1). Аутентификационные данные по умолчанию:

- имя пользователя — «root»;
- пароль — «root».

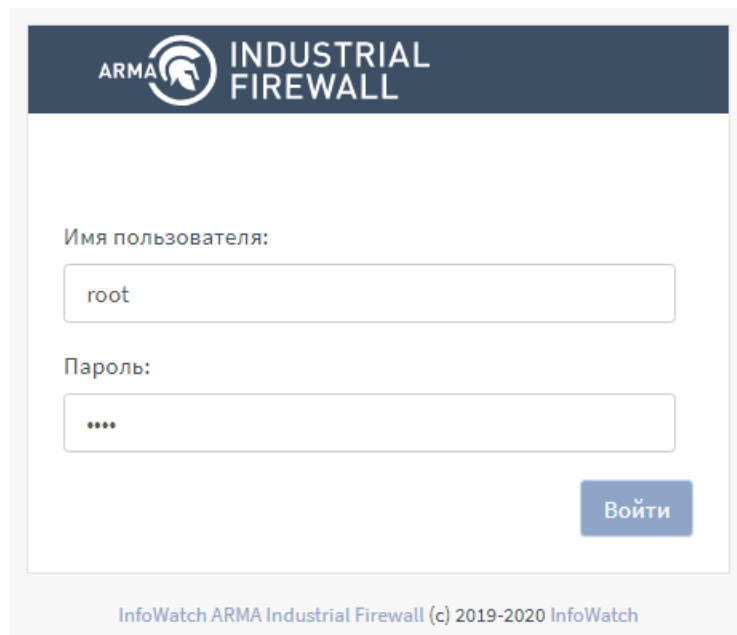


Рисунок 1 – Вход в систему

1.2 Описание графического интерфейса

Внешний вид графического интерфейса в разделе «Инструментальная панель» показан на рисунке 2.

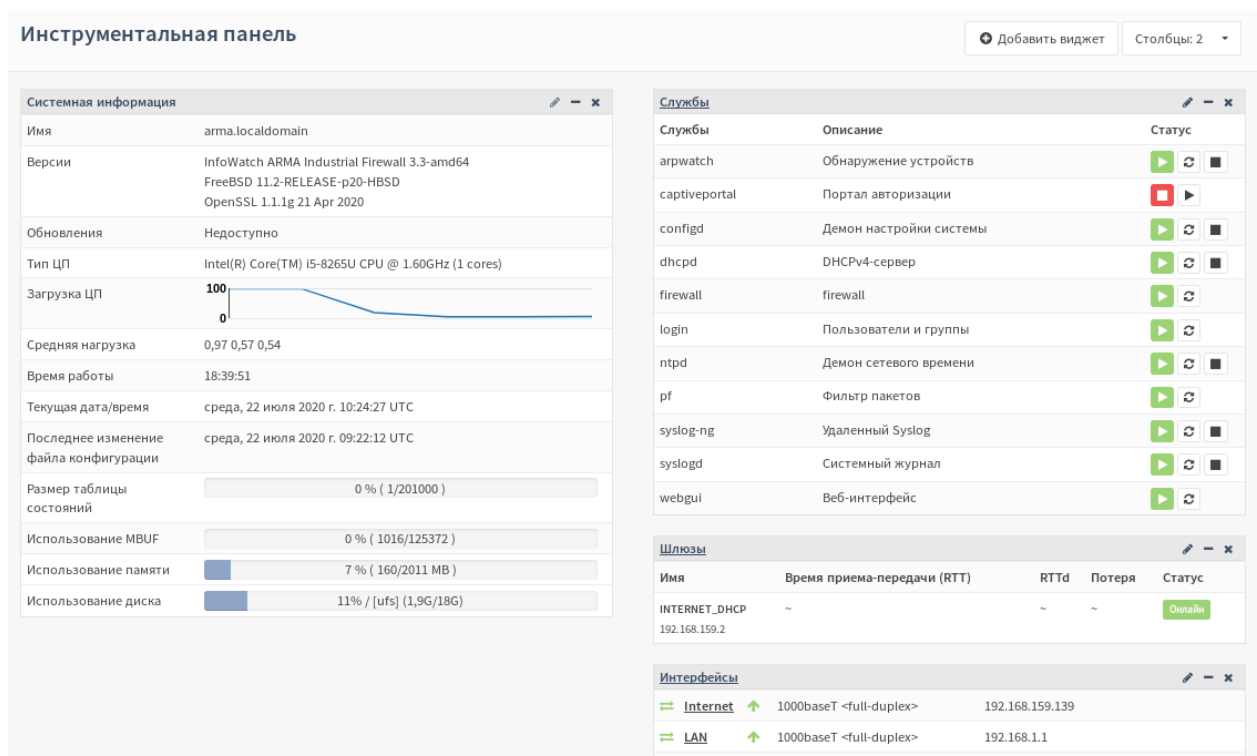


Рисунок 2 – Вид графического интерфейса (раздел «Инструментальная панель»)

1.2.1 Логотип и ссылка на «Инструментальную панель»

Для перехода в раздел меню «Инструментальная панель» необходимо нажать на кнопку логотип ПК «InfoWatch ARMA Industrial Firewall» (из любой

страницы веб-интерфейса) в верхнем левом углу экрана или выбрать соответствующий пункт меню.

1.2.2 Область меню

Область меню (Рисунок 3) находится в левой части экрана и содержит все разделы и их подразделы. С помощью меню предоставляется доступ к различным функциям ПК «InfoWatch ARMA Industrial Firewall». Переход по пунктам осуществляется нажатием левой кнопки мыши.

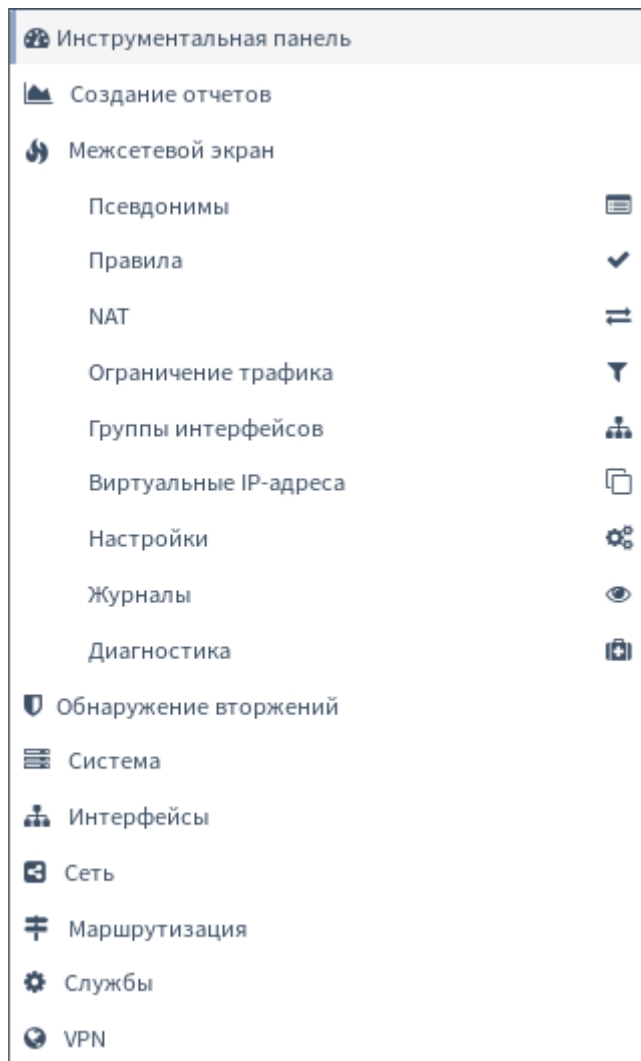


Рисунок 3 – Область меню

Существует три уровня вложенности меню:

- раздел;
- подраздел;
- категория (может не существовать, если подраздел простой).

На рисунке (Рисунок 4) представлен раздел – «Система» с подразделом «Доступ» и категорией «Пользователи».

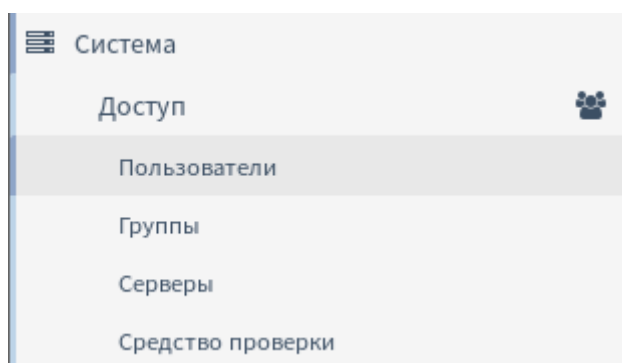


Рисунок 4 – Пример категории системы

1.2.3 Область быстрой навигации

Для быстрой навигации по графическому интерфейсу имеется возможность использовать область поиска в правом верхнем углу экрана. Для выбора области поиска необходимо нажать на текстовое поле в правом верхнем углу экрана, после чего будет активирован режим ввода текста.

Поле для поиска при наборе текста предоставляет предложения поисковых запросов в зависимости от того, какие ключевые слова для поиска набирает пользователь. Пример таких предложений представлен на рисунке (Рисунок 5). Для перехода на страницу, необходимо нажать на строку с её именем. Также возможен выбор предложения поискового запроса с помощью клавиш со стрелкой вверх и вниз, а для подтверждения выбора необходимо нажать на клавишу «ENTER».

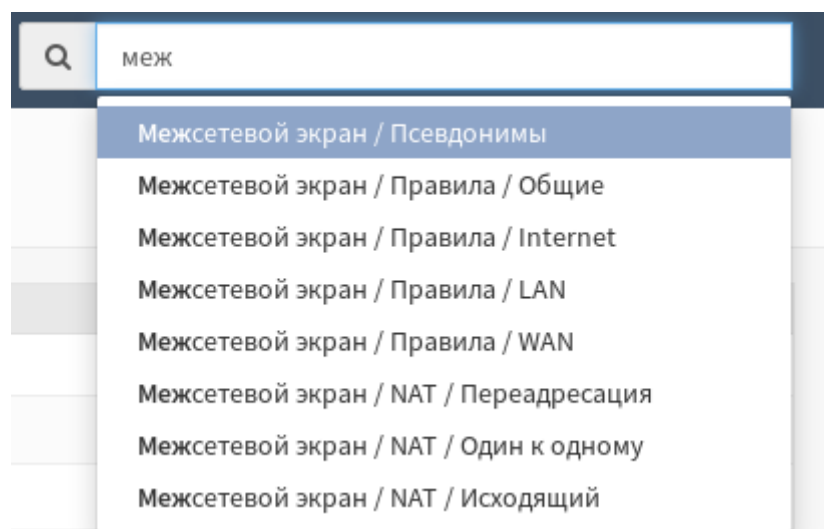



Рисунок 5 – Пример применения поиска

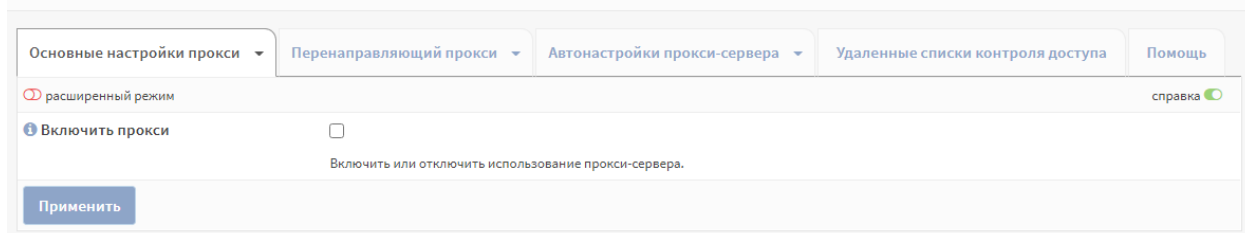
1.2.4 Имя пользователя и доменное имя

В правом углу слева от поля быстрой навигации показано имя пользователя и полное доменное имя, в котором настроен ПК «InfoWatch ARMA Industrial Firewall» (чтобы изменить имя или полное доменное имя необходимо перейти в раздел меню «Система» - «Настройки» - «Общие настройки»).

1.2.5 Справочная информация

Формы веб-интерфейса многих страниц оснащены встроенной справкой (Рисунок 6). Для того чтобы включить её в правом верхнем углу формы необходимо нажать на кнопку-переключатель «Справка » для отображения всех справочных сообщений под соответствующими элементами.


Службы: Веб-прокси: Администрирование



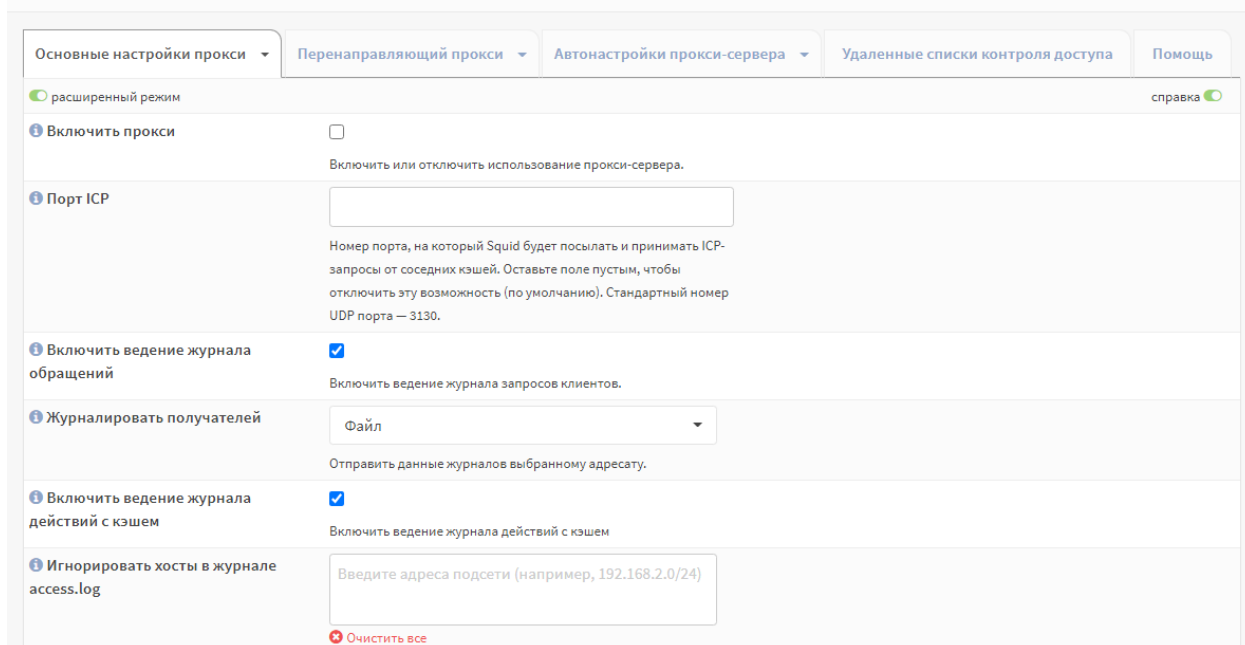
The screenshot shows the 'Службы: Веб-прокси: Администрирование' interface. At the top, there are five tabs: 'Основные настройки прокси', 'Перенаправляющий прокси', 'Автонастройки прокси-сервера', 'Удаленные списки контроля доступа', and 'Помощь'. Below the tabs, there is a section for 'расширенный режим' (advanced mode) with a toggle switch. To the right of this section, there is a 'справка' (help) toggle switch, which is currently turned on (green).

Рисунок 6 – Справочная информация

1.2.6 Расширенный режим

На некоторых страницах имеются расширенные функции (Рисунок 7). Для просмотра расширенных функций в левом углу формы необходимо нажать на кнопку-переключатель «Расширенный режим ».



Службы: Веб-прокси: Администрирование



The screenshot shows the 'Службы: Веб-прокси: Администрирование' interface with the 'расширенный режим' (advanced mode) toggle switch turned on (green) in the top left corner. The interface displays various configuration options for the proxy service, including 'Включить прокси', 'Порт ICP', 'Включить ведение журнала обращений', 'Журналировать получателей', 'Включить ведение журнала действий с кэшем', and 'Игнорировать хосты в журнале access.log'. Each option has a corresponding checkbox or input field.

Рисунок 7 – Расширенный режим

1.2.7 Подсказки

Для вывода строки подсказок для элемента формы необходимо нажать на кнопку , которая расположена слева от него, если она отображается синим цветом (Рисунок 8). Если кнопка  отображается серым цветом, то элемент формы не включает в себя подсказок.

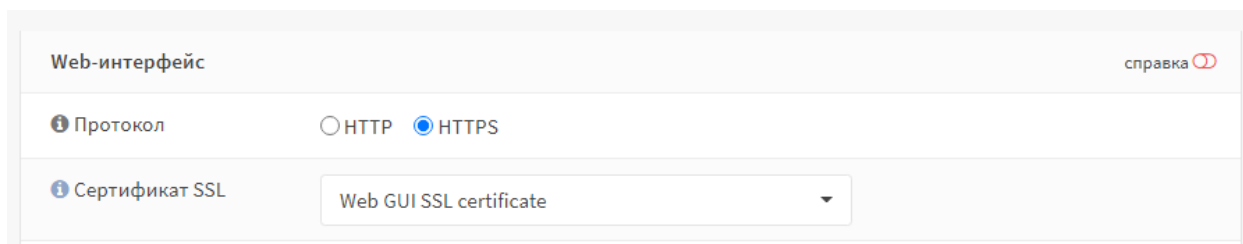


Рисунок 8 – Включение подсказки

1.2.8 Вкладки

Для перехода к вложенной странице (Рисунок 9) и открытия соответствующей формы необходимо нажать на заголовок вкладки.

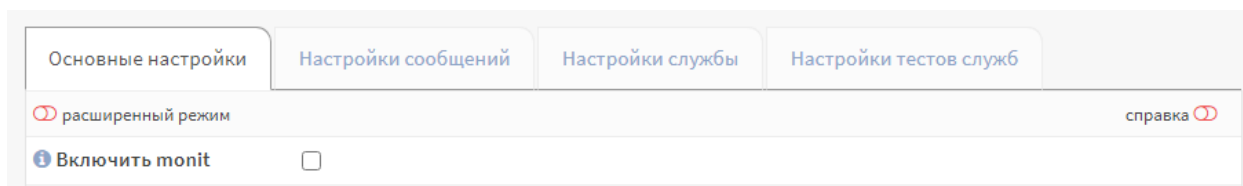


Рисунок 9 – Открытие формы вкладки

1.2.9 Выпадающие списки

Для просмотра всех элементов выпадающего списка необходимо нажать на стрелку в его правой части, например как показано на рисунке (Рисунок 10). В некоторых случаях, при большом количестве элементов выпадающего списка в правой части области доступных элементов списка появится полоса прокрутки. Прокрутка списка возможна с помощью перемещения ползунка полосы прокрутки или с помощью колёсика мыши.

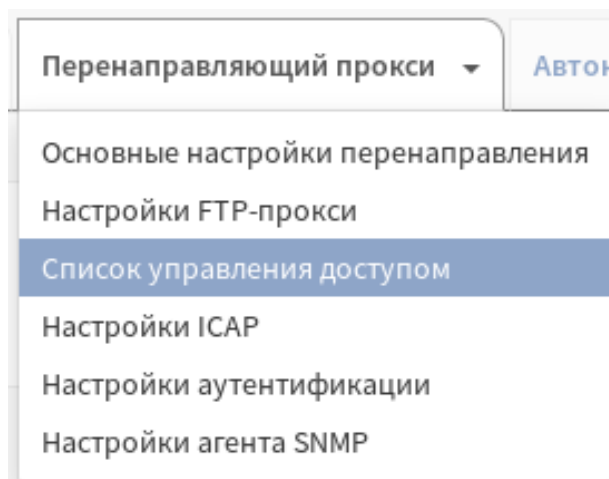


Рисунок 10 – Выпадающий список

1.3 Описание основных разделов графического интерфейса

1.3.1 Инструментальная панель

Раздел «Инструментальная панель» позволяет:

- просматривать информацию, выдаваемую информационными виджетами;

- добавлять, скрывать и/или настраивать виджеты;
- выбирать формат отображения виджетов на инструментальной панели (от 1 до 6 столбцов) и их компоновку (виджеты можно менять местами).

1.3.2 Создание отчетов

Раздел «Создание отчетов» позволяет:

- просматривать общее состояние и производительность системы в течение времени;
- просматривать и экспортировать в формате «*.csv» для дальнейшего анализа статистику количества пакетов в течение времени на определенном сетевом интерфейсе (в виде графика или таблицы);
- просматривать и экспортировать в формате «*.csv» для дальнейшего анализа статистику использования памяти, mbuf, состояний, загруженности процессора и (когда доступна) температуры процессора (в виде графика или таблицы);
- просматривать и экспортировать в формате «*.csv» для дальнейшего анализа статистику использования сервисов (в виде графика или таблицы);
- просматривать и экспортировать в формате «*.csv» для дальнейшего анализа статистику трафика (полный входящий/исходящий трафик в пакетах и байтах) по всем сетевым интерфейсам (в виде графика или таблицы);
- просматривать и экспортировать в формате «*.csv» для дальнейшего анализа данные Netflow;
- просматривать статистику использования портов и IP-адресов на выбранном сетевом интерфейсе;
- просматривать 25 наиболее используемых пользователей для выбранного сетевого интерфейса.

1.3.3 Межсетевой экран

Раздел меню «Межсетевой экран» позволяет:

- задавать правила фильтрации трафика (блокирование, разрешение, отклонение) для существующих сетевых интерфейсов на промышленном, сетевом, прикладном уровнях;
- настраивать ограничение трафика (настраивать приоритеты, пропускную способность каналов);
- задавать NAT правила;
- создавать виртуальные IP-адреса;
- просматривать журнал событий межсетевого экрана;
- экспортировать события межсетевого экрана за промежуток времени на выбранном интерфейсе.

1.3.4 Обнаружение вторжений

Раздел меню «Обнаружение вторжений» позволяет включить систему обнаружения (предотвращения, если настроено блокирование, то есть «Режим IPS») вторжений и настроить ее работу.

- В данном разделе меню графического интерфейса имеется возможность:
- создавать правила системы обнаружения вторжений по шаблону,
 - локально загружать правила в систему обнаружения вторжений,
 - мониторинга событий системы обнаружения вторжений в соответствующем журнале событий,
 - включения системы предотвращения вторжений,
 - настроить импорт баз решающих правил по ftp.

1.3.5 Система

Раздел меню «Система» позволяет:

- добавлять, редактировать, удалять пользователей/группы пользователей;
- назначать привилегии пользователям/группам пользователей;
- задавать сложность паролей;
- создавать, редактировать, удалять серверы аутентификации пользователей;
- просматривать контрольные суммы;
- просматривать отчеты об ошибках работы ПК «InfoWatch ARMA Industrial Firewall»;
- обновлять ПО ПК «InfoWatch ARMA Industrial Firewall»;
- настраивать ПК «InfoWatch ARMA Industrial Firewall»:
- выбирать часовой пояс;
- выбирать язык веб-интерфейса;
- настраивать доступ по SSH;
- настраивать консольный интерфейс;
- настраивать веб-интерфейс;
- изменять пароль;
- настраивать системный журнал (сколько записей содержит, какие события отображать и другое);
- настраивать SNMP;
- настраивать планировщик задач (Cron);
- создавать, редактировать, удалять сетевые шлюзы;
- задавать статические маршруты;
- настраивать кластеризацию;
- настраивать отказоустойчивый кластер и просматривать статус ПК «InfoWatch ARMA Industrial Firewall» при работе в режиме отказоустойчивого кластера;
- просматривать, обновлять, останавливать/включать настроенные службы;
- сохранять текущую конфигурацию;
- настраивать экспорт конфигурации на удаленный сервер;
- восстанавливать конфигурацию;
- просматривать и отменять изменения конфигурации ПК «InfoWatch ARMA Industrial Firewall»;
- настраивать экспорт конфигурации по ftp;
- создавать, редактировать и удалять сертификаты;

- осуществлять начальную настройку системы;
- просматривать журнал системных событий;
- просматривать журнал веб-интерфейса;
- просматривать журнал сервера;
- экспортировать события по SYSLOG;
- экспортировать события по SYSLOG по CEF;
- перезагружать или выключать ПК «InfoWatch ARMA Industrial Firewall»;
- выходить из учетной записи пользователя.

1.3.6 Интерфейсы

Раздел меню «Интерфейсы» позволяет:

- создавать, редактировать и удалять сетевые интерфейсы;
- выставлять соответствие между логическими и физическими сетевыми интерфейсами;
- просматривать количество входящих/исходящих (разрешенных/заблокированных) пакетов на выбранном сетевом интерфейсе;
- настраивать VLAN;
- производить захват пакетов на выбранном сетевом интерфейсе (возможен просмотр и выгрузка результата в виде файла);
- осуществлять проверку работы и приема соединения хоста на выбранном порту;
- отправлять ping запрос.

1.3.7 Сеть

Раздел меню «Сеть» позволяет запускать сервис Arpwatch, просматривать таблицу подключаемых устройств к ПК «InfoWatch ARMA Industrial Firewall», запускать анализ дампов трафика, просматривать в виде таблицы все пакеты (удовлетворяющие заданным фильтрам), проходящие через выбранный сетевой интерфейс ПК «InfoWatch ARMA Industrial Firewall».

1.3.8 Маршрутизация

Раздел меню «Маршрутизация» позволяет настраивать динамическую маршрутизацию по протоколам RIPv1, RIPv2, OSPF, а также просматривать журнал событий служб динамической маршрутизации.

1.3.9 Службы

Раздел меню «Службы» позволяет:

- настраивать и просматривать журнал событий Портала авторизации;
- настраивать и просматривать журнал событий DHCP-сервера;
- настраивать «Monit»;
- настраивать синхронизацию времени (по протоколу NTP);
- настраивать и просматривать журнал событий прокси-сервера.

1.3.10 VPN

Раздел меню «VPN» позволяет настраивать виртуальную частную сеть (Virtual Private Network) с помощью технологий IPsec и OpenVPN.

1.4 Журналирование

В ПК «InfoWatch ARMA Industrial Firewall» журналы разделены на категории, отличающиеся в зависимости от сервиса, который использует данный журнал.

В таблице 1 приведена информация о соответствии различных сервисов определенным журналам с указанием дополнительной информации по типу событий и формату сообщений для этого журнала.

Таблица 1 – Журналирование

Журнал	Путь в интерфейсе	Сохраняемые события	Формат сообщений
Системные события			
Журнал Syslog	«Система» - «Журналы» - «Журнал Syslog»	Системные события	Дата Сервис: Сообщение
Журнал сервера (Backend журнал)	«Система» - «Журналы» - «Backend журнал»	События, сгенерированные за счет использования API сервера и изменения конфигурации	Дата Сервис: Сообщение
Журнал событий веб-интерфейса	«Система» - «Журналы» - «Журнал веб-интерфейса»	События сервера (lighthttpd)	Дата Сервис [pid]: Сообщение
Журнал изменения настроек шлюза	«Система» - «Шлюзы» - «Журнал»	Изменения настроек шлюза	Дата Сервис: Сообщение
Журнал маршрутизации	«Система» - «Маршруты» - «Журнал»	Изменения маршрутов	Дата Сервис [pid]: Сообщение
Журнал системных событий	«Система» - «Журналы» - «Журнал системных событий»	Определенные системные события (описано ниже)	Дата Сервис: Сообщение
Журнал событий	«Система» - «Журналы» -	События системы обнаружения	Дата Событие

Журнал	Путь в интерфейсе	Сохраняемые события	Формат сообщений
безопасности	«Журнал событий безопасности»	вторжений, события межсетевого экрана, события arwatch, события Портала авторизации	Механизм отправки, получатель, действие, описание действия пользователя, дополнительная информация
Журнал действий пользователя	«Система» - «Журналы» - «Журнал действий пользователей»	События действий пользователей	Дата Имя пользователя Адрес Действия Успешно
Межсетевой экран			
Журнал событий МЭ в реальном времени	«Межсетевой экран» - «Журналы» - «Реальное время»	События МЭ в реальном времени	Интерфейс Время IP отправителя: Порт отправителя IP получателя: Порт получателя Протокол транспортного уровня Метка и результат обработки
Журнал необработанных событий от pf	«Межсетевой экран» - «Журналы» - «pflog»	Необработанные события из filter.log	Формат зависит от версий протоколов (формат pflog)
Журналы сервисов			
Журнал портала авторизации	«Службы» - «Портал авторизации» - «Журнал»	События Портал авторизации	Дата Сервис: Сообщение
Журнал DHCPv4	«Службы» - «DHCPv4» - «Журнал»	События DHCPv4	Дата Сервис: Сообщение
Системный журнал системы обнаружения вторжений	«Обнаружение вторжений» - «Журнал»	События срабатывания правил системы обнаружения вторжений	Дата Сервис: Сообщение

Журнал	Путь в интерфейсе	Сохраняемые события	Формат сообщений
Журнал инцидентов системы обнаружения вторжений	«Обнаружение вторжений» - «Администрирование» - «Предупреждения (Alert)»	События системы обнаружения вторжений	Дата Сервис: Сообщение
Журнал NTP	«Службы» - «Синхронизация времени» - «Журнал»	События NTP	Дата Сервис: Сообщение
Журнал веб-прокси	«Службы» - «Прокси» - «Журнал»	События прокси-сервера	Дата Сервис: Сообщение

В журнале **Syslog** содержатся уведомления следующего типа:

- вход в систему (удачный или неудачный);
- изменения внутреннего представления времени;
- изменение пароля пользователя;
- изменения настроек системы;
- события на добавление, изменение, удаление и получение информации

о следующих элементах:

- пользователи;
- правила МЭ;
- правила и группы правил COB;
- уведомления в случае отказа каких-либо модулей МЭ.

В журнале **сервера** (Backend журнал) содержатся уведомления следующего типа:

- события, сгенерированные за счет использования API сервера;
- события изменения конфигурации.

В журнале **веб-интерфейса** содержатся уведомления следующего типа:

- события сервера lighthttpd.

В журнале **изменений настроек шлюза** содержатся уведомления следующего типа:

- события настроек шлюзов.

В журнале **маршрутизации** содержатся уведомления следующего типа:

- события изменения маршрутов.

В журнале **системных событий** содержатся следующие события:

- запуск ntp-сервера;
- нет подключения к ntp-серверу;
- выключение ntp-сервера;
- изменение настроек ntp-сервера;
- сбой Портала авторизации (неуспешная попытка входа в Портал авторизации;
- сбой системы обнаружения вторжений;
- события контроля целостности;
- запуск веб-сервера;
- неуспешный доступ к странице графического интерфейса;
- загрузка системы.

В журнале **действий пользователей** содержатся следующие события:

- включение и отключение межсетевого экрана;
- включение и отключение системы обнаружения вторжений;
- успешный/неуспешный доступ к страницам интерфейса;
- изменение/добавление/удаление правил межсетевого экрана;
- изменение настроек межсетевого экрана;
- изменение правил системы обнаружения вторжений;
- изменение настроек системы обнаружения вторжений;
- успешная/неуспешная авторизация в графическом и консольном интерфейсах;
- изменение размера записей в WebGUI журнале;
- создание нового пользователя;
- включение «сложного» пароля;
- изменение настроек мониторинга состояния системы на странице анализа трафика, настроек monit;
- перезагрузка системы.

В журнале **событий безопасности** содержатся следующие события:

- для системы обнаружения вторжений:
 - срабатывание сигнатур;
- для межсетевого экрана:
 - срабатывания правил межсетевого экрана;
- для arprwatch:
 - подключение несанкционированного устройства;
 - обнаружение конфликта IP-адресов;
 - обнаружение изменения IP, MAC адреса;
 - обнаружение подмены IP-адресов.
- для Портала авторизации:
 - удачная/неудачная авторизация пользователя.
- для Портала авторизации:
 - удачная/неудачная авторизация пользователя;
 - запуск портала авторизации.

Журнал **событий МЭ** в реальном времени динамически отображает все события сети в виде таблицы со следующими полями:

- время инцидента;
- название интерфейса;
- сетевой адрес и порт источника;
- сетевой адрес и порт получателя;
- статус (действие, произведенное с пакетом, инициировавшим запись);
- действие (предпринимаемое в ответ на возможные нарушения безопасности);
- комментарий (дополнительная информация по данному инциденту).

Журнал **необработанных событий от pf** отображает все события сети в виде таблицы со следующими полями:

- номер сработавшего правила;
- номер зависимого правила;
- действие (предпринимаемое в ответ на возможные нарушения безопасности);
- имя правила;
- ID правила;
- физический интерфейс;
- причина сохранения (обычно match – совпало с правилом);
- направление (in или out);
- версия IP (4 или 6);
- TOS;
- ECN;
- TTL;
- ID;
- Offset;
- Flags;
- Protocol ID;
- порт источника;
- порт назначения;
- длина данных;
- флаги;
- Seq ID;
- ACK номер;
- размер окна;
- указатель URG;
- опции TCP.

Журнал **Портала авторизации** содержит уведомления следующего типа:

- события Портала авторизации.

Журнал **DHCPv4** содержит уведомления следующего типа:

- события сервиса DHCPv4.

Системный журнал **системы обнаружения вторжений** отображает информацию обо всех системных событиях системы обнаружения вторжений в виде таблицы со следующими полями:

- время/дата;
- действие (предпринимаемое в ответ на возможные нарушения безопасности);
- сетевой интерфейс;
- сетевой адрес отправителя;
- порт отправителя;
- сетевой адрес получателя;
- порт получателя;
- описание инцидента.

В журнале **инцидентов системы обнаружения вторжений** содержатся уведомления следующего типа:

- события о срабатывании правил системы обнаружения вторжений.

В журнале **NTP** содержатся уведомления следующего типа:

- события сервиса NTP.

В журнале **прокси-сервера** уведомления следующего типа:

- события прокси-сервера.

2 РАЗДЕЛ «ИНСТРУМЕНТАЛЬНАЯ ПАНЕЛЬ»

В разделе «Инструментальная панель» отображается информация, выдаваемая следующими информационными виджетами (Рисунок 11).

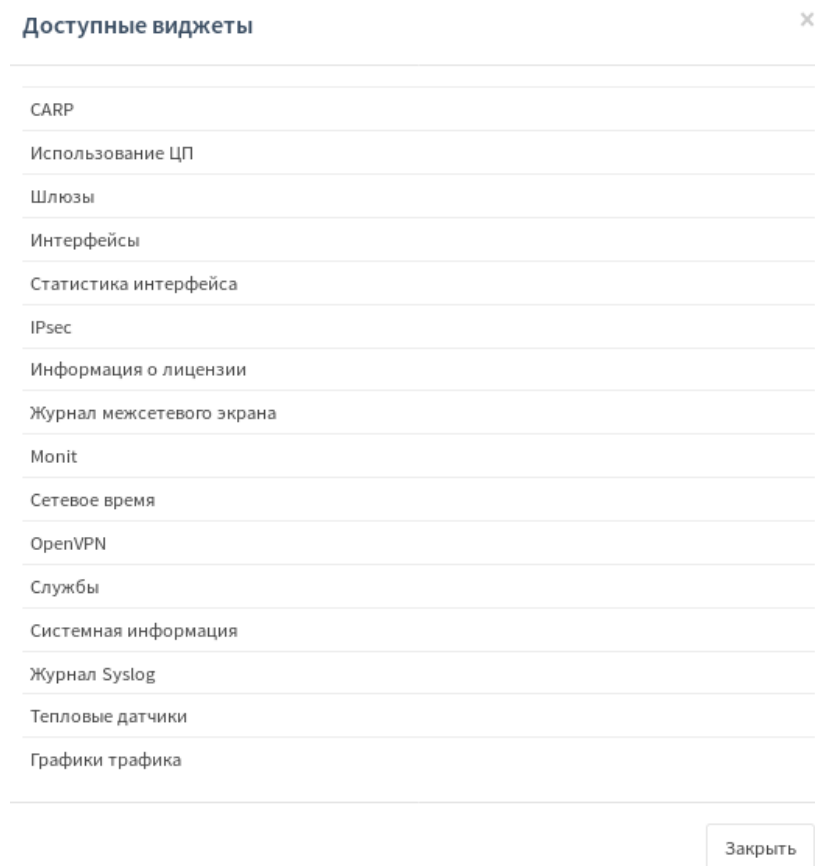


Рисунок 11 – Доступные виджеты

2.1 Виджет «Система информации»

В виджете «Системная информация» отображается основная информация о системе (Рисунок 12):

- имя системы;
- версия системы ПК «InfoWatch ARMA Industrial Firewall», операционной системы, OpenSSL;
- доступные обновления;
- тип процессора;
- загрузка процессора (отображается в виде графика);
- средняя нагрузка;
- время работы системы;
- текущее дата/время;
- последние изменения файла конфигурации (отображается последнее дата, время последнего изменения файла конфигурации);
- размер таблицы состояний;
- использование MBUF;
- использование памяти;

- использование диска.

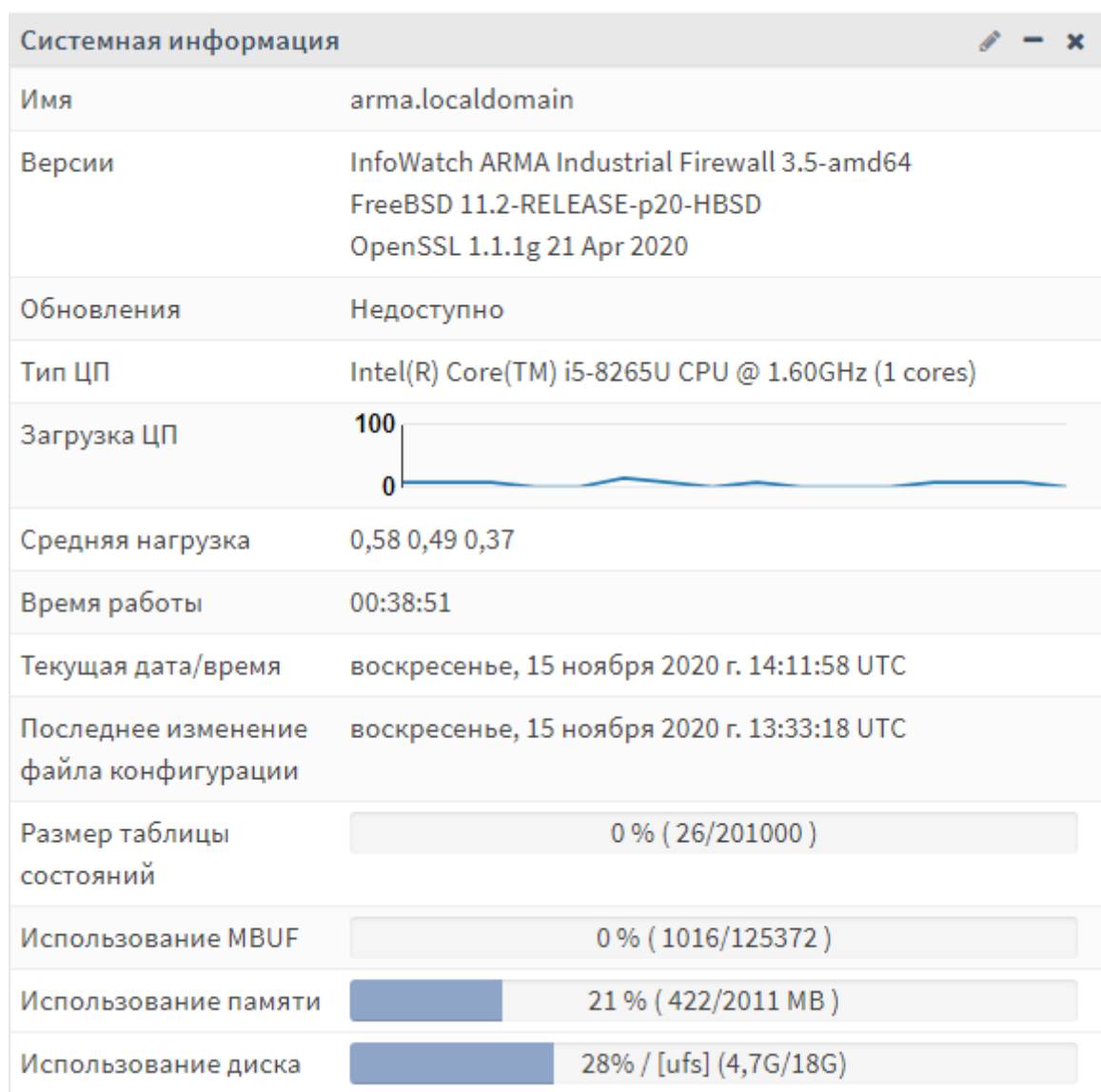


Рисунок 12 – Виджет «Системная информация»

2.2 Виджет «Службы»

В виджете «Службы» отображаются настроенные службы. Со службами имеется возможность производить следующие действия:

- «остановить»
- «запустить»
- «перезагрузить»

Взаимодействие (остановка, запуск, перезапуск) со службами происходит путём нажатия соответствующей кнопки. Если кнопка «запустить» зеленого цвета , значит служба работает. Если кнопка «остановить» красная , значит служба выключена. Для удаления из виджета определенных служб необходимо нажать на кнопку и в появившемся поле ввода ввести названия служб (через запятую), которые необходимо скрыть из виджета (Рисунок 13). Название необходимо

указывать в соответствии с названием службы в колонке «Службы» информационного виджета.































Службы		
Службы	Описание	Статус
configd	Демон настройки системы	  
dhcpcd	DHCPv4-сервер	  
dhcpcd6	DHCPv6-сервер	 
firewall	firewall	 
login	Пользователи и группы	 
ntpd	Демон сетевого времени	  
openssh	Демон SSH	  
pf	Фильтр пакетов	 
radvd	Демон объявления маршрутизатора	 
syslog-ng	Remote Syslog	  
syslogd	Системный журнал	  
webgui	WebGui	 

Рисунок 13 – Виджет «Службы»

2.3 Виджет «Шлюзы»

В виджете «Шлюзы» отображаются настроенные шлюзы, их статус, время приема-передачи (RTT), потеря передачи (Рисунок 14).

Шлюзы				
Имя	Время приема-передачи (RTT)	RTTd	Потеря	Статус
INTERNET_DHCP 192.168.159.2	0.0 ms	0.0 ms	0.0 %	Онлайн

Рисунок 14 – Виджет «Шлюзы»

2.4 Виджет «Интерфейсы»

В виджете «Интерфейсы» отображаются включенные сетевые интерфейсы, их IP-адрес, скорость и режим передачи данных (Рисунок 15).









Интерфейсы			
 <u>Internet</u>		1000baseT <full-duplex>	192.168.0.19
 <u>LAN</u>		1000baseT <full-duplex>	192.168.1.1
 <u>PFSYNC</u>		1000baseT <full-duplex>	172.16.0.1
 <u>WAN</u>		1000baseT <full-duplex>	192.168.2.1

Рисунок 15 – Виджет «Интерфейсы»

2.5 Виджет «Использование ЦП»

В виджете «Использование ЦП» отображается загрузка центрального процессора в виде графика (в режиме реального времени) (Рисунок 16).

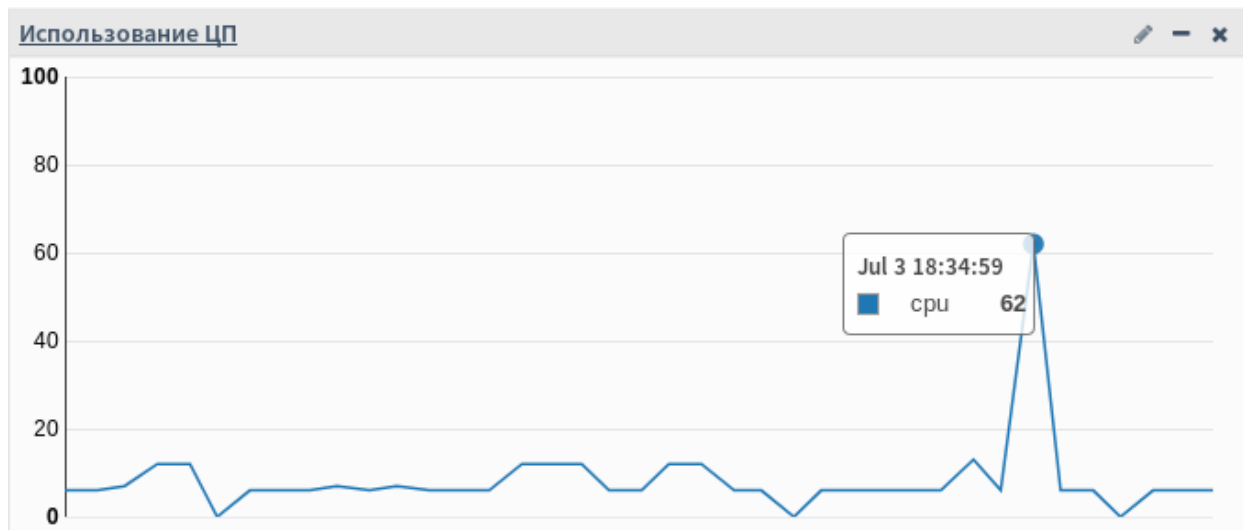



Рисунок 16 – Виджет «Использование ЦП»

2.6 Виджет «Журнал Syslog»

В виджете «Журнал Syslog» (Рисунок 17) отображается журнал Syslog в виде таблицы (в режиме реального времени). В таблице присутствует информация о времени, дате события, а также описания этих событий. Для выбора количества отображаемых событий необходимо нажать на кнопку  и ввести необходимое количество событий, которые будут отображены в виджете

Журнал Syslog	
Jul 3 14:44:35	armaif: /index.php: Successful login for user 'root' from: 192.168.1.100
Jul 3 14:44:12	api[10327]: no active session, user not found
Jul 3 14:43:56	login: ROOT LOGIN (root) ON ttyv0
Jul 3 14:43:56	login: ROOT LOGIN (root) ON ttyv0
Jul 3 14:43:56	login: login on ttyv0 as root
Jul 3 14:43:56	armaif:
Jul 3 14:43:56	armaif: user 'root' authenticated successfully
Jul 3 14:42:34	kernel: SHA256 B3 E2 9C 30 CB 4A 4B 6A 40 05 50 EF DD 78 5F B8
Jul 3 14:42:34	sshlockout[23239]: sshlockout/webConfigurator v3.0 starting up
Jul 3 14:42:34	root: /usr/local/etc/rc.d/lccontrol: WARNING: failed to start lccontrol
Jul 3 14:42:32	kernel: OK
Jul 3 14:42:28	kernel: done.
Jul 3 14:42:28	syslog-ng[97412]: syslog-ng starting up; version='3.25.1'

Рисунок 17 – Виджет «Журнал Syslog»

2.7 Виджет «CARP»

В виджете «CARP» отображается статус устройства при работе в режиме отказоустойчивого кластера, общий совместно используемый виртуальный IP-адрес и сетевой интерфейс (Рисунок 18).

CARP	
⇄ GUESTNET@2	▶ ВЕДУЩЕЕ УСТРОЙСТВО 192.168.0.3

Рисунок 18 – Виджет «CARP»

2.8 Виджет «Статистика интерфейса»


В виджете «Статистика интерфейса» отображается сводная таблица по всем настроенным сетевым интерфейсам в режиме реального времени (Рисунок 19):

- количество входящих/исходящих пакетов;
- количество входящих/исходящих байтов;
- количество ошибок входящего/исходящего трафика;
- количество коллизий для каждого настроенного сетевого интерфейса.

Статистика интерфейса		LAN
Входящие пакеты		1661
Исходящие пакеты		2731
Входящие байты		318 KB
Исходящие байты		2.16 MB
Входящие ошибки		0
Исходящие ошибки		0
Коллизии		0

Рисунок 19 – Виджет «Статистика интерфейса»

2.9 Виджет «Журнал межсетевого экрана»

В виджете «Журнал межсетевого экрана» отображаются события межсетевого экрана в виде таблицы (в режиме реального времени) (Рисунок 13). В таблице содержится информация о времени/дате события, об интерфейсе, через который прошел трафик, о действии, которое было применено к трафику, об отправителе и получателе. Для настройки дополнительных параметров отображения событий межсетевого экрана необходимо нажать на кнопку . В дополнительных параметрах возможен выбор количества отображаемых событий, интервал обновления таблицы, выбор сетевых интерфейсов, события которых будут отображены в журнале межсетевого экрана, а также возможна фильтрация по действию (разрешить, блокировать, отклонить) (Рисунок 20).






Журнал межсетевого экрана				
Действие	Время	Интерфейс	Отправитель	Получатель
	Jul 3 15:42	lo0	127.0.0.1	127.0.0.1
	Jul 3 15:42	lo0	127.0.0.1	127.0.0.1
	Jul 3 15:41	lo0	127.0.0.1	127.0.0.1
	Jul 3 15:41	lo0	127.0.0.1	127.0.0.1
	Jul 3 15:41	lan	192.168.1.100	192.168.1.1

Рисунок 20 – Виджет «Журнал межсетевого экрана»

2.10 Виджет «Monit»

В виджете «Monit» отображаются состояния почтовых серверов (доступность, потребление ресурсов), состояния сервисов (потребляемые ресурсы, количество и другое), состояния сетевых сервисов (в режиме реального времени) (Рисунок 21).

Monit		
Имя	Тип	Статус
Bumerang.localdomain	Система	Может быть изменено
RootFs	Файловая система	ОК

Рисунок 21 – Виджет «Monit»

2.11 Виджет «Сетевое время»

В виджете «Сетевое время» отображается текущее время системы, а также информация о сервере, с которым синхронизируется время в ПК «InfoWatch ARMA Industrial Firewall» (Рисунок 22).

Сетевое время	
Server Time	15:44:04

Рисунок 22 – Виджет «Сетевое время»

2.12 Виджет «Тепловые датчики»

В виджете «Тепловые датчики» (Рисунок 23) отображается температура центрального процессора, материнской платы (по данным ACPI), если в системе имеется поддерживаемый чип датчика температуры. В настройке отображения индикатора температуры возможен ввод следующих значений:

- пороговое значение температуры предупреждения (то имеется значение температуры материнской платы, достигнув которое индикатор температуры материнской платы будет отображаться оранжевым цветом);
- критическая температура МП (то имеется значение температуры материнской платы, достигнув которое индикатор температуры материнской платы будет отображаться красным цветом);
- температура предупреждения ЦПУ (то имеется значение температуры процессора, достигнув которое индикатор температуры процессора будет отображаться оранжевым цветом);
- критической температурой ЦПУ (то имеется значение температуры процессора, достигнув которое индикатор температуры процессора будет отображаться красным цветом).

Датчики температуры

Пороговое значение в °C (от 1 до 100):

Температура предупреждения (МП):	70
Критическая температура (МП):	80
Температура предупреждения (ЦПУ):	70
Критическая температура (ЦПУ):	80

☐ Показывать только первую найденную температуру ядра процессора

Сохранить

* Вы можете настроить нужный тепловой датчик или модуль (-и) [здесь](#).

60 °C	Материнская плата
75 °C	ЦПУ

Рисунок 23 – Виджет «Тепловые датчики»

2.13 Виджет «Графики трафика»

В виджете «Графики трафика» (Рисунок 24) отображается входящий/исходящий трафик в виде графика (в режиме реального времени). Отображение в легенде графика сетевого интерфейса **● LAN** означает, что график сетевого интерфейса включен. Для того чтобы убрать график сетевого интерфейса необходимо нажать на кнопку него в легенде. Отображение в легенде графика сетевого интерфейса **○ LAN** означает, что график сетевого интерфейса выключен. Для того, чтобы добавить график сетевого интерфейса необходимо нажать на кнопку него в легенде.

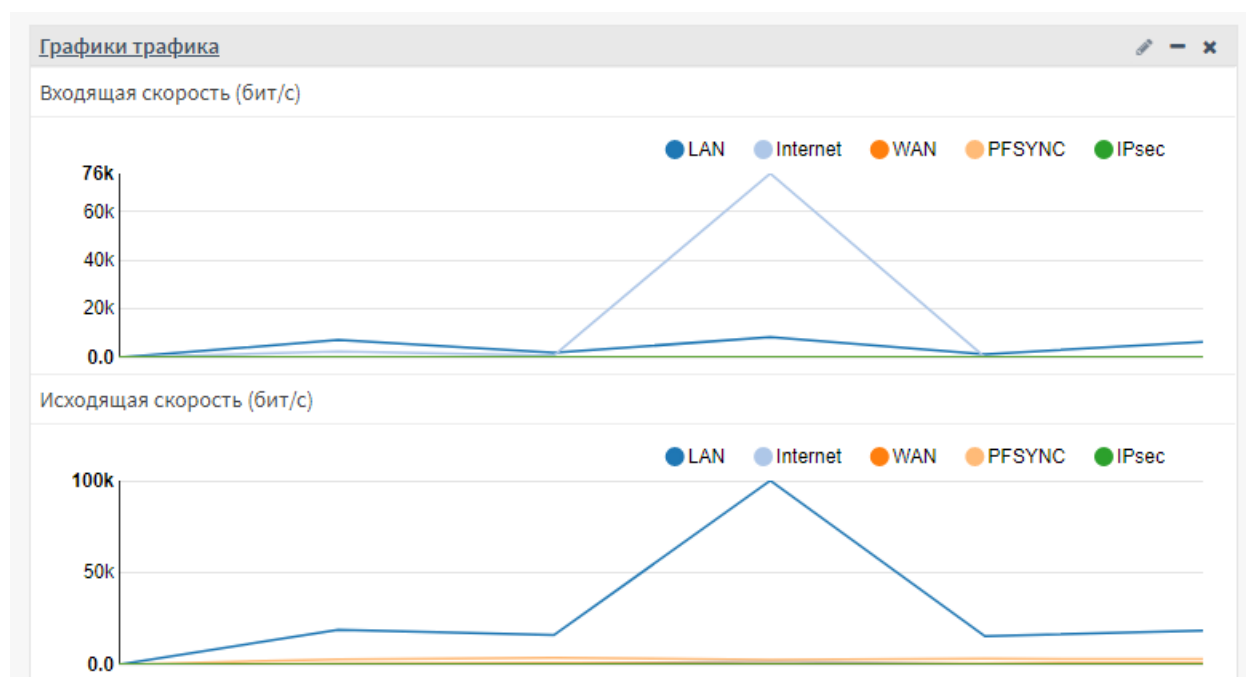
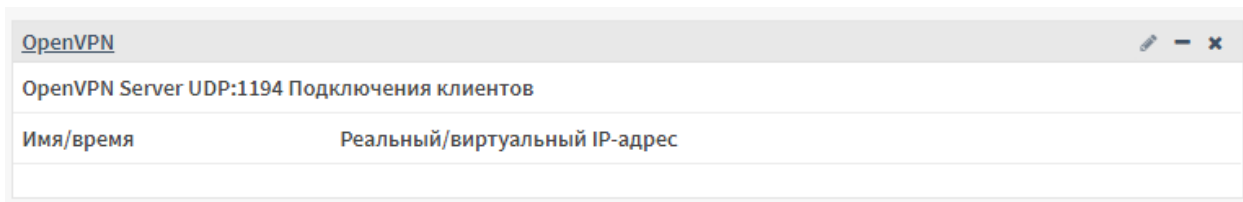


Рисунок 24 – Виджет «Графики трафика»

2.14 Виджет «OpenVPN»

В виджете «OpenVPN» (Рисунок 25) отображаются настроенные OpenVPN серверы.

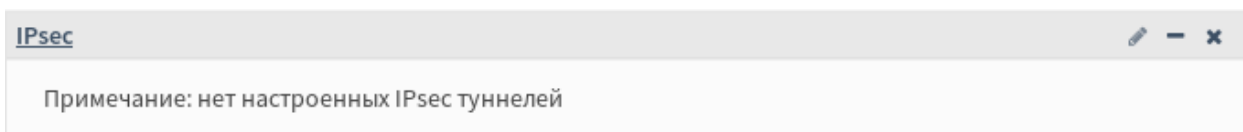


OpenVPN	
OpenVPN Server UDP:1194 Подключения клиентов	
Имя/время	Реальный/виртуальный IP-адрес

Рисунок 25 – Виджет «OpenVPN»

2.15 Виджет «IPsec»

В виджете «IPsec» (Рисунок 26) отображаются настроенные IPsec туннели.

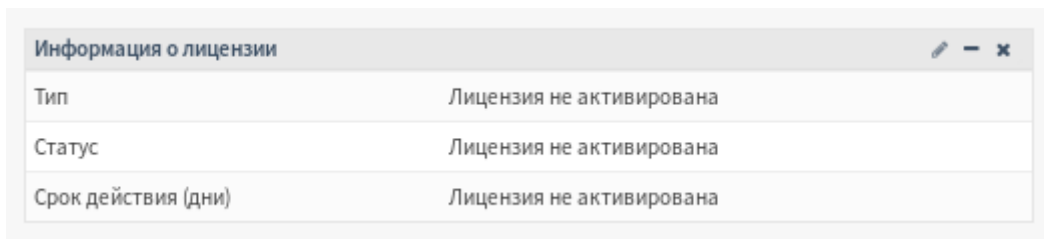


IPsec	
Примечание: нет настроенных IPsec туннелей	

Рисунок 26 – Виджет «IPsec»

2.16 Виджет «Информация о лицензии»

В виджете «Информация о лицензии» (Рисунок 27) отображается информация о лицензии.



Информация о лицензии	
Тип	Лицензия не активирована
Статус	Лицензия не активирована
Срок действия (дни)	Лицензия не активирована

Рисунок 27 – Виджет «Информация о лицензии»

3 РАЗДЕЛ «СОЗДАНИЕ ОТЧЕТОВ»


Раздел «Создание отчетов» состоит из следующих подразделов:

- Состояние;
- Анализ;
- Netflow;
- Настройки;
- Трафик.

3.1 Подраздел «Состояние»

Подраздел «Состояние» – это динамическое представление циклической базы данных (RRD), собранной системой, которое отражает общее состояние и производительность системы с течением времени.

3.1.1 Скрытие области «Параметры»

Для сокрытия/отображения области «Параметры» необходимо нажать на кнопку  рядом с пунктом «Параметры».

3.1.2 Выбор категорий

Элементы области «Параметры» — выпадающий список, состоящий из следующих пунктов списка:

- пакеты;
- система (в котором отображается отчет об использовании памяти, mbufs, о состояниях, о загрузке процессора, о температуре процессора (когда доступна));
- трафик (в котором отображается зависимость объема сетевого трафика от времени для каждого интерфейса).

Пакеты

При выборе категории «Пакеты» любого интерфейса отобразится график зависимости количества входящих/исходящих пакетов (заблокированных и пропущенных по протоколам IPv4, IPv6) выбранного интерфейса от времени (Рисунок 28). Графики обновляются в режиме реального времени.

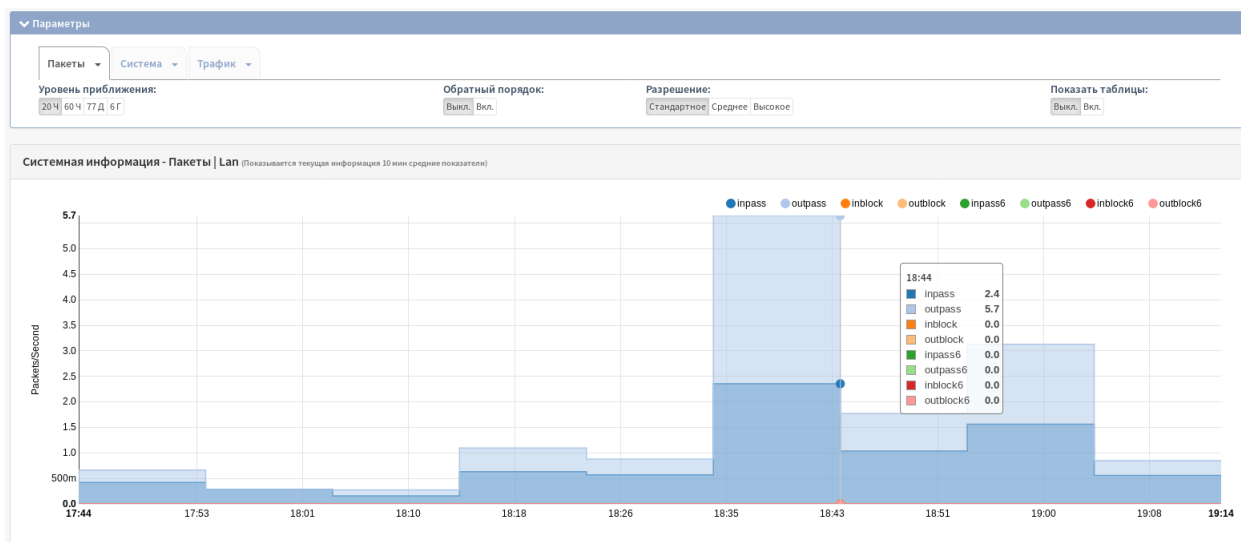


Рисунок 28 – Состояние: Пакеты

Система

При выборе категории «Система» любого системного параметра (память, mbufs, состояния, процессор, температура процессора) будет показан график зависимости использования выбранного параметра системы от времени (Рисунок 29). Графики обновляются в режиме реального времени.

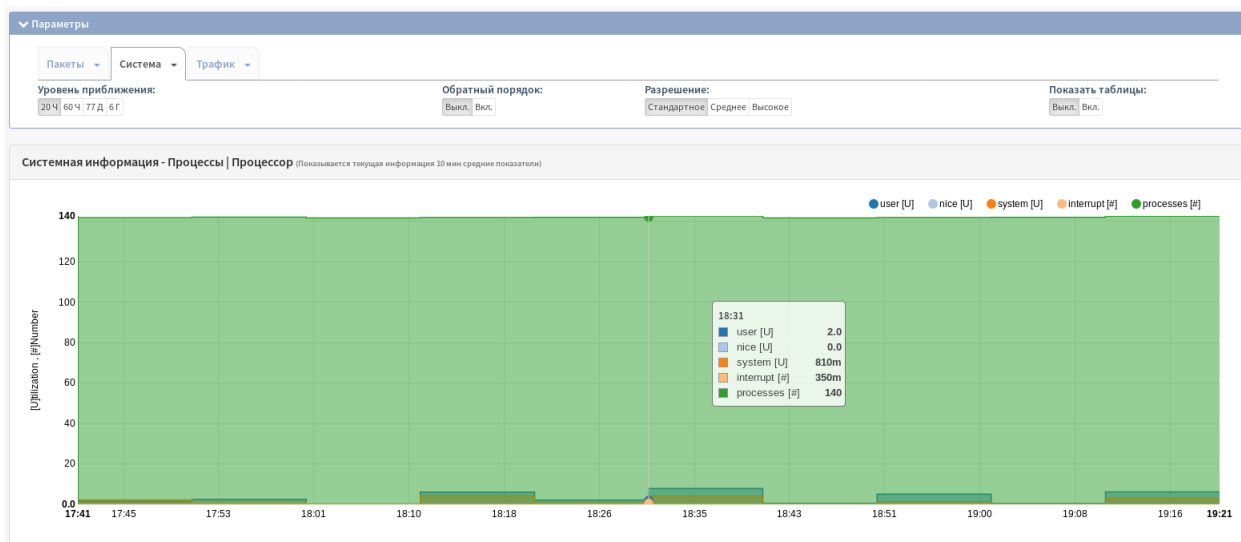


Рисунок 29 – Состояние: Система

Трафик

При выборе категории «Трафик» любого интерфейса будет показан график зависимости количества входящего/исходящего трафика (заблокированных и пропущенных по протоколам IPv4, IPv6) выбранного интерфейса от времени (Рисунок 30). Графики обновляются в режиме реального времени.

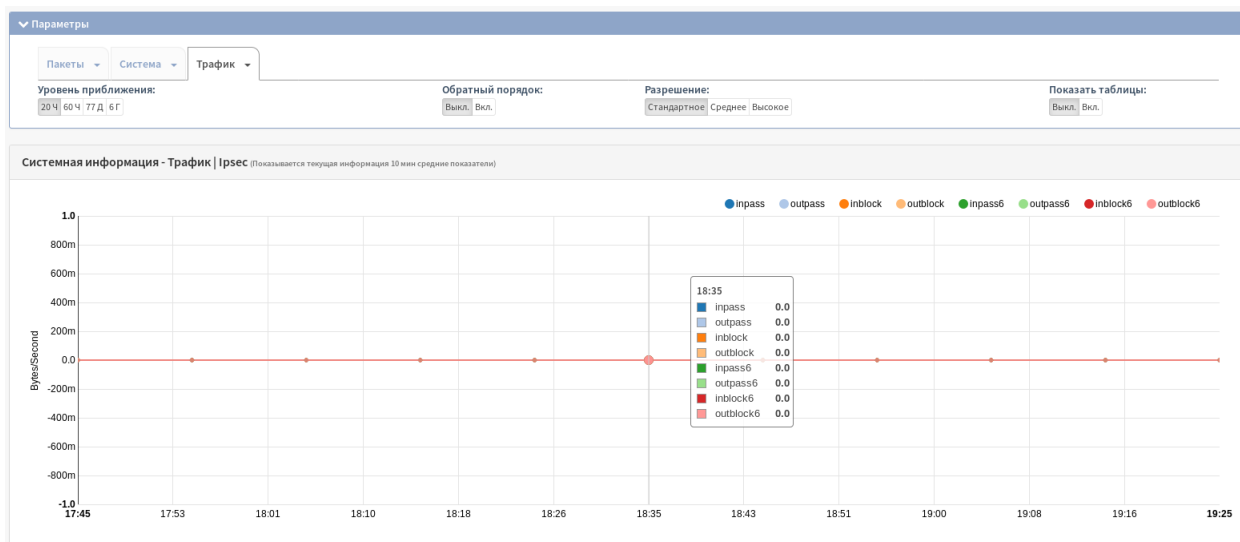


Рисунок 30 – Состояние: Трафик

3.1.3 Выбор уровня приближения

Из набора данных графика для анализа имеется возможность выбрать, за какой промежуток времени отображать данные. Чем больше промежуток времени, тем ниже максимальное разрешение. По умолчанию графики открываются с самым высоким доступным разрешением.

3.1.4 Функция «Обратный порядок»

При выборе «Обратный порядок», каждый нечетный набор данных меняет направление, это необходимо для потоков трафика, где имеется возможность создавать входящие и исходящие потоки в разных направлениях (Рисунок 31).

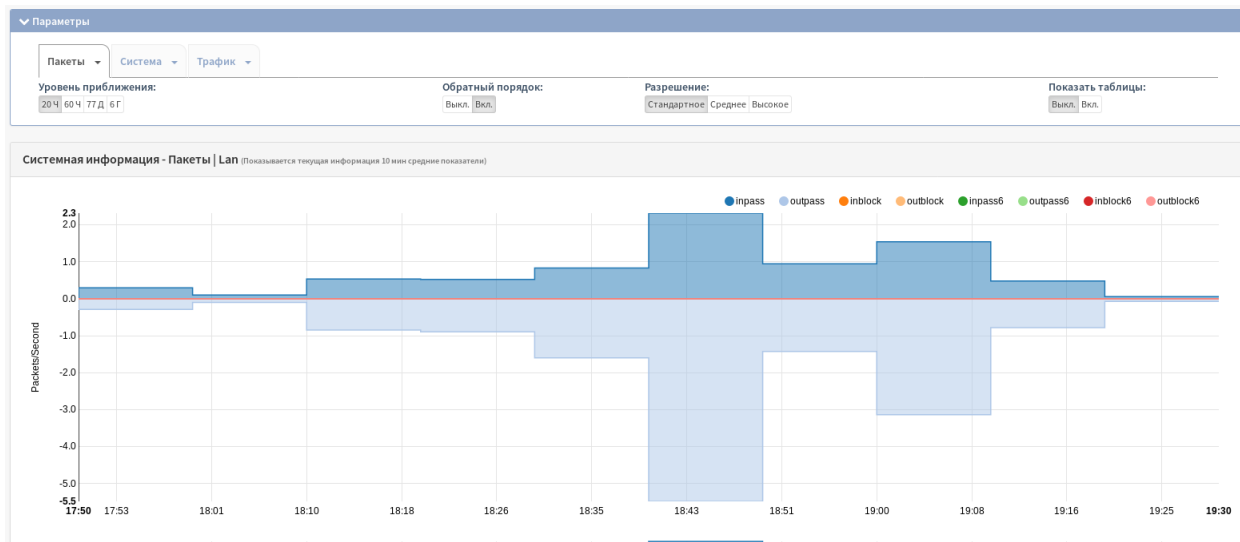


Рисунок 31 – Пример работы функции «Обратный порядок»

3.1.5 Разрешение графика

В параметре «Разрешение графика» возможен выбор максимального количества точек данных, которые будут отображаться на графике.

3.1.6 Функция «Показать таблицы»

По умолчанию таблицы данных скрыты. Чтобы включить их отображение необходимо нажать на кнопку переключатель «Показать таблицы» на параметр «Вкл».

3.1.7 Название графика

Отображает название выбранного графика.

3.1.8 Фильтр меток

Фильтр меток используется для фильтрации данных, которые отображаются. Для отключения — необходимо нажать на кнопку один раз, для выбора только этого набора — два раза (Рисунок 32). Соответственно inpass — входящий прошедший трафик, outpass — исходящий прошедший трафик, inblock — входящий заблокированный трафик, outblock — исходящий заблокированный трафик, inpass6 — входящий прошедший трафик IPv6, outpass6 — исходящий прошедший трафик IPv6, inblock6 — входящий заблокированный трафик IPv6, outblock6 — исходящий заблокированный трафик IPv6.



Рисунок 32 – Фильтр меток

3.1.9 Область графика

Область графика показывает полный график или только часть, которая выбрана в области масштабирования с более высокой детализацией.

3.1.10 Область масштабирования

Область масштабирования используется для выбора и увеличения масштаба на одной части графика, шкала адаптируются автоматически.

Для использования этой функции необходимо нажать на кнопку график и удерживать, перемещая курсор на другую часть области масштабирования. При этом область графика будет обновляться.

Выбор области масштабирования показан на рисунке (Рисунок 33).

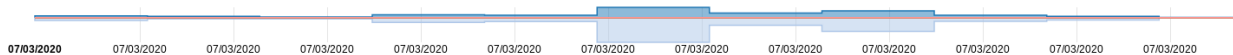


Рисунок 33 – Выбор области масштабирования

Результат увеличения масштаба показан на рисунке (Рисунок 34).

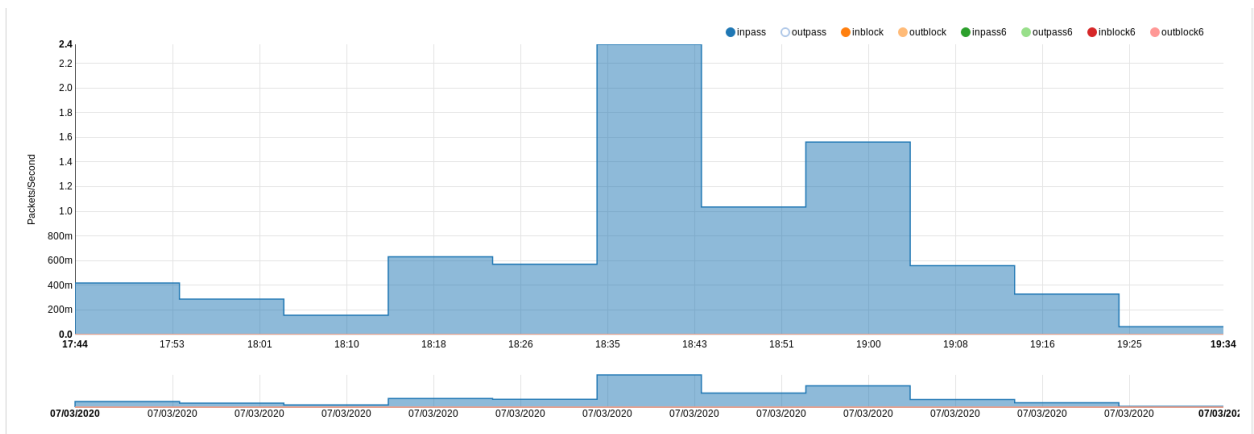


Рисунок 34 – Результат увеличения масштаба

3.1.11 Текущий вид – Общий

Если в пункте «Показать таблицы» выбрано значение «вкл.», то во вкладке «Текущий вид — Общий» (Рисунок 35) будут отображаться:

- минимальное значение каждого набора данных;
- максимальное значение каждого набора данных;
- среднее значение каждого набора данных.

Текущий вид — Общий			
item	min	max	average
user [U]	0	4.37142981471	1.8954562007625
nice [U]	0	0	0
system [U]	0	2.981230391837	1.2852629992117501
interrupt [#]	0	0.24488861866599998	0.09936923674982501
processes [#]	0	141.10196126199997	105.75928470849999

Рисунок 35 – Вкладка «Текущий вид – Общий»

3.1.12 Текущий вид – Подробный

Если в пункте «Показать таблицы» выбрано значение «вкл.», то во вкладке «Текущий вид — Подробный» (Рисунок 36) будет отображаться каждое значение, которое отображается на графике. Имеется возможность переключать режим отображения времени и даты, выбрав режим в поле «Режим отображения времени:». А также экспортировать данные в файл формата «*.csv», нажав кнопку «Загрузить в .CSV».

Текущий вид — Подробный									
<div>Режим отображения времени:</div> <div> <div>Временная метка</div> <div>Full Date & Time</div> <div> <div>загрузить как CSV</div> </div> </div>									
#	временная метка	inpass	outpass	inblock	outblock	inpass6	outpass6	inblock6	outblock6
1	1593787620	0	0	0	0	0	0	0	0
2	1593788220	0.2620747344152	-0.2554257815605	0	0	0	0	0	0
3	1593788820	0.21343961620500002	-0.20842190239299999	0	0	0	0	0	0
4	1593789420	0.39415983026999996	-0.647624705326	0	0	0	0	0	0
5	1593790020	0.523487271696	-0.903742132503	0	0	0	0	0	0
6	1593790620	0.6485127745279999	-1.121296848102	0	0	0	0	0	0
7	1593791220	2.360764710662	-5.610444957705999	0	0	0	0	0	0
8	1593791820	0.966352902747	-1.534278095923	0	0	0	0	0	0
9	1593792420	1.655497502631	-3.3767783283849995	0	0	0	0	0	0
10	1593793020	0.6145039653200001	-0.975708846445	0	0	0	0	0	0
11	1593793620	0.046494352557	-0.0560927235823	0	0	0	0	0	0
12	1593794220	0.0685600229231	-0.09736669532049999	0	0	0	0	0	0
13	1593794820	0.0713944501253	-0.08951581939560001	0	0	0	0	0	0

Рисунок 36 – Вкладка «Текущий вид – Подробный»

Экспортированный набор данных может использоваться для построения отчетов (Рисунок 37).

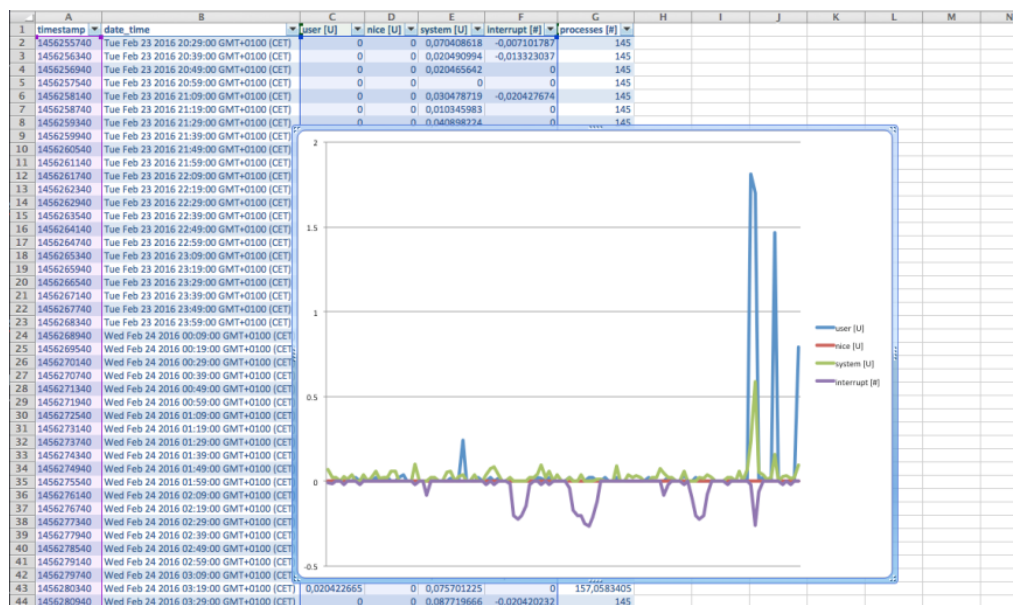


Рисунок 37 – Отчет на основе экспортированных данных

3.2 Подраздел «Анализ»

Подраздел «Анализ» разделен на четыре категории:

- информация;
- всего;
- подробности;
- экспорт.

Netflow – технология мониторинга, разработанная Cisco для статистического анализа трафика. По Netflow передается информация о сетевых соединениях, включая IP-адрес и номер порта в рамках сетевого соединения.

3.2.1 Категория «Всего»

В категории «Всего» реализованы следующие функции:

- графическое представление соединений;

- визуальное отображение наилучшего использования для каждого интерфейса, как IP-адресов, так и портов;
- визуальное отображение входящего/исходящего трафика в пакетах и байтах.

Дополнительно имеется возможность просмотра данных о потоках, интерфейсах, трафике за следующие промежутки времени:

- последние 2 часа, средний показатель за 30 секунд;
- последние 8 часов, средний показатель за 5 минут;
- на прошлой неделе средний показатель за 1 час;
- в прошлом месяце, средний показатель за 24 часа;
- в прошлом году средний показатель за 24 часа;

Общие данные по интерфейсам

В категории «Всего» показаны графики потоков входящего и исходящего трафика для каждого сконфигурированного интерфейса.

Данный раздел позволяет отображать потоки трафика для всех сетевых интерфейсов в виде «Stacked» (график с накоплениями, по умолчанию) (Рисунок 38), в виде «Stream» (поточный график) или в расширенном виде «Expanded» (график зависимости процента трафика выбранного сетевого интерфейса относительно общего трафика всех настроенных сетевых интерфейсов от времени).



Отображение в легенде графика сетевого интерфейса  LAN означает, что график сетевого интерфейса включен. Для того, чтобы убрать график сетевого интерфейса необходимо нажать на кнопку него в легенде. Отображение в легенде графика сетевого интерфейса  LAN означает, что график сетевого интерфейса выключен. При двойном нажатии выбирается отображение графика только этого интерфейса.



Рисунок 38 – Общие данные по интерфейсам

Самые используемые порты/источники

Круговая диаграмма (показанная справа на рисунке (Рисунок 39)) отображает наиболее часто используемые порты назначения/службы в процентном соотношении. Нажатие по сектору круговой диаграммы позволяет открыть страницу с более детализированной информацией.

Круговая диаграмма по IP-адресам (показанная слева на рисунке (Рисунок 39)) работает аналогично круговой диаграмме по портам и показывает наиболее часто используемые IP-адреса назначения.

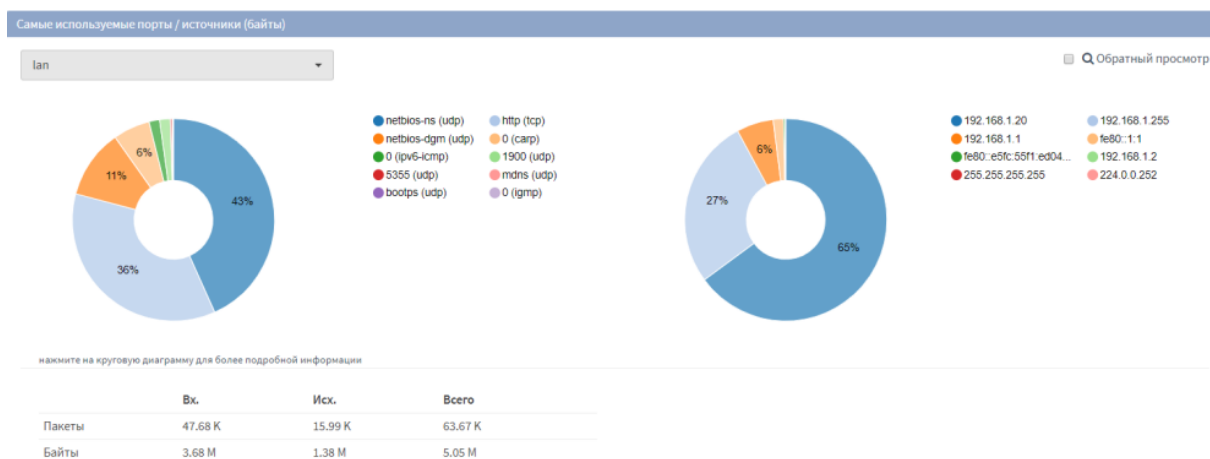


Рисунок 39 – Самые используемые порты/источники

3.2.2 Категория «Подробности»

В категории «Подробности» (Рисунок 40) показан отчет по сетевой статистике в виде таблицы.

В рамках данного отчета отображается идентификатор компьютера, адрес и порт обращения данного компьютера, а также количество переданных данных в рамках данного взаимодействия.

Раздел позволяет ограничить вывод данных с помощью фильтров по диапазону дат, порту назначения и IP-адресу источника.


Всего	Подробности	Экспорт				
С даты	До даты	Интерфейс	Порт назначения	Адрес (назначения)	Адрес источника	
2019-03-16	2019-03-21	lan				
Службы	Отправитель	Получатель	Байты	В последний раз был		
netbios-ns (udp)	192.168.1.20	192.168.1.255	50 MB	Mar 21 15:27:23	88.21 %	
netbios-ns (udp)	192.168.1.255	192.168.1.20	50 MB	Mar 21 15:27:23	88.21 %	
http (tcp)	192.168.1.20	192.168.1.99	14 MB	Mar 21 15:32:14	10.34 %	
netbios-dgm (udp)	192.168.1.20	192.168.1.255	5 MB	Mar 21 15:32:10	3.97 %	
netbios-dgm (udp)	192.168.1.255	192.168.1.20	5 MB	Mar 21 15:32:10	3.97 %	
https (tcp)	192.168.1.20	192.168.1.65	3 MB	Mar 20 00:15:54	2.02 %	
1900 (udp)	192.168.1.20	239.255.255.250	2 MB	Mar 21 15:32:07	1.15 %	
0 (carp)	192.168.1.1	224.0.0.18	1 MB	Mar 21 15:06:08	0.77 %	
1900 (udp)	239.255.255.250	192.168.1.20	309 KB	Mar 21 12:58:18	0.23 %	
0 (ipv6-icmp)	fe80::1:1	ff02::1	287 KB	Mar 21 15:07:47	0.21 %	

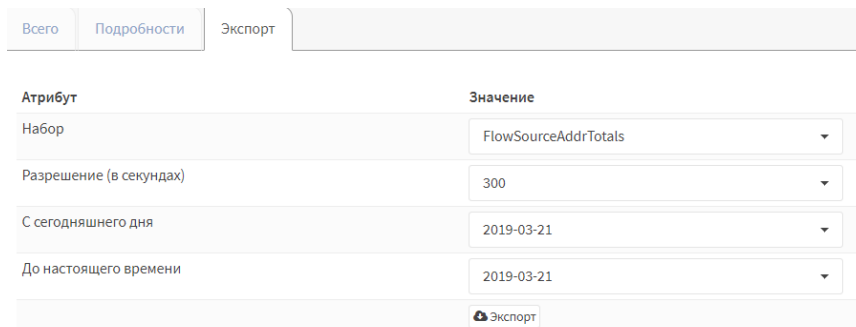
Рисунок 40 – Отчет сетевой статистики

3.2.3 Категория «Экспорт»

Категория «Экспорт» позволяет экспортировать данные в формате «*.csv» для последующего анализа. Для экспорта, необходимо выбрать набор:

- FlowSourceAddrTotals (суммарные данные по IP-адресу источника);
- FlowInterfaceTotals (суммарные данные по интерфейсу);
- FlowDstPortTotals (суммарные данные по порту назначения);
- FlowSourceAddrDetails (полные данные по IP-адресу источника).

Также необходимо выбрать разрешающую точность в секундах (300, 3600, 86400) и диапазон дат. Для экспорта необходимо нажать на кнопку  (Рисунок 41).



Атрибут	Значение
Набор	FlowSourceAddrTotals
Разрешение (в секундах)	300
С сегодняшнего дня	2019-03-21
До настоящего времени	2019-03-21




Рисунок 41 – Экспорт данных

3.3 Подраздел «Netflow»

3.3.1 Категория «Захват»

В категории «Захват» возможна настройка сервиса Netflow.

В поле «Прослушиваемые интерфейсы» необходимо выбрать все интерфейсы, с которых необходимо собирать данные; в большинстве случаев выбираются все доступные интерфейсы. В поле «Интерфейсы WAN» необходимо выбрать WAN-интерфейсы, чтобы избежать повторного подсчета транслированного трафика. Для возможности локального анализа с использованием внутреннего трафика, необходимо установить флажок напротив поля «Захватывать внутренний трафик». Далее необходимо выбрать версию Netflow 5 или 9 в поле «Версия». Версия 5 не поддерживает IPv6. Для передачи данных Netflow на внешние сервисы необходимо добавить получателей в поле «Получатели» (IP-адрес: порт, затем нажать клавишу «ENTER»). Локальный IP-адрес будет добавлен автоматически, если стоит флажок в поле «Захватывать внутренний трафик» (Рисунок 42).

Создание отчетов: NetFlow

Захват

Кэш

расширенный режим

справка

Прослушиваемые интерфейсы

LAN

Очистить все

Интерфейсы WAN

WAN

Очистить все

Захватывать внутренний трафик

☒

Версия

v9

Получатели

192.168.0.1

Очистить все

Таймаут активности

1800

Таймаут неактивности

15

Применить

Рисунок 42 – Настройка Netflow

3.3.2 Категория «Кэш»

В категории «Кэш» отображаются потоки данных в виде таблицы, в которой присутствует информация о названии потока данных, интерфейсе, количестве получателей/отправителей и количестве пакетов (Рисунок 43).

Поток	Интерфейс	Получатели	Отправители	Пакеты
netflow_em1	em1	4	3	1821

Обновить

Рисунок 43 – Netflow: Кэш

3.4 Подраздел «Настройки»

Циклическая база данных (RRD) — набор динамических данных (т.е. последовательность замеров некоторого изменяющегося во времени параметра). Примером таких данных может служить температура, загрузка процессора, сетевой трафик. Все данные хранятся в циклической базе данных, размер которой остаётся неизменным.

Настройка циклической базы данных осуществляется в подразделе «Настройки». Данный подраздел позволяет включить серверную обработку для построения аналитических графиков. Для этого необходимо нажать на флажок напротив поля «Циклическая база данных». А также данный раздел позволяет очистить данные аналитических графиков, очистить данные Netflow, восстановить данные Netflow, нажав соответствующие кнопки (Рисунок 44).

Создание отчетов: Настройки

Параметры базы данных отчетов

Циклическая база данных

☒ Включает серверный процесс для RRD-графиков.

Сохранить

Очистить данные RRD

Очистить данные Netflow

Исправить данные Netflow

Графики не будут повторно создаваться в течение 1 минуты, помните об этом, если решите изменить стиль.

Собранные отчеты

Отчеты

ipsec-packets

ipsec-traffic

lan-packets

lan-traffic

opt1-packets

opt1-traffic



system-cputemp

system-mbuf

system-memory

Рисунок 44 – Настройка циклической базы данных

3.5 Подраздел «Трафик»

Подраздел «Трафик» (Рисунок 45) позволяет увидеть текущую загрузку всех сетевых интерфейсов в режиме реального времени. Фильтр сетевых интерфейсов используется для фильтрации данных в соответствии с выбранным сетевым интерфейсом. Отображение в легенде графика сетевого интерфейса  LAN означает, что график сетевого интерфейса включен. Для того, чтобы убрать график сетевого интерфейса необходимо нажать на кнопку него в легенде. Отображение в легенде графика сетевого интерфейса  LAN означает, что график сетевого интерфейса выключен. При двойном нажатии выбирается отображение графика только этого интерфейса. Также отображается весь трафик в виде таблицы (по выбранным интерфейсам и направлению), в которой отображаются данные о пропускной способности входящего/исходящего трафика, данные об отправителе, полное значение в битах входящего/исходящего трафика.

Создание отчетов: Трафик

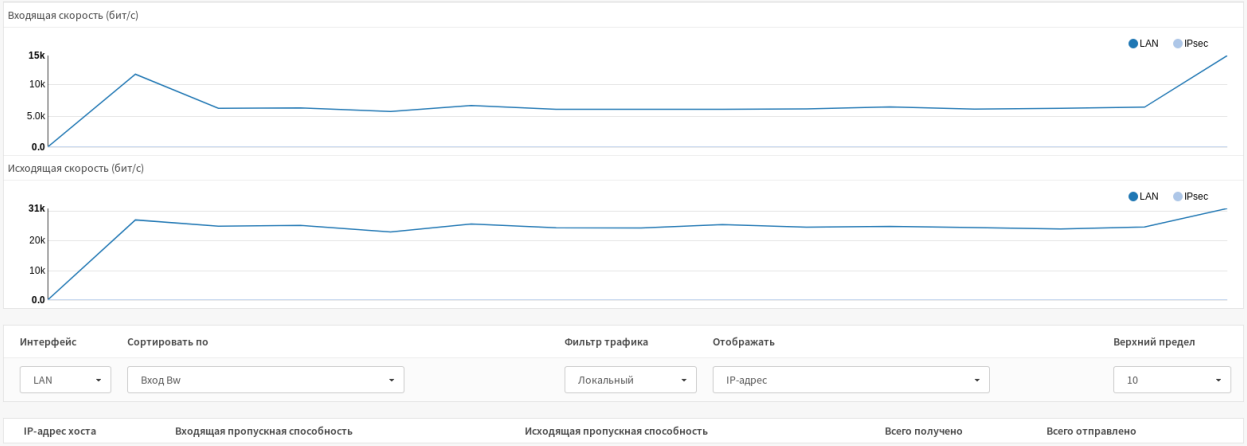


Рисунок 45 – Трафик

4 РАЗДЕЛ «МЕЖСЕТЕВОЙ ЭКРАН»

Раздел «Межсетевой экран» состоит из следующих подразделов:

- Псевдонимы;
- Правила;
- NAT;
- Ограничение трафика;
- Группы интерфейсов;
- Виртуальные IP-адреса;
- Настройки;
- Журналы;
- Диагностика.

4.1 Подраздел «Псевдонимы»

Система позволяет создавать псевдонимы – именованные множества сетей, IP-адресов или портов, которые могут использоваться как один объект в различных разделах межсетевого экрана.

4.1.1 Типы псевдонимов

ПК «InfoWatch ARMA Industrial Firewall» предлагает к использованию следующие типы псевдонимов:

- Порт (-ы);
- таблица URL (IP-адреса);
- URL (IP-адреса);
- GeoIP;
- сетевая группа;
- хост (-ы);
- сеть (-и);
- внешний (расширенный).

Порты

Порты могут быть указаны в качестве одного числа или диапазона, используя двоеточие. Например, чтобы добавить диапазон от 20 до 25, необходимо ввести 20:25.

Таблицы URL-адресов (IP-адресов)

Таблицы URL-адресов используются для получения списка IP-адресов с удаленного сервера URL страницы.

URL (IP-адреса)

URL-адреса используются для получения IP-адреса с удаленного сервера URL страницы.

GeoIP

С помощью псевдонима GeoIP возможно выбрать одну или несколько стран, или целые континенты, чтобы в последующем их заблокировать или разрешить. Необходимо установить флажок «Название континента (выбрать все)», чтобы выбрать все страны в данном регионе (Рисунок 46).

справка

Включен ☒

Активировать псевдоним

Имя

Имя псевдонима может состоять только из символов "a-z, A-Z, 0-9 и _". Псевдонимы могут быть вложены, используя это имя.

Тип

GeolP

Содержание

Region	Countries
Africa	<div>Не выбрано</div> <div><input checked="" type="checkbox"/> <input type="checkbox"/></div>
America	<div>Не выбрано</div> <div><input checked="" type="checkbox"/> <input type="checkbox"/></div>
Antarctica	<div>Не выбрано</div> <div><input checked="" type="checkbox"/> <input type="checkbox"/></div>
Arctic	<div>Не выбрано</div> <div><input checked="" type="checkbox"/> <input type="checkbox"/></div>

Рисунок 46 – Применение псевдонима GeolP

Хосты

При создании псевдонимов тип «Хост» возможен ввод любого количества хостов. Однако, необходимо указать для каждого IP-адрес или полностью определенное имя домена (FQDN). FQDN-имена хостов периодически преобразовываются и обновляются. Если DNS-запрос возвращает множественные IP-адреса, они все используются.

Сети

Сети задаются в формате CIDR. Для определения псевдонима необходимо задать сеть и указать её маску CIDR. Маска /32 означает один IPv4-хост, /128 означает один IPv6-хост, /24 означает представление маски в десятичной форме (255.255.255.0), /64 означает нормальную IPv6-сеть и т. д. Также могут быть указаны FQDN-имена хостов с помощью маски /32 для IPv4 или /128 для IPv6.

Внешний (расширенный)

Используется для задания версии протокола IP.

Сетевая группа

Предназначено для объединения нескольких сетей.

4.1.2 Таблица псевдонимов

В таблице псевдонимов отображаются все псевдонимы со следующими параметрами:

- название;
- тип;
- описание;
- значение.

В таблице представлена возможность создавать или редактировать псевдоним. Для редактирования необходимо нажать на кнопку напротив созданного ранее псевдонима. Для создания нового псевдонима необходимо нажать на кнопку .

4.1.3 Редактирование/создание псевдонима

В поле «Включить» необходимо поставить флажок для включения псевдонима. В поле «Имя» необходимо ввести название псевдонима. В поле «Тип» необходимо выбрать тип псевдонима (типы псевдонимов описаны в подразделе 4.1.1). В поле «Содержание» ввести содержание псевдонима. В поле «Описание» необходимо ввести описание псевдонима и нажать кнопку «Сохранить», после чего нажать кнопку «Применить изменения» (Рисунок 47).

Изменить псевдоним

справка ⓘ

1 Включен ☒

1 Имя

1 Тип

1 Содержание Очистить все

1 Статистические данные ☐

1 Описание

Отменить Сохранить

Рисунок 47 – Редактирование псевдонима

4.1.4 Настройки GeoIP

Вкладка «Настройки GeoIP» позволяет настраивать обновление GeoIP.

В поле «Последнее обновление» отображается время последнего обновления. В поле «Совокупное количество диапазонов» отображается число записей в скачанном наборе. В поле «URL» необходимо указать адрес, откуда будут браться диапазоны GeoIP-адресов (Рисунок 48).

Межсетевой экран: Псевдонимы

Псевдонимы Настройки GeoIP

справка ⓘ

1 Последнее обновление

1 Совокупное количество диапазонов 0

1 URL

Применить

Рисунок 48 – Межсетевой экран: Псевдонимы: Настройки GeoIP

4.2 Подраздел «Правила»

Для удобства в веб-интерфейсе правила межсетевого экрана задаются отдельно для каждого из сетевых интерфейсов, настроенных в ПК «InfoWatch ARMA Industrial Firewall». Правила располагаются в виде списка с приоритетом от

верхнего к нижнему. Иными словами, сетевой пакет проверяется на совпадение с критериями правил по порядку, сверху вниз.


Если сетевой пакет удовлетворяет критериям правила, то к пакету применяется действие, заданное в правиле. Если к пакету уже применено правило, то обработка пакета сетевым экраном прекращается. Такой пакет далее не будет сверяться с оставшимися правилами в списке.

Действия «блокировать (block)» и «отклонить (reject)» предполагают блокирование пакета межсетевым экраном (причем в первом случае, удаленная сторона никак не оповещается о свершившейся блокировке). Действие пропустить (pass) разрешает прохождение пакета через межсетевой экран.



Если сетевой пакет не удовлетворяет критериям ни одного правила, то пакет блокируется (т.е. отбрасывается без индикации удаленной стороне).

4.2.1 Категория «Общие»






















В категории «Общие» приведена таблица правил, которые могут применяться как ко всем сетевым интерфейсам, так и к выбранным. Таблица содержит следующие данные (Рисунок 49):







- графическое отображение состояния правила (включено/выключено, какое действие выполняет (для отключения/включения правила необходимо нажать на кнопку ));
- протокол, к которому применяется правило;
- данные отправителя;
- порт;
- шлюз;
- расписание;
- описание правила.

Межсетевой экран: Правила: Общие

Не выбрано  

Плавающие правила не определены. Плавающие правила не привязаны к одному интерфейсу и могут быть использованы, чтобы охватить политики нескольких сетей одновременно.

	Протокол	Отправитель	Порт	Получатель	Порт	Шлюз	Расписание	Описание 
	IPv4+6 *	*	*	*	*	*	*	Автоматически сгенерированные правила 
	IPv6 IPv6-ICMP	*	*	*	*	*	*	Default deny rule
	IPv6 IPv6-ICMP	*	*	fe80::10, fe02::16	*	*	*	IPv6 requirements (ICMP)
	IPv6 IPv6-ICMP	fe80::10	*	fe80::10, fe02::16	*	*	*	IPv6 requirements (ICMP)
	IPv6 IPv6-ICMP	fe02::16	*	fe80::10	*	*	*	IPv6 requirements (ICMP)
	IPv6 IPv6-ICMP	::	*	fe02::16	*	*	*	IPv6 requirements (ICMP)
	IPv4+6 TCP/UDP	*	*	*	*	*	*	block all targeting port 0
	IPv4+6 TCP/UDP	*	*	*	*	*	*	block all targeting port 0
	IPv4+6 CARP	(self)	*	*	*	*	*	CARP defaults 
	IPv4+6 CARP	*	*	*	*	*	*	CARP defaults 
	IPv4+6 TCP	<sshlockout>	*	(self)	22	*	*	sshlockout
	IPv4+6 TCP	<webConfiguratorlockout>	*	(self)	443	*	*	webConfiguratorlockout
	IPv4+6 *	<virusprot>	*	*	*	*	*	virusprot overload table
	IPv4+6 *	*	*	*	*	*	*	let out anything from firewall host itself
	IPv4+6 *	em2	*	*	*	INTERNET_DHCP	*	let out anything from firewall host itself (force gw) 



 разрешение  блокирование (отключено)  отклонение (отключено)  журналирование (отключено)  входящий/исходящий  первое/последнее совпадение

Активное/неактивное расписание (нажмите для просмотра/редактирования)

Псевдоним (нажмите для просмотра/редактирования)

Рисунок 49 – Межсетевой экран: Правила: Общие



Для редактирования существующего правила необходимо нажать на кнопку  напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку .

При редактировании/создании правила в поле «Действие» необходимо выбрать действие правила (разрешение, блокирование, отклонение). При необходимости отключить правило - установить флажок напротив поля «Отключить». При необходимости сразу применять действие к пакету, который соответствует этому правилу (вне зависимости от приоритета правила) необходимо установить флажок напротив пункта «Быстрая проверка». В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Направление» необходимо выбрать направление пакетов, на которое будет распространяться правило. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (Рисунок 50).

Межсетевой экран: Правила: Общие

Редактировать правило межсетевого экрана	
1 Действие	Блокирование
2 Отключена	<input type="checkbox"/> Отключить это правило
3 Быстрая проверка	<input checked="" type="checkbox"/> При совпадении сразу выполнить действие.
4 Интерфейс	LAN
5 Направление	Вх.
6 Версии TCP/IP	IPv4
7 Протокол	TCP
8 Отправитель / Инвертировать	<input type="checkbox"/>
9 Отправитель	любой

Рисунок 50 – Межсетевой экран: Правила: Общие (редактирование, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Диапазон портов источника» необходимо указать порт источника или диапазон портов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Журналирование» необходимо поставить флажок, если необходимо журналирование пакетов, которые будут соответствовать

редактируемому правилу. В поле «Диапазон портов получателя» необходимо указать порт получателя или диапазон портов. Поле «Категория» позволяет указать категорию группы правил (необязательно). В поле «Описание» необходимо ввести описание правила (Рисунок 51).

Диапазон портов источника	от: <input type="text" value="любой"/>	к: <input type="text" value="любой"/>
Получатель / Инвертировать	<input type="checkbox"/>	
Получатель	<input type="text" value="любой"/>	
Диапазон портов назначения	от: <input type="text" value="любой"/>	к: <input type="text" value="любой"/>
Журналирование	<input checked="" type="checkbox"/> Журналировать пакеты, соответствующие правилу	
Категория	<input type="text"/>	
Описание	<input type="text"/>	

Рисунок 51 – Межсетевой экран: Правила: Общие (редактирование, часть 2)

В разделе «Дополнительные возможности» присутствуют дополнительные параметры настройки правила. В поле «ОС источника» имеется возможность выбрать тип ОС (только при выборе ранее TCP протокола). В поле «Не синхронизировать XMLRPC» необходимо поставить флажок, если необходимо отключить синхронизацию данного правила на ведущем устройстве с другими участниками отказоустойчивого кластера CARP. При необходимости выбора времени работы правила в поле «Расписание» необходимо выбрать настроенное расписание (для настройки расписания необходимо перейти в поле «Межсетевой экран» - «Настройки» - «Расписание»). Для того чтобы правило работало все время, необходимо выбрать «отсутствует». В поле «Шлюз» необходимо выбрать шлюз при использовании маршрутизации (значение «по умолчанию» используется в случае необходимости использования системной таблицы маршрутизации) (Рисунок 52).

дополнительные возможности	
ОС источника	<input type="text" value="BeOS"/>
Не синхронизировать через XMLRPC	<input checked="" type="checkbox"/>
Расписание	<input type="text" value="отсутствует"/>
Шлюз	<input type="text" value="по умолчанию"/>
Дополнительные параметры	<input type="button" value="Показать/скрыть"/>

Рисунок 52 – Межсетевой экран: Правила: Общие (редактирование, часть 3)

При нажатии на кнопку «Показать/скрыть» напротив пункта «Дополнительные параметры» появятся дополнительные поля настройки правила (Рисунок 53). В поле «Разрешить параметры» необходимо установить флажок для разрешения пакетов с параметрами IP, которые блокируются по умолчанию. В поле «Отключить ответ» необходимо установить флажок в случае необходимости отключения автоматически созданного ответа для этого правила. В поле «Установить приоритет» необходимо установить приоритет пакетов, которые будут попадать под это правило, если это необходимо. В поле «Совпадение приоритета» необходимо выбрать приоритет, который будет совпадать с приоритетом пакета. Поле «Установить локальный тег» позволяет вписать метку (в пакет также необходимо вписать эту же метку) для того, чтобы все пакеты, имеющие такую же метку, попадали под правило. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенному для другого правила. В поле «Макс. состояний» необходимо ввести максимальное число записей состояний, которые может создать это правило. В поле «Макс. узлов-источников» необходимо ввести максимальное количество уникальных хостов-источников. В поле «Макс. установленных соединений» необходимо ввести максимальное количество установленных соединений для хоста. В поле «Макс. состояний-источников» необходимо ввести максимальное количество записей состояний для хоста. В поле «Макс. новых соединений» необходимо ввести максимальное количество новых соединений для хоста за секунду. В поле «Тайм-аут состояния» необходимо ввести состояние тайм-аута в секундах. В поле «TCP-флаги» необходимо выбрать флаги, которые должны быть установлены и которые не должны быть установлены для этого правила. В поле «Тип состояния/не rfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через rfsync в кластере высокой доступности. В поле «Тип состояния» необходимо выбрать тип механизма отслеживания состояний:

- Keep state (используется для отслеживания состояния подключения);
- Sloppy state (работает как keep state, но не проверяет порядковые номера);
- Synproxy state (проксирует входящие соединения TCP для защиты серверов от Spoofed TCP и SYN-flood атак, этот тип включает в себя комбинацию функций keep state и modulate state);
- Отсутствует (невозможно использовать механизмы отслеживания состояний, если используется функция управления очередями).

Дополнительные параметры

Показать/скрыть

Применение: оставьте поля пустыми, чтобы применить эту функцию.

разрешить параметры

отказаться от ответа

установить приоритет

Все пакеты

Сохранить текущий приоритет

Низкая задержка/TCP ACK

Использовать основной приоритет

соединение приоритета

Любой приоритет

установить локальный тег

проверка на соответствие локального тега

Макс. состояние

Макс. узлы источника

Макс. установленные соединения

Макс. состояние источника

Макс. новые соединения

Тайм-аут состояния

Флажки TCP

установить

SYN

ACK

FIN

RST

PSH

URG

ECE

CWR

или

Любые флажки.

Тип состояния / нет сброса

Тип состояния

сохранение состояния

Рисунок 53 – Межсетевой экран: Правила: Общие (редактирование, часть 4)

После редактирования правила необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

4.2.2 Категория «[Название интерфейса]»

В категории «[Название интерфейса]» приведена таблица правил, которые применяются к сетевому интерфейсу «[Название интерфейса]», где [Название интерфейса] – это имя интерфейса, установленное при ассоциации этого сетевого интерфейса с физическим сетевым интерфейсом. Таблица правил включает в себя следующие данные (Рисунок 54):




- графическое отображение состояния правила (включено/выключено, какое действие выполняет (для отключения/включения правила необходимо нажать на кнопку ));
- протокол, к которому применяется правило;
- данные отправителя;
- порт;
- шлюз;
- расписание;
- описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то есть правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

Для редактирования существующего правила, необходимо нажать на кнопку  напротив правила. Для того чтобы создать новое правило необходимо нажать на кнопку  **Добавить**.

При редактировании/создании правила необходимо установить флажок напротив поля «Отключить», если необходимо выключить редактируемое правило. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (Рисунок 56).

Межсетевой экран: NAT: Переадресация портов






Редактировать запись перенаправления	
 Отключена	<input type="checkbox"/> Отключить это правило
 Отключить перенаправление (НЕТ)	<input type="checkbox"/>
 Интерфейс	LAN ▾
 Версии TCP/IP	IPv4 ▾
 Протокол	TCP ▾
Отправитель	<input type="button" value="Дополнительно"/>

Рисунок 56 – Межсетевой экран: NAT: Переадресация портов (редактирование, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Диапазон портов источника» необходимо указать порт источника или диапазон портов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Диапазон портов назначения» необходимо указать порт получателя или диапазон портов (Рисунок 57).

Отправитель / Инвертировать	<input type="checkbox"/>	
Отправитель	любой	
Диапазон портов источника	от: любой	к: любой
Получатель / Инвертировать	<input type="checkbox"/>	
Получатель	Единственный хост или сеть	
		32
Диапазон портов назначения	от: HTTP	к: HTTP

Рисунок 57 – Межсетевой экран: NAT: Переадресация портов (редактирование, часть 2)

В поле «Перенаправление целевого IP-адреса» необходимо ввести внутренний IP-адрес сервера для перенаправления портов. В поле «Целевой порт перенаправления» необходимо ввести порт компьютера с введенным в поле «Перенаправление целевого IP-адреса» IP-адресом. В поле «Параметры пула:» необходимо выбрать параметры пула:

- Циклический: перебирает транслируемые IP-адреса;
- Случайный: выбирает случайный адрес из пула транслируемых IP-адресов;
- Хеш источника: использует хеш адреса источника для определения транслируемого IP-адреса и проверяет, чтобы IP-адрес перенаправления для указанного источника всегда был один и то же;
- Битовая маска: применяет маску подсети;
- Фиксированные адреса: параметр может использоваться со случайным и циклическим типами, чтобы конкретный IP-адрес источника преобразовывался в одинаковый транслируемый адрес.

В поле «Описание» необходимо ввести описание правила. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенного для другого правила. В поле «Тип состояния/не rfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через rfsync. В поле «Зеркальный NAT» необходимо выбрать состояние (включить, отключить, использовать системное значение по умолчанию). В поле «Связные правила фильтрации» необходимо выбрать связанные правила фильтрации (Рисунок 58).

1 Перенаправление целевого IP-адреса	<div>Единственный хост или сеть ▾</div> <div>192.168.1.45</div>
1 Целевой порт перенаправления	<div>HTTP ▴</div>
1 Параметры пула:	<div>По умолчанию. ▴</div>
1 Журналирование	<input type="checkbox"/>
1 Описание	<div>Публикация веб-сервера в Интернет</div>
1 Установить локальный тег	<div></div>
1 Проверка на соответствие локального тега	<div></div>
1 Не синхронизировать через XMLRPC	<input type="checkbox"/>
1 Зеркальный NAT	<div>Включен ▾</div>
1 Ассоциация правила фильтрации	<div>Добавить ассоциированное правило ▾</div>
<div>Сохранить Отменить</div>	

Рисунок 58 – Межсетевой экран: NAT: Переадресация портов (редактирование, часть 3)

После редактирования записи перенаправления необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

4.3.2 Категория «Один к одному»

В категории «Один к одному» приведена таблица правил, которые могут применяться для трансляции сетевых адресов в режиме «один к одному». Таблица содержит следующие данные (Рисунок 59):

- графическое отображение состояния правила (включено/выключено, какое действие выполняет (для отключения/включения правила необходимо нажать на кнопку ►));
- интерфейс;
- внешний IP-адрес;
- внутренний IP-адрес;
- IP-адрес назначения;
- описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то есть правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

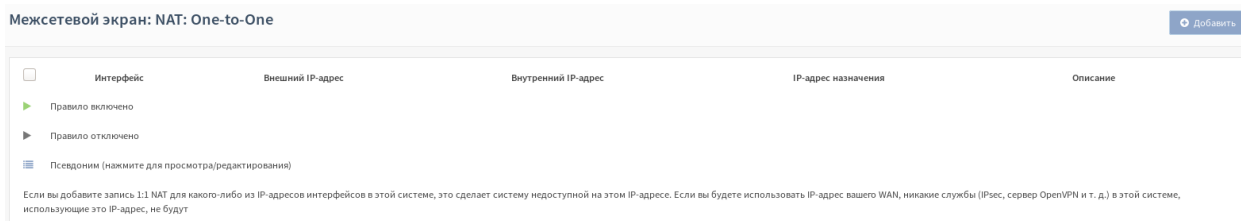

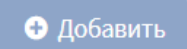


Рисунок 59 – Межсетевой экран: NAT: Один к одному

Для редактирования существующего правила необходимо нажать на кнопку  напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку .

При редактировании/создании правила необходимо установить флажок напротив поля «Отключить», если необходимо выключить редактируемое правило. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле тип необходимо выбрать BINAT (по умолчанию) или NAT. Если сети одного размера, обычно используется BINAT. Правило BINAT определяет двунаправленное отображение между внешней и внутренней сетью и может быть использовано в обоих направлениях, NAT применяется только в одном направлении. В поле «Внешняя сеть» необходимо указать начальный адрес внешней подсети для трансляции в режиме «1:1». В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо ввести внутреннюю подсеть для отображения режима «1:1». В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо ввести получателя, с которым будет использоваться режим «1:1». В поле «Описание» необходимо ввести описание данного правила. В поле «Зеркальный NAT» необходимо выбрать состояние (включен, отключить, использовать системное значение по умолчанию) (Рисунок 60).

Межсетевой экран: NAT: Один-к-одному

Редактировать NAT 1:1 запись

Отключена	<input type="checkbox"/>
Интерфейс	LAN
Тип	BINAT
Внешняя сеть	192.168.1.3
Отправитель / Инвертировать	<input type="checkbox"/>
Отправитель	<div>Единственный хост или сеть</div> <div>lan 32</div>
Получатель / Инвертировать	<input type="checkbox"/>
Получатель	Этот межсетевой экран
Описание	test
Зеркальный NAT	Использовать системное значение по умолчанию

Сохранить Отменить

Рисунок 60 – Межсетевой экран: NAT: Один к одному (редактирование)

После редактирования записи 1:1 необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

4.3.3 Категория «Исходящий»

Категория «Исходящий» позволяет выбрать один из четырех режимов работы исходящего NAT:

- автоматическое создание правил исходящего NAT (нельзя использовать созданные вручную правила);
- ручное создание правил исходящего NAT (правила не будут созданы автоматически);
- смешанное создание правил исходящего NAT (автоматически созданные правила применяются после созданных вручную правил);
- отключить создание правил исходящего NAT (исходящий NAT отключен).

Автоматическое создание правил исходящего NAT

В режиме автоматического создания правил исходящего NAT система автоматически добавляет правила NAT, которые обеспечивают соединение между сетью WAN и внутренней сетью LAN (Рисунок 61).

Межсетевой экран: NAT: Исходящий

Режим:

☒ Автоматическое создание правил исходящего NAT
(нельзя использовать созданные вручную правила)

☐ Смешанное создание правил исходящего NAT
(автоматически созданные правила применяются после созданных вручную правил)

☐ Ручное создание правил исходящего NAT
(правила не будут созданы автоматически)

☐ Отключить создание правил исходящего NAT
(исходящий NAT отключен)

Сохранить

Автоматические настройки

Интерфейс	Сеть-источник	Порт источника	Получатель	Порт назначения	Адрес NAT	NAT порт	Статический порт	Описание
▶ WAN	Сеть GUESTNET, Сеть LAN, Сеть OPT2, 127.0.0.0/8	*	*	500	WAN	*	ДА	Автоматически созданное правило для протокола ISAKMP
▶ WAN	Сеть GUESTNET, Сеть LAN, Сеть OPT2, 127.0.0.0/8	*	*	*	WAN	*	НЕТ	Автоматически созданное правило

Рисунок 61 – Автоматический режим создания правил исходящего NAT

Ручное создание правил исходящего NAT

Режим ручного создания правил исходящего NAT позволяет вручную создавать правила исходящего NAT. Для этого необходимо нажать на кнопку

➕ Добавить

При редактировании правила необходимо установить флажок напротив поля «Отключить», если необходимо выключить редактируемое правило. В поле «Не использовать NAT» необходимо поставить флажок, если необходимо отключить NAT. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на который будут приходить пакеты для проверки соответствия данному правилу. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Инвертировать источник» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «IP-адрес назначения» необходимо ввести адрес исходной сети для преобразования с помощью исходящего NAT. В поле «Порт назначения» необходимо выбрать порт получателя (Рисунок 62).

Межсетевой экран: NAT: Исходящий

Редактировать запись расширенного исходящего NAT

Отключена	<input type="checkbox"/> Отключить это правило
Не использовать NAT	<input type="checkbox"/>
Интерфейс	LAN
Версии TCP/IP	IPv4
Протокол	TCP
Инвертировать источник	<input type="checkbox"/>
IP-адрес источника	Этот межсетевой экран
Порт источника	HTTP
Инвертировать получателя	<input type="checkbox"/>
IP-адрес назначения	любой
Порт назначения	DNS

Рисунок 62 – Ручной режим создания правил исходящего NAT (часть 1)

В поле «Транслируемый IP-адрес/целевой IP-адрес» необходимо ввести IP-адрес для использования другого IP-адреса (не выбранного интерфейса). Необходимо установить флажок напротив поля «Журналирование» для включения журналирования событий правила. В поле «Статический порт» необходимо установить флажок для использования статического порта. В поле «Параметры пула:» необходимо выбрать параметры пула:

- Циклический: перебирает транслируемые IP-адреса;
- Случайный: выбирает случайный адрес из пула транслируемых IP-адресов;
- Хеш источника: использует хеш адреса источника для определения транслируемого IP-адреса и проверяет, чтобы IP-адрес перенаправления для указанного источника всегда был один и тот же;
- Битовая маска: применяет маску подсети;
- Фиксированные адреса: параметр может использоваться со случайным и циклическим типами, чтобы конкретный IP-адрес источника преобразовывался в одинаковый транслируемый адрес.

Поле «Установить локальный тег» позволяет вписать метку (в пакет необходимо вписать эту же метку) для того, чтобы все пакеты, имеющие такую же

метку, попадали под правило. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенному для другого правила. В поле «Тип состояния/не rfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через rfsync. В поле «Описание» необходимо ввести описание правила (Рисунок 63).

Транслируемый IP-адрес / целевой IP-адрес	Адрес интерфейса
Журналирование	<input type="checkbox"/> Журналировать пакеты, соответствующие правилу
Транслируемый / порт:	5000
Статический порт:	<input type="checkbox"/>
Параметры пула:	Циклический
Установить локальный тег	
Проверка на соответствие локального тега	
Не синхронизировать через XMLRPC	<input type="checkbox"/>
Описание	
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/>	

Рисунок 63 – Ручной режим создания правил исходящего NAT (часть 2)

Смешанное создание правил исходящего NAT

Режим смешанного создания правил исходящего NAT позволяет создавать правила исходящего NAT, но также присутствуют автоматические правила исходящего NAT. Автоматически добавленные правила показаны на рисунке (Рисунок 61). Добавление правил исходящего NAT описано в подразделе 4.3.3 настоящего руководства.

Отключить создание правил исходящего NAT

Режим отключения создания правил исходящего NAT отключает все правила исходящего NAT.

4.3.4 Категория «NPTv6»

В категории «NPTv6» приведена таблица правил, которые могут применяться для преобразования адресов IPv6. Чаще всего это используется для перевода глобальных («WAN») IP-адресов в локальные. Таблица содержит следующие данные (Рисунок 64):

- графическое отображение состояния правила (включено/выключено, какое действие выполняет);

- интерфейс;
- внешний префикс;
- внутренний префикс;
- описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

Межсетевой экран: NAT: NPTv6 + Добавить

<input type="checkbox"/>	Интерфейс	Внешний префикс	Внутренний префикс	Описание	
<input type="checkbox"/>	▶ LAN	123.23.2.3/128	192.123.22.2/128	33	← ↗ ✖ ☐
← ☐					
▶ Правило включено					
▶ Правило отключено					

Рисунок 64 – Межсетевой экран: NAT: NPTv6



Для редактирования существующего правила необходимо нажать на кнопку напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку + Добавить.

При редактировании правила необходимо установить флажок напротив пункта «Отключить» для выключения редактируемого правила. В поле «Интерфейс» необходимо выбрать сетевой интерфейс, на который будут приходить пакеты для проверки соответствия данному правилу. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель/Адрес» необходимо ввести внутренний (LAN) IPv6-префикс уникального локального адреса для трансляции сетевых префиксов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель/адрес» необходимо ввести глобальный индивидуальный маршрутизируемый IPv6-префикс. В поле «Описание» необходимо ввести описание правила (Рисунок 65).

Межсетевой экран: NAT: NPTv6

Редактировать запись NAT NPTv6

Отключена ☐

Интерфейс LAN

Внутренний IPv6-префикс

Отправитель / Инвертировать ☐

Отправитель / Адрес 192.123.22.2 128

IPv6-префикс назначения

Получатель / Инвертировать ☐

Получатель / Адрес 123.23.2.3 128

Описание 33

Сохранить Отменить

Рисунок 65 – Межсетевой экран: NAT: NPTv6 (редактирование правила)

После редактирования записи NAT NPTv6 необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

4.4 Подраздел «Ограничение трафика»

Ограничитель трафика позволяет разграничивать пропускную способность каналов связи между пользователями или сегментами сети и назначать приоритет обработки трафика.

Подраздел «Ограничение трафика» позволяет просматривать и настраивать:

- каналы;
- очереди;
- правила;
- статус.

4.4.1 Категория «Каналы»

В категории «Каналы» приведена таблица каналов, доступных для ограничения трафика. Таблица содержит следующие данные (Рисунок 66):

- состояние канала (включен/выключен);
- пропускная способность;
- метрика;
- маска;
- описание канала.

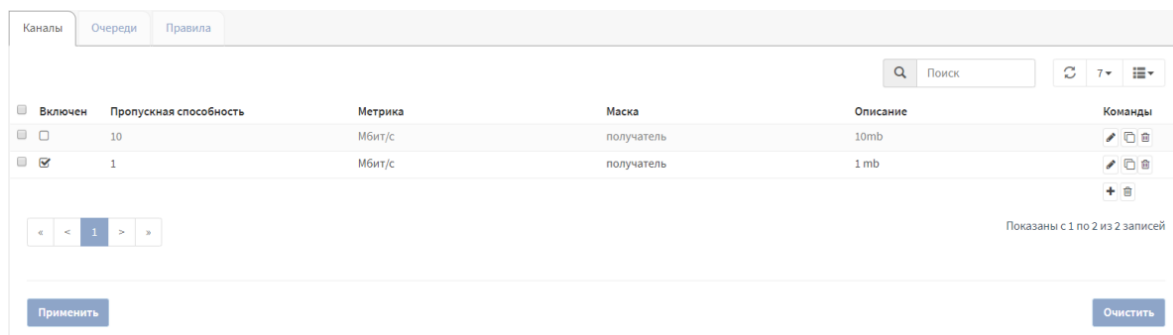




Рисунок 66 – Межсетевой экран: Ограничение трафика: Настройки: Каналы

Для того чтобы редактировать существующие каналы необходимо нажать на кнопку  напротив канала. Для того чтобы создать новый канал, необходимо нажать на кнопку .

При редактировании канала необходимо установить флажок напротив поля «Включен». В поле «Пропускная способность» необходимо ввести пропускную способность канала. В поле «Единицы измерения пропускной способности» необходимо выбрать единицы измерения пропускной способности. В поле «Очередь» необходимо ввести количество динамических очередей. В поле маска необходимо выбрать:

- «получатель», чтобы каждому IP-адресу получателя была указана пропускная способность;
- «отправитель», чтобы каждому IP-адресу отправителя была указана пропускная способность;
- «не выбрано», если необходимо создать канал с фиксированной пропускной способностью.

В поле «Buckets» необходимо ввести размер хеш-таблицы, используемой для хранения динамических каналов. В поле «Тип планировщика» необходимо выбрать алгоритм планирования. В поле «Включить CoDel» необходимо установить флажок для включения CoDel (планировщик задержек). В поле «(FQ-)CoDel цель» необходимо ввести минимально допустимую задержку персистентной очереди. В поле «(FQ-)CoDel интервал» необходимо ввести интервал перед отбросом пакетов. В поле «(FQ-)CoDel ECN» необходимо установить флажок для включения уведомления. В поле «(FQ-)CoDel квант» необходимо ввести количество байт, которое может принять очередь перед тем, как она будет передвинута в конец списка очередей. В поле «Включить PIE» необходимо поставить флажок для включения активного управления очередью. В поле «Задержка» необходимо ввести задержку по этому каналу. В поле «Описание» необходимо добавить описание этого канала. Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (Рисунок 67).

Редактировать канал ✕

расширенный режим справка

Включен ☒

Пропускная способность

Единицы измерения пропускной способности

Мбит/с

Очередь

Маска

Не выбрано

Buckets

Тип планировщика

FIFO

Включить CoDel ☒

(FQ-)CoDel target

(FQ-)CoDel интервал

(FQ-)CoDel ECN ☐

FQ-CoDel quantum

FQ-CoDel ограничение

FQ-CoDel потоки

Включить PIE ☒

Задержка

Описание

Отменить

Сохранить

Рисунок 67 – Межсетевой экран: Ограничение трафика: Настройки: Каналы (редактирование)

4.4.2 Категория «Очереди»

В категории «Очереди» приведена таблица каналов. Таблица содержит следующие данные (Рисунок 68):

- состояние очереди (включена/выключена);
- название очереди;
- весовой коэффициент;
- описание очереди.

74

arma.infowatch.ru

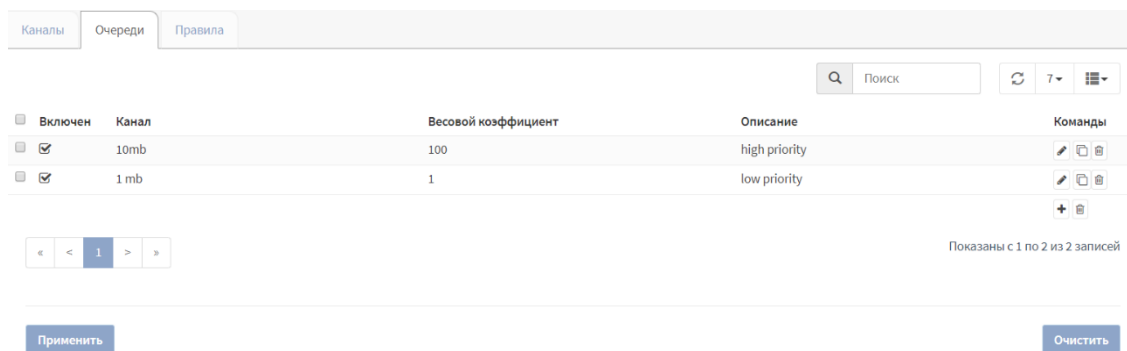


Рисунок 68 – Межсетевой экран: Ограничение трафика: Настройки: Очереди

Для того чтобы редактировать существующие очереди необходимо нажать на кнопку напротив канала. Для того чтобы создать новую очередь, необходимо нажать на кнопку .

При редактировании очереди необходимо установить флажок напротив поля «Включен». В поле «Канал» необходимо выбрать канал, для которого настраивается очередь. В поле «Весовой коэффициент» необходимо ввести приоритет канала от 1 до 100. В поле маска необходимо выбрать:

- «получатель», чтобы каждому IP-адресу получателя была указана пропускная способность;
- «отправитель», чтобы каждому IP-адресу отправителя была указана пропускная способность;
- «не выбрано», если необходимо создать канал с фиксированной пропускной способностью.

В поле «Buckets» необходимо ввести размер хеш-таблицы, используемой для хранения динамических каналов. В поле «Включить CoDel» необходимо установить флажок для включения CoDel. В поле «(FQ-)CoDel цель» необходимо ввести минимально допустимую задержку персистентной очереди. В поле «(FQ-)CoDel интервал» необходимо ввести интервал перед отбросом пакетов. В поле «(FQ-)CoDel ECN» необходимо установить флажок для уведомления. В поле «Включить PIE» необходимо поставить флажок для включения активного управления очередью. В поле «Описание» необходимо добавить описание этого канала. Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (Рисунок 69).

расширенный режим

справка

Включен	<input checked="" type="checkbox"/>
Канал	Не выбрано
Весовой коэффициент	100
маска	Не выбрано
Buckets	
Включить CoDel	<input type="checkbox"/>
(FQ-)CoDel target	
(FQ-)CoDel интервал	
(FQ-)CoDel ECN	<input type="checkbox"/>
Включить PIE	<input type="checkbox"/>
Описание	test

Отменить

Рисунок 69 – Межсетевой экран: Ограничение трафика: Настройки: Очереди (редактирование)



4.4.3 Категория «Правила»

В категории «Правила» приведена таблица правил, которые применяются к настроенным каналам и очередям. Таблица содержит следующие данные (Рисунок 70):

- состояние правила (включен/выключен);
- последовательность проверки правил;
- интерфейс;
- протокол;
- отправитель;
- получатель;
- описание правила.

Каналы		Очереди		Правила									
						<input type="text" value="Поиск"/>		<input type="button" value="↺"/> <input type="button" value="7"/> <input type="button" value="☰"/>					
<input type="checkbox"/>	Включен	#	Интерфейс	Протокол	Отправитель	Получатель	Получатель	Описание	Команды				
<input checked="" type="checkbox"/>		1	WAN	ip	10.0.0.1/24	any	high priority	high priority	<input type="button" value="✎"/> <input type="button" value="📄"/> <input type="button" value="🗑"/>				
<input checked="" type="checkbox"/>		1	WAN	ip	any	any	1 mb	1mb out	<input type="button" value="✎"/> <input type="button" value="📄"/> <input type="button" value="🗑"/>				
									<input type="button" value="+"/> <input type="button" value="🗑"/>				
<input type="button" value="«"/> <input type="button" value="<"/> <input type="button" value="1"/> <input type="button" value=">"/> <input type="button" value="»"/>									Показаны с 1 по 2 из 2 записей				
<input type="button" value="Применить"/>					<input type="button" value="Очистить"/>								

Рисунок 70 – Межсетевой экран: Ограничение трафика: Настройки: Правила

Для того чтобы редактировать существующие правила, необходимо нажать на кнопку  напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку .

При редактировании правила необходимо установить флажок напротив поля «Включить» при необходимости включения редактируемого правила. В поле «Последовательность» необходимо выбрать порядок проверки правил в наборе правил. В поле «Интерфейс» необходимо выбрать сетевой интерфейс, на который будут приходить пакеты для проверки соответствия данному правилу. В поле «Интерфейс 2» необходимо выбрать вспомогательный интерфейс, при этом ПК будет проверять на соответствие правилам пакеты, проходящие от интерфейса 1 к интерфейсу 2 и наоборот. В поле «Протокол» необходимо выбрать протокол, для которого будет выполняться это правило. В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила. В поле «Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Получатель» необходимо ввести отправителя. В поле «Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Получатель». В поле «Dst-port» необходимо ввести порт получателя. В поле «Направление» выбрать направление правила. В поле «Цель» необходимо выбрать созданный канал. В поле «Описание» необходимо ввести описание правила (Рисунок 71). Необходимо нажать «Сохранить».

расширенный режим
справка

Включен	<input checked="" type="checkbox"/>
Последовательность	1
Интерфейс	LAN
Интерфейс 2	отсутствует
Протокол	ICMP
Отправитель	<input type="text" value="any"/> <div>Очистить все</div>
Инвертировать отправителя	<input type="checkbox"/>
Порт источника	any
Получатель	<input type="text" value="any"/> <div>Очистить все</div>
Инвертировать получателя	<input type="checkbox"/>
Порт назначения	any
DSCP	<div>Не выбрано</div> <div>Очистить все</div>
Направление	оба (-е)
Получатель	Не выбрано
Описание	test

Отменить

Сохранить

Рисунок 71 – Межсетевой экран: Ограничение трафика: Настройки: Правила (редактирование)

4.4.4 Категория «Статус»

Категория «Статус» позволяет просматривать статус всех настроенных каналов и очередей (Рисунок 72).

```

Limiters:
10000: 10.000 Mbit/s    0 ms burst 0
q141072 50 sl. 0 flows (1 buckets) sched 75536 weight 0 lmax 0 pri 0 droptail
  sched 75536 type FIFO flags 0x1 256 buckets 0 active
  mask: 0x00 0x00000000/0x0000 -> 0xffffffff/0x0000
10001: 1.000 Mbit/s    0 ms burst 0
q141073 50 sl. 0 flows (1 buckets) sched 75537 weight 0 lmax 0 pri 0 droptail
  sched 75537 type FIFO flags 0x1 256 buckets 0 active
  mask: 0x00 0x00000000/0x0000 -> 0xffffffff/0x0000

Queues:
q10000 50 sl. 0 flows (256 buckets) sched 10000 weight 100 lmax 0 pri 0 droptail
  mask: 0x00 0x00000000/0x0000 -> 0xffffffff/0x0000
q10001 50 sl. 0 flows (256 buckets) sched 10001 weight 1 lmax 0 pri 0 droptail
  mask: 0x00 0x00000000/0x0000 -> 0xffffffff/0x0000

```

Рисунок 72 – Межсетевой экран: Ограничение трафика: Статус

4.5 Подраздел «Группы интерфейсов»

Подраздел «Группы интерфейсов» позволяет создавать правила, применяемые к нескольким интерфейсам без дублирования правил (Рисунок 73).

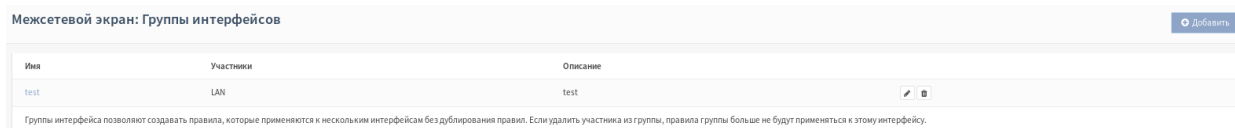




Рисунок 73 – Межсетевой экран: Группы интерфейсов

Для того чтобы редактировать существующие группы, необходимо нажать на кнопку  напротив группы интерфейсов. Для того чтобы создать новую группу интерфейсов, необходимо нажать на кнопку  **Добавить**.

При редактировании группы в поле «Имя» необходимо ввести название группы интерфейсов. В поле «Описание» необходимо ввести описание группы интерфейсов. В поле «Участники» необходимо выбрать интерфейс/интерфейсы, которые относятся к этой группе (Рисунок 74). Необходимо нажать на кнопку «Сохранить» для сохранения настроек.

Межсетевой экран: Группы интерфейсов

Редактировать группы интерфейсов

Имя

test

Описание

test

Участники

LAN

Сохранить

Отменить

Рисунок 74 – Межсетевой экран: Группы интерфейсов (редактирование)

4.6 Подраздел «Виртуальные IP-адреса»

Виртуальные IP-адреса необходимы для поддержки работы в режиме отказоустойчивого кластера.

4.6.1 Категория «Настройка»

В категории «Настройка» приведена таблица настроенных виртуальных IP-адресов, если таковые имеются. Таблица содержит следующие данные (Рисунок 75):

- виртуальный IP-адрес;
- интерфейс;
- тип (режим);
- описание виртуального IP-адреса.







<input type="checkbox"/>	Виртуальный IP-адрес	Интерфейс	Тип	Описание
<input type="checkbox"/>	192.168.0.3/32 (vhid 2, freq. 1 / 0)	GUESTNET	CARP	  
 				

Рисунок 75 – Межсетевой экран: Виртуальные IP-адреса: Настройки

Для того чтобы редактировать существующие виртуальные IP-адреса, необходимо нажать на кнопку  напротив виртуального IP-адреса. Для того чтобы создать новый виртуальный IP-адрес, необходимо нажать на кнопку

 **Добавить**

При редактировании виртуального IP-адреса в поле «Режим» необходимо выбрать режим (тип) виртуального IP-адреса:

- CARP;
- IP-псевдоним;
- Proxy ARP;
- другое.

В поле «Интерфейс» необходимо выбрать сетевой интерфейс для редактируемого виртуального IP-адреса. В поле «Тип» необходимо выбрать тип IP-адреса:

- одиночный IP-адрес;
- сеть.

В поле «Адрес» необходимо ввести IP-адрес и маску подсети. В поле «Шлюз» необходимо ввести адрес шлюза. Для входа через шлюз на некоторых типах интерфейсов требуется конфигурирование IP-псевдонимов. В других случаях это поле не заполняется. В поле «Пароль виртуального IP-адреса» необходимо ввести пароль группы VHID. Виртуальная группа (VHID) – это группа, в которую объединяются серверы CARP. Виртуальной группе назначается виртуальный IP-адрес, которому протокол CARP выделяет виртуальный MAC-адрес. В поле «Группа VHID» необходимо ввести группу VHID, которая будет распределена между устройствами. В поле «Частота синхронизации» необходимо выбрать частоту, с которой это устройство будет отправлять сообщения. В поле «Описание»

необходимо ввести описание редактируемого виртуального IP-адреса и нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» (Рисунок 76).

Редактировать виртуальный IP-адрес

Режим:

CARP

Интерфейс

GUESTNET

IP-адрес (-а)

Тип

Одиночный IP-адрес

Адрес

192.168.0.3

32

Шлюз

Пароль виртуального IP-адреса

.

Группа VHID

2

Выберите невыделенный VHID

Частота синхронизации

Базовая:

1

Со сдвигом времени:

0

Описание

Рисунок 76 – Межсетевой экран: Виртуальные IP-адреса: Настройки (редактирование)

4.6.2 Категория «Статус»

В категории «Статус» отображается информация о статусе работы CARP. Эта категория позволяет просматривать статус CARP всех настроенных IP-адресов, приостанавливать/включать CARP и включать/выключать CARP, нажимая соответствующие кнопки, а также просматривать pfSync узлы (Рисунок 77).

Межсетевой экран: Виртуальные IP-адреса: Статус

Временно отключить CARP

Включить режим CARP для продолжительного обслуживания

CARP-интерфейс	Виртуальный IP-адрес	Статус
Не удалось обнаружить определенные CARP-интерфейсы.		
Current CARP demotion level		0
pfSync узлы		
bad035d7		

Рисунок 77 – Межсетевой экран: Виртуальные IP-адреса: Статус

4.7 Подраздел «Настройки»

Подраздел «Настройки» позволяет производить настройку дополнительных параметров межсетевого экрана, настройку нормализации (в том числе правил нормализации) и настройку расписания, которое используется в правилах межсетевого экрана.

4.7.1 Категория «Дополнительно»

Категория «Дополнительно» позволяет настраивать дополнительные параметры межсетевого экрана.

В группе настроек «Параметры IPv6» необходимо установить флажок напротив поля «Разрешить IPv6» для разрешения трафика IPv6, если флажок отсутствует, то межсетевой экран будет блокировать весь трафик IPv6 (Рисунок 78).

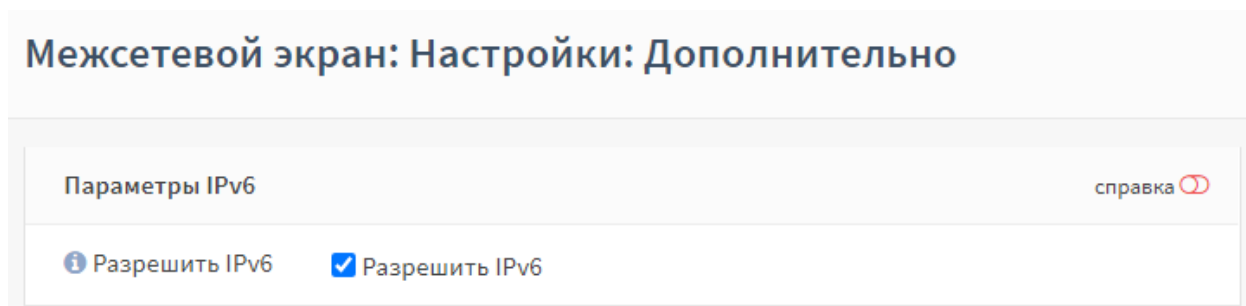


Рисунок 78 – Межсетевой экран: Настройки: Дополнительно (параметры IPv6)

В группе настроек «Преобразование сетевых адресов» необходимо установить флажок напротив поля «Отображение перенаправленных портов» при необходимости автоматического создания правил переадресации NAT, которые нужны для обеспечения доступа к перенаправляющему порту внешнего IP-адреса из внутренних сетей. Необходимо установить флажок напротив поля «Включить отражение для 1:1» для включения автоматического создания дополнительных правил переадресации NAT, которые нужны для обеспечения доступа к преобразованиям 1:1 внешних IP-адресов из внутренних сетей. В поле «Автоматический исходящий NAT для отражения» необходимо установить флажок для автоматического создания правил исходящего NAT, позволяющие правилам входящего NAT направлять трафик обратно (Рисунок 79).

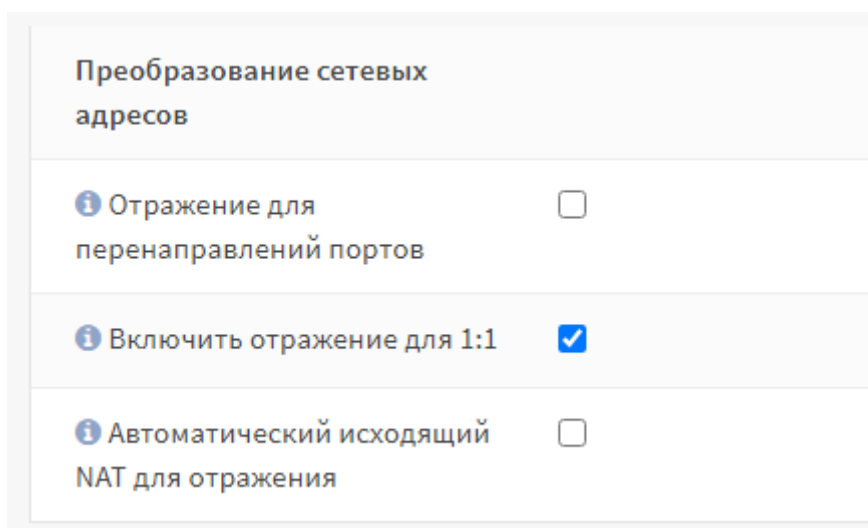


Рисунок 79 – Межсетевой экран: Настройки: Дополнительно (Преобразование сетевых адресов)

В группе настроек «Vogon-сети» в поле «Частота обновлений» необходимо выбрать частоту обновлений зарезервированных или еще не назначенных IANA списков IP-адресов, не относящихся к RFC 1918 (Рисунок 80).

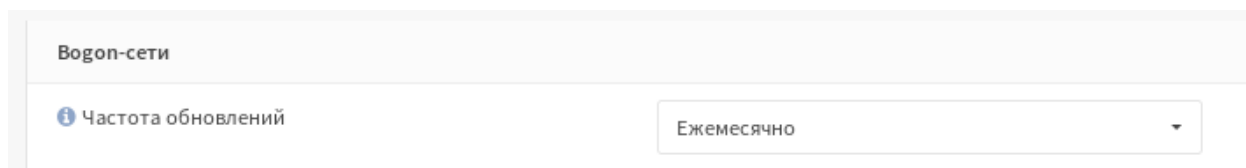


Рисунок 80 – Межсетевой экран: Настройки: Дополнительно (Vogon-сети)

В группе настроек «Мониторинг шлюза» в поле «Сбросить состояния» необходимо установить флажок напротив поля «Отключить сброс состояний при отключении шлюза» при необходимости сохранять состояния для отключенного шлюза. В поле «Игнорировать правила» необходимо установить флажок напротив поля «Игнорировать правила, если шлюз отключен» для отключения правил передачи шлюза по умолчанию при его отключении (Рисунок 81).

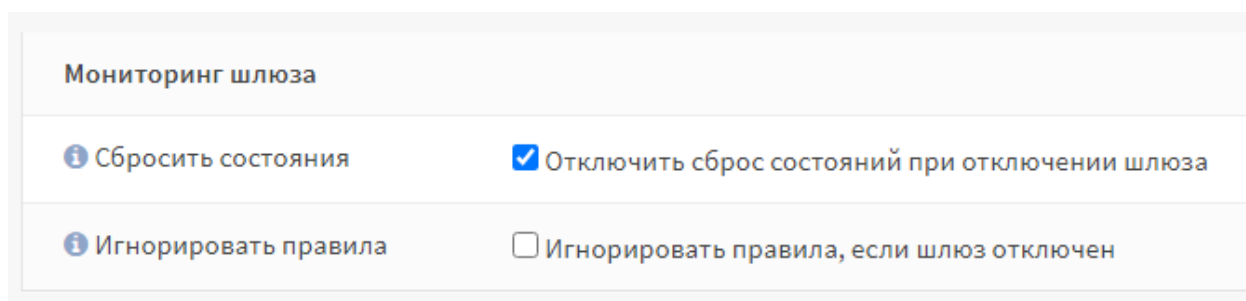


Рисунок 81 – Межсетевой экран: Настройки: Дополнительно (Мониторинг шлюза)

В группе настроек «Мульти-WAN» в поле «Фиксированные соединения» необходимо установить флажок напротив поля «Использовать фиксированные соединения» при необходимости использования «фиксированных соединений». Последовательные соединения будут перенаправлены на серверы в циклическом порядке, а соединения из того же источника будут отправлены на тот же шлюз. Поле «Фиксированное соединение» будет существовать до тех пор, пока существуют состояния, которые относятся к этому соединению. Как только количество состояний становится равным нулю, происходит разрыв фиксированного соединения. Дальнейшие соединения от этого хоста будут перенаправлены на следующий шлюз в циклическом порядке. В поле «Тайм-аут отслеживания источника» необходимо ввести тайм-аут отслеживания источника для «фиксированных соединений» (в секундах). В поле «Общая переадресация» необходимо установить флажок напротив поля «Использовать общую переадресацию между фильтром пакетов, ограничением трафика и Порталом авторизации» при необходимости использования фильтрации пакетов, которые не проходят проверку правилами ограничения трафика и Порталом авторизации. Эта опция позволяет принимать совместное решение о пропуске/фильтрации пакета всех компонентов в особых случаях. В поле «Отключение назначенного шлюза» необходимо установить флажок для отключения использования шлюза по

умолчанию (при отключении маршрут будет выбран с помощью таблицы маршрутизации) (Рисунок 82).

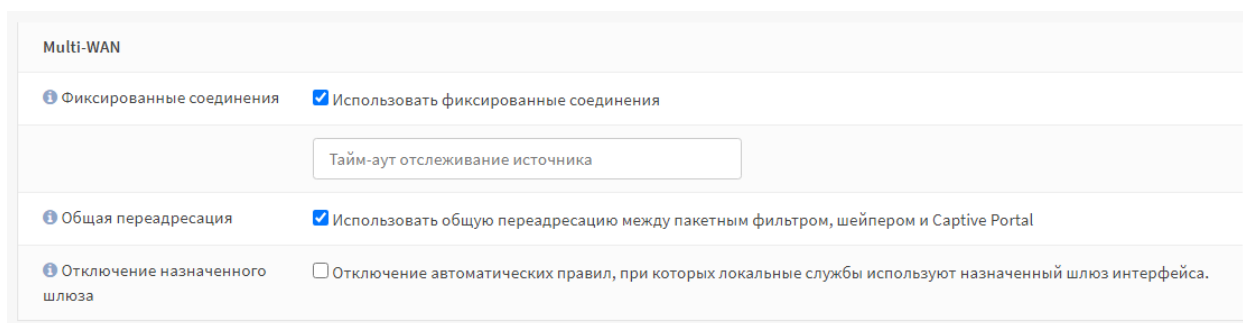


Рисунок 82 – Межсетевой экран: Настройки: Дополнительно (Мульти-WAN)

В группе настроек «Расписания» в поле «Состояния расписания» необходимо установить флажок для сохранения состояний для существующих соединений (Рисунок 83).

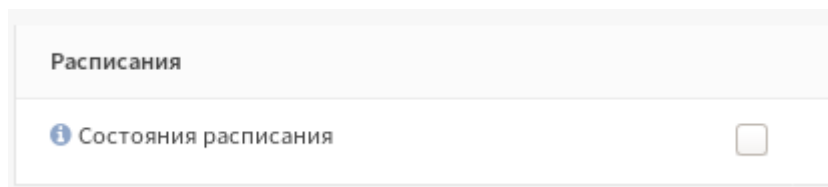


Рисунок 83 – Межсетевой экран: Настройки: Дополнительно (Расписание)

В группе настроек «Прочее» в поле «Оптимизация межсетевого экрана» необходимо выбрать тип оптимизации таблицы состояний:

- нормальный (нормальный алгоритм оптимизации);
- большая задержка (используется для каналов с высокой задержкой, таких как спутниковый канал);
- агрессивный (простаивающие соединения истекают быстрее, более эффективное использование процессора и памяти, но возможен разрыв разрешенных простаивающих соединений);
- консервативный (пытается избежать разрыва любых разрешенных простаивающих соединений за счет дополнительных ресурсов памяти и процессора).

В поле «Оптимизация правил межсетевого экрана» необходимо выбрать тип оптимизации правил:

- базовый (по умолчанию базовая оптимизация правил удаляет дублирующиеся правила, удаляет правила, которые являются подмножеством других правил, комбинирует несколько правил в таблицу если это целесообразно, изменяет порядок правил для увеличения производительности);
- профиль (использовать текущий набор правил как профиль обратной связи для адаптации порядка «Быстрых правил» к актуальному трафику).

В пункте «Привязка состояний к интерфейсу» необходимо установить флажок для привязки состояния к определенному интерфейсу, по умолчанию состояния являются общими, но, когда эта опция установлена, они должны соответствовать интерфейсу. В поле «Отключить межсетевой экран» необходимо установить флажок напротив поля «Отключить фильтрацию пакетов» для

выключения фильтрации (будут выполняться функции маршрутизации). В поле «Адаптивные тайм-ауты межсетевого экрана» необходимо ввести тайм-ауты для состояний межсетевого экрана. В поле «начало» необходимо ввести пороговое количество записей состояний, при котором начинает применяться адаптивное масштабирование. В поле «конец» необходимо ввести максимальное количество записей состояний, при достижении которого значения тайм-аутов становятся равными «0». В поле «Максимальное количество состояний межсетевого экрана» необходимо ввести максимальное количество соединений, которые будут храниться в таблице состояний межсетевого экрана. В поле «Максимальное число фрагментов» необходимо ввести максимальное число записей в пул памяти для пересборки фрагмента. В поле «Максимальное количество записей в таблице» необходимо ввести максимальное количество записей для таких систем, как псевдонимы, sshlockout, bogon и другие. В поле «Фильтрация статических маршрутов» необходимо установить флажок напротив поля «Правила обхода межсетевого экрана для трафика на одном интерфейсе» при необходимости отключения проверки межсетевым экраном входящего/исходящего трафика через один интерфейс. В поле «Отключить reply-to» необходимо установить флажок для отключения reply-to в WAN правилах. В поле «Отключить антиблокировку» необходимо установить флажок для отключения автоматического создания правила антиблокировки. В поле «Интервал разрешения псевдонимов» необходимо ввести интервал, который будет использоваться для разрешения хостов, сконфигурированных на псевдонимах. В поле «Проверить сертификат URL-псевдонимов» необходимо установить флажок для проверки HTTPS-сертификатов при загрузке URL-псевдонимов. В поле «Сброс текущих настроек» необходимо установить флажок для сброса всех настроек в ходе изменения текущего IP-адреса (Рисунок 84). Для сохранения настроек необходимо нажать на кнопку «Сохранить».

Прочее	
Оптимизация межсетевого экрана	нормальный
Оптимизация правил межсетевого экрана	базовый
Привязка состояний к интерфейсу	<input checked="" type="checkbox"/>
Отключить межсетевой экран	<input checked="" type="checkbox"/> Отключить фильтрацию пакетов.
Адаптивные Тайм-ауты файрволла	<div>начало</div> <input type="text"/> <div>конец</div> <input type="text"/>
Максимальное количество состояний межсетевого экрана	<input type="text"/>
Максимальное число фрагментов межсетевого экрана	<input type="text"/>
Максимальное количество записей в таблице	<input type="text"/>
Фильтрация статических маршрутов	<input checked="" type="checkbox"/> Правила обхода межсетевого экрана для трафика на одном интерфейсе
Отключить reply-to	<input checked="" type="checkbox"/> Отключить reply-to в WAN-правилах
Отключить антиблокировку	<input checked="" type="checkbox"/> Отключить автоматическое создание правила антиблокировки
Интервал разрешения алиасов	<input type="text"/>
Проверить сертификат для URL-алиасов	<input type="checkbox"/> Проверить HTTPS-сертификаты при загрузке URL-псевдонимов
Сброс текущих настроек	<input type="checkbox"/> Сбросить все настройки в ходе изменения текущего IP адреса

Рисунок 84 – Межсетевой экран: Настройки: Дополнительно (Прочее)

4.7.2 Категория «Нормализация»

Категория «Нормализация» позволяет настраивать нормализацию, просматривать настроенные правила нормализации и добавлять новые правила нормализации (Рисунок 85).

В пункте «Общие настройки» в поле «Отключить нормализацию пакетов на интерфейсе» необходимо установить флажок для отключения всех правил нормализации по умолчанию и ограничения размера MSS. В поле «IP не фрагментирован» необходимо установить флажок для того, чтобы осуществлять связь с хостами, которые генерируют фрагментированные пакеты с установленным битом (DF). В поле «Случайный идентификатор IP» необходимо установить флажок для замены значения поля идентификации IP в пакетах случайными значениями, с целью защитить операционные системы, которые используют прогнозируемые значения. Для сохранения настроек необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений соответственно.

Межсетевой экран: Настройки: Нормализация + Добавить

Общие настройки справка ⓘ


Отключить нормализацию пакетов на интерфейсе	<input type="checkbox"/>
IP не фрагментирован	<input type="checkbox"/>
Случайный идентификатор IP	<input type="checkbox"/>

[Сохранить](#)

Дополнительные настройки

<input type="checkbox"/>	Интерфейс	Отправитель	Получатель	Описание
<input checked="" type="checkbox"/>	Последним (нажмите для просмотра/редактирования)			

Рисунок 85 – Межсетевой экран: Настройки: Нормализация

Для того чтобы редактировать существующие правила нормализации, необходимо нажать на кнопку  напротив правила. Для того чтобы создать новое правило нормализации, необходимо нажать на кнопку [+ Добавить](#).

При редактировании правила нормализации необходимо установить флажок напротив поля «Отключить» для выключения редактируемого правила. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Направление» необходимо выбрать направление пакетов, на которое будет распространяться правило. В поле «Протокол» необходимо выбрать протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (Рисунок 86).

Межсетевой экран: Настройки: Нормализация

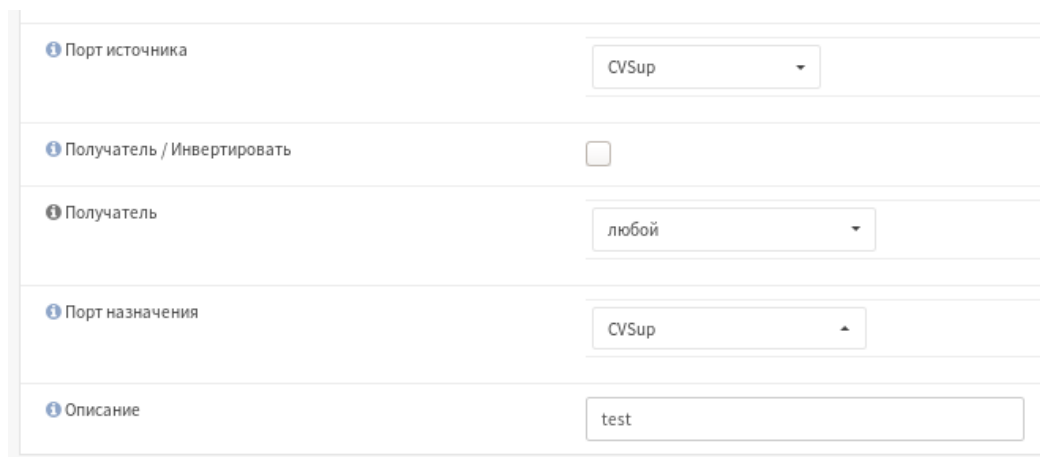
Редактировать правило нормализации пакетов

Отключена	<input type="checkbox"/>
Интерфейс	test ▾
Направление	Вх. ▾
Протокол	TCP ▾
Отправитель / Инвертировать	<input type="checkbox"/>
Отправитель	test ▾

Рисунок 86 – Межсетевой экран: Настройки: Нормализация (редактирование правила нормализации, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Порт источника» необходимо указать порт или диапазон портов источника. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать

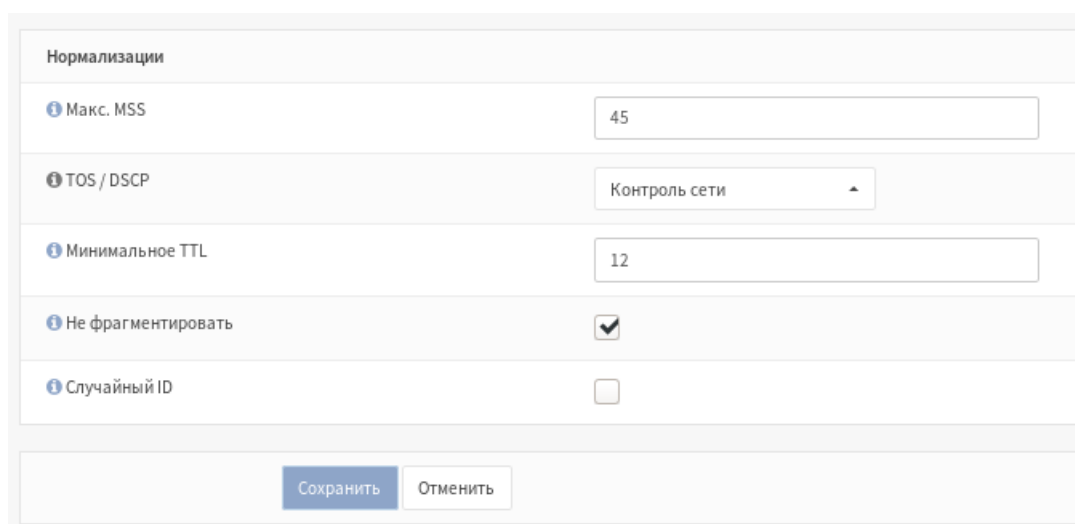
получателя. В поле «Порт назначения» необходимо указать порт или диапазон портов получателя. В поле «Описание» необходимо ввести описание правила (Рисунок 87).



Порт источника	CVSup
Получатель / Инвертировать	<input type="checkbox"/>
Получатель	любой
Порт назначения	CVSup
Описание	test

Рисунок 87 – Межсетевой экран: Настройки: Нормализация (редактирование правила нормализации, часть 2)

В пункте «Нормализация» в поле «Макс. MSS» необходимо ввести максимальное значение MSS в TCP-пакетах, соответствующим требованиям. В поле «TOS/DSCP» необходимо выбрать изменение полей TOS/DSCP в проходящих пакетах, в поле «Минимальное TTL» необходимо ввести минимальное значение TTL в IP-пакетах, соответствующим требованиям. В поле «Не фрагментировать» необходимо установить флажок для удаления бит DF (не фрагментированных) в IP-пакетах, соответствующим требованиям. В поле «Случайный ID» необходимо установить флажок для замены идентификационного поля IP-адресом случайными значениями для компенсации прогнозируемых значений, генерируемых большим количеством хостов (Рисунок 88).



Нормализации	
Макс. MSS	45
TOS / DSCP	Контроль сети
Минимальное TTL	12
Не фрагментировать	<input checked="" type="checkbox"/>
Случайный ID	<input type="checkbox"/>
<div>Сохранить Отменить</div>	

Рисунок 88 – Межсетевой экран: Настройки: Нормализация (редактирование правила нормализации, часть 3)

После редактирования правила нормализации необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

4.7.3 Категория «Расписания»

Категория «Расписания» позволяет просмотреть/редактировать настроенные расписания и настроить новое расписание для правил межсетевого экрана (Рисунок 89).

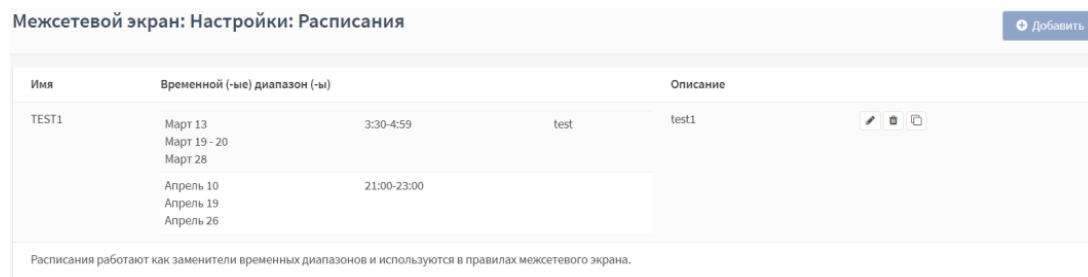





Рисунок 89 – Межсетевой экран: Настройки: Расписания

Для того чтобы отредактировать существующие расписания, необходимо нажать на кнопку  напротив строки расписания. Для того чтобы создать новое расписание, необходимо нажать на кнопку  **Добавить**.

При редактировании расписания в поле «Имя» необходимо ввести название расписания, а в поле «Описание» ввести описание расписания. В поле «Месяц» необходимо выбрать месяц для настройки расписания и в появившемся календаре при необходимости выбрать дни месяца. В поле «Время» необходимо выбрать диапазон времени действия расписания. В поле «Описание временного диапазона» необходимо ввести описание диапазона времени, выбранного ранее. Для добавления диапазона в расписание необходимо нажать на кнопку «Добавить время». Для очистки выделенных дат необходимо нажать на кнопку «Очистить выделенное». В поле «Повторение расписания» появится настроенный диапазон времени, имеется возможность добавлять еще диапазоны времени или редактировать существующие, нажав на  напротив диапазона. Необходимо нажать на кнопку «Сохранить» для сохранения правила (Рисунок 90).

Информация о расписании справка

Имя:

Описание:

Месяц:

March_2019						
Пн	Вт	Ср	Чт	Пт	Сб	Вс
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Время: Начальное время Конечное время

Описание временного диапазона:

Повторение расписания

Настроенные диапазоны	День (дни)	Начальное время	Конечное время	Описание	
Март 13, Март 19 - 20, Март 28		3:30	4:59	test	<input type="button" value="✎"/> <input type="button" value="✖"/>
Апрель 10, Апрель 19, Апрель 26		21:00	23:00		<input type="button" value="✎"/> <input type="button" value="✖"/>

Рисунок 90 – Межсетевой экран: Настройки: Расписания (редактирование)

4.8 Подраздел «Журналы»

В подразделе «Журналы» поддерживается ряд форматов отображения журнала межсетевого экрана:

- динамическое представление («В реальном времени»);
- сводное представление («Обзор»);
- открытый вид.

4.8.1 Категория «В реальном времени»

В категории «В реальном времени» отображается каждый пакет, обработанный межсетевым экраном в режиме реального времени. Отображается IP-адрес и порт источника, IP-адрес и порт назначения, входящий интерфейс, время обработки пакета и действие, которое было применено к пакету. Красным отображаются заблокированные записи, зеленым отображаются разрешенные записи (Рисунок 91).

Межсетевой экран: Журналы: В реальном времени

фильтр

25

☒ Автоматическое обновление
☐ Отображать имена хостов

Интерфейс	Время	Отправитель	Получатель	Протокол	Метка
▶ Internet	← Jul 22 10:18:10	192.168.159.139:123	91.209.94.10:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ Internet	← Jul 22 10:18:10	192.168.159.139:123	81.211.37.18:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ Internet	← Jul 22 10:18:09	192.168.159.139:123	85.21.78.8:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ lan	→ Jul 22 10:18:07	192.168.1.100:55222	192.168.1.1:443	tcp	правило антиблокировки ⓘ
▶ Internet	← Jul 22 10:18:05	192.168.159.139:123	195.3.254.2:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ lan	→ Jul 22 10:17:51	192.168.1.100:55214	192.168.1.1:443	tcp	правило антиблокировки ⓘ
▶ lan	→ Jul 22 10:17:37	192.168.1.100:55206	192.168.1.1:443	tcp	правило антиблокировки ⓘ
▶ lan	→ Jul 22 10:17:00	192.168.1.100:55190	192.168.1.1:443	tcp	правило антиблокировки ⓘ
▶ Internet	← Jul 22 10:16:34	192.168.159.139:123	91.209.94.10:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ Internet	← Jul 22 10:16:34	192.168.159.139:123	81.211.37.18:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ Internet	← Jul 22 10:16:33	192.168.159.139:123	85.21.78.8:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ Internet	← Jul 22 10:16:30	192.168.159.139:123	195.3.254.2:123	udp	разрешить исходящие пакеты (force gw) ⓘ
⊘ Internet	→ Jul 22 10:16:26	192.168.159.1:57855	239.255.255.250:1900	udp	Правило блокировки по умолчанию ⓘ
⊘ Internet	→ Jul 22 10:16:25	192.168.159.1:57855	239.255.255.250:1900	udp	Правило блокировки по умолчанию ⓘ
⊘ Internet	→ Jul 22 10:16:24	192.168.159.1:57855	239.255.255.250:1900	udp	Правило блокировки по умолчанию ⓘ
▶ lan	→ Jul 22 10:16:23	192.168.1.100:55172	192.168.1.1:443	tcp	правило антиблокировки ⓘ
⊘ Internet	→ Jul 22 10:16:23	192.168.159.1:57855	239.255.255.250:1900	udp	Правило блокировки по умолчанию ⓘ
▶ Internet	← Jul 22 10:14:58	192.168.159.139:123	91.209.94.10:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ Internet	← Jul 22 10:14:58	192.168.159.139:123	81.211.37.18:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ Internet	← Jul 22 10:14:57	192.168.159.139:123	85.21.78.8:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ Internet	← Jul 22 10:14:49	192.168.159.139:123	195.3.254.2:123	udp	разрешить исходящие пакеты (force gw) ⓘ
▶ lan	→ Jul 22 10:14:32	192.168.1.100:55126	192.168.1.1:443	tcp	правило антиблокировки ⓘ
▶ lan	→ Jul 22 10:14:32	192.168.1.100:55124	192.168.1.1:443	tcp	правило антиблокировки ⓘ

Рисунок 91 – Межсетевой экран: Журналы: В реальном времени

4.8.2 Категория «Обзор»

В категории «Обзор» приведены диаграммы распределения сетевого трафика, обработанного межсетевым экраном с отображением действий (Рисунок 92), интерфейсов (Рисунок 93), протоколов (Рисунок 94), IP-адресов источников (Рисунок 95), IP-адресов назначения (Рисунок 96), портов источника (Рисунок 97), портов назначения (Рисунок 98).

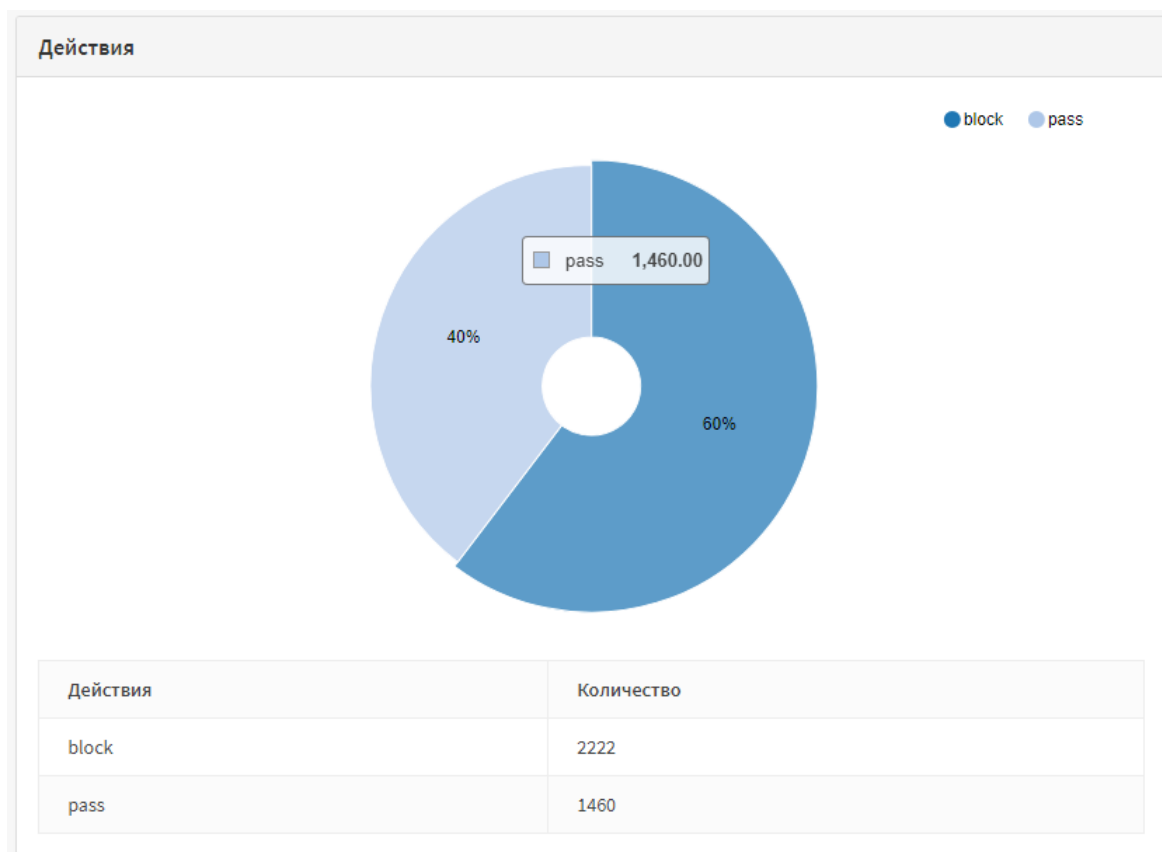


Рисунок 92 – Межсетевой экран: Журналы: Обзор (Действия)

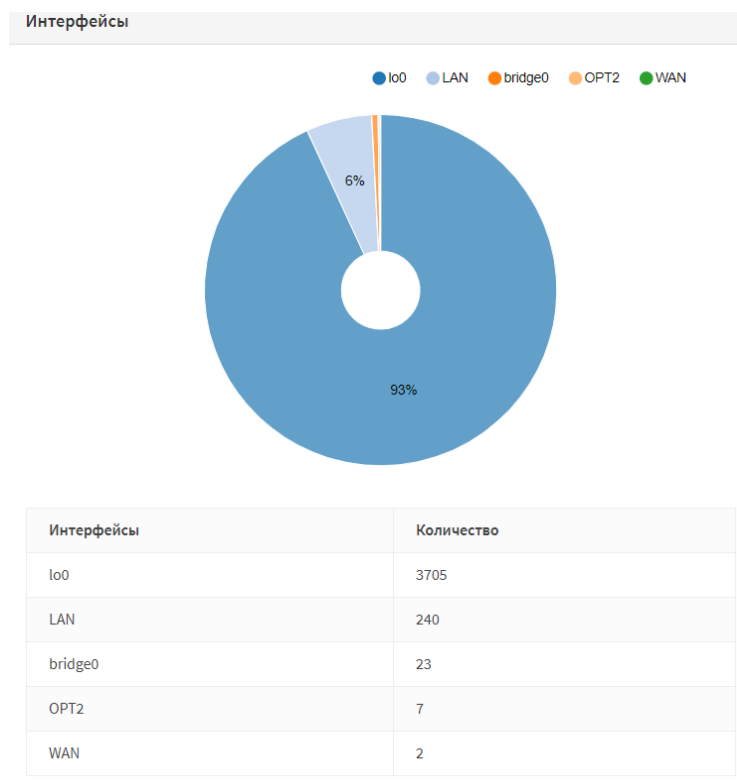


Рисунок 93 – Межсетевой экран: Журналы: Обзор (Интерфейсы)

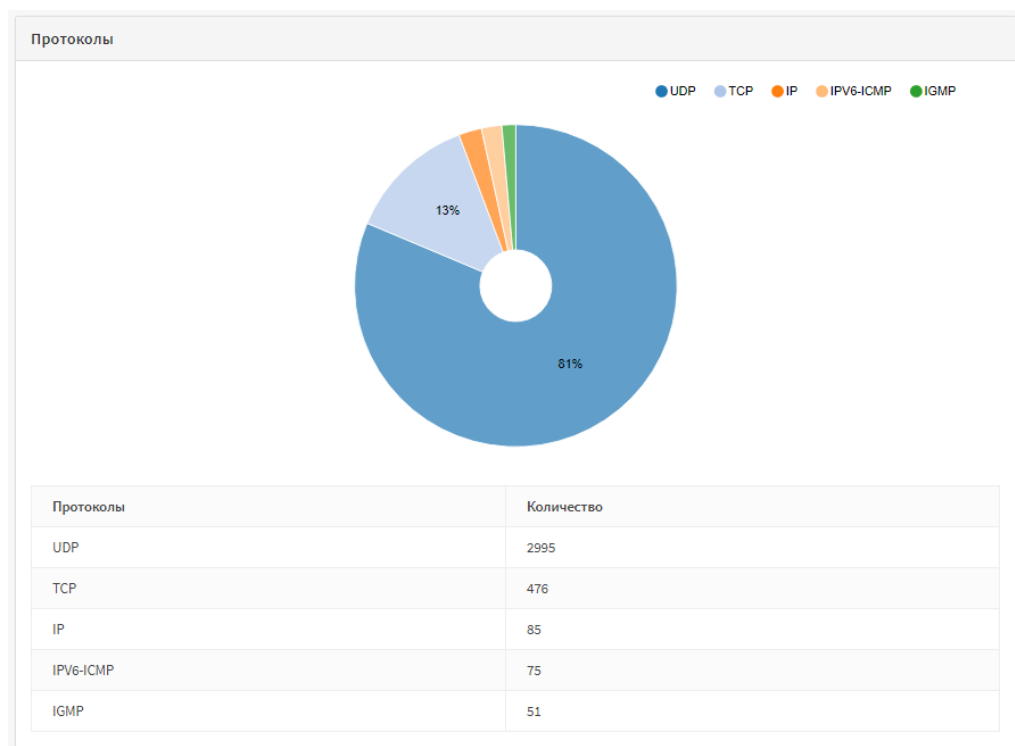


Рисунок 94 – Межсетевой экран: Журналы: Обзор (Протоколы)

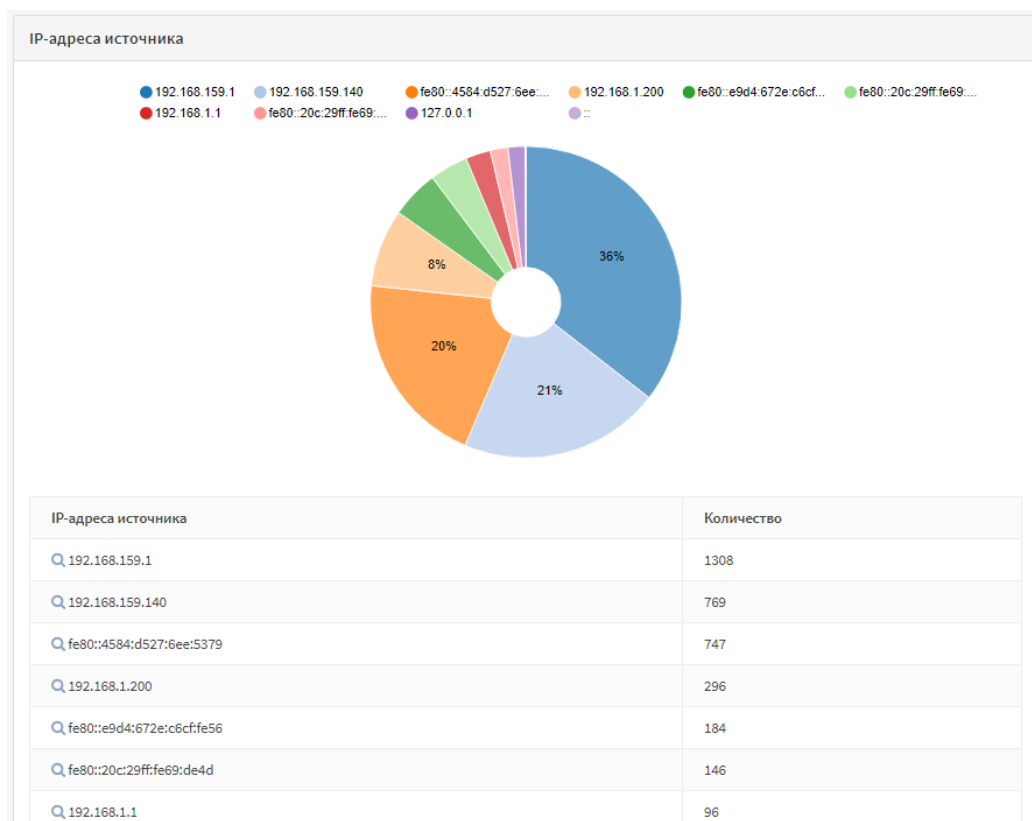


Рисунок 95 – Межсетевой экран: Журналы: Обзор (IP-адреса источника)

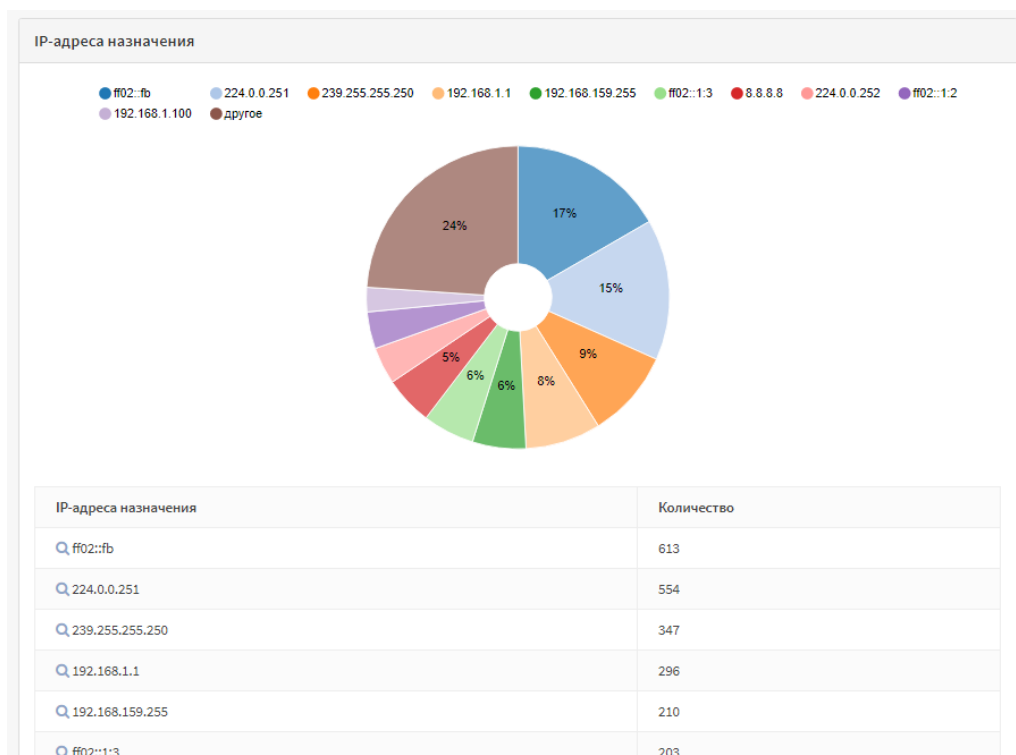


Рисунок 96 – Межсетевой экран: Журналы: Обзор (IP-адреса назначения)

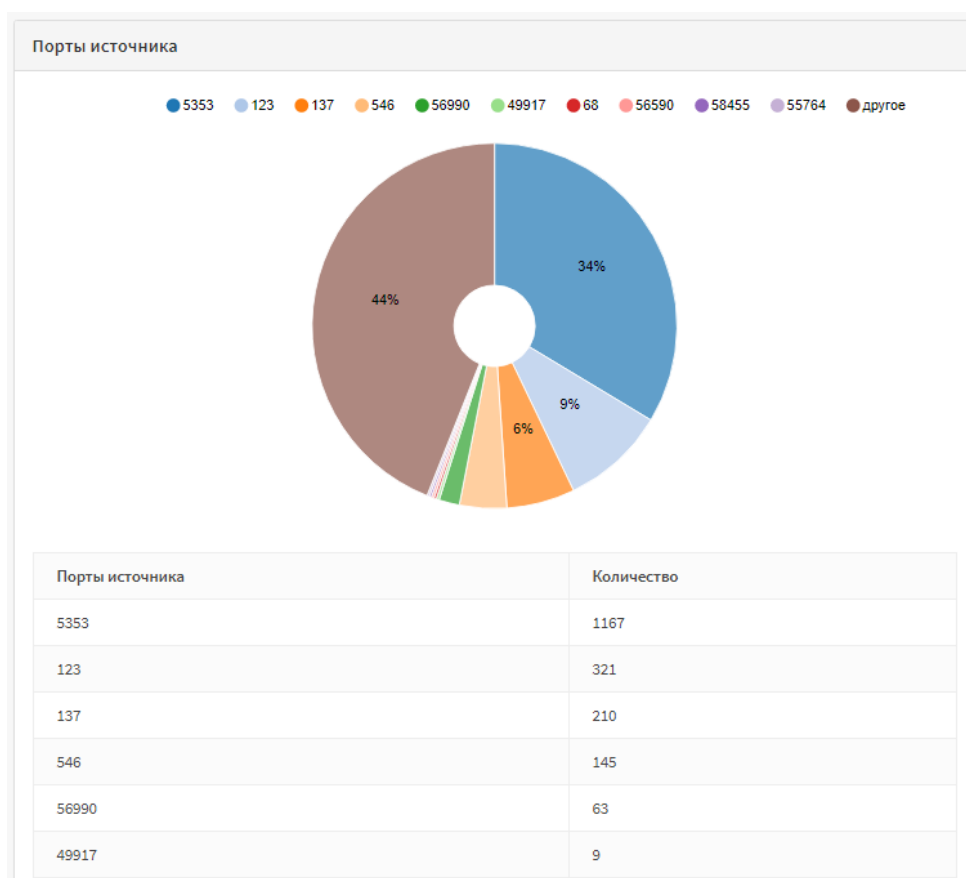


Рисунок 97 – Межсетевой экран: Журналы: Обзор (Порты источника)

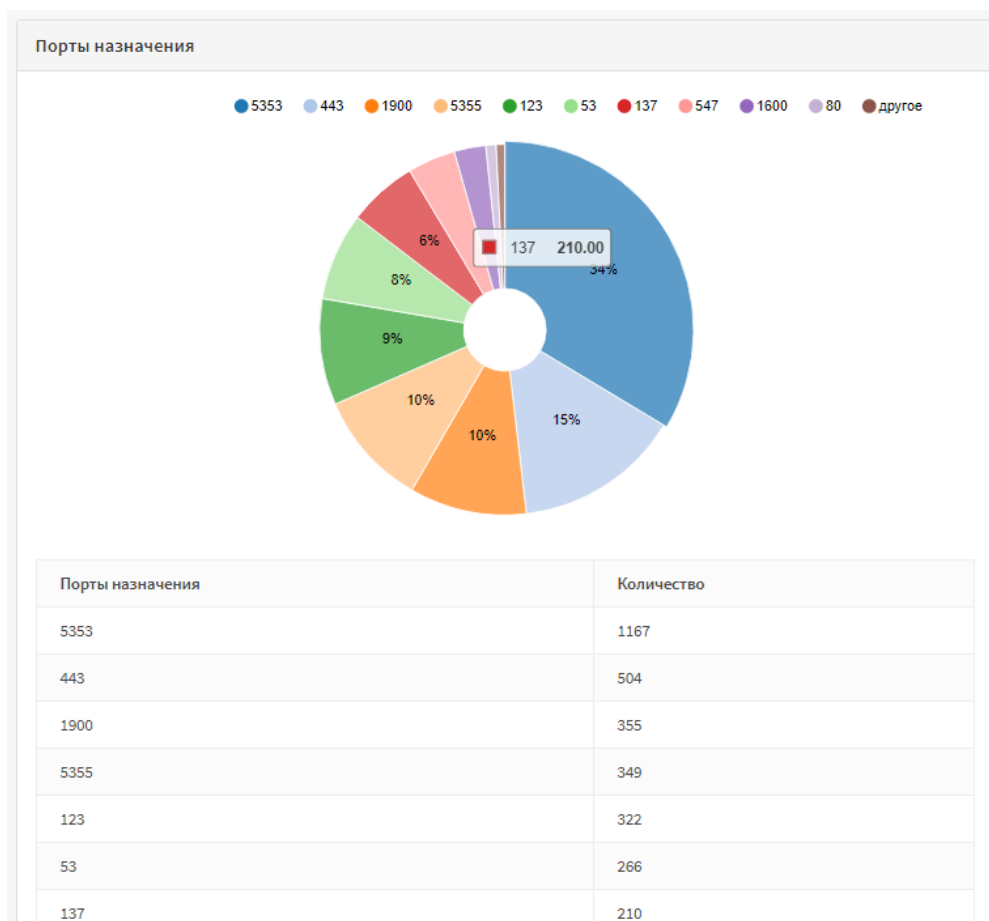


Рисунок 98 – Межсетевой экран: Журналы: Обзор (Порты назначения)

4.8.3 Категория «Открытый вид»

В категории «Открытый вид» выводится журнал результатов обработки межсетевого экрана (Рисунок 99) в «сыром» виде, на основе которого генерируется таблица журнала «В реальном времени».

Журнал «Открытый вид» содержит следующую информацию (разделенную «,»):

- номер сработавшего правила фильтрации;
- номер зависимого правила;
- имя правила;
- идентификатор правила;
- имя физического интерфейса, через который проходит пакет;
- причина срабатывания правила (обычно match – совпало с правилом);
- действие (pass, drop);
- направление правила (in, out);
- версия IP протокола;
- обозначения специального байта данных стандартного заголовка IP-пакета (Type of Service);
- уведомление о перегруженности (Explicit Congestion Notification);
- время жизни IP-пакета;
- идентификатор;
- смещение фрагмента;

- флаг;
- порт протокол;
- протокол;
- длина пакета;
- IP-адрес отправителя;
- порт отправителя;
- порт получателя;
- длина данных;
- флаги;
- Seq ID;
- ACK номер;
- размер окна;
- указатель URG;
- опции TCP.

Межсетевой экран: Журналы: Открытый вид

Дата	Сообщение
2020-11-15T16:02:49	filterlog: 73,,,0,em1,match,block,in,4,0x0,,1,37425,0,none,17,udp,202,192.168.159.1,239.255.255.250,50154,1900,182
2020-11-15T16:02:48	filterlog: 73,,,0,em1,match,block,in,4,0x0,,1,37424,0,none,17,udp,202,192.168.159.1,239.255.255.250,50154,1900,182
2020-11-15T16:02:47	filterlog: 73,,,0,em1,match,block,in,4,0x0,,1,37423,0,none,17,udp,202,192.168.159.1,239.255.255.250,50154,1900,182
2020-11-15T16:02:46	filterlog: 60,,,0,em1,match,pass,out,6,0x00,0x000000,1,udp,17,76,fe80::20c:29ff:fe69:de4d,ff02::1:2,546,547,76
2020-11-15T16:02:46	filterlog: 80,,,0,lo0,match,pass,in,6,0x00,0x000000,1,udp,17,76,fe80::20c:29ff:fe69:de4d,ff02::1:2,546,547,76
2020-11-15T16:02:46	filterlog: 73,,,0,em1,match,block,in,4,0x0,,1,37422,0,none,17,udp,202,192.168.159.1,239.255.255.250,50154,1900,182
2020-11-15T16:02:27	filterlog: 81,,,0,em0,match,pass,out,6,0x00,0x000000,1,ip,0,36,fe80::20c:29ff:fe69:de43,ff02::16,HBH,PADN,RTALERT,0x0000,
2020-11-15T16:02:27	filterlog: 20,,,0,em0,match,pass,out,6,0x00,0x000000,255,ipv6-icmp,58,56,fe80::20c:29ff:fe69:de43,ff02::1,
2020-11-15T16:02:27	filterlog: 30,,,0,lo0,match,pass,in,6,0x00,0x000000,255,ipv6-icmp,58,56,fe80::20c:29ff:fe69:de43,ff02::1,
2020-11-15T16:01:58	filterlog: 81,,,0,em0,match,pass,out,4,0x0,,64,20554,0,none,17,udp,724,192.168.1.1,192.168.1.100,51422,1600,704
2020-11-15T16:00:58	filterlog: 60,,,0,em1,match,pass,out,6,0x00,0x000000,1,udp,17,76,fe80::20c:29ff:fe69:de4d,ff02::1:2,546,547,76
2020-11-15T16:00:58	filterlog: 80,,,0,lo0,match,pass,in,6,0x00,0x000000,1,udp,17,76,fe80::20c:29ff:fe69:de4d,ff02::1:2,546,547,76
2020-11-15T16:00:49	filterlog: 73,,,0,em1,match,block,in,4,0x0,,1,37421,0,none,17,udp,202,192.168.159.1,239.255.255.250,59272,1900,182
2020-11-15T16:00:48	filterlog: 73,,,0,em1,match,block,in,4,0x0,,1,37420,0,none,17,udp,202,192.168.159.1,239.255.255.250,59272,1900,182
2020-11-15T16:00:47	filterlog: 73,,,0,em1,match,block,in,4,0x0,,1,37419,0,none,17,udp,202,192.168.159.1,239.255.255.250,59272,1900,182
2020-11-15T16:00:46	filterlog: 73,,,0,em1,match,block,in,4,0x0,,1,37418,0,none,17,udp,202,192.168.159.1,239.255.255.250,59272,1900,182
2020-11-15T16:00:29	filterlog: 84,,,0,em1,match,pass,out,4,0xb8,,64,39589,0,none,17,udp,76,192.168.159.140,188.225.9.167,123,123,56
2020-11-15T16:00:07	filterlog: 81,,,0,em0,match,pass,out,4,0xb8,,64,36789,0,none,17,udp,745,192.168.1.1,192.168.1.100,39509,1600,725
2020-11-15T15:59:44	filterlog: 84,,,0,em1,match,pass,out,4,0xb8,,64,31242,0,none,17,udp,76,192.168.159.140,85.21.78.23,123,123,56
2020-11-15T15:59:42	filterlog: 84,,,0,em1,match,pass,out,4,0xb8,,64,47506,0,none,17,udp,76,192.168.159.140,80.240.216.155,123,123,56

Рисунок 99 – Межсетевой экран: Журналы: Открытый вид

4.9 Подраздел «Диагностика»

Подраздел «Диагностика» позволяет просматривать общую информацию и статистику pf, активные в текущее время маршруты, IP-адреса, записанные как псевдонимы, прослушивающие сокет для Ipv4 и Ipv6, активные состояния, отсортированные состояния по различным критериям. Помимо просмотра информации имеется возможность удаления активных состояний и отслеживания источника.

4.9.1 Категория «pfinfo»

Категория «pfinfo» позволяет просматривать общую информацию и статистику (Рисунок 100, Рисунок 101, Рисунок 102, Рисунок 103, Рисунок 104).

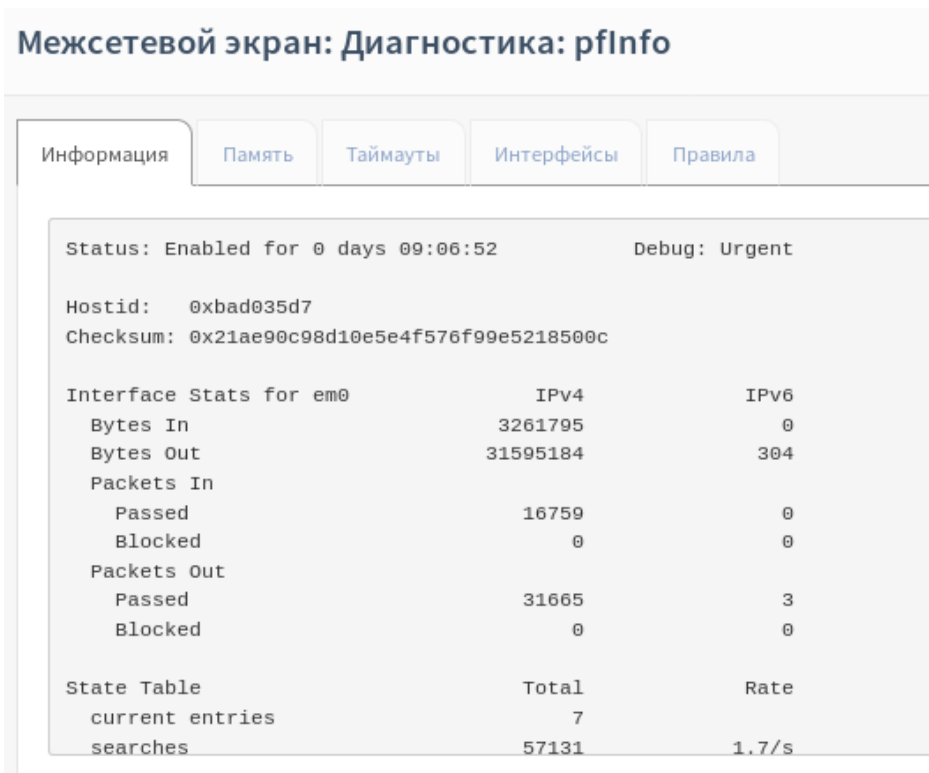


Рисунок 100 – Межсетевой экран: Диагностика: pfinfo (Информация)

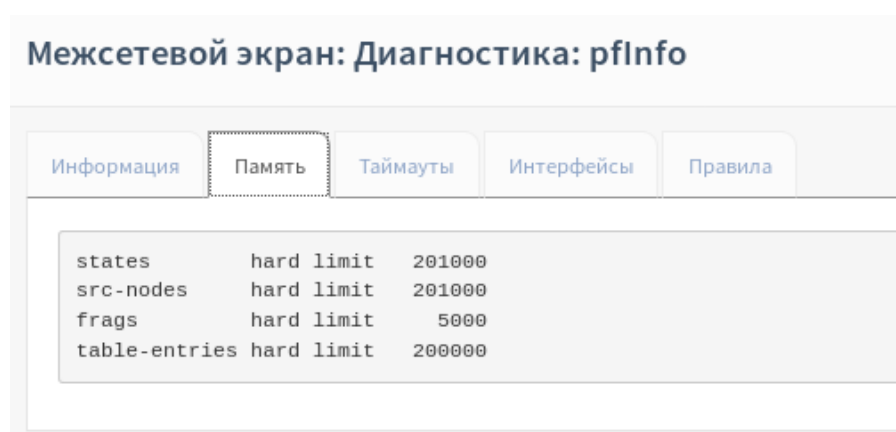


Рисунок 101 – Межсетевой экран: Диагностика: pfinfo (Память)

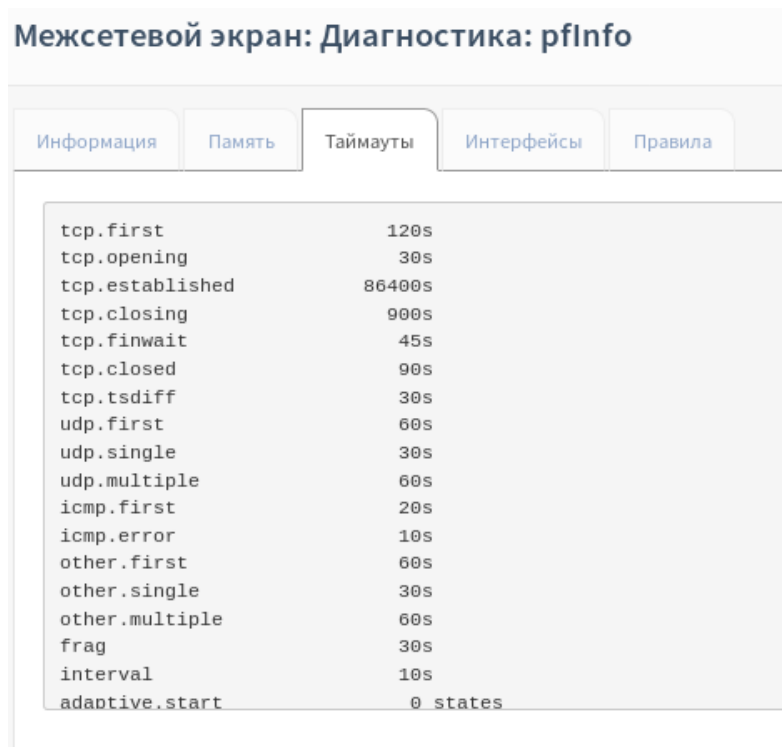


Рисунок 102 – Межсетевой экран: Диагностика: pfinfo (Тайм-ауты)

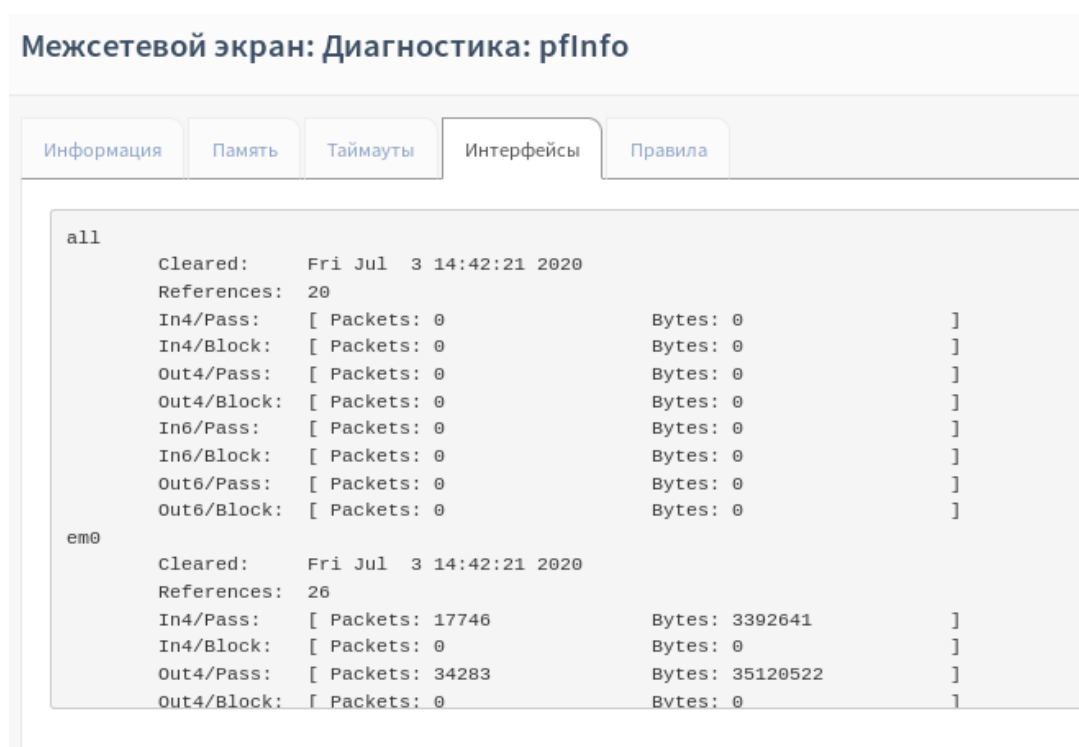


Рисунок 103 – Межсетевой экран: Диагностика: pfinfo (Интерфейсы)

Межсетевой экран: Диагностика: pfInfo

Информация

Память

Таймауты

Интерфейсы

Правила

```
@0 scrub on lo0 all fragment reassemble
[ Evaluations: 31306 Packets: 1598 Bytes: 0 States: 0 ]
[ Inserted: uid 0 pid 79415 State Creations: 0 ]
@1 scrub on em0 all fragment reassemble
[ Evaluations: 29708 Packets: 29708 Bytes: 12115625 States: 0 ]
[ Inserted: uid 0 pid 79415 State Creations: 0 ]
@0 block drop in log on ! em0 inet from 192.168.1.0/24 to any
[ Evaluations: 890 Packets: 0 Bytes: 0 States: 0 ]
[ Inserted: uid 0 pid 79415 State Creations: 0 ]
@1 block drop in log inet from 192.168.1.1 to any
[ Evaluations: 491 Packets: 0 Bytes: 0 States: 0 ]
[ Inserted: uid 0 pid 79415 State Creations: 0 ]
@2 block drop in log on em0 inet6 from fe80::20c:29ff:fea2:e987 to any
[ Evaluations: 491 Packets: 0 Bytes: 0 States: 0 ]
[ Inserted: uid 0 pid 79415 State Creations: 0 ]
@3 block drop in log inet all label "02f4bab031b57d1e30553ce08e0ec131"
[ Evaluations: 491 Packets: 0 Bytes: 0 States: 0 ]
[ Inserted: uid 0 pid 79415 State Creations: 0 ]
```

Рисунок 104 – Межсетевой экран: Диагностика: pfinfo (Правила)

4.9.2 Категория «pfTop»

В категории «pfTop» отображаются доступные маршруты в текущее время (Рисунок 105). Поле «Вид» позволяет выбрать вид таблицы состояний, «Сортировать по» позволяет выбрать по каким графам таблицы отсортировать, «Количество состояний» позволяет выбрать количество состояний для отображения.

Межсетевой экран: Диагностика: pfTop

Вид:

Сортировать по:

Количество состояний:

По умолчанию.

Возраст

200

pfTop: Up State 1-14/14, View: default, Order: age

PR	DIR	SRC	DEST	STATE	AGE	EXP	PKTS	BYTES
tcp	In	192.168.1.100:41624	192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	00:01:41	00:00:25	575	553362
tcp	In	192.168.1.100:41642	192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	00:01:03	00:01:02	560	552582
udp	Out	127.0.0.1:49484	127.0.0.1:53	SINGLE:NO_TRAFFIC	00:00:37	00:00:00	2	138
udp	In	127.0.0.1:49484	127.0.0.1:53	NO_TRAFFIC:SINGLE	00:00:37	00:00:00	2	138
tcp	In	192.168.1.100:41658	192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	00:00:26	00:01:08	186	162753
tcp	In	192.168.1.100:41662	192.168.1.1:443	ESTABLISHED:ESTABLISHED	00:00:22	23:59:58	31	5985
tcp	In	192.168.1.100:41664	192.168.1.1:443	ESTABLISHED:ESTABLISHED	00:00:22	23:59:59	30	8932
tcp	In	192.168.1.100:41666	192.168.1.1:443	ESTABLISHED:ESTABLISHED	00:00:22	24:00:00	147	109027
tcp	In	192.168.1.100:41668	192.168.1.1:443	ESTABLISHED:ESTABLISHED	00:00:22	23:59:59	27	5019
tcp	In	192.168.1.100:41670	192.168.1.1:443	ESTABLISHED:ESTABLISHED	00:00:22	23:59:58	27	5015
udp	Out	127.0.0.1:45912	127.0.0.1:53	SINGLE:NO_TRAFFIC	00:00:22	00:00:13	2	162
udp	In	127.0.0.1:45912	127.0.0.1:53	NO_TRAFFIC:SINGLE	00:00:22	00:00:13	2	162
udp	Out	127.0.0.1:50244	127.0.0.1:53	SINGLE:NO_TRAFFIC	00:00:07	00:00:28	2	162
udp	In	127.0.0.1:50244	127.0.0.1:53	NO_TRAFFIC:SINGLE	00:00:07	00:00:28	2	162

Рисунок 105 – Межсетевой экран: Диагностика: pfTop

4.9.3 Категория «pfTables»

Категория «pfTables» позволяет просматривать IP-адреса, которые указаны в псевдонимах (Рисунок 106). Выпадающий список позволяет выбрать псевдоним, очистить и обновить базу псевдонима, нажав соответствующие кнопки.

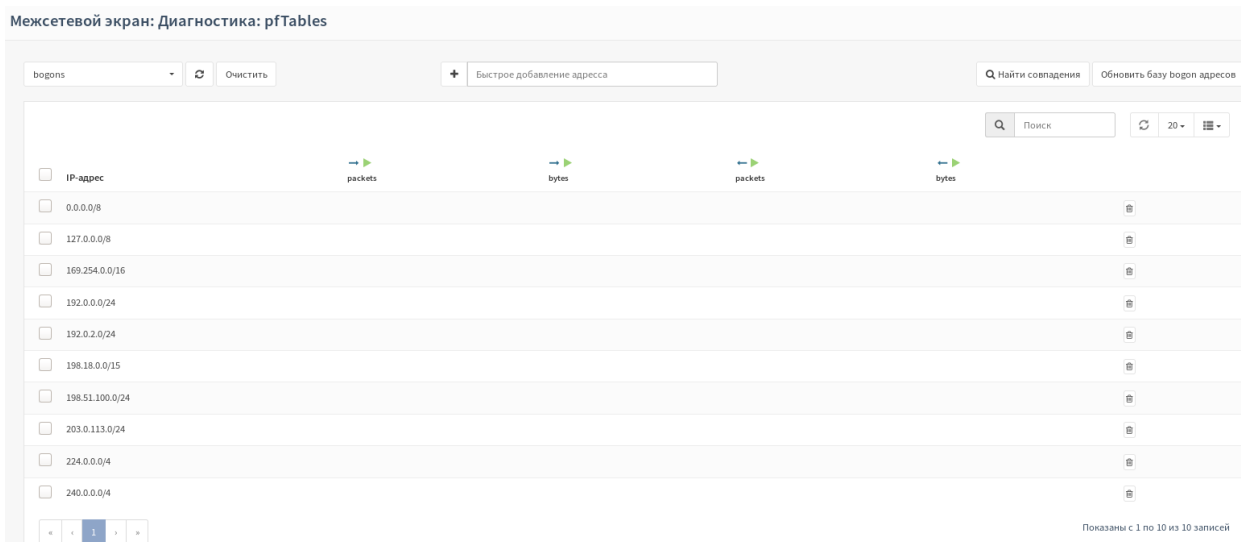


Рисунок 106 – Межсетевой экран: Диагностика: pfTables

4.9.4 Категория «Снимок состояний»

Категория «Снимок состояний» позволяет просматривать активные состояния в текущий момент времени (Рисунок 107). В поле «Общее количество состояний в данный момент» отображается количество состояний в текущий момент времени. Поле «Выражение фильтра» позволяет ввести фильтр для фильтрации данных таблицы и нажать на кнопку «Фильтр трафика».

Межсетевой экран: Диагностика: Снимок состояний

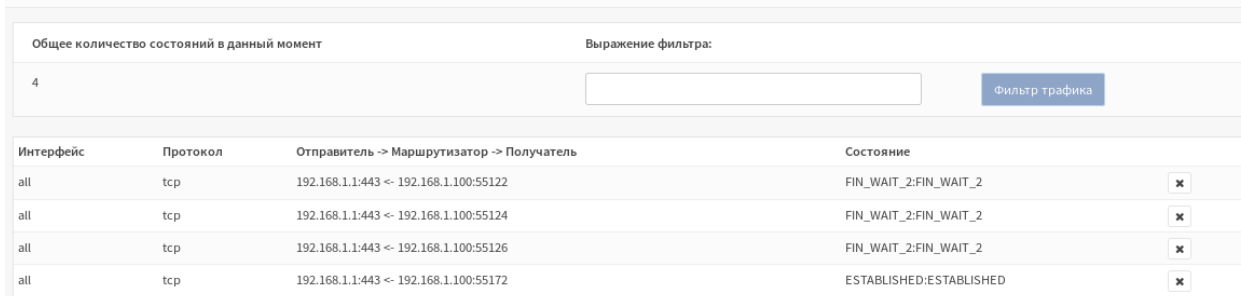


Рисунок 107 – Межсетевой экран: Диагностика: Снимок состояний

4.9.5 Категория «Сброс состояний»

Категория «Сброс состояний» позволяет удалить активные состояния и (или) отслеживания источника. Для этого необходимо установить флажок напротив поля «Таблица состояния межсетевого экрана» и (или) «Проверка источника межсетевым экраном» и нажать на кнопку «Очистить» (Рисунок 108).

Межсетевой экран: Диагностика: Сброс состояний

☒ Таблица состояний межсетевого экрана

Очистка таблиц состояний удалит все записи из соответствующих таблиц. Это означает, что все соединения будут разорваны, и нужно будет их повторно установить. Эта функция может потребоваться, если были внесены значительные изменения в правила межсетевого экрана и/или NAT, особенно если присутствуют открытые соединения по сопоставляемым адресам с использованием протокола IP (например, для PPTP или IPv6).

Обычно межсетевой экран оставляет таблицы состояний без изменений, когда правила меняются.

Примечание: если вы очистили таблицу состояний межсетевого экрана, сеанс браузера может зависнуть после нажатия на клавишу «Очистить». В таком случае просто обновите страницу для продолжения.

☒ Проверка источника межсетевым экраном

Очистка таблицы проверок источника удалит все ассоциации адресов источника/назначения. Это значит, что «фиксированные» ассоциации адрес источника/назначения будут стерты для всех клиентов.

Состояния активных соединений не будут очищены, только проверки источников.

Очистить

Рисунок 108 – Межсетевой экран: Диагностика: Сброс состояний

4.9.6 Категория «Сводка состояний»

Категория «Сводка состояний» позволяет просматривать состояния, отсортированные по таблицам:

- «По IP-адресу источника» (Рисунок 109);
- «По IP-адресу назначения» (Рисунок 110);
- «Всего по IP-адресу» (Рисунок 111);
- «По паре IP-адресов» (Рисунок 112).

Межсетевой экран: Диагностика: Сводка состояний

По IP-адресу источника					
IP-адрес	# Состояния	Протокол	# Состояния	Порт источника	Порт назначения
192.168.1.1	2				
		tcp	2	1	2
192.168.159.139	4				
		udp	4	1	1

Рисунок 109 – Межсетевой экран: Диагностика: Сводка состояний (по IP-адресу источника)

По IP-адресу назначения					
IP-адрес	# Состояния	Proto	# Состояния	Порт источника	Порт назначения
127.0.0.1	4				
		udp	4	3	3
192.168.1.100	5				
		tcp	5	1	5

Рисунок 110 – Межсетевой экран: Диагностика: Сводка состояний (по IP-адресу назначения)

Всего по IP-адресу					
IP-адрес	# Состояния	Proto	# Состояния	Порт источника	Порт назначения
127.0.0.1	8				
		udp	8	3	3
192.168.1.1	5				
		tcp	5	1	5
192.168.1.100	5				
		tcp	5	1	5

Рисунок 111 – Межсетевой экран: Диагностика: Сводка состояний (Всего по IP-адресу)

По паре IP-адресов					
IP-адрес	# Состояния	Proto	# Состояния	Порт источника	Порт назначения
192.168.1.1 -> 192.168.1.100	5				
		tcp	5	1	5
127.0.0.1 -> 127.0.0.1	4				
		udp	4	3	3

Рисунок 112 – Межсетевой экран: Диагностика: Сводка состояний (по паре IP-адресов)

5 РАЗДЕЛ «ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ»

Система обнаружения/предотвращения вторжений основана на ПО Suricata с открытым исходным кодом и использует метод захвата пакетов NETMAP для увеличения производительности и уменьшения нагрузки на центральный процессор.

5.1 Подраздел «Администрирование»

Подраздел «Администрирование» делится на следующие категории меню:

- настройки;
- сохранение;
- правила;
- предупреждения.

5.1.1 Категория «Настройки»

Категория «Настройки» позволяет настраивать систему обнаружения и предотвращения вторжений.

При использовании системы обнаружения и системы предотвращения вторжений необходимо убедиться, что отключен режим Hardware Offloading. Для выключения режима Hardware Offloading необходимо перейти в «Интерфейсы» - «Настройки» и поставить флажки напротив «CRC аппаратного обеспечения», «TSO аппаратного обеспечения», «LRO аппаратного обеспечения» и нажать кнопку «Сохранить» внизу страницы.

Для включения системы обнаружения вторжений необходимо установить флажок напротив поля «Включен». Для включения системы предотвращения вторжений необходимо установить флажок напротив поля «Режим IPS». Для включения смешанного режима (на некоторых конфигурациях, таких как IPS с VLAN, работа в этом режиме требуется для захвата данных на физическом интерфейсе) необходимо установить флажок напротив поля «Смешанный режим». В поле «Передавать предупреждения (alerts) в syslog» необходимо установить флажок при необходимости отправления предупреждений (alerts) в syslog в формате fast log. В поле «Сравнение шаблонов» необходимо выбрать используемый алгоритм поиска подстроки при обработке пакетов:

- по умолчанию (используется алгоритм Aho-Corasick);
- Aho-Corasick (алгоритм сопоставления со «словарем», который находит подстроки из «словаря» в пакетах);
- Hyperscan (высокопроизводительная библиотека сопоставления регулярных выражений от Intel).

В поле «Интерфейсы» необходимо выбрать интерфейсы, которые будут использоваться системой обнаружения и предотвращения вторжений. В поле «Домашние сети (\$HOME_NET)» необходимо ввести сети, которые будут определяться как домашние. В поле «Размер пакета по умолчанию» необходимо ввести размер пакетов сети по умолчанию. В поле «Архивировать журнал» необходимо выбрать периодичность архивирования журнала предупреждений. В поле «Сохранить журналы» необходимо ввести количество журналов, которые

необходимо сохранять. В поле «Содержимое пакета для журнала» необходимо установить флажок для отправки полезной нагрузки (часть пакета данных без служебной информации) в журнал для дальнейшего анализа. Для сохранения настроек необходимо нажать на кнопку «Применить» (Рисунок 113).

Обнаружение вторжений: Администрирование ▶ ↺ ■

Настройки Сохранение Правила Предупреждения (Alerts) Расписание

расширенный режим справка ⓘ

Включен	<input checked="" type="checkbox"/>
Режим IPS	<input type="checkbox"/>
Смешанный режим	<input type="checkbox"/>
Передавать предупреждения (alerts) в syslog	<input checked="" type="checkbox"/>
Активировать eve логирование в syslog	<input checked="" type="checkbox"/>
Сравнение маршрутов	Aho-Corasick
Интерфейсы	LAN
<input checked="" type="checkbox"/> Очистить все	
Домашние сети (SHOME_NET)	192.168.0.0/16 × 10.0.0.0/8 × 172.16.0.0/12 ×
<input checked="" type="checkbox"/> Очистить все	
размер пакета по-умолчанию	
Архивировать журнал	Еженедельно
Сохранить журналы	4
Содержимое пакета для журнала	<input type="checkbox"/>

Рисунок 113 – Обнаружение вторжений: Администрирование: Настройки

5.1.2 Категория «Сохранение»

Категория «Сохранение» позволяет просматривать подгружаемые правила системы обнаружения и предотвращения вторжений, загружать файлы обновления правил.

Для включения имеющихся правил необходимо поставить галочку напротив группы правил и нажать кнопку «Включить выбранные», а затем нажать на кнопку «Скачать и обновить правила» (Рисунок 114).

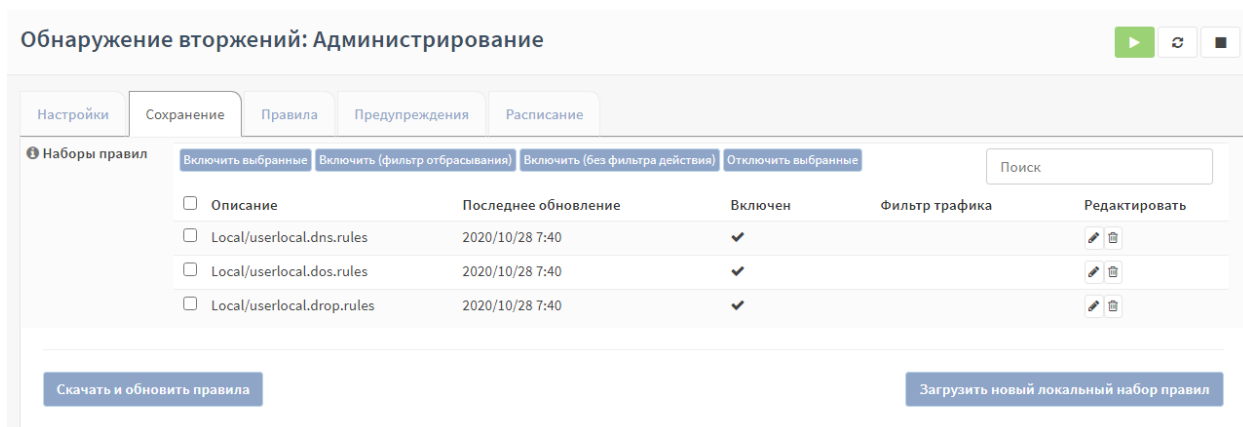


Рисунок 114 – Обнаружение вторжений: Администрирование: Сохранение (включение групп правил)

Для загрузки локальных правил необходимо нажать на кнопку «Загрузить новый локальный набор правил». После этого появится всплывающее окно об успешном загрузке правил (Рисунок 115). Правила добавятся в список (Рисунок 116).

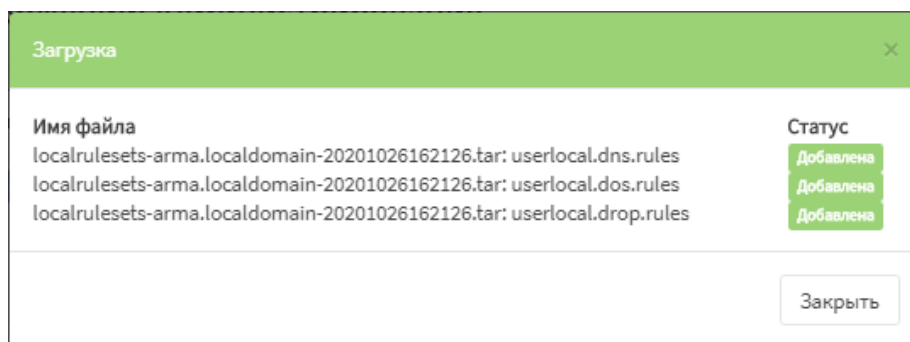


Рисунок 115 – Обнаружение вторжений: Администрирование: Обновление (загрузка локальных правил)

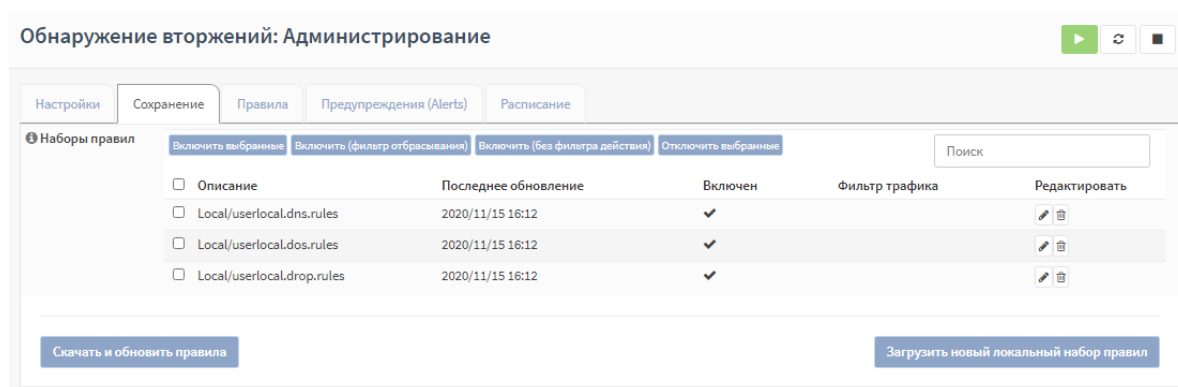


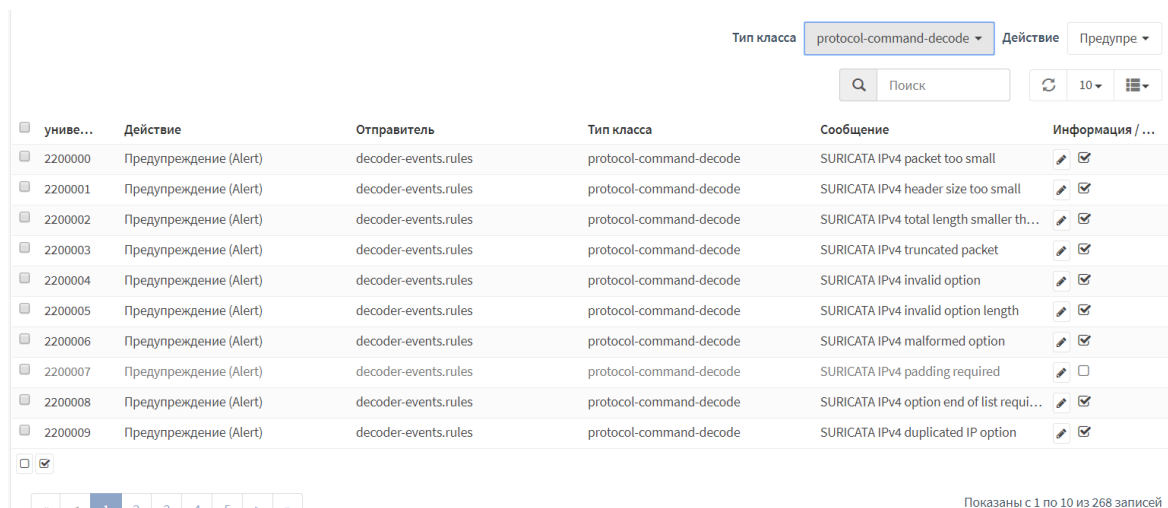
Рисунок 116 – Обнаружение вторжений: Администрирование: Обновление

После этого необходимо нажать на кнопку «Скачать и обновить правила» для того, чтобы активировать выбранные настройки.

Для отключения файла правил необходимо установить флажок напротив правила, нажать на кнопку «Отключить выбранные» и нажать на кнопку «Скачать и обновить правила».

5.1.3 Категория «Правила»

Категория «Правила» позволяет просматривать все действующие (в том числе из включенных групп правил из категории «Сохранение») правила, а также позволяет отсортировать все правила по действию и типу класса, нажав на выпадающий список в соответствующих полях (Рисунок 117).

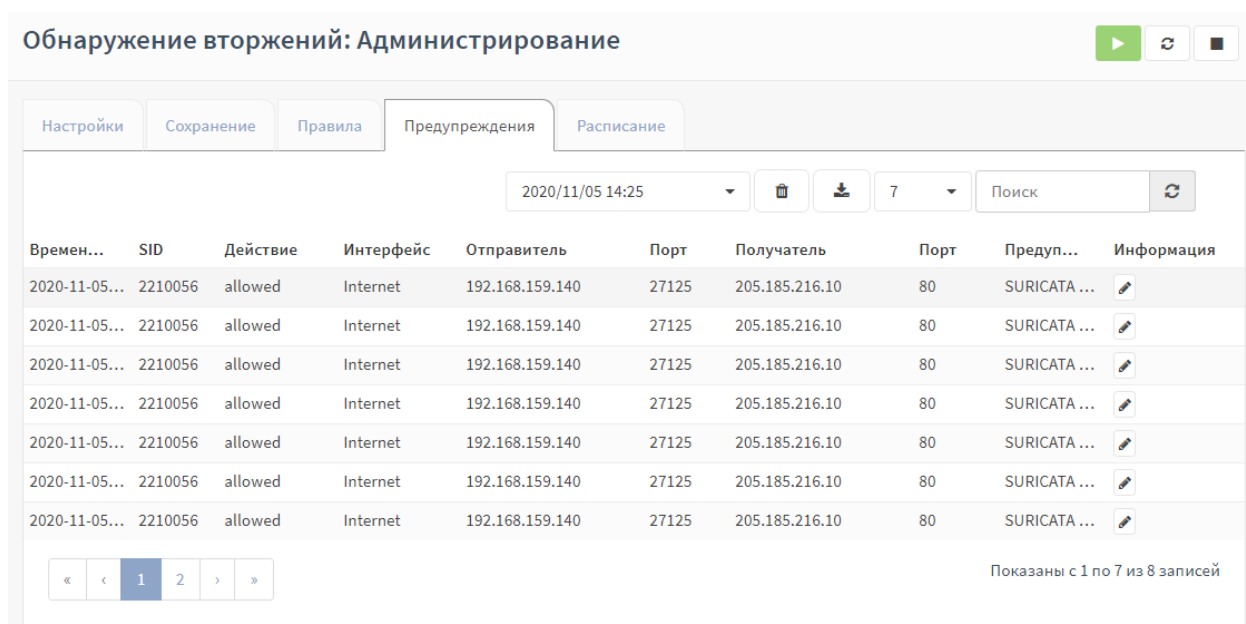


универс...	Действие	Отправитель	Тип класса	Сообщение	Информация / ...
2200000	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 packet too small	
2200001	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 header size too small	
2200002	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 total length smaller th...	
2200003	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 truncated packet	
2200004	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 invalid option	
2200005	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 invalid option length	
2200006	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 malformed option	
2200007	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 padding required	
2200008	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 option end of list requi...	
2200009	Предупреждение (Alert)	decoder-events.rules	protocol-command-decode	SURICATA IPv4 duplicated IP option	

Рисунок 117 – Обнаружение вторжений: Администрирование: Правила

5.1.4 Категория «Предупреждения»

Категория «Предупреждения» позволяет просматривать журнал срабатывания правил системы обнаружения и предотвращения вторжений, а также отсортировать по дате/времени, выполнить поиск, очистить весь журнал оповещений и выбрать, сколько последних предупреждений, нажав на соответствующий заголовок (Рисунок 118).



Времен...	SID	Действие	Интерфейс	Отправитель	Порт	Получатель	Порт	Предуп...	Информация
2020-11-05...	2210056	allowed	Internet	192.168.159.140	27125	205.185.216.10	80	SURICATA ...	
2020-11-05...	2210056	allowed	Internet	192.168.159.140	27125	205.185.216.10	80	SURICATA ...	
2020-11-05...	2210056	allowed	Internet	192.168.159.140	27125	205.185.216.10	80	SURICATA ...	
2020-11-05...	2210056	allowed	Internet	192.168.159.140	27125	205.185.216.10	80	SURICATA ...	
2020-11-05...	2210056	allowed	Internet	192.168.159.140	27125	205.185.216.10	80	SURICATA ...	
2020-11-05...	2210056	allowed	Internet	192.168.159.140	27125	205.185.216.10	80	SURICATA ...	
2020-11-05...	2210056	allowed	Internet	192.168.159.140	27125	205.185.216.10	80	SURICATA ...	

Рисунок 118 – Обнаружение вторжений: Администрирование: Предупреждения

Для настройки расписания импорта правил необходимо задать настройки во вкладке «Настройки», нажать кнопку «Применить» и перейти во вкладку «Расписание».

При нажатии на категорию «Расписание» происходит автоматическое перенаправление в редактирование расписания системы предотвращения вторжений, которое находится в разделе «Система» - «Настройки» - «Планировщик задач Cron». При редактировании расписания в поле «Команда» необходимо выбрать «Импорт правил COB» (Рисунок 119).

Редактировать задачу ✕

справка ⓘ

включен ⓘ	<input type="checkbox"/>
Мин ⓘ	<input type="text" value="0"/>
Ч ⓘ	<input type="text" value="0"/>
День месяца ⓘ	<input type="text" value="*/"/>
Месяцы ⓘ	<input type="text" value="*/"/>
День недели ⓘ	<input type="text" value="*/"/>
Команда ⓘ	<input type="text" value="Импорт правил COB"/>
Параметры ⓘ	<input type="text"/>
Описание ⓘ	<input type="text" value="importoptions updates"/>

Отменить

Сохранить

Рисунок 119 – Обнаружение вторжений: Настройки импорта правил: Расписание

Остальные параметры расписания расписаны более подробно в подразделе 6.3.8 настоящего руководства.

5.2 Подраздел «Контроль уровня приложений»

Подраздел «Контроль уровня приложений» позволяет включать, выключать, просматривать, редактировать, удалять и создавать правила системы обнаружения (предотвращения) вторжений, используя шаблоны протоколов, либо вручную (Рисунок 120).

Обнаружение вторжений: Контроль уровня приложений

Настройка правил

Поиск

7

Включен	Заголовок	Тип протокола	Группа	Действие	Редакти...
<input checked="" type="checkbox"/>	test	modbus		Предупреждение	

Показаны с 1 по 1 из 1 записей

Рисунок 120 – Обнаружение вторжений: Контроль уровня приложений

Ниже представлен список поддерживаемых протоколов, для которых представлены шаблоны форм и степень их разбора (Таблица 2).

Таблица 2 – Поддерживаемые протоколы с указанием степени их разбора



Протокол	Стандарт	Степень разбора
Modbus TCP	MODBUS Application Protocol Specification V1.1b3	<p>Для сообщений по протоколу Modbus TCP можно задать правило обнаружения на основе признака совпадения:</p> <ul style="list-style-type: none"> – свойство функции (код или категория функции); – тип доступа к данным (тип доступа и основная модель данных); – диапазон функции (ввод кода функции, адреса и значения переменной вручную). <p>При обнаружении по свойству функции возможно задать дополнительные опции:</p> <ul style="list-style-type: none"> – используемую функцию, подфункцию; – категория кодов функции (назначенная (коды функций, который определены в Modbus спецификации), не назначенная, общедоступная (стандартные и организационные коды), пользовательская (два диапазона кодов, для которых пользователь может назначить произвольную функцию, зарезервированная (коды функций, которые не являются стандартными), все категории). <p>При классификации по доступу к данным возможно задать следующие дополнительные опции:</p> <ul style="list-style-type: none"> – тип доступа к данным (записать / считать); – модель данных: <ul style="list-style-type: none"> ○ «Регистры флагов (Coils)» (битовые данные, доступ чтение / запись);

Протокол	Стандарт	Степень разбора
		<ul style="list-style-type: none"> ○ «Регистры хранения (Holding Registers)» (16 битовые данные, доступ чтение / запись); ○ «Дискретные входы (Discrete Inputs)» (битовые данные, доступ чтение); ○ «Регистры ввода (Input Registers)» (16 битовые данные, доступ чтение).
IEC 60870-5-104	ГОСТ Р МЭК 60870-5-104-2004	<p>Сообщения по протоколу IEC 60870-5-104 могут быть определены по типу пакета (полный APDU, либо для целей управления — только поля APCI);</p> <p>При классификации по типу пакета APCI возможен выбор формата пакета:</p> <ul style="list-style-type: none"> – любой; – «U-format (unnumbered control functions)» — функции управления без нумерации; – «S-format (numbered supervisory functions)» — функции контроля с нумерацией. <p>При классификации по типу пакета ASDU возможно задание:</p> <ul style="list-style-type: none"> – диапазона разрешенных входящих пакетов (RX); – диапазона разрешенных исходящих пакетов (TX); – типа ASDU; – причины передачи (ASDU cause of transfer); – числового значения ASDU адреса; – адреса объекта информации в формате диапазона; – значения IOA.
S7 Communication	Стандарт протокола связи коммуникационных модулей серий Siemens SIMATIC S7-300/400	<p>Сообщения по протоколу S7Communication разделяются по функции:</p> <ul style="list-style-type: none"> – CPUSERVICE; – SETUPCOMM; – READVAR; – WRITEVAR; – REQUESTDOWNLOAD; – DOWNLOADBLOCK; – DOWNLOADENDED; – STARTUPLOAD; – UPLOAD; – ENDUPLOAD; – PLCCONTROL; – PLCSTOP. <p>При выборе в поле «Функция» функции</p>

Протокол	Стандарт	Степень разбора
		<p>«READVAR» необходимо выбрать тип области чтения и поля ввода имени области, типа данных, количества данных и смещения данных.</p> <p>При выборе в поле «Функция» функции «WRITEVAR» необходимо выбрать тип области чтения и поля ввода имени области, типа данных, количества данных и смещения данных, типа передаваемого значения, количество передаваемых данных, список значений данных.</p> <p>При выборе в поле «Функция» функции «REQUESTDOWNLOAD» появятся поле выбора типа блока, номера блока и целевой файловой системы.</p> <p>При выборе в поле «Функция» функции «DOWNLOADBLOCK» появятся поле выбора типа блока, номера блока и целевой файловой системы.</p> <p>При выборе в поле «Функция» функции «STARTUPLOAD» появятся поле выбора типа блока, номера блока и целевой файловой системы.</p> <p>При выборе в поле «Функция» функции «PLCCONTROL» появятся поле выбора функции управления ПЛК:</p> <ul style="list-style-type: none"> – «INSE (Активация скаченного блока, параметром выступает имя блока)»; – «DELE (Удаление блока, параметром выступает имя блока)»; – «PPROGRAM (Запуск программы, параметром выступает имя программы)»; – «GARB (Сжатие памяти)»; – «MODU (Копирование RAM в ROM, параметр содержит идентификатор файловой системы A/E/P)»; – «OFF (Выключение ПЛК)»; – «ON (Включение ПЛК)».
OPC UA	IEC 62541	<p>Сообщения по протоколу OPC UA разделяются по тип сообщения:</p> <ul style="list-style-type: none"> – HELLO (маркер начала передачи данных между клиентом и сервером); – ACKNOWLEDGE (ответ на сообщение типа HELLO); – OPEN (открытие канала передачи данных с предложенным методом шифрования данных); – MESSAGE (передаваемое

Протокол	Стандарт	Степень разбора
		<p>сообщение);</p> <ul style="list-style-type: none"> – CLOSE (конец сессии). <p>При выборе «OPEN» появятся поле выбора политика безопасности.</p> <p>При выборе «MESSAGE» в поле появятся поле выбора типа запроса.</p> <p>При выборе «BROWSE» в поле «Тип запроса» появятся поле ввода диапазон запроса.</p> <p>При выборе «READ» в поле «Тип запроса» появятся поле ввода диапазон запроса.</p> <p>При выборе «WRITE» в поле «Тип запроса» появятся поле ввода диапазон запроса.</p> <p>При выборе «CALL» в поле «Тип запроса» появятся поле ввода идентификатора узла, содержащий вызываемую процедуру и поле ввода идентификатора узла вызываемой процедуры.</p>
OPC DA	OLE for Process Control Data Access Automation Interface Standard v.2.0	<p>Сообщения по протоколу OPC DA разделяются по типу сообщения:</p> <ul style="list-style-type: none"> – REQUEST; – PING; – RESPONSE; – FAULT; – WORKING; – NOCALL; – REJECT; – ACK; – CI_CANCEL; – FACK; – CANCEL_ACK; – BIND; – BIND_ACK; – BIND_NACK; – ALTER_CONTEXT; – ALTER_CONTEXT_RESP; – SHUTDOWN; – AUTH3; – CO_CANCEL; – ORPHANED. <p>При выборе «REQUEST» в поле появятся поле ввода идентификатора вызываемого объекта и поле ввода номера вызываемой функции объекта.</p>
UMAS	Основан на протоколе Xway Unite. Протокол Umas используется для настройки и мониторинга ПЛК	<p>Сообщения по протоколу UMAS разделяются по функциям:</p> <ul style="list-style-type: none"> – инициализация UMAS сессии; – чтение информации о проекте; – чтение внутренней информации PLC;

Протокол	Стандарт	Степень разбора
	Schneider-Electric.	<ul style="list-style-type: none"> – назначение PLC владельца; – инициализация загрузки (копирование с инженерного ПК на PLC); – завершение загрузки (копирования с инженерного ПК на PLC); – инициализация скачивания (копирование с PLC на инженерный ПК); – конец скачивания (копирования с PLC на инженерный ПК); – включение PLC; – выключение PLC.
MMS	IEC 61850-8-1	<p>Сообщения по протоколу MMS разделяются по типу сообщения.</p> <p>Для типа сообщения «CONFIRMED_REQUEST» возможен выбор типа служб.</p> <p>Для службы «READ» возможен ввод имени переменной и адреса переменной для функции чтения.</p> <p>Для службы «WRITE» возможен ввод имени переменной для функции записи.</p>
GOOSE	IEC 61850-8-1	Сообщения по протоколу GOOSE разделяются по идентификатору приложения, по значению поля dataset, по значению поля gocbref, по значению поля goid.

Для того чтобы редактировать существующие правила, необходимо нажать на кнопку  напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку .

При редактировании правила необходимо нажать на флажок напротив поля «Включен» при необходимости включения правила. В поле «Заголовок» необходимо ввести название правила. В поле «Использовать шаблон» необходимо выбрать шаблон протокола, который необходимо использовать (Рисунок 121).

Редактировать правило

справка 

 Включен
 ☒

 Заголовок

 Группа

 Использовать шаблон

modbus 

Рисунок 121 – Обнаружение вторжений: Контроль уровня приложений (редактирование)

5.2.1 Шаблон протокола Modbus

При использовании шаблона протокола Modbus появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert) » – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject) » – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop) » – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass) » – при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать:

- «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола;
- «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола;
- «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Совпадение по» необходимо выбрать признаки совпадения правила:

- свойство функции (код или категория функции);
- доступ к данным (тип доступа и основная таблица);
- диапазон функции (ввод кода функции, адреса и значения переменной вручную).

При выборе «Свойство функции» в поле «Совпадение по» появится поле «Совпадение по» со следующими признаками совпадения:

- код функции (запрашиваемое действие).
- категория функции (категория кодов функции).

При выборе «Код функции» в поле «Совпадение по» появятся следующие поля:

- код функции (необходимо выбрать функцию);

При выборе «08:Diagnostic» в поле «Код функции» появится поле:

- код подфункции (необходимо выбрать код подфункции).

При выборе «Категория функции» в поле «Совпадение по» появятся следующие поля:

- отрицание выбранной категории (необходимо поставить флажок при выборе все категорий кроме указанной в поле «Категория совпадения»);
- категория совпадения (необходимо выбрать категорию кодов функции:
 - назначенный (коды функций, который определены в Modbus спецификации);
 - не назначено;
 - общедоступный (стандартные и организационные коды);
 - пользователь (два диапазона кодов (65 – 72, 100 – 110), для которых пользователь может назначить произвольную функцию;
 - зарезервировано (коды функций, которые не являются стандартными (9, 10, 13, 14, 41, 42, 90, 91, 125, 126, 127);
 - все.

При выборе «Доступ к данным» в поле «Совпадение по» появится поле «Совпадение по» со следующими признаками совпадения:

- тип доступа к данным (необходимо выбрать):
 - записать (для записи значений в таблицы данных используются функции с кодами 5, 6, 15, 16, 21, 22 и другие);
 - считать (для чтения значений из таблиц данных используются функции с кодами 1 – 4, 7, 8, 11, 12, 20, 24 и другие);
- доступ к основной таблице (необходимо выбрать модель данных):
 - «Регистры флагов (Coils)» (битовые данные, доступ чтение / запись);
 - «Регистры хранения (Holding Registers)» (16 битовые данные, доступ чтение / запись);
 - «Дискретные входы (Discrete Inputs)» (битовые данные, доступ чтение);
 - «Регистры ввода (Input Registers)» (16 битовые данные, доступ чтение).


При выборе «Диапазон функции» в поле «Совпадение по» появятся следующие поля.

В поле «Код функции» необходимо ввести диапазон функции. Данное поле может принимать значения от 0 до 255.

В поле «Адрес» необходимо ввести диапазон номеров адреса. Данное поле может принимать значения от 0 до 65535.

В поле «Значение» необходимо ввести диапазон значений выбранного адреса. Данное поле может принимать значения от 0 до 65535.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (Рисунок 122).

справка 

1 Включен	<input checked="" type="checkbox"/>
1 Заголовок	<input type="text" value="modbus"/>
1 Группа	<input type="text"/>
1 Использовать шаблон	<input type="text" value="modbus"/>
1 Действие	<input type="text" value="Предупредить (Alert)"/>
1 Сообщение	<input type="text" value="modbus"/>
1 IP-адрес отправителя	<input type="text" value="any"/>
1 Порт источника	<input type="text" value="any"/>
1 Выберите направление	<input type="text" value="Прямое"/>
1 IP-адрес получателя	<input type="text" value="any"/>
1 Порт назначения	<input type="text" value="502"/>
1 Фильтровать на основе протокола	<input type="text" value="Указать дополнительные параметры"/>
1 Совпадение по	<input type="text" value="Функции"/>
1 Совпадение по	<input type="text" value="Код функции"/>
1 Код функции	<input type="text" value="01:Read Coils"/>

Отменить

Сохранить

Рисунок 122 – Обнаружение вторжений: Контроль уровня приложений
(редактирование: Modbus)

5.2.2 Шаблон протокола IEC 104

При использовании шаблона протокола IEC 104 появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert) » – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject) » – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop) » – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass) » – при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника»

необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать:

- «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола;
- «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола;
- «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Функция приложения» необходимо выбрать тип пакета (может быть передан либо полный APDU, либо (для целей управления) только поля APCI):

- «ASDU (блок данных прикладного уровня)»;
- «APCI (управляющая информация прикладного уровня)» используется, чтобы определить начало и конец ASDU, каждый заголовок APCI включает следующие маркировочные элементы:

- стартовый символ;
- указание длины ASDU вместе с полем управления.

При выборе «APCI (управляющая информация прикладного уровня)» в поле «Функция приложения» появится поле «Формат». В поле «Формат» необходимо выбрать формат:

- любой;
- «U-format (unnumbered control functions)» – функции управления без нумерации;
- «S-format (numbered supervisory functions)» – функции контроля с нумерацией.

При выборе «ASDU (блок данных прикладного уровня)» в поле «Функция приложения» появятся следующие поля. В поле «RX» необходимо ввести диапазон разрешенных входящих пакетов или оставить пустым, в случае отсутствия ограничений (например, [:10] – пропустить первые 10 входящих пакетов). В поле «TX» необходимо ввести диапазон разрешенных исходящих пакетов или оставить пустым, в случае отсутствия ограничений (например, [:10] – пропустить первые 10 исходящих пакетов).

В поле «Тип ASDU» необходимо выбрать тип ASDU. Все возможные типы приведены в таблице 3.

Таблица 3 – Типы ASDU

Идентификатор типа	Описание	Метка ASDU
<0>	:= не определяется	
<1>	:= одноэлементная информация	M_SP_NA_1
<3>	:= двухэлементная информация	M_DP_NA_1
<5>	:= информация о положении отпаяк	M_ST_NA_1
<7>	:= строка из 32 битов	M_BO_NA_1
<9>	:= значение измеряемой величины, нормализованное значение	M_ME_NA_1
<11>	:= значение измеряемой величины, масштабированное значение	M_ME_NB_1
<13>	:= значение измеряемой величины, короткий формат с плавающей запятой	M_ME_NC_1
<15>	:= интегральные суммы	M_IT_NA_1
<20>	:= упакованная одноэлементная информация с определением изменения состояния	M_PS_NA_1
<21>	:= значение измеряемой величины, нормализованное значение без описателя качества	M_ME_ND_1
<22..29>	:= резерв для дальнейших совместимых определений	
*<30>	:= одноэлементная информация с меткой времени CP56Время2а	M_SP_TB_1
*<31>	:= двухэлементная информация с меткой времени CP56Время2а	M_DP_TB_1
*<32>	:= информация о положении отпаяк с меткой времени CP56Время2а	M_ST_TB_1
*<33>	:= строка из 32 битов с меткой времени CP56Время2а	M_BO_TB_1
*<34>	:= значение измеряемой величины, нормализованное значение с меткой времени CP56Время2а	M_ME_TD_1
*<35>	:= значение измеряемой величины, масштабированное значение с меткой времени CP56Время2а	M_ME_TE_1
*<36>	:= значение измеряемой величины, короткий формат с плавающей запятой с меткой времени CP56Время2а	M_ME_TF_1
*<37>	:= интегральная сумма с меткой времени CP56Время2а	M_IT_TB_1
*<38>	:= информация о работе релейной защиты с меткой времени CP56Время2а	M_EP_TD_1
*<39>	:= упакованная информация о срабатывании пусковых органов защиты с меткой времени CP56Время2а	M_EP_TE_1
*<40>	:= упакованная информация о срабатывании выходных цепей защиты с меткой времени CP56Время2а	M_EP_TF_1
<41>.. <44>	:= резерв для дальнейших совместимых определений	
<45>	:= одноэлементная команда	C_SC_NA_1
<46>	:= двухэлементная команда	C_DC_NA_1

Идентификатор типа	Описание	Метка ASDU
<47>	:= команда пошагового регулирования	C_RC_NA_1
<48>	:= команда установки, нормализованное значение	C_SE_NA_1
<49>	:= команда установки, масштабированное значение	C_SE_NB_1
<50>	:= команда установки, короткое число с плавающей запятой	C_SE_NC_1
<51>	:= строка из 32 битов	C_BO_NA_1
<52>..<>57>	:= резерв для дальнейших совместимых определений	
<58>	:= одноэлементная команда с меткой времени CP56Время2a	C_SC_TA_1
<59>	:= двухэлементная команда с меткой времени CP56Время2a	C_DC_TA_1
<60>	:= команда пошагового регулирования с меткой времени CP56Время2a	C_RC_TA_1
<61>	:= команда уставки, нормализованное значение с меткой времени CP56Время2a	C_SE_TA_1
<62>	:= команда уставки, масштабированное значение с меткой времени CP56Время2a	C_SE_TB_1
<63>	:= команда уставки, короткое число с плавающей запятой с меткой времени CP56Время2a	C_SE_TC_1
<64>	:= строка из 32 битов с меткой времени CP56Время2a	C_BO_TA_1
<65>..<>69>	:= резерв для дальнейших совместимых определений	
<70>	:= конец инициализации	M_EI_NA_1
<71>..<>99>	:= резерв для дальнейших совместимых определений	M_EI_NA_1
<100>	:= команда опроса	C_IC_NA_1
<101>	:= команда опроса счетчика	C_CI_NA_1
<102>	:= команда считывания	C_RD_NA_1
<103>	:= команда синхронизации времени (опция, см. 7.6)	C_CS_NA_1
<105>	:= команда установки процесса в исходное состояние	C_RP_NA_1
<107>	:= команда тестирования с меткой времени CP56Время2a	C_TS_NA_1
<108>..<>109>	:= резерв для дальнейших совместимых определений	C_IC_NA_1
<110>	:= параметр измеряемой величины, нормализованное значение	P_ME_NA_1
<111>	:= параметр измеряемой величины, масштабированное значение	P_ME_NB_1
<112>	:= параметр измеряемой величины, короткий формат с плавающей запятой	P_ME_NC_1
<113>	:= параметр активации	P_AC_NA_1
<114>..<>119>	:= резерв для дальнейших совместимых определений	P_AC_NA_1
<120>	:= файл готов	F_FR_NA_1
<121>	:= секция готова	F_SR_NA_1
<122>	:= вызов директории, выбор файла, вызов файла, вызов	F_SC_NA_1

Идентификатор типа	Описание	Метка ASDU
	секции	
<123>	:= последняя секция, последний сегмент	F_LS_NA_1
<124>	:= подтверждение файла, подтверждение секции	F_AF_NA_1
<125>	:= сегмент	F_SG_NA_1
<126>	:= директория	F_DR_TA_1

В поле «ASDU COT (cause of transfer)» необходимо выбрать причину передачи. В поле «AD (ASDU адрес)» необходимо ввести числовое значение ASDU адреса (это адрес станции длиной 1 или 2 байта, который может быть структурирован, чтобы иметь возможность обращаться ко всей станции или к отдельному ее сектору). В поле «IOA (адрес объекта информации)» необходимо ввести адрес объекта информации в формате диапазона. В поле «IOA значение» необходимо ввести IOA значение или оставить пустым и нажать на кнопку «Сохранить» для сохранения внесенных изменений (Рисунок 123).

Редактировать правило

справка

Включен	<input checked="" type="checkbox"/>
Заголовок	IEC 104
Группа	
Использовать шаблон	IEC 104
Действие	Предупредить (Alert)
Сообщение	IEC 104
IP-адрес отправителя	any
Порт источника	any
Выберите направление	Прямое и обратное
IP-адрес получателя	any
Порт назначения	2404
Фильтровать на основе протокола	Указать дополнительные параметры
Функция приложения	ASDU (блок данных прикладного уровня)
RX	
TX	
Тип ASDU	Любой
ASDU COT (cause of transfer)	Любой
AD (ASDU адрес)	
IOA (адрес объекта информации)	
IOA значение	

Отменить

Сохранить

Рисунок 123 – Обнаружение вторжений: Контроль уровня приложений (редактирование IEC104)

5.2.3 Шаблон протокола S7comm

При использовании шаблона протокола S7comm появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert) » – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject) » – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop) » – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass) » – при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес

отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать:

- «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола;
- «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола;
- «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Тип сообщения» необходимо выбрать тип сообщения в соответствии с таблицей 4.

Таблица 4 – Типы сообщений

№	Тип сообщения	Описание
1	JOBREQUEST	Пакет с запросом на выполнение функции
2	ACK	Пакет с результатом выполнения операции
3	ACKDATA	Пакет с ответом на запрос
4	USERDATA	Пакет с данными пользователя

При выборе типа сообщения «JOBREQUEST» появится поле «Функция», в котором необходимо выбрать функцию в соответствии с таблицей 5.

Таблица 5 – Функции протокола S7comm

№	Функция	Описание
1	CPUSERVICE	Сервисы ЦП
2	SETUPCOMM	Запрос на подключение к ПЛК
3	READVAR	Запрос на чтение
4	WRITEVAR	Запрос на запись
5	REQUESTDOWNLOAD	Запрос на загрузку прошивки
6	DOWNLOADBLOCK	Загрузка прошивки на ПЛК
7	DOWNLOADEDDED	Запрос на завершение загрузки прошивки на ПЛК
8	STARTUPLOAD	Запрос на выгрузку прошивки
9	UPLOAD	Выгрузка прошивки с ПЛК
10	ENDUPLOAD	Окончание выгрузки прошивки с ПЛК
11	PLCCONTROL	Управление ПЛК
12	PLCSTOP	Остановка ПЛК

При выборе функции «READVAR» появится поле «Тип области», в котором необходимо выбрать тип области чтения (Таблица 6).

Таблица 6 – Типы области

№	Тип области	Описание
1	Любой	Любая область чтения
2	SI (System info)	Системная информация
3	SF (System flags)	Системные флаги
4	AI (Analog inputs)	Аналоговый ввод
5	AO (Analog outputs)	Аналоговый вывод
6	C (Counters)	Счетчики
7	T (Timers)	Таймеры
8	IC (IEC Counters)	Счетчики IEC
9	IT (IEC Timers)	Таймеры IEC
10	P (Direct peripheral access)	Прямой доступ к периферии
11	I (Inputs)	Ввод
12	Q (Outputs)	Вывод
13	M (Flags)	Флаги
14	DB (Data blocks)	Блоки данных
15	DI (Instance data blocks)	Блоки данных экземпляра
16	LV (Local data)	Локальные данные

При выборе в поле «Тип области» всех значений кроме значения «Любой» появятся следующие поля:

- «Имя области»;
- «Тип данных»;
- «Количество данных»;
- «Смещение данных».

В поле «Имя области» необходимо ввести номер области (от 0 до 65535).

В поле «Тип данных» необходимо выбрать тип данных.

В поле «Количество данных» необходимо ввести количество записей указанного типа.

В поле «Смещение данных» необходимо указать целочисленное значение в шестнадцатеричной системе счисления в формате 0x000000.

При выборе функции «WRITEVAR» появится поле «Тип области», в котором необходимо выбрать тип области записи (Таблица 6).

При выборе в поле «Тип области» всех значений кроме значения «Любой» появятся следующие поля:

- «Имя области»;
- «Тип данных»;
- «Количество данных»;
- «Смещение данных»;
- «Тип передаваемого значения»;
- «Количество передаваемых данных»;
- «Список значений данных».

В поле «Имя области» необходимо ввести номер области (от 0 до 65535).

В поле «Тип данных» необходимо выбрать тип данных.

В поле «Количество данных» необходимо ввести количество записей указанного типа.

В поле «Смещение данных» необходимо указать целочисленное значение в шестнадцатеричной системе счисления в формате 0x000000.

В поле «Тип передаваемого значения» необходимо выбрать тип данных из следующих типов значений:

- «NULL» – не выбрано;
- «BIT» – значение в битах;
- «BYTE» – значение в байтах;
- «INT» – целочисленное значение;
- «REAL» – вещественное;
- «STR» – строковое значение.

В поле «Количество передаваемых данных» необходимо ввести число значений указанного типа, которое будет передано в данном сообщении.

В поле «Список значений данных» необходимо ввести число значений указанного типа в 16-ой системе счисления, которое будет передано в данном сообщении.

При выборе функций «REQUESTDOWNLOAD», «DOWNLOADBLOCK», «STARTUPLOAD» появится поле «Тип блока», в котором необходимо выбрать тип блока скачивания (Таблица 7).

Таблица 7 – Типы блока

№	Тип блока	Описание
1	Любой	-
2	OB (Organisation Block, stores the main programs)	Организационный блок (хранит основные программы)
3	DB (Data Block, stores data required by the PLC program)	Блок данных (хранит данные для ПЛК программы)
4	SDB (System Data Block, stores data required by the PLC program)	Системный блок (хранит данные необходимые для ПЛК программы)
5	FC (Function, functions that are stateless (do not have their own memory), they can be called from other programs)	Функция (функции, которые не имеют состояния и могут быть вызваны другими программами)
6	SFC (System Function, functions that are stateless (do not have their own memory), they can be called from other programs)	Система функций (функции, которые не имеют состояния и могут быть вызваны другими программами)
7	FB (Function Block, functions that are stateful, they usually have an associated SDB)	Блок функций (функции, которые имеют состояния)
8	SFB (System Function Block, functions that are stateful, they usually have an associated SDB)	Блок системы функций (функции, которые не имеют состояния и могут быть вызваны другими программами)

При выборе в поле «Тип блока» всех значений кроме «Любой» появятся следующие поля:

- «Номер блока»;
- «Целевая файловая система».

В поле «Номер блока» необходимо ввести пятизначное число в 10-ой системе счисления.

В поле «Целевая файловая система» необходимо выбрать:

- «P – пассивная (блок требует активации после скачивания)»;
- «A – активная (блок будет активизирован после скачивания)».

При выборе функции «PLCCONTROL» появится поле «Функция», в котором необходимо выбрать функцию управления ПЛК:

- «INSE (Активация скаченного блока, параметром выступает имя блока)»;
- «DELE (Удаление блока, параметром выступает имя блока)»;
- «PPROGRAM (Запуск программы, параметром выступает имя программы)»;
- «GARB (Сжатие памяти)»;
- «MODU (Копирование RAM в ROM, параметр содержит идентификаторы файловой системы A/E/P)»;
- «OFF (Выключение ПЛК)»;
- «ON (Включение ПЛК)».

После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 124).

1 Использовать шаблон	S7comm
1 Действие	Предупреждение
1 Сообщение	
1 IP-адрес отправителя	any
1 Порт источника	any
1 Выберите направление	Прямое
1 IP-адрес получателя	any
1 Порт назначения	any
1 Фильтровать на основе протокола	Указать дополнительные параметры
1 Тип сообщения	JOBREQUEST
1 Функция	READVAR
1 Тип области	SF (System flags)
1 Имя области	1
1 Тип данных	BIT
1 Количество данных	1
1 Смещение данных	0x000000

Отменить Сохранить

Рисунок 124 – Обнаружение вторжений: Контроль уровня приложений
(редактирование: S7comm)

5.2.4 Шаблон протокола OPC UA

При использовании шаблона протокола OPC UA появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert) » – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject) » – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop) » – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass) » – при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать:

- «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола;
- «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола;
- «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появится поле «Тип сообщения», в котором необходимо выбрать тип сообщения:

- HELLO (маркер начала передачи данных между клиентом и сервером);
- ACKNOWLEDGE (ответ на сообщение типа HELLO);
- OPEN (открытие канала передачи данных с предложенным методом шифрования данных);
- MESSAGE (передаваемое сообщение);
- CLOSE (конец сессии).

При выборе типа сообщения «OPEN» появится поле «Политика безопасности», в котором необходимо выбрать политику безопасности:

- «Любой» — любая политика безопасности;
- «NONE» — политика безопасности для конфигураций с самыми низкими требованиями безопасности, нет алгоритмов шифрования;
- BASIC128RSA15 — политика безопасности для конфигураций со средними требованиями безопасности такие как:
 - проверка сертификата безопасности;
 - необходимо шифрование;
 - необходима безопасная подпись;
 - использование алгоритма шифрования SHA 1;
 - использование алгоритма шифрования AES 128 CBC;
 - использование алгоритма шифрования RSA-PKCS15-SHA1;
 - использование алгоритма шифрования RSA-PKCS15;
 - использование алгоритма получения ключа P-SHA1;
 - использование алгоритма подписи сертификата RSA-PKCS15-SHA1;
 - использование ограниченного алгоритма получения ключа RSA15;
- BASIC256 — политика безопасности для конфигураций со средними требованиями безопасности такие как:
 - проверка сертификата безопасности;
 - необходимо шифрование;
 - необходима безопасная подпись;
 - использование алгоритма шифрования SHA 1;
 - использование алгоритма шифрования AES 128 CBC;
 - использование алгоритма шифрования RSA-PKCS15-SHA1;
 - использование алгоритма шифрования RSA-OAEP-SHA1;
 - использование алгоритма получения ключа P-SHA1;

- использование алгоритма подписи сертификата RSA-PKCS15-SHA1;
- использование ограниченного алгоритма получения ключа RSA15;
- BASIC256SHA256 — политика безопасности для конфигураций со средними требованиями безопасности такие как:
 - проверка сертификата безопасности;
 - необходимо шифрование;
 - необходима безопасная подпись;
 - использование алгоритма шифрования SHA 2;
 - использование алгоритма шифрования AES 256 CBC;
 - использование алгоритма шифрования RSA-PKCS15-SHA2-256;
 - использование алгоритма шифрования RSA-OAEP-SHA1;
 - использование алгоритма получения ключа P-SHA2-256;
 - использование алгоритма подписи сертификата RSA-PKCS15-SHA2-256;
- использование ограниченного алгоритма получения ключа SHA2-256;
- AES128_SHA256_RSAAEP — политика безопасности для конфигураций со средними требованиями безопасности такие как:
 - проверка сертификата безопасности;
 - необходимо шифрование;
 - необходима безопасная подпись;
 - использование алгоритма шифрования AES 128 SHA-256;
- PUBSUB_AES128_CTR — политика безопасности для конфигураций со средними требованиями безопасности такие как:
 - необходимо шифрование;
 - необходима безопасная подпись;
 - использование алгоритма шифрования AES 128 CTR;
- PUBSUB_AES256_CTR — политика безопасности для конфигураций со средними требованиями безопасности такие как:
 - необходимо шифрование;
 - необходима безопасная подпись;
 - использование алгоритма шифрования AES 128 CTR.

При выборе типа сообщения «MESSAGE» появится поле «Тип запроса», в котором необходимо выбрать тип запроса в соответствии с таблицей 8.

Таблица 8 – Типы запросов OPC UA

№	Тип запроса	Описание
1	FINDSERVERS	Запрос известных серверов
2	FINDSERVERSONNETWORK	Запрос известных работающих серверов
3	GETENDPOINTS	Запрос на поддерживаемые сервером конечные точки
4	REGISTERSERVER	Запрос на регистрацию сервера
5	REGISTERSERVER2	Запрос на регистрацию сервера с дополнительной информацией для FINDSERVERSONNETWORK

№	Тип запроса	Описание
6	CREATESESSION	Запрос на создание сессии
7	ACTIVATESESSION	Запрос на создание сессии (передача идентификационных данных клиента)
8	CLOSESESSION	Запрос на завершение сессии
9	CANCEL	Запрос отмены невыполненных запросов на обслуживание
10	ADDNODES	Запрос на добавление узла как дочерний в адресное пространство
11	ADDREFERENCES	Запрос на добавление ссылки на узел
12	DELETENODES	Запрос на удаление узла из адресного пространства
13	DELETEREFERENCES	Запрос на удаление ссылки узла
14	BROWSE	Запрос на просмотр узлов
15	BROWSENEXT	Запрос на продолжение просмотра результата запроса BROWSE, если результат этого запроса превышает максимального значения
16	TRANSLATEBROWSEPATHSTONODEIDS	Запрос на преобразование пути узла в идентификатор узла
17	REGISTERNODES	Запрос на регистрацию узла (например узла, информация о котором пользователю известна)
18	UNREGISTERNODES	Запрос на отмену регистрации узла
19	QUERYFIRST	Запрос просмотр данных из определенного экземпляра
20	QUERYNEXT	Запрос на продолжение просмотра результата запроса QUERYFIRST, если результат этого запроса превышает максимального значения
21	READ	Запрос на чтение данных
22	HISTORYREAD	Запрос на просмотр значений или событий узлов
23	WRITE	Запрос на изменение узла
24	HISTORYUPDATE	Запрос на обновление значений или событий узлов
25	CALLMETHOD	Запрос на получение результатов вызова удаленной процедуры
26	CALL	Запрос на вызов удаленной процедуры
27	MONITOREDITEMCREATE	Запрос на начало подписки на событие
28	CREATEMONITOREDITEMS	Запрос на подписку на событие
29	MONITOREDITEMMODIFY	Запрос на изменение параметров подписки на события
30	MODIFYMONITOREDITEMS	Запрос на изменение подписки
31	SETMONITORINGMODE	Запрос на установку режима подписки
32	SETTRIGGERING	Запрос на создание связи между событием и узлом
33	DELETEMONITOREDITEMS	Запрос на завершение подписки

№	Тип запроса	Описание
34	CREATESUBSCRIPTION	Запрос на создание подписки на событие
35	MODIFYSUBSCRIPTION	Запрос на изменение подписки на событие
36	SETPUBLISHINGMODE	Запрос на включение отправки уведомлений по подпискам на событие
37	PUBLISH	Запрос на подтверждение получения уведомлений по подпискам на события
38	REPUBLISH	Запрос на повторную отправку уведомлений по подпискам на события
39	TRANSFERSUBSCRIPTIONS	Запрос на передачу подписки на событие из одной сессии в другую
40	DELETESUBSCRIPTIONS	Запрос на удаление подписки на событие

При выборе типа запроса «BROSE», «READ», «WRITE» появится поле «Значение», в котором необходимо ввести диапазон запроса, например, «[2:]», «[:2]», «[2:3]».

При выборе типа запроса «CALL» появятся следующие поля:

- «Имя вызываемого объекта»;
- «Имя вызываемой процедуры».

В поле «Имя вызываемого объекта» необходимо ввести идентификатор узла, содержащий вызываемую процедуру.

В поле «Имя вызываемой процедуры» необходимо ввести идентификатор узла вызываемой процедуры.

После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 125).

1 Использовать шаблон	OPC UA
1 Действие	Предупреждение
1 Сообщение	
1 IP-адрес отправителя	any
1 Порт источника	any
1 Выберите направление	Прямое
1 IP-адрес получателя	any
1 Порт назначения	any
1 Фильтровать на основе протокола	Указать дополнительные параметры
1 Тип сообщения	MESSAGE
1 Тип запроса	READ
1 Значение	[2:]

Рисунок 125 – Обнаружение вторжений: Контроль уровня приложений (редактирование: OPC UA)

5.2.5 Шаблон протокола OPC DA

При использовании шаблона протокола OPC DA появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert) » – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject) » – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop) » – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass) » – при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать:

- «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола;

- «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола;
- «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появится поле «Тип сообщения» необходимо выбрать тип сообщения в соответствии с таблицей 9.

Таблица 9 – Типы сообщений OPC DA

№	Тип сообщения	Описание
1	REQUEST	Сообщение запроса на операцию
2	PING	Сообщение запроса обратного вызова
3	RESPONSE	Сообщение ответа
4	FAULT	Сообщение сбоя
5	WORKING	Сообщение подтверждающее, что все исходящие пакеты получены
6	NOCALL	Ответ на команду PING
7	REJECT	Сообщение отклонения пакета
8	ACK	Подтверждение получения ответа
9	CI_CANCEL	Отмена операции
10	FAK	Если состояние вызова не STATE_SEND_FRAGS, отбросить пакет
11	CANCEL_ACK	Подтверждение отмены операции
12	BIND	Установка сессии
13	BIND_ACK	Подтверждение установки сессии
14	BIND_NACK	Отказ в установке сессии с выбранными параметрами
15	ALTER_CONTEXT	Изменение параметров сессии
16	ALTER_CONTEXT_RESP	Подтверждение изменения параметров сессии
17	SHUTDOWN	Сброс соединения
18	AUTH3	Обновление авторизации пользователя
19	CO_CANCEL	Передача команды отмены
20	ORPHANED	Флаг невозможности отмены операции

При выборе типа сообщения «REQUEST» появятся следующие поля:

- «Идентификатор вызываемого объекта»;
- «Номер вызываемой функции объекта».

В поле «Идентификатор вызываемого объекта» необходимо ввести идентификатор объекта, например, «99fcfec4-5260-101b-bbcb-00aa0021347a».

В поле «Номер вызываемой функции объекта» необходимо ввести номер вызываемой функции, например, «3».

После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 126).

1 Использовать шаблон	OPC DA
1 Действие	Предупреждение
1 Сообщение	
1 IP-адрес отправителя	any
1 Порт источника	any
1 Выберите направление	Прямое
1 IP-адрес получателя	any
1 Порт назначения	any
1 Фильтровать на основе протокола	Указать дополнительные параметры
1 Тип сообщения	REQUEST
1 Идентификатор вызываемого объекта	99fcfec4-5260-101b-bbcb-00aa0021347a
1 Номер вызываемой функции объекта	3

Отменить Сохранить

Рисунок 126 – Обнаружение вторжений: Контроль уровня приложений (редактирование: OPC DA)

5.2.6 Шаблон протокола UMAS

При использовании шаблона протокола UMAS появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert)» – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject)» – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop)» – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass)» – при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать:

- «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола;

- «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола;
- «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появится поле «Функция», в котором необходимо выбрать одну из функций, перечисленных в таблице 10.

Таблица 10 – Функции протокола UMAS

Код	Название	Описание
0x01	INIT_COMM	Инициализация UMAS сессии
0x02	READ_ID	Запрос PLC ID
0x03	READ_PROJECT_INFO	Чтение информации о проекте
0x04	READ_PLC_INFO	Чтение внутренней информации PLC
0x06	READ_CARD_INFO	Чтение информации о внутренней SD карты PLC
0x0A	REPEAT	Отправить информацию обратно PLC. Используется для синхронизации
0x10	TAKE_PLC_RESERVATION	Назначить PLC владельца
0x11	RELEASE_PLC_RESERVATION	Снять владельца PLC
0x12	KEEP_ALIVE	Поддержка активного соединения
0x20	READ_MEMORY_BLOCK	Чтение блока памяти с PLC
0x22	READ_VARIABLES	Чтение системных битов, системных слов и переменных
0x23	WRITE_VARIABLES	Запись системных битов, системных слов и переменных
0x24	READ_COILS_REGISTERS	Чтение coils и регистров с PLC
0x25	WRITE_COILS_REGISTERS	Запись катушек и регистров в PLC
0x30	INITIALIZE_UPLOAD	Инициализация загрузки (копирование с инженерного ПК на PLC)
0x31	UPLOAD_BLOCK	Загрузка блока данных с инженерного ПК на PLC
0x32	END_STRATEGY_UPLOAD	Завершение загрузки (копирования с инженерного ПК на PLC)

Код	Название	Описание
0x33	INITIALIZE_DOWNLOAD	Инициализация скачивания (копирование с PLC на инженерный ПК)
0x34	DOWNLOAD_BLOCK	Скачивание блока данных с PLC на инженерный ПК
0x35	END_STRATEGY_DOWNLOAD	Конец скачивания (копирования с PLC на инженерный ПК)
0x39	READ_ETH_MASTER_DATA	Чтение Ethernet Master Data
0x40	START_PLC	Включение PLC
0x41	STOP_PLC	Выключение PLC
0x50	MONITOR_PLC	Мониторинг системных битов, системных слов и переменных
0x58	CHECK_PLC	Проверка статуса подключения PLC
0x70	READ_IO_OBJECT	Чтение IO объекта
0x71	WRITE_IO_OBJECT	Запись IO объекта
0x73	GET_STATUS_MODULE	Получение статуса модуля

При выборе функций «INIT_COMM», «READ_ID», «READ_PROJECT_INFO», «READ_PLC_INFO», «READ_CARD_INFO», «REPEAT», «TAKE_PLC_RESERVATION», «RELEASE_PLC_RESERVATION», «KEEP_ALIVE», «INITIALIZE_UPLOAD», «UPLOAD_BLOCK», «END_STRATEGY_UPLOAD», «INITIALIZE_DOWNLOAD», «DOWNLOAD_BLOCK», «END_STRATEGY_DOWNLOAD», «READ_ETH_MASTER_DATA», «START_PLC», «STOP_PLC», «MONITOR_PLC», «CHECK_PLC», «READ_IO_OBJECT», «WRITE_IO_OBJECT», «GET_STATUS_MODULE» появятся следующие поля:

- «Информация о проекте»;
- «Тип сообщения».

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

- «REQ» – запрос;
- «RES» – ответ.

При выборе функции «READ_MEMORY_BLOCK» появятся следующие поля:

- «Информация о проекте»;
- «Тип сообщения»;
- «Номер блока»;
- «Количество данных»;
- «Смещение».

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

- «REQ» – запрос;
- «RES» – ответ.

В поле «Номер блока» необходимо ввести номер блока команды в формате диапазона.

В поле «Количество данных» необходимо ввести количество данных команды в формате диапазона.

В поле «Смещение» необходимо ввести смещение команды в формате диапазона.

При выборе функции «READ_VARIABLES» появятся следующие поля:

- «Информация о проекте»;
- «Тип сообщения»;
- «Базовое смещение»;
- «Относительное смещение»;
- «Номер блока»;
- «Количество значений»;
- «Тип значений».

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

- «REQ» – запрос;
- «RES» – ответ.

В поле «Базовое смещение» необходимо ввести базовое смещение команды.

В поле «Относительное смещение» необходимо ввести относительное смещение команды.

В поле «Номер блока» необходимо ввести номер блока команды.

В поле «Количество значений» необходимо ввести количество значений команды.

В поле «Тип значений» необходимо выбрать тип значения:

- «BIT»;
- «WORD»;
- «DWORD».

При выборе функции «WRITE_VARIABLES» появятся следующие поля:

- «Информация о проекте»;
- «Тип сообщения»;
- «Номер блока»;
- «Смещение»;
- «Тип значений»;
- «Значение».

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

- «REQ» – запрос;
- «RES» – ответ.

В поле «Номер блока» необходимо ввести номер блока команды.

В поле «Смещение» необходимо ввести смещение команды.

В поле «Тип значений» необходимо выбрать тип значения:

- «BIT»;
- «WORD»;
- «DWORD».

В поле «Значение» необходимо ввести значение переменных команды.

При выборе функции «READ_COILS_REGISTERS» появятся следующие поля:

- «Информация о проекте»;
- «Тип сообщения»;
- «Условие»;
- «Номер регистров флагов (Coils)»;
- «Смещение»;
- «Тип значений».

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

- «REQ» – запрос;
- «RES» – ответ.

В поле «Условие» необходимо выбрать условие из выпадающего списка:

- «Отсутствует»;
- «Больше чем»;
- «Меньше чем»;
- «Равно»;
- «Not».

В поле «Номер регистров флагов (Coils)» необходимо ввести номера регистров флагов (Coils).

В поле «Смещение» необходимо ввести смещение команды.

В поле «Тип значений» необходимо выбрать тип значений:

- «Регистр»;
- «Регистр флага (Coil)»;
- «Отсутствует».

При выборе функции «WRITE_COILS_REGISTERS» появятся следующие поля:

- «Информация о проекте»;
- «Тип сообщения»;
- «Условие»;
- «Номер регистров флагов (Coils)»;
- «Смещение»;
- «Тип значений».

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

- «REQ» – запрос;
- «RES» – ответ.

В поле «Условие» необходимо выбрать условие из выпадающего списка:

- «Отсутствует»;
- «Больше чем»;
- «Меньше чем»;
- «Равно»;
- «Not».

В поле «Номер регистров флагов (Coils)» необходимо ввести номера регистров флагов (Coils).

В поле «Смещение» необходимо ввести смещение команды.

В поле «Тип значений» необходимо выбрать тип значений:

- «Регистр»;
- «Регистр флага (Coil)»;
- «Отсутствует».

После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 127).

1 Использовать шаблон	UMAS
1 Действие	Предупреждение
1 Сообщение	
1 IP-адрес отправителя	any
1 Порт источника	any
1 Выберите направление	Прямое
1 IP-адрес получателя	any
1 Порт назначения	any
1 Фильтровать на основе протокола	Указать дополнительные параметры
1 Функция	WRITE_COILS_REGISTERS
1 Информация о проекте	
1 Тип сообщения	REQ
1 Условие	отсутствует
1 Номер регистров флагов (Coils)	
1 Смещение	
1 Тип значений	отсутствует
1 Условие	отсутствует

Отменить Сохранить

Рисунок 127 – Обнаружение вторжений: Контроль уровня приложений (редактирование: UMAS)

5.2.7 Шаблон протокола MMS

При использовании шаблона протокола MMS появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert) » – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject) » – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop) » – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass) » – при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать:

- «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола;
- «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола;
- «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» появится поле «Тип сообщения», в котором необходимо выбрать тип сообщения. Допустимы следующие значения:

- CONFIRMED_REQUEST;
- CONFIRMED_RESPONSE;
- CONFIRMED_ERROR;
- UNCONFIRMED;
- REJECT;
- CANCEL_REQUEST;
- CANCEL_RESPONSE;
- CANCEL_ERROR;
- INITIATE_REQUEST;
- INITIATE_RESPONSE;
- INITIATE_ERROR;
- CONCLUDE_REQUEST;
- CONCLUDE_RESPONSE;
- CONCLUDE_ERROR.

При выборе типа сообщения «CONFIRMED_REQUEST» появится поле «Тип службы», в котором необходимо выбрать тип используемой службы. Допустимы следующие значения:

- STATUS;
- GETNAMELIST;
- IDENTIFY;
- RENAME;
- READ;
- WRITE;
- GETVARIABLEACCESSATTRIBUTES;
- DEFINENAMEDVARIABLE;
- DEFINESCATTEREDACCESS;
- GETSCATTEREDACCESSATTRIBUTES;
- DELETEVARIABLEACCESS;
- DEFINENAMEDVARIABLELIST;
- GETNAMEDVARIABLELISTATTRIBUTES;
- DELETENAMEDVARIABLELIST;
- DEFINENAMEDTYPE;
- GETNAMEDTYPEATTRIBUTES;
- DELETENAMEDTYPE;
- INPUT;
- OUTPUT;
- TAKECONTROL;
- RELINQUISHCONTROL;
- DEFINESEMAPHORE;
- DELETESEMAPHORE;
- REPORTSEMAPHORESTATUS;
- REPORTPOOLSEMAPHORESTATUS;
- REPORTSEMAPHOREENTRYSTATUS;
- INITIATEDOWNLOADSEQUENCE;
- DOWNLOADSEGMENT;
- TERMINATEDOWNLOADSEQUENCE;
- INITIATEUPLOADSEQUENCE;
- UPLOADSEGMENT;
- TERMINATEUPLOADSEQUENCE;
- REQUESTDOMAINDOWNLOAD;
- REQUESTDOMAINUPLOAD;
- LOADDOMAINCONTENT;
- STOREDOMAINCONTENT;
- DELETEDOMAIN;
- GETDOMAINATTRIBUTES;
- CREATEPROGRAMINVOCATION;
- DELETEPROGRAMINVOCATION;
- START;
- STOP;

- RESUME;
- RESET;
- KILL;
- GETPROGRAMINVOCATIONATTRIBUTES;
- OBTAINFILE;
- DEFINEEVENTCONDITION;
- DELETEEVENTCONDITION;
- GETEVENTCONDITIONATTRIBUTES;
- REPORTEVENTCONDITIONSTATUS;
- ALTEREVENTCONDITIONMONITORING;
- TRIGGEREVENT;
- DEFINEEVENTACTION;
- DELETEEVENTACTION;
- GETEVENTACTIONATTRIBUTES;
- REPORTEVENTACTIONSTATUS;
- DEFINEEVENTENROLLMENT;
- DELETEEVENTENROLLMENT;
- ALTEREVENTENROLLMENT;
- REPORTEVENTENROLLMENTSTATUS;
- GETEVENTENROLLMENTATTRIBUTES;
- ACKNOWLEDGEEVENTNOTIFICATION;
- GETALARMSUMMARY;
- GETALARMENROLLMENTSUMMARY;
- READJOURNAL;
- WRITEJOURNAL;
- INITIALIZEJOURNAL;
- REPORTJOURNALSTATUS;
- CREATEJOURNAL;
- DELETEJOURNAL;
- GETCAPABILITYLIST;
- FILEOPEN;
- FILEREAD;
- FILECLOSE;
- FILERENAME;
- FILEDELETE;
- FILEDIRECTORY;
- ADDITIONALSERVICE;
- GETDATAEXCHANGEATTRIBUTES;
- EXCHANGEDATA;
- DEFINEACCESSCONTROLLIST;
- GETACCESSCONTROLLISTATTRIBUTES;
- REPORTACCESSCONTROLLEDOBJECTS;
- DELETEACCESSCONTROLLIST;
- CHANGEACCESSCONTROL;
- RECONFIGUREPROGRAMINVOCATION.

При выборе типа службы «ADDITIONALSERVICE» появится поле «Дополнительный тип сервиса», в котором необходимо выбрать тип дополнительного сервиса. Допустимы следующие значения:

- VMDSTOP;
- VMDRESET;
- SELECT;
- ALTERPI;
- INITIATEUCLOAD;
- UCLOAD;
- UCUPLOAD;
- STARTUC;
- STOPUC;
- CREATEUC;
- ADDTOUC;
- REMOVEFROMUC;
- GETUCATTRIBUTES;
- LOADUCFROMFILE;
- STOREUCTOFILE;
- DELETEUC;
- DEFINEECL;
- DELETEECL;
- ADDECLREFERENCE;
- REMOVEECLREFERENCE;
- GETECLATTRIBUTES;
- REPORTECLSTATUS;
- ALTERECLMONITORING.

При выборе типа службы «READ» появятся следующие поля:

- «ItemID запроса чтения»;
- «DomainID запроса чтения»;
- «Адрес запроса чтения».

В поле «ItemID запроса чтения» необходимо ввести значение переменной ItemID для функции чтения.

В поле «DomainID запроса чтения» необходимо ввести значение переменной DomainID для функции чтения.

В поле «Адрес запроса чтения» необходимо ввести адрес переменной для функции чтения в формате строки. Например, «123» или «test».

При выборе типа службы «WRITE» появятся следующие поля:

- «ItemID запроса чтения»;
- «DomainID запроса чтения»;

В поле «ItemID запроса записи» необходимо ввести значение переменной ItemID для функции записи.

В поле «DomainID запроса записи» необходимо ввести значение переменной DomainID для функции записи.

После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 128).

Использовать шаблон	MMS
Действие	Предупреждение
Сообщение	
IP-адрес отправителя	any
Порт источника	any
Выберите направление	Прямое
IP-адрес получателя	any
Порт назначения	any
Фильтровать на основе протокола	Указать дополнительные параметры
Тип сообщения	CONFIRMED_REQUEST
Тип службы	WRITE
Item ID запроса записи	test
Domain ID запроса записи	test

Отменить Сохранить

Рисунок 128 – Обнаружение вторжений: Контроль уровня приложений
(редактирование: MMS)

5.2.8 Шаблон протокола GOOSE

При использовании шаблона протокола GOOSE появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert) » – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject) » – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop) » – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass) » – при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать:

- «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола;
- «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола;
- «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля:

- «APP ID»;
- «Dataset»;
- «GoCBRef»;
- «GoID».


В поле «APP ID» необходимо ввести диапазон значений идентификаторов приложений.

В поле «Dataset» необходимо ввести значение поля dataset (значение не может быть пустым и должно содержать не более 150 символов).

В поле «GoCBRef» необходимо ввести значение поля gocbref (значение не может быть пустым и должно содержать не более 150 символов).

В поле «GoID» необходимо ввести значение поля goid (значение не может быть пустым и должно содержать не более 150 символов).

После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 129).

справка 

Включен	<input checked="" type="checkbox"/>
Заголовок	GOOSE
Группа	
Использовать шаблон	GOOSE ▼
Действие	Предупредить (Alert) ▼
Сообщение	GOOSE
IP-адрес отправителя	any
Порт источника	any
Выберите направление	Прямое и обратное ▼
IP-адрес получателя	any
Порт назначения	any
Фильтровать на основе протокола	Указать дополнительные параметры ▼
APPID	[1000:1000]
Dataset	
GoCRef	
GoID	

Отменить Сохранить

Рисунок 129 – Обнаружение вторжений: Контроль уровня приложений
(редактирование: GOOSE)

5.2.9 Шаблон «Настроенное пользователем»

При использовании шаблона «Настроенное пользователем» появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

- «Предупредить (Alert) » – при необходимости оповещения при срабатывании правила;
- «Отклонить (Reject) » – при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;
- «Отбросить (Drop) » – при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;
- «Разрешить (Pass) » – при необходимости разрешить прохождение пакета при срабатывании правила.


В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт источника» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт назначения» необходимо ввести порт получателя.

В поле «Протокол» необходимо ввести часть протокола в правиле. В поле «Специфичная часть правила» необходимо ввести дополнительные параметры правила в соответствии с подсказками и форматом написания правил Snort/Suricata. После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 130).

Редактировать правило ×

справка 

1 Включен	<input checked="" type="checkbox"/>
1 Заголовок	<input type="text" value="test"/>
1 Группа	<input type="text"/>
1 Использовать шаблон	<input type="text" value="Настроенное пользователем"/>
1 Действие	<input type="text" value="Предупредить (Alert)"/>
1 Сообщение	<input type="text" value="test"/>
1 IP-адрес отправителя	<input type="text" value="any"/>
1 Порт источника	<input type="text" value="any"/>
1 Выберите направление	<input type="text" value="Прямое"/>
1 IP-адрес получателя	<input type="text" value="any"/>
1 Порт назначения	<input type="text" value="any"/>
1 Протокол	<input type="text" value="tcp"/>
1 Специфичная часть правила	<input type="text"/>

Рисунок 130 – Обнаружение вторжений: Контроль уровня приложений
(редактирование: Настроенное пользователем)

5.3 Подраздел «Журнал»

В подразделе «Журнал» отображается журнал внутренних событий Suricata. Имеется возможность производить поиск по журналу в поле «Поиск» и очищать журнал, нажав кнопку «Очистить журнал» (Рисунок 131).

Обнаружение вторжений: Журнал

<div> <div>Q</div> <div>Поиск</div> <div>↺</div> <div>20</div> <div>☰</div> </div>	
Дата	Сообщение
2020-11-05T14:25:42	suricata[3563]: [1:2210056:1] SURICATA STREAM bad window update [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.159.140:27125 -> 205.185.216.10:80
2020-11-05T14:25:42	suricata[3563]: {"timestamp": "2020-11-05T14:25:41.943883+0000", "flow_id": 215790085439548, "in_iface": "em1", "event_type": "alert", "src_ip": "192.168.159.140", "src_port": 27125, "dest_ip": "205.185.216.10", "dest_port": 80, "proto": "TCP", "alert": {"action": "allowed", "gid": 1, "signature_id": 2210056, "rev": 1, "signature": "SURICATA STREAM bad window update", "category": "Generic Protocol Command Decode", "severity": 3}, "app_proto": "http", "flow": {"pkts_toserver": 253, "pkts_toclient": 908, "bytes_toserver": 15384, "bytes_toclient": 1349939, "start": "2020-11-05T14:25:39.032828+0000"}}
2020-11-05T14:25:42	suricata[3563]: [1:2210056:1] SURICATA STREAM bad window update [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.159.140:27125 -> 205.185.216.10:80
2020-11-05T14:25:42	suricata[3563]: {"timestamp": "2020-11-05T14:25:41.943823+0000", "flow_id": 215790085439548, "in_iface": "em1", "event_type": "alert", "src_ip": "192.168.159.140", "src_port": 27125, "dest_ip": "205.185.216.10", "dest_port": 80, "proto": "TCP", "alert": {"action": "allowed", "gid": 1, "signature_id": 2210056, "rev": 1, "signature": "SURICATA STREAM bad window update", "category": "Generic Protocol Command Decode", "severity": 3}, "app_proto": "http", "flow": {"pkts_toserver": 252, "pkts_toclient": 908, "bytes_toserver": 15330, "bytes_toclient": 1349939, "start": "2020-11-05T14:25:39.032828+0000"}}
2020-11-05T14:25:42	suricata[3563]: [1:2210056:1] SURICATA STREAM bad window update [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.159.140:27125 -> 205.185.216.10:80

Рисунок 131 – Обнаружение вторжений: Журнал

Если поставлен флажок в поле «Передавать предупреждения (alerts) в syslog» («Обнаружение вторжений» - «Администрирование» - «Настройки») в журнале отображаются сообщения о срабатывании правил, которые имеют следующую информацию:

- значение gid (ключевое слово для различных групп правил);
- значение sid (идентификатор правила);
- значение rev (версия правила);
- сообщение правила;
- тип классификации правила (ClassType);
- priority типа классификации правила;
- протокол;
- IP-адрес отправителя;
- порт отправителя;
- IP-адрес получателя;
- порт получателя.

5.4 Подраздел «Настройки импорта правил»

Для настройки импорта базы решающих правил по запросу пользователя по протоколу FTP/SMB необходимо настроить подключение к FTP-серверу/samba-серверу.

Для импорта базы решающих правил по запросу пользователя по протоколу FTP во вкладке «Настройки» в поле «Включен» поставить флажок для включения импорта. В поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения на FTP сервер. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости.

В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах).

Нажать кнопку «Выполнить» для сохранения настроек и импорта правил. Нажать кнопку «Применить» только для сохранения настроек (Рисунок 132).

Перед импортом баз решающих правил необходимо их заархивировать (при импорте правил используются архив наборов решающих правил формата «tar.gz»). Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz». При импорте правил выбирается файл правил с наиболее новой версией.

Обнаружение вторжений: Настройки импорта правил

Настройки

справка

Включен	<input checked="" type="checkbox"/>
Протокол	FTP
Адрес	192.168.2.222
Имя пользователя	root
Пароль	*****
Путь к корневой папке	
Интервал	1

Сохранить

Сохранить и импортировать

Рисунок 132 – Обнаружение вторжений: Настройки импорта правил (FTP):
Настройки

Для импорта базы решающих правил по запросу пользователя по протоколу SMB во вкладке «Настройки» в поле «Включен» поставить флажок для включения импорта. В поле «Протокол» необходимо выбрать «SMB». В поле «Samba сервис» необходимо ввести название samba-сервера. В поле «Адрес» необходимо ввести IP-адрес samba-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения на samba-сервер. Поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах).

Нажать кнопку «Выполнить» для сохранения настроек и импорта правил. Нажать кнопку «Применить» только для сохранения настроек (Рисунок 133).

Перед импортом баз решающих правил необходимо их заархивировать (при импорте правил используются архив наборов решающих правил формата «tar.gz»). Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial

Firewall»]_[версия правил].tar.gz». При импорте правил выбирается файл правил с наиболее новой версией.

Обнаружение вторжений: Настройки импорта правил

Настройки

справка

Включен	<input checked="" type="checkbox"/>
Протокол	SMB
Адрес	192.168.2.222
Samba сервис	samba
Имя пользователя	root
Пароль	*****
Путь к корневой папке	
Интервал	1

Сохранить

Сохранить и импортировать

Рисунок 133 – Обнаружение вторжений: Настройки импорта правил (SMB):
Настройки

6 РАЗДЕЛ «СИСТЕМА»

Раздел «Система» состоит из следующих подразделов:

- Доступ;
- Прошивка;
- Настройки;
- Шлюзы;
- Маршруты;
- Высокий уровень доступности;
- Диагностика;
- Конфигурация;
- Доверенные сертификаты;
- Мастер;
- Журналы;
- Питание.

6.1 Подраздел «Доступ»

Подраздел «Доступ» позволяет настраивать пользователей, группы пользователей, серверы аутентификации, а также произвести проверку работы серверов аутентификации.

6.1.1 Категория «Пользователи»

Категория «Пользователи» описана в документе «Руководство администратора» в разделе 4, подразделе 4.3.

6.1.2 Категория «Группы»

Категория «Группы» описана в документе «Руководство администратора» в разделе 4, подразделе 4.4.

6.1.3 Категория «Серверы»

Категория «Серверы» описана в документе «Руководство администратора» в разделе 4, подразделе 4.1.

6.1.4 Категория «Средство проверки»

Категория «Средство проверки» описана в документе «Руководство администратора» в разделе 4, подразделе 4.1.

6.2 Подраздел «Прошивка»

Подраздел «Прошивка» позволяет загружать обновления ПО, просматривать таблицу контроля целостности и, в случае ошибки, информацию об ошибке системы.

6.2.1 Категория «Обновления»

Категория «Обновления» позволяет загружать обновления ПО ПК «InfoWatch ARMA Industrial Firewall».

Категория «Обновления» описана в документе «Руководство администратора» в разделе 7, подразделе 7.2.

6.2.2 Категория «Контроль целостности»

Категория «Контроль целостности» позволяет просматривать таблицу контроля целостности программных частей ПК:

- scripts — вспомогательные скрипты для различных задач;
- site python — вспомогательные модули Python, подключаемые в северный код;
- contrib — сторонние вспомогательные библиотеки;
- version — версия продукта;
- legacy www, mvc — программный код, связанный с веб сервером;
- service — программный код связанный с северным кодом (не связанный с веб интерфейсом).

В таблице содержится информация о названии ПО, ожидаемое значение контрольной суммы, вычисленное значение контрольной суммы (в случае совпадения с ожидаемым значением, оно будет выделено зеленым цветом, в противном случае — красным и появится уведомление о несовпадении контрольной суммы вверху страницы), время и дату вычисления контрольной суммы, а также позволяет пересчитать контрольную сумму файла, нажав на значок «обновить» напротив файла или пересчитать все контрольные суммы, нажав на кнопку «Все», находящуюся под таблицей. Также в таблице возможен выбор элементов и столбцов таблицы, которые необходимо отобразить (Рисунок 134).

<div><input type="text" value="Поиск"/> <input type="button" value="Обновить"/> <input type="button" value="Все"/></div>				
Имя	Ожидаемое	Вычисленное	Дата вычисления	Пересчитать
firmware-product	d41d8cd98f00b204e9800998ecf8427e	d41d8cd98f00b204e9800998ecf8427e	18 hours ago	
mvc	c1b835905486cd8684fbb9466998b8b8	3cda6ef9ce6a3f57a48236fc7178a0	18 hours ago	
contrib	d6ed272250309a130856eccdb40cb7a8	d6ed272250309a130856eccdb40cb7a8	18 hours ago	
version	b7786a00bd9d36fd66262ae094de5af	b7786a00bd9d36fd66262ae094de5af	18 hours ago	
scripts	0d335e746cb8e6b5b780a8ae0727f984	0d335e746cb8e6b5b780a8ae0727f984	18 hours ago	
service	cc29fe7d27829c19fe35a3d5b0cbae7c	cc29fe7d27829c19fe35a3d5b0cbae7c	18 hours ago	
site-python	11d4575f313b702b5082c7f0e5c6b6a	11d4575f313b702b5082c7f0e5c6b6a	18 hours ago	
www	05d7361121a94f0b2a5065e2463f3565	05d7361121a94f0b2a5065e2463f3565	18 hours ago	
legacy-www	ea3d32434777af011adc4e0ee6227743	8b2c5901942aff5685ac49ae344276e	18 hours ago	
legacy-includes	fb944aaca550cccb8457ce04856be6e3	fb944aaca550cccb8457ce04856be6e3	18 hours ago	
<div><input type="button" value="Все"/></div>				

Показаны с 1 по 2 из 2 записей

Рисунок 134 – Система: Прошивка: Контроль целостности

6.2.3 Категория «Средство создания отчетов»

В категории «Средство создания отчетов» отображается информация об ошибках системы (Рисунок 135), в случае их отсутствия, отображается запись об отсутствии ошибок системы (Рисунок 136).

К сожалению, обнаружено по крайней мере одна ошибка программирования.

System Information:

```

user-agent Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
FreeBSD 11.2-RELEASE-p20-HBSD: 07f6face(stable/20.1) amd64
Infowatch ARMA Industrial Firewall 3.3.5 f5fe83dfe
Plugins os-dynids-1.20 os-export-configuration-1.1 os-export-journals-1.3 os-import-conf-arma-1.1 os-security-logs-arma-1.3 os-tshark-arma-1.3
Time Sat, 04 Jul 2020 11:02:55 +0000
OpenSSL 1.1.1g 21 Apr 2020
PHP 7.3.19
  
```

PHP Errors:

```

[03-Jul-2020 14:42:10 Etc/UTC] PHP Fatal error: Access level to OPNsense\Base\FieldTypes\NetworkAliasField::getValidationMessage() must be public (as in class OPNsense\Base\FieldTypes\BaseField) in /usr/local/opnsense/mvc/app/models/OPNsense/Base/Field.php on line 1846
[03-Jul-2020 21:20:29 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1847
[04-Jul-2020 00:12:30 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1846
[04-Jul-2020 00:12:30 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1847
[04-Jul-2020 00:12:40 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1846
[04-Jul-2020 00:12:40 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1847
[04-Jul-2020 04:12:00 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1846
[04-Jul-2020 04:12:00 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1847
[04-Jul-2020 04:13:00 Etc/UTC] Phalcon\Validation\Exception: [OPNsense\IDS\IDS\general.interfaces] Опущено отсылаемый в списке
in /usr/local/opnsense/mvc/app/models/OPNsense/Base/BaseModel.php:575
Stack trace:
#0 /usr/local/opnsense/mvc/app/controllers/OPNsense/IDS/Api/ServiceController.php(514): OPNsense\Base\BaseModel->serializeToConfig()
#1 [internal function]: OPNsense\IDS\Api\ServiceController->addUserLocalRulesetAction()
#2 [internal function]: Phalcon\Dispatcher->callActionMethod(Object(OPNsense\IDS\Api\ServiceController), 'addUserLocalRul...', Array)
#3 [internal function]: Phalcon\Dispatcher->dispatch()
#4 /usr/local/opnsense/www/api.php(26): Phalcon\Mvc\Application->handle()
#5 (main)
[04-Jul-2020 18:31:12 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1846
[04-Jul-2020 18:31:12 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1847
[04-Jul-2020 18:31:40 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1846
[04-Jul-2020 18:31:40 Etc/UTC] PHP Notice: Undefined variable: permissionClearStatus in /usr/local/opnsense/mvc/app/cache/_usr_local_opnsense_mvc_app_views_opnsense_ids_index_volt.php on line 1847
  
```

dmesg boot:

```

Copyright (c) 2013-2018 The HardenedBSD Project.
Copyright (c) 1992-2018 The FreeBSD Project.
  
```

Закреть этот отчет

Рисунок 135 – Система: Прошивка: Ошибки работы системы (обнаружена ошибка)

К счастью, ошибки программирования не обнаружены.

Рисунок 136 – Система: Прошивка: Ошибки работы системы (ошибки отсутствуют)

6.3 Подраздел «Настройки»



Подраздел «Настройки» позволяет ввести общие настройки системы и построения сети, настроить веб-интерфейс, доступ по SSH, консольный интерфейс, серверы аутентификации, изменить пароль входа в систему, настроить журналирование, SNMP, расписания с помощью планировщика Cron, параметры ядра.

6.3.1 Категория «Экспорт событий»

Категория «Экспорт событий» позволяет настраивать, создавать и редактировать каналы экспорта событий по SYSLOG.

Вкладка «Получатели»

Во вкладке «Получатели» осуществляются основные настройки каналов экспорта событий по SYSLOG.

Для того чтобы редактировать существующие каналы необходимо нажать на кнопку  напротив канала. Для того чтобы создать новый канал необходимо нажать на кнопку .

При редактировании/создании канала необходимо установить флажок напротив поля «Включен». В поле «Транспортный протокол» выбрать транспортный протокол, на основании которого будет передаваться информация. В поле «Формат» необходимо выбрать формат сообщения. В поле «Приложения» выбрать приложения, которые будут пересылать трафик. В поле «Уровни» выбрать

уровни передачи сообщений (по умолчанию выбрано все). В Поле «Категории» выбрать категории, которые необходимо включить. В поле «Имя хоста» указать адрес хоста. В поле «Порт» указать порт (по умолчанию указан 514). В поле «Описание» при необходимости добавить описание канала (Рисунок 137).

Редактировать назначение

справка

Включен

☒

Транспортный протокол

UDP(4)

Формат

SYSLOG

Приложения

Не выбрано

Очистить все

Уровни

INFO, NOTICE, WARN, ERROR, CRITICAL, ALERT, EMI

Очистить все

Категории

user-level messages, security/authorization messa

Очистить все

Имя хоста

Порт

514

Описание

test

Отменить

Сохранить

Рисунок 137 – Система: Настройки: Экспорт событий (редактирование канала)

Для сохранения и применения внесенных изменений необходимо нажать на кнопку «Сохранить», а затем «Применить».

Вкладка «Статистические данные»

Во вкладке «Статистические данные» отображается информация о переданных сообщениях (Рисунок 138).

Система: Настройки: Экспорт событий

Получатели

Статистические данные

Поиск

7

Имя	ID	Отправитель	Состояние	Тип	Номер	Описание
global	payload_reallocs		a	processed	186	
global	sdata_updates		a	processed	0	
dst.unix-dgram	legacy_dst#0	unix-dgram,localhost.af...	a	dropped	0	
dst.unix-dgram	legacy_dst#0	unix-dgram,localhost.af...	a	processed	9962	
dst.unix-dgram	legacy_dst#0	unix-dgram,localhost.af...	a	queued	0	
dst.unix-dgram	legacy_dst#0	unix-dgram,localhost.af...	a	written	9962	
global	scratch_buffers_bytes		a	queued	0	

«

«

1

2

3

»

»

Показаны с 1 по 7 из 16 записей

Применить

Рисунок 138 – Система: Настройки: Экспорт событий (Статистические данные)

6.3.2 Категория «Общие настройки»

Категория «Общие настройки» позволяет настраивать систему и построение сетей.

В группе настроек «Система» в поле «Имя хоста» необходимо ввести имя хоста без доменной части. В поле «Домен» необходимо ввести доменное имя. В поле «Часовой пояс» необходимо выбрать часовой пояс. В поле «Язык» необходимо выбрать язык. В поле «Тема» необходимо выбрать тему визуального оформления интерфейса (Рисунок 139).

Система: Настройки: Общие настройки	
Система	
Имя хоста	arma
Домен	localdomain
Часовой пояс	Etc/UTC
Перезагрузить сервисы	<input type="checkbox"/> Перезагрузить сервисы при изменении часового пояса
Язык	Русский
Тема	ARMA

Рисунок 139 – Система: Настройки: Общие настройки (Система)

В группе настроек «Построение сетей» при необходимости принудительного использования IPv4 » необходимо установить флажок в графе «Выбрать IPv4 через IPv6». В поле «DNS-серверы» необходимо выбрать IP-адреса, которые должны

использоваться системой для разрешения DNS. В поле «Настройки DNS-сервера» необходимо установить флажок напротив поля «Позволить переопределять список DNS-серверов DHCP/PPP на WAN» для использования DNS-серверов, назначенных DHCP/PPP-сервером на WAN-интерфейсе. При необходимости отключения службы DNS как сервера имен необходимо установить флажок напротив поля «Не использовать службу DNS как сервер имен для данной системы» (Рисунок 140).

Построение сетей

☒ Выбрать IPv4 через IPv6 ☐ Использовать IPv4, даже если доступен IPv6

DNS-серверы

DNS-сервер	Использовать шлюз
8.8.8.8	отсутствует
	отсутствует
	отсутствует
	отсутствует
	отсутствует
	отсутствует
	отсутствует
	отсутствует

Настройки DNS-сервера

☒ Позволить переопределять список DNS-серверов DHCP/PPP на WAN

Исключить интерфейсы

Не выбрано

☐ Не использовать службу DNS как сервер имен для данной системы

Переключение шлюзов

☐ Разрешить переключение шлюзов по умолчанию

Сохранить

Рисунок 140 – Система: Настройки: Общие настройки (Построение сетей)

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

6.3.3 Категория «Администрирование»

Категория «Администрирование» позволяет настраивать веб-интерфейс, доступ через SSH, консольный интерфейс, а также серверы аутентификации.

В группе настроек «Веб-интерфейс» в поле «Протокол» необходимо выбрать протокол для подключения веб-интерфейсу (HTTP/HTTPS). В поле «Сертификат SSL» выбрать сертификат. Для ограничения выбора SSL шифрования в выпадающем списке необходимо выбрать системные настройки. В поле «Протокол Strict Transport Security HTTP» необходимо установить флажок напротив поля «Включить протокол Strict Transport Security HTTP» при необходимости включения защиты веб-интерфейса от низкоуровневых атак взлома cookie по данному протоколу. В поле «Порт TCP» необходимо ввести номер порта для веб-интерфейса (по умолчанию 80 для HTTP, 443 для HTTPS). Для отключения правила перенаправления web-интерфейса необходимо установить флажок напротив поля «Переадресация HTTP». В поле «Тайм-аут сессии» необходимо ввести время простоя для сеансов. В поле «Проверка DNS Rebinding» необходимо установить

флажок напротив поля «Отключить проверку DNS Rebinding» для отключения защиты системы от DNS Rebinding атак. В поле «Альтернативные имена хостов» необходимо ввести альтернативные имена хостов DNS Rebinding и HTTP_REFERER проверки. В поле «Сжатие HTTP» необходимо выбрать сжатие HTTP-страниц и динамического содержимого. Для включения доступа к журналу веб-интерфейса для отладки и анализа в графе «Журнал доступа» необходимо установить флажок напротив «Включить журналирование доступа». В поле «Прослушиваемые интерфейсы» необходимо выбрать сетевые интерфейсы, от которых необходимо принимать соединения для доступа к веб-интерфейсу. В поле «Обеспечение соблюдения HTTP_REFERER» необходимо установить флажок напротив поля «Отключить принудительное использование HTTP_REFERER» для отключения защиты доступа к веб-интерфейсу от попыток перенаправления HTTP_REFERER (Рисунок 141).

Система: Настройки: Администрирование

Web-интерфейс	
Протокол	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Сертификат SSL	Web GUI SSL certificate
SSL шифрование	Системные настройки по-умолчанию
Протокол Strict Transport Security HTTP	<input type="checkbox"/> Включить протокол Strict Transport Security HTTP
Порт TCP	443
Переадресация HTTP	<input type="checkbox"/> Отключить правило перенаправления web-интерфейса
Сообщения входа	<input type="checkbox"/> Отключить протоколирование успешных входов в web-интерфейс
Тайм-аут сессии	240
Проверка DNS Rebinding	<input type="checkbox"/> Отключите проверку DNS Rebinding
Альтернативные имена хостов	<input type="text"/> Альтернативные имена хостов для DNS Rebinding и HTTP_REFERER проверки
Сжатие HTTP	Выкл.
Журнал доступа	<input type="checkbox"/> Включить журналирование доступа
Прослушиваемые интерфейсы	Все (рекомендуется)
Обеспечение соблюдения HTTP_REFERER	<input type="checkbox"/> Отключите проверку обеспечения соблюдения HTTP_REFERER

Рисунок 141 – Система: Настройки: Администрирование (Веб-интерфейс)

В группе настроек «SSH» в поле «SSH-сервер» необходимо установить флажок для включения SSH-сервера. В поле «Группа логина» необходимо выбрать разрешенные группы пользователей для удаленной авторизации по SSH. В поле «Вход суперпользователей в учетную запись» необходимо установить флажок

напротив «Разрешите вход суперпользователей в учетную запись» для разрешения входа пользователя «root» через SSH. В поле «Метод аутентификации» необходимо установить флажок напротив «Разрешите парольный вход в учетную запись» для разрешения парольного входа в учетную запись по SSH. В поле «Порт SSH» необходимо ввести порт SSH или оставьте по умолчанию (22 порт). В поле «Прослушиваемые интерфейсы» необходимо выбрать сетевые интерфейсы, через которые будет осуществляться доступ к SSH. В поле «Алгоритмы обмена ключа» необходимо выбрать алгоритм обмена ключа, используемый для генерации ключей соединения. В поле «Шифры» необходимо ввести шифр для шифрования соединения. В поле «MACs» необходимо указать код аутентификации сообщений. В поле «Алгоритмы ключа хоста» необходимо указать алгоритм ключа хоста (Рисунок 142).

The image shows a configuration window for SSH settings. It includes sections for enabling the SSH server, selecting login groups (wheel, admins), allowing superuser login, setting the authentication method to password, specifying the SSH port (22), selecting listenable interfaces (all recommended), choosing key exchange algorithms (diffie-hellman-group1-sha1), selecting ciphers (aes192-cbc), choosing MACs (hmac-sha2-256), and setting host key algorithms to system defaults.

Рисунок 142 – Система: Настройки: Администрирование (SSH)

В группе настроек «Консоль» в поле «Драйвер консоли» необходимо установить флажок напротив поля «Использовать драйвер виртуального терминала» для использования драйвера виртуального терминала. В поле «Главная консоль» необходимо выбрать основную консоль, которая будет показывать вывод сценариев загрузки. В поле «Вспомогательная консоль» необходимо выбрать вспомогательные консоли, которые будут отображать сообщения загрузчика ОС, сообщения консоли и меню консоли. В поле «Скорость последовательного порта» необходимо ввести значение скорости последовательного порта консоли. В поле «USB-порт» необходимо установить флажок для использования USB-порта. В поле «Меню консоли» необходимо установить флажок для защиты паролем меню консоли (Рисунок 143).

Консоль	
Драйвер консоли	<input checked="" type="checkbox"/> Использовать драйвер виртуального терминала (vt)
Главная консоль	Консоль VGA
Вспомогательная консоль	Отсутствует
Скорость последовательного порта	115200
USB-порт	<input type="checkbox"/> Использовать USB-порт
Меню консоли	<input checked="" type="checkbox"/> Защита паролем меню консоли

Рисунок 143 – Система: Настройки: Администрирование (Консоль)

В группе настроек «Аутентификация» в поле «Серверы» необходимо выбрать серверы аутентификации для проверки учетных данных пользователей. В поле «Sudo (выполнение от имени суперпользователя)» необходимо выбрать разрешать или запрещать использование команды sudo для администраторов с доступом к командной строке. В поле «Система» необходимо установить флажок для отключения встроенной аутентификации (Рисунок 144).

Аутентификация	
Сервер	Локальная база данных
<input type="checkbox"/> Отключить встроенную аутентификацию	
Sudo (выполнение от имени суперпользователя)	Запретить
wheel	

Рисунок 144 – Система: Настройки: Администрирование (Аутентификация)

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

6.3.4 Категория «Пароль»

Категория «Пароль» позволяет изменить пароль учетной записи. Для этого в поле «Старый пароль» необходимо ввести действующий пароль. В поле «Новый пароль» необходимо ввести новый пароль. В поле «Подтверждение» необходимо ввести новый пароль еще раз. В поле «Язык» необходимо выбрать язык веб-

интерфейса, который будет установлен после авторизации пользователя (Рисунок 145).

Система: Настройки: Пароль

Настройки пользователя

Старый пароль

Новый пароль

Подтверждение

Язык

Системные настройки по-умолчанию

Сохранить

Рисунок 145 – Система: Настройки: Пароль

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

6.3.5 Категория «Журналирование»

Категория «Журналирование» позволяет настраивать опции локальной и удаленной записи.

В группе настроек «Локальные опции записи» для представления сохраняемых записей в обратном порядке в поле «Обратный порядок отображения» необходимо установить флажок. В поле «Размер журнала (байт)» необходимо ввести размер журнала веб-интерфейса в байтах. В поле «События межсетевого экрана по умолчанию» необходимо установить флажок для включения/выключения журналирования следующих пакетов:

- пакеты, соответствующие правилам блокировки по умолчанию из набора правил»;
- пакеты, соответствующие правилам разрешения по умолчанию из набора правил»;
- пакеты, заблокированные правилом «Блокировать bogon сети»;
- пакеты, заблокированные правилом «Блокировать частные сети».

В поле «Журнал веб-сервера» необходимо установить флажок напротив поля «Ошибка записи из-за сбоя сервера» для записи ошибок веб-сервера lighttpd в главном системном журнале. В поле «Локальные записи» необходимо установить флажок для выключения записи журнала на локальный диск. В поле «Сброс записей» необходимо нажать на кнопку «Очистить журналы» при необходимости очистить все локальные журналы (Рисунок 146).

Система: Настройки: Журналирование

Локальные опции записи справка ⓘ

Обратный порядок отображения	<input checked="" type="checkbox"/>
Размер журнала (байт)	<input type="text"/>
События межсетевого экрана по умолчанию	<input checked="" type="checkbox"/> Журналировать пакеты, соответствующие правилам блокировки по умолчанию из набора правил <input checked="" type="checkbox"/> Журналировать пакеты, соответствующие правилам разрешения по умолчанию из набора правил <input checked="" type="checkbox"/> Журналировать пакеты, блокированные правилом «Блокировать bogon сети» <input checked="" type="checkbox"/> Журналировать пакеты, блокированные правилом «Блокировать частные сети»
Журнал веб-сервера	<input checked="" type="checkbox"/> Ошибка записи из-за сбоя сервера
Локальные записи	<input type="checkbox"/> Выключить запись журнала на локальный диск
Сброс записей	<input type="button" value="Очистить файлы журналов"/>

Рисунок 146 – Система: Настройки: Журналирование (Локальные опции записи)

Для сохранения настроек журналирования необходимо нажать на кнопку «Сохранить».

6.3.6 Категория «SNMP»

Категория «SNMP» позволяет настраивать службу SNMP версии 2 и версии 3.

Во вкладке «Общие настройки» имеется возможность настроить SNMPv2 и SNMPv3. Для включения сервиса SNMP в поле «Включен» необходимо установить флажок. В поле «Community String» необходимо ввести значение «Community String» (по умолчанию значение «public»). В поле «Расположение SNMP» необходимо ввести расположение системы. В поле «Контактная информация» необходимо ввести контактную информацию. В поле «Отображать себя как Layer3 устройство» необходимо поставить флажок для выставления значения iso.3.6.1.2.1.1.7.0 равным 76, что означает, что это оборудование будет видно, как оборудование, работающее на сетевом уровне 3 модели ISO OSI. При необходимости запроса текущей установленной версии установить флажок в поле «Отображать версию в OID». В поле «IP для прослушивания» необходимо ввести IP-адрес, на который будет принимать сервис (Рисунок 147).

Система: Настройки: SNMP

Общие настройки Пользователи SNMPv3

Включить ☒

Community String

Расположение SNMP

Контактная информация

Отображать себя как Layer3 устройство ☒

Отображать версию в OID ☐

IP для прослушивания

✖ Очистить все

Сохранить

Рисунок 147 – Система: Настройки: SNMP: Общие настройки

Во вкладке «Пользователи SNMPv3» отображается таблица пользователей для возможности доступа по SNMPv3. Вкладка «Пользователи SNMPv3» позволяет включать, выключать, просматривать, редактировать, удалять и создавать пользователей (Рисунок 148).

Система: Настройки: SNMP

Общие настройки Пользователи SNMPv3

🔄 7 ▾

Включен	Имя пользователя	Пароль	Ключ шифрования	Команды
<input checked="" type="checkbox"/>	user	0-9a-zA-Z_-!\$%/()+=	qwerty1234567890	✎ 🗑 +

« < 1 > » Показаны с 1 по 1 из 1 записей

Сохранить

Рисунок 148 – Система: Настройки: SNMP: Пользователи SNMPv3

Для того чтобы редактировать существующего пользователя необходимо нажать на кнопку ✎ напротив пользователя. Для того, чтобы создать нового пользователя, необходимо нажать на кнопку +.

При редактировании пользователя в поле «Включен» необходимо установить флажок для возможности использования этого пользователя в SNMPv3. В поле «Имя пользователя» необходимо ввести имя пользователя. В поле «Пароль» необходимо ввести пароль пользователя. В поле «Ключ шифрования» необходимо ввести ключ шифрования для защиты соединения между клиентом и этим хостом.

В поле «Разрешить запись» необходимо установить флажок для включения возможности изменения параметров этому пользователю (Рисунок 149).

Редактировать пользователя

справка ⓘ

Включен ☒

Имя пользователя

Пароль

Ключ шифрования

Разрешить запись ☒

Отменить Сохранить

Рисунок 149 – Система: Настройки: SNMP: Пользователи SNMPv3 (редактирование)

После внесения изменений необходимо нажать на кнопку «Сохранить».

6.3.7 Категория «Прочее»

Категория «Прочее» позволяет задавать криптографические настройки, настройки диска/памяти, а также настраивать датчики температуры, периодичность резервного копирования, средства энергосбережения и системные звуки.

В группе настроек «Криптографические настройки» в поле «Параметры Диффи-Хеллмана» необходимо выбрать параметры обновления. В поле «Аппаратное ускорение» при необходимости выбрать модуль криптографического ускорителя. Для использования старых пользовательских устройств для криптографического ускорения в поле «Использовать /dev/crypto» необходимо установить флажок (Рисунок 150).

Система: Настройки: Прочее

Криптографические настройки

справка ⓘ

Параметры Диффи-Хеллмана

Аппаратное ускорение

Использовать /dev/crypto ☐ Включить использование старых пользовательских устройств для криптографического ускорения

Рисунок 150 – Система: Настройки: Прочее (Криптографические настройки)

В группе настроек «Тепловые датчики» в поле «Аппаратное обеспечение» необходимо выбрать аппаратное обеспечение (датчик температуры выхода из строя процессоров AMD K8, K10 (amdttemp) и процессоров Intel Core (coretemp), датчик температуры материнской платы ACPI), на которое будет загружен драйвер для считывания его температуры (Рисунок 151).

Тепловые датчики	
<div> <div>?</div> <div>Аппаратное обеспечение</div> </div>	<div>Отсутствует/ACPI</div> <div>▼</div>

Рисунок 151 – Система: Настройки: Прочее (Тепловые датчики)

В группе настроек «Периодические резервные копии» в поле «Периодическая резервная копия RRD» необходимо выбрать периодичность резервирования данных графиков анализа. В поле «Периодическая резервная копия DHCP» необходимо выбрать периодичность резервирования данных аренд DHCP. В поле «Периодическая резервная копия Netflow» необходимо выбрать периодичность резервирования данных Netflow. В поле «Периодическое сохранение портала авторизации» необходимо выбрать периодичность резервирования данных сессий Портала авторизации (Рисунок 152).

Периодические резервные копии	
<div> <div>?</div> <div>Периодическая резервная копия RRD</div> </div>	<div>5 ч</div> <div>▲</div>
<div> <div>?</div> <div>Периодическая резервная копия аренд DHCP</div> </div>	<div>1 ч</div> <div>▲</div>
<div> <div>?</div> <div>Периодическая резервная копия NetFlow</div> </div>	<div>1 ч</div> <div>▲</div>
<div> <div>?</div> <div>Периодическое сохранение портала авторизации</div> </div>	<div>12 ч</div> <div>▲</div>

Рисунок 152 – Система: Настройки: Прочее (Периодические резервные копии)

В группе настроек «Средства энергосбережения» в графе «Использовать PowerD» необходимо установить флажок для использования сервисной программы PowerD. В поле «В режиме питания от сети переменного тока» необходимо выбрать состояние питания в режиме питания от сети переменного тока. В поле «В режиме питания от батареи» необходимо выбрать состояние питания в режиме питания от батареи. В поле «В режиме нормального питания» необходимо выбрать состояние питания в режиме нормального питания (питания от сети) (Рисунок 153).

Средства энергосбережения	
Использовать PowerD	<input checked="" type="checkbox"/>
В режиме питания от сети переменного тока	Адаптивный
В режиме питания от батареи	Максимальный
В режиме нормального питания	Высокоадаптивный

Рисунок 153 – Система: Настройки: Прочее (Средства сбережения)

В группе настроек «Настройки диска/памяти (требуется перезагрузка)» в поле «Файл обмена» необходимо установить флажок для добавления 2 Гб swap-файла в систему, при этом при сохранении изменений после установки данного флажка потребуются перезагрузка ПК. В поле «RAM-диск /var» необходимо установить флажок для использования файловой системы в качестве оперативной памяти в /var. В поле «RAM-диск /tmp» необходимо установить флажок для использования файловой системы в качестве оперативной памяти /tmp (Рисунок 154).

Настройки диска / памяти (требуется перезагрузка)	
Файл обмена	<input checked="" type="checkbox"/> Добавить 2 Гб swap-файл в систему
RAM-диск /var	<input checked="" type="checkbox"/> Использовать файловую систему в памяти для /var
RAM-диск /tmp	<input type="checkbox"/> Использовать файловую систему в памяти для /tmp

Рисунок 154 – Система: Настройки: Прочее (Настройки диска/памяти (требуется перезагрузка))

В группе настроек «Системные звуки» в поле «Звук включения/выключения» необходимо поставить флажок для отключения звуков включения/выключения устройства (Рисунок 155).

Системные звуки	
Звук включения/выключения	<input type="checkbox"/> Отключить звук включения/выключения
Сохранить	

Рисунок 155 – Система: Настройки: Прочее (Системные звуки)

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

6.3.8 Категория «Параметры»

В категории «Параметры» приведена таблица параметров ядра. Таблица содержит следующие данные (Рисунок 156):

- имя параметра;
- описание параметра;
- значение параметра.

Система: Настройки: Параметры			По умолчанию	Добавить
Имя параметра	Описание	Значение		
vfs.read_max	Увеличение скорости чтения UFS для соответствия с состоянием жестких дисков и NCQ	default (32)		
net.inet.ip.portrange.first	Установка более низкого эфемерного диапазона портов.	default (1024)		
net.inet.tcp.blackhole	Отбрасывание (drop) пакетов на закрытые TCP-порты без возврата RST	default (2)		
net.inet.udp.blackhole	Не посылайте сообщения с ICMP-порта на закрытые UDP-порты	default (1)		
net.inet.ip.random_id	Randomize the ID field in IP packets	default (1)		
net.inet.ip.sourceroute	Маршрутизация источника - это еще один способ для злоумышленника попытаться достичь не маршрутизируемых адресов. Его можно также использовать для того, чтобы получить информацию о ваших внутренних сетях. Эти функции включены, так как являются стандартными в FreeBSD.	default (0)		
net.inet.ip.accept_sourceroute	Маршрутизация источника - это еще один способ для злоумышленника попытаться достичь не маршрутизируемых адресов. Его можно также использовать для того, чтобы получить информацию о ваших внутренних сетях. Эти функции включены, так как являются стандартными в FreeBSD.	default (0)		
net.inet.icmp.log_redirect	Этот параметр отключает ведение журнала пакетов перенаправления, это связано с тем, что нет ограничений записей журнала, которые могут заполнить и заполнить весь жесткий диск.	default (0)		
net.inet.tcp.drop_synfin	Разбейте пакеты SYN-FIN (разрывается также RFC 1379, но его никто не использует так или иначе)	default (1)		
net.inet6.ip6.redirect	Включить отправку перенаправлений IPv6	default (1)		
net.inet6.ip6.use_tempaddr	Включить приватную настройку IPv6 (RFC 4941)	default (0)		
net.inet6.ip6.prefer_tempaddr	Предпочитаемые приватные адреса и их использование по нормальным адресам	default (0)		
net.inet.tcp.synccookies	Генерация SYN-куки для исходящих пакетов SYN-ACK	default (1)		
net.inet.tcp.recvspace	Максимальный размер входящей / исходящей датаграммы TCP (получить)	default (65528)		
net.inet.tcp.sendspace	Максимальный размер входящей / исходящей датаграммы TCP (отослать)	default (65528)		

Рисунок 156 – Система: Настройки: Параметры

Для того чтобы редактировать существующие параметры, необходимо нажать на кнопку напротив параметра. Для того чтобы создать новый параметр системы, необходимо нажать на кнопку **Добавить**. Для того чтобы вернуть все настройки по умолчанию необходимо нажать на кнопку

По умолчанию.

При редактировании параметра системы в поле «Параметр» необходимо ввести название параметра. В поле «Описание» необходимо ввести описание параметра. В поле «Значение» необходимо ввести значение параметра (Рисунок 157).

Система: Настройки: Параметры

Редактировать параметры системы

Параметр

vfs.read_max

Описание

Increase UFS read-ahead speeds to match the state of hard drives and NCQ.

Значение

default

Сохранить

Отменить

Рисунок 157 – Система: Настройки: Параметры (редактирование)

6.3.9 Категория «Планировщик задач Cron»

В категории «Планировщик задач Cron» приведена таблица планировщика задач системы. Таблица содержит следующие данные (Рисунок 158):

- данные о состоянии задачи (включено/выключено);
- данные о задаче:
 - минуты;
 - часы;
 - дни;
 - месяцы;
 - дни недели;
 - описание;
 - команды.

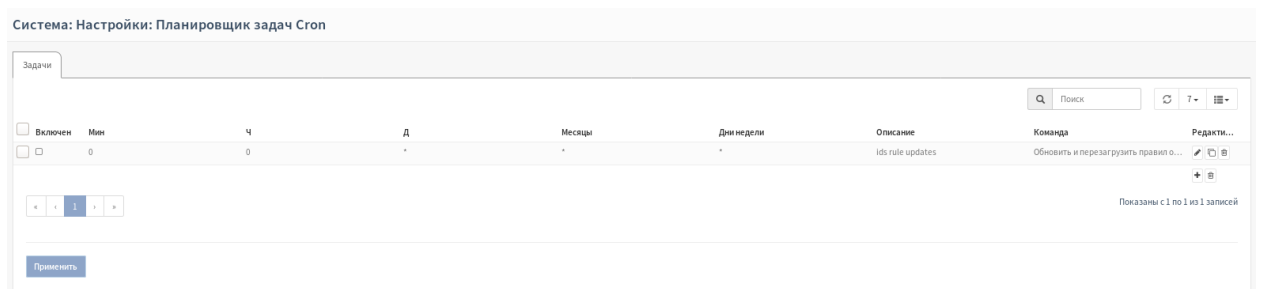




Рисунок 158 – Система: Настройки: Планировщик задач Cron

Для того чтобы редактировать существующие задачи, необходимо нажать на кнопку  напротив задачи. Для того чтобы создать новую задачу, необходимо нажать на кнопку  **Добавить**. Стоит обратить внимание, что в правилах задается не конкретное время запуска задачи, а периодичность запуска задачи.

При редактировании задачи Cron в поле «Включен» необходимо установить флажок для разрешения выполнения задачи Cron. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле «Ч» необходимо выбрать время в часах, когда будет запущена задача. В поле «День месяца» необходимо выбрать день месяца, когда будет запущена задача. В поле «Месяцы» необходимо выбрать месяцы, когда будет запущена задача. В поле «День недели» необходимо выбрать день недели, когда будет запущена задача. В поле «Команда» необходимо выбрать команду, которая должна быть выполнена в определенный момент времени. В поле «Параметры» необходимо ввести параметры задачи. В поле «Описание» необходимо ввести описание задачи. Пример готовой строки сценария Cron: «Выполнять перезагрузку в 18 часов 7 минут 13 мая, если это пятница» (Рисунок 159).

Редактировать задачу

справка

включен	<input checked="" type="checkbox"/>
Мин	<input type="text" value="7"/>
Ч	<input type="text" value="18"/>
День месяца	<input type="text" value="13"/>
Месяцы	<input type="text" value="may"/>
День недели	<input type="text" value="friday"/>
Команда	Обновить и перезагрузить правил обнаружения ▾
Параметры	<input type="text"/>
Описание	Выполнять задание в 18 часов 7 минут 13 мая, ...

Отменить

Сохранить

Рисунок 159 – Система: Настройки: Планировщик задач Cron (редактирование)

При редактировании расписания системы обнаружения вторжений в поле «Команда» можно выбрать следующие команды:

- «Обновить ACL с внешнего прокси и перезагрузить сервис»;
- «Обновить ACL с внешнего прокси»;
- «Выполнять периодическое обновление интерфейса»;
- «Восстановить ДН параметры»;
- «Перезагрузить правила обнаружения вторжений»;
- «Выполнить удаленное резервное копирование»;
- «Обновить и перезагрузить псевдонимы межсетевого экрана»;
- «Обновить и перезагрузить правила обнаружения вторжений»;
- «Выполнить перезагрузку»;
- «Пересчитать все чек-суммы».
- «Импорт правил COB»;
- «Экспорт конфигурации»;
- «Dynamic DNS Update»;
- «Restart Captive Portal service»;
- «Restart IPsec service».

Для сохранения задачи Cron необходимо нажать на кнопку «Сохранить».

6.4 Подраздел «Шлюзы»





Подраздел «Шлюзы» позволяет просматривать / редактировать / удалять / создавать шлюзы и группы шлюзов, а также просматривать журнал шлюзов / группы шлюзов.

6.4.1 Категория «Единичный»

В категории «Единичный» приведена таблица единичных шлюзов. Таблица содержит следующие данные (Рисунок 160):

- имя шлюза;
- интерфейс;
- протокол;
- приоритет;
- IP-адрес шлюза;
- монитор IP;
- время приема-передачи (RTT);
- RTTd;
- потеря;
- статус;
- описание.

Система: Шлюзы: Единичный + Добавить

Имя	Интерфейс	Протокол	Приоритет	Шлюз	Монитор IP	Время приема-передачи (RTT)	RTTd	Потеря	Статус	Описание	
▶ INTERNET_DHCP6 (active)	Internet	IPv6	254		~	~	~	~	Онлайн	Interface INTERNET_DHCP6 Gateway	 
▶ INTERNET_DHCP (active)	Internet	IPv4	254	192.168.159.2	~	~	~	~	Онлайн	Interface INTERNET_DHCP Gateway	 





Рисунок 160 – Система: Шлюзы: Единичный

Для того чтобы редактировать существующие шлюзы, необходимо нажать на кнопку  напротив шлюза. Для того чтобы создать новый шлюз, необходимо нажать на кнопку + Добавить.

При редактировании шлюза в поле «Отключена» необходимо установить флажок для отключения шлюза. В поле «Имя» необходимо ввести название шлюза. В поле «Описание» необходимо добавить описание шлюза. В поле «Интерфейс» необходимо выбрать сетевой интерфейс. В поле «Семейство адресов» необходимо выбрать версию IP протокола. В поле «IP-адрес» необходимо ввести IP-адрес шлюза. В поле «Основной шлюз» необходимо установить флажок для использования данного шлюза по умолчанию. В поле «Удаленный шлюз» необходимо установить флажок для создания шлюза вне интерфейса подсети. В поле «Отключите мониторинг шлюзов» необходимо установить флажок для отключения мониторинга шлюза. В поле «Монитор IP» необходимо ввести IP-адрес альтернативного монитора. В поле «Пометить шлюз как недоступный» необходимо установить флажок для того, чтобы принудительно считать каждый шлюз недоступным. В поле «Приоритет» необходимо выбрать приоритет шлюза от 1 до 255 (Рисунок 161).

Система: Шлюзы: Единичный

Редактировать шлюз

Отключена	<input type="checkbox"/>
Имя	<input type="text" value="test"/>
Описание	<input type="text"/>
Интерфейс	<input type="text" value="LAN"/>
Семейство адресов	<input type="text" value="IPv4"/>
IP-адрес	<input type="text" value="192.168.1.2"/>
Основной шлюз	<input checked="" type="checkbox"/>
Удаленный шлюз	<input checked="" type="checkbox"/>
Отключите Мониторинг шлюзов	<input checked="" type="checkbox"/>
Монитор IP	<input type="text"/>
Пометить шлюз как недоступный	<input type="checkbox"/>
Приоритет	<input type="text" value="255"/>
Дополнительно	<input type="button" value="Дополнительно"/> Показать дополнительные параметры

Рисунок 161 – Система: Шлюзы: Единичный (редактирование)

При нажатии на кнопку «Дополнительно» появятся дополнительные настройки. В поле «Весовой коэффициент» необходимо ввести приоритет данного шлюза. В поле «Пороговое значение задержки» необходимо ввести диапазон задержки шлюза. В поле «Пороговые значения потери пакетов» необходимо ввести диапазон потери пакетов. В поле «Интервал опроса» необходимо ввести, как часто будет отправляться ICMP запрос. В поле «Интервал уведомлений» необходимо ввести интервал времени между уведомлениями. В поле «Период усреднения» необходимо ввести время, за которое результаты будут усредняться. В поле «Интервал потери» необходимо ввести интервал времени, по истечении которого пакеты будут считаться потерянными. В поле «Размер данных» необходимо указать количество данных (в байтах) для отправки (Рисунок 162).

Дополнительно

Весовой коэффициент
Вес (приоритет) данного шлюза при использовании в Группе шлюзов.

Пороговое значение задержки
От
К
Нижний и верхний пороги для задержки в миллисекундах. Значение по умолчанию 200/500.

Пороговые значения потери пакетов
От
К
Нижний и верхний пороги для потери пакетов в %. Значение по умолчанию 10/20.

Интервал опроса
Как часто будет отправляться ICMP опрос в секундах. Значение по умолчанию 1

Интервал уведомлений
Интервал времени между оповещениями. По умолчанию 1.

Период усреднения
Период времени, за который результаты усредняются. По умолчанию 60.

Интервал потери
Интервал времени, в течение которого пакеты считаются потерянными. По умолчанию 2.

Размер данных
Укажите количество байт данных для отправки. По умолчанию 0.

Рисунок 162 – Система: Шлюзы: Единичный (редактирование: дополнительное)

Для сохранения шлюза необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

6.4.2 Категория «Группа»


В категории «Группы» приведена таблица группы шлюзов. Таблица содержит следующие данные (Рисунок 163):

- имя группы шлюзов;
- шлюзы в группе;
- описание.

Система: Шлюзы: Группа

Имя	Шлюзы	Описание
TEST	Ранг 1 <input type="button" value="test, Disable"/>	test <input type="button" value="edit"/> <input type="button" value="delete"/>

Рисунок 163— Система: Шлюзы: Группы

Для того чтобы редактировать существующие группы шлюзов, необходимо нажать на кнопку  напротив группы шлюзов. Для того чтобы создать новую группу шлюзов, необходимо нажать на кнопку .

При редактировании группы шлюзов в поле «Имя группы» необходимо ввести название группы шлюзов. В «Приоритет шлюзов» необходимо выбрать в поле «Ранг» приоритет шлюза в группе (то имеется в каком порядке будет происходить аварийное переключение и балансировка), в поле «Виртуальный IP-адрес» необходимо выбрать виртуальный IP-адрес. В поле «Уровень срабатывания» необходимо выбрать уровень срабатывания исключения шлюза. В поле «Описание» необходимо ввести описание группы шлюзов (Рисунок 164).

Система: Шлюзы: Группа

Имя группы:

Приоритет шлюзов:

Шлюз	Ранг	Виртуальный IP-адрес	Описание
test	Ранг 1	Адрес интерфейса	test

Уровень срабатывания:

Описание:

Рисунок 164 – Система: Шлюзы: Группы (редактирование)

Для сохранения группы шлюзов необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

6.4.3 Категория «Журнал»

В категории «Журнал» отображаются сообщения журнала aringer, связанные со шлюзами (Рисунок 165).

Система: Шлюзы: Журнал

Поиск:

20

Дата	Сообщение
Нет данных	

« 1 »

Показаны с 0 по 0 из 0 записей

Рисунок 165 – Система: Шлюзы: Журнал

6.5 Подраздел «Маршруты»

Подраздел «Маршруты» позволяет просматривать / редактировать / удалять / создавать статические маршруты, а также таблицу всех маршрутов в режиме реального времени и журнал изменения маршрутов.

6.5.1 Категория «Конфигурация»

В категории «Конфигурация» приведена таблица статических маршрутов. Таблица содержит следующие данные (Рисунок 166):

- статус (включен/выключен маршрут);
- сеть;
- шлюз;
- описание маршрута;
- команды.

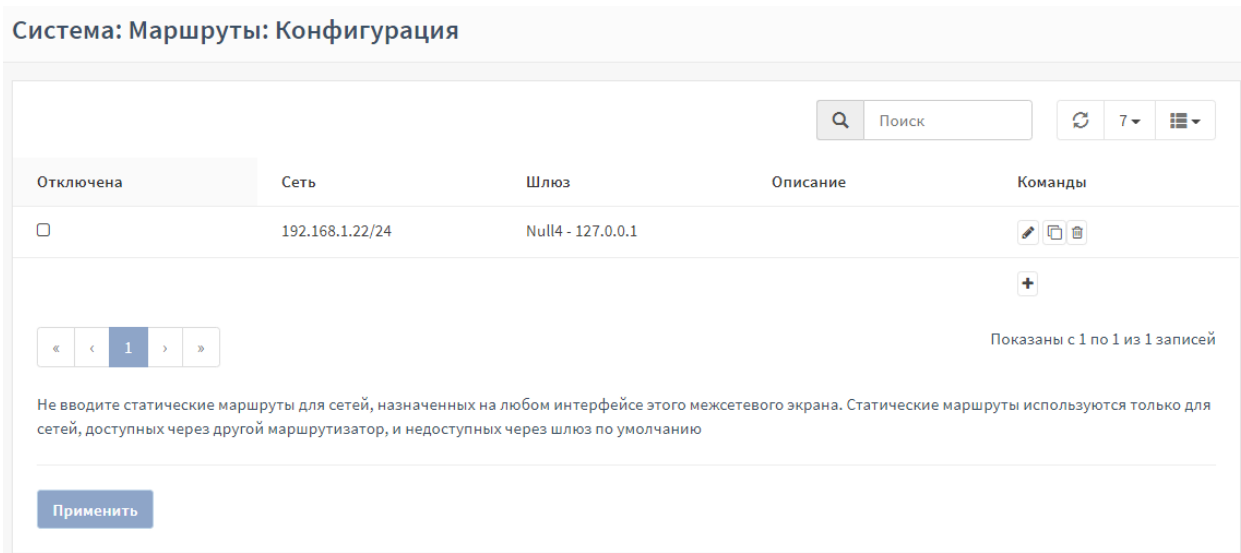




Рисунок 166 – Система: Маршруты: Конфигурация

Для того чтобы редактировать существующие маршруты, необходимо нажать на кнопку  напротив маршрута. Для того чтобы создать новый статический маршрут, необходимо нажать на кнопку .

При редактировании маршрута в поле «Отключена» необходимо установить флажок для отключения статического маршрута. В поле «Адрес сети» необходимо ввести сеть назначения для статического маршрута. В поле «Шлюз» необходимо выбрать шлюз, к которому применяется этот маршрут. В поле «Описание» необходимо ввести описание маршрута (Рисунок 167).

Рисунок 167 – Система: Маршруты: Конфигурация (редактирование)

Для сохранения маршрута необходимо нажать на кнопку «Сохранить», а затем «Применить изменения».

6.5.2 Категория «Статус»

В категории «Статус» приведена таблица маршрутов системы. Таблица содержит следующие данные (Рисунок 168):

- протокол;
- получатель;
- шлюз;

- флажки протокола;
- использовать;
- максимальный размер кадра;
- физический интерфейс;
- название сетевого интерфейса;
- истекает.

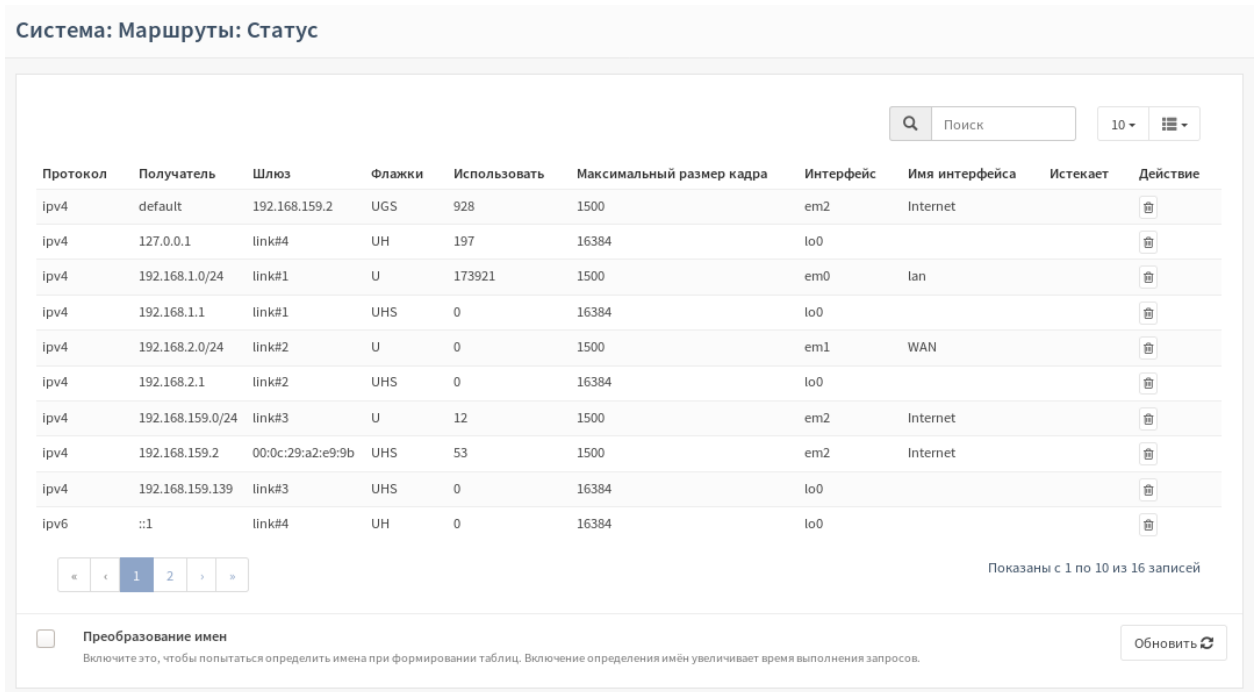


Рисунок 168 – Система: Маршруты: Статус

В таблице можно осуществлять поиск, выбирать, сколько маршрутов отображать на странице и добавлять/убирать графы таблицы, нажав соответствующие кнопки.

6.5.3 Категория «Журнал»

В категории «Журнал» отображаются события изменения маршрутов (Рисунок 169).

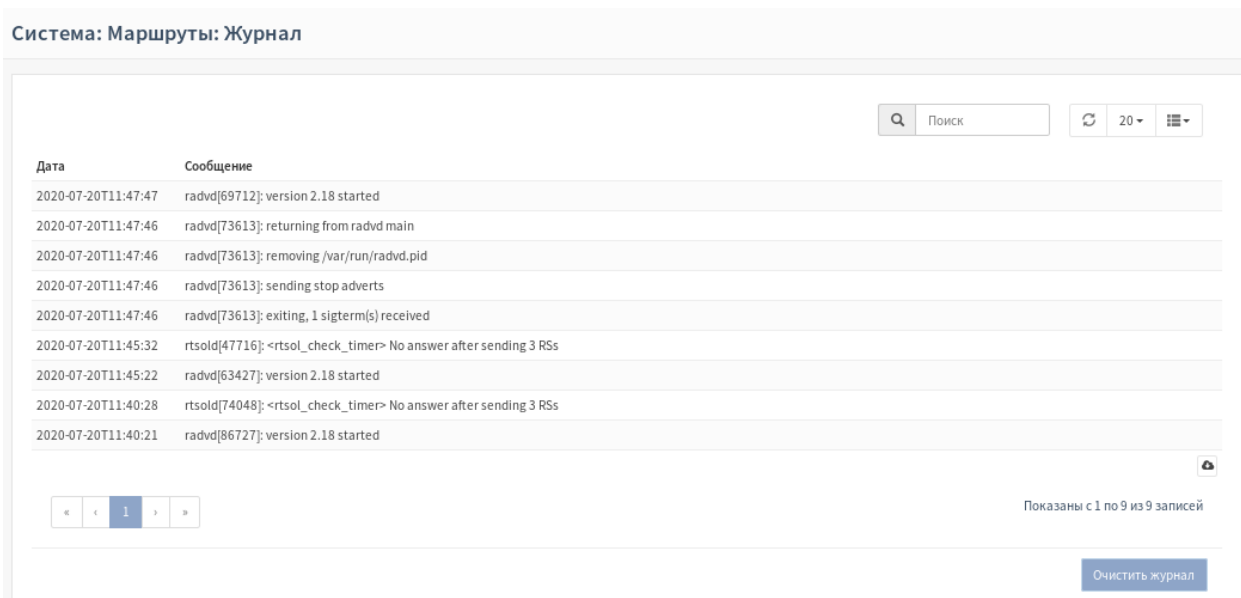


Рисунок 169 – Система: Маршруты: Журнал

6.6 Подраздел «Высокий уровень доступности»

Подраздел «Высокий уровень доступности» при работе системы в режиме отказоустойчивого кластера позволяет настраивать синхронизацию устройств, а также просматривать статус устройства.

6.6.1 Категория «Настройки»

Категория «Настройки» позволяет настраивать синхронизацию состояния и синхронизацию конфигурации (XMLRPC Sync).

В группе настроек «Синхронизация состояния» в поле «Синхронизировать состояния» необходимо установить флажок для включения механизма rfsync. В поле «Отключить упреждение» необходимо установить флажок для того, чтобы оставить устройство в режиме «Резервный». В поле «Синхронизировать интерфейс» необходимо выбрать сетевой интерфейс, через который будет происходить обмен данными. В поле «Синхронизировать IP-адреса пира» необходимо ввести IP-адрес пира для включения синхронизации таблицы состояний для этого IP-адреса (Рисунок 170).

Система: Высокий уровень доступности: Настройки

Синхронизация состояния	
Синхронизировать состояния	<input checked="" type="checkbox"/>
Отключить упреждение	<input type="checkbox"/>
Синхронизировать интерфейс	LAN
Синхронизировать IP-адрес пира	224.0.0.240

Рисунок 170 – Система: Высокий уровень доступности: Настройки (синхронизация состояния)

В группе настроек «Настройки синхронизации конфигурации (XMLRPC Sync)» в поле «Синхронизировать конфигурацию с IP-адресом» необходимо ввести IP-адрес межсетевого экрана, с которым необходимо синхронизировать выбранные секции конфигурации. В поле «Имя пользователя удаленной системы» необходимо ввести имя пользователя удаленной системы для авторизации в ней. В поле «Пароль удаленной системы» необходимо ввести пароль удаленной системы для авторизации в ней. При необходимости добавить виджет «Настройки синхронизации конфигурации» на инструментальную панель в поле «Инструментальная панель» установить флажок. В поле «Пользователи и группы» необходимо установить флажок для включения автоматической синхронизации пользователей и группы пользователей с другим хостом. В поле «Серверы аутентификации» необходимо установить флажок для включения синхронизации настроек серверов аутентификации с другим хостом. В поле «Сертификаты» необходимо установить флажок для включения автоматической синхронизации сертификатов с другим хостом. В поле «Правила межсетевого экрана» необходимо установить флажок для включения автоматической синхронизации правил межсетевого экрана с другим хостом. В поле «Расписания межсетевого экрана» необходимо установить флажок для включения автоматической синхронизации расписания межсетевого экрана с другим хостом. В поле «Псевдонимы» необходимо установить флажок для включения автоматической синхронизации псевдонимов с другим хостом. В поле «NAT» необходимо установить флажок для включения автоматической синхронизации настроек NAT с другим хостом. В поле «DHCPD» необходимо установить флажок для включения автоматической синхронизации настроек DHCP с другим хостом. В поле «Статические маршруты» необходимо установить флажок для включения автоматической синхронизации настроек статических маршрутов с другим хостом. В поле «Виртуальные IP-адреса» необходимо установить флажок для включения автоматической синхронизации виртуальных IP-адресов с другим хостом. В поле «Ограничение трафика» необходимо установить флажок для включения автоматической синхронизации

настроек ограничения трафика с другим хостом. В поле «Портал авторизации» необходимо установить флажок для включения автоматической синхронизации Портала авторизации с другим хостом. В поле «IPsec» необходимо установить флажок для включения автоматической синхронизации настроек IPsec с другим хостом. В поле «Monit мониторинг системы» необходимо установить флажок для включения автоматической синхронизации настроек Monit с другим хостом. В поле «OpenVPN» необходимо установить флажок для включения автоматической синхронизации настроек OpenVPN с другим хостом. В поле «Firewall Groups» необходимо установить флажок для включения автоматической синхронизации настроек Firewall Groups с другим хостом. В поле «Веб-прокси» необходимо установить флажок для включения автоматической синхронизации настроек прокси-сервера с другим хостом. В поле «Обнаружение вторжений» необходимо установить флажок для включения автоматической синхронизации настроек системы обнаружения вторжений с другим хостом (Рисунок 171, Рисунок 172).

Настройки синхронизации конфигурации (XMLRPC Sync) Выполнить синхронизацию	
i Синхронизировать конфигурацию с IP-адресом	<input type="text"/>
i Имя пользователя удаленной системы	<input type="text" value="root"/>
i Пароль удаленной системы	<input type="password" value="...."/>
i Инструментальная панель	<input type="checkbox"/>
i Пользователи и группы	<input type="checkbox"/>
i Серверы аутентификации	<input type="checkbox"/>
i Сертификаты	<input type="checkbox"/>
i Правила межсетевого экрана	<input type="checkbox"/>
i Расписания межсетевого экрана	<input type="checkbox"/>
i Псевдонимы	<input type="checkbox"/>
i NAT	<input type="checkbox"/>
i DHCPD	<input type="checkbox"/>
i Статические маршруты	<input type="checkbox"/>

Рисунок 171 – Система: Высокий уровень доступности: Настройки (Настройки синхронизации конфигурации (XMLRPC Sync), часть 1)











 Виртуальные IP-адреса	<input type="checkbox"/>
 FRR	<input type="checkbox"/>
 Ограничение трафика	<input type="checkbox"/>
 Портал авторизации	<input type="checkbox"/>
 IPsec	<input type="checkbox"/>
 Monit мониторинг системы	<input type="checkbox"/>
 OpenVPN	<input type="checkbox"/>
 Группы межсетевого экрана	<input type="checkbox"/>
 Веб-прокси	<input type="checkbox"/>
 Обнаружение вторжений	<input type="checkbox"/>

Рисунок 172 – Система: Высокий уровень доступности: Настройки (Настройки синхронизации конфигурации (XMLRPC Sync), часть 2)

6.6.2 Категория «Статус»

В категории «Статус» отображается статус работы системы в режиме отказоустойчивого кластера.

Если система работает в режиме отказоустойчивого кластера, на ведущем устройстве будет показан статус работы (данные о версии резервного устройства) с возможностью управления настроенными службами резервного устройства (Рисунок 173).

Система: Высокий уровень доступности: Статус





















Резервное копирование версий межсетевого экрана		
Прошивка	Базовая	Ядро
0.1_61-b2a769366	18.7-amd64	18.7-amd64
Службы резервного копирования		
Службы	Описание	Статус
configd	System Configuration Daemon	  
login	Users and Groups	 
ntpd	Network Time Daemon	  
openssh	Secure Shell Daemon	  
pf	Packet Filter	 
syslog	Syslog	  
unbound	Unbound DNS	  
шаблоны		
все (*)		

Рисунок 173 – Система: Высокий уровень доступности: Статус (работа в режиме отказоустойчивого кластера)

В противном случае будет отображаться сообщение о том, что резервное копирование недоступно (Рисунок 174).

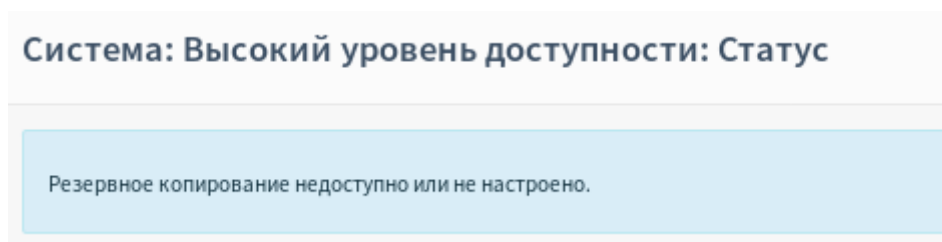


Рисунок 174 – Система: Высокий уровень доступности: Статус (резервное копирование)

6.7 Подраздел «Диагностика»

Подраздел «Диагностика» позволяет просматривать таблицу выполнения действий пользователей (в том числе системных) с различными параметрами и просматривать (управлять) настроенными службами.

6.7.1 Категория «Активность»

В категории «Активность» приведена таблица всех действий пользователей (в том числе системных) в системе. Таблица содержит следующие данные (Рисунок 175):

- идентификационный номер;
- имя пользователя;
- информация интерфейса первичного уровня;
- задействованная память;
- размер Res-файлов;
- состояние;

- время;
- загруженность ЦПУ;
- описание выполненной команды.

Система: Диагностика: Активность

<input type="checkbox"/>	PID	USERNAME	PRI	NICE	SIZE	RES	STATE	C	TIME	WCPU	COMMAND
<input type="checkbox"/>	11	root	155	4131	0	16K	RUN		31.0H	100.00%	[idle]
<input type="checkbox"/>	1858	root	21	0	38M	29M	select		0:05	0.98%	/usr/local/bin/php-cgi
<input type="checkbox"/>	12	root	-60	-	0	752K	WAIT		5:22	0.00%	[intr(pw4: clock [0])]
<input type="checkbox"/>	8	root	-16	-	0	16K	-		2:03	0.00%	[rand_harvestq]
<input type="checkbox"/>	78088	root	16	-	0	16K	syncer		0:51	0.00%	[syncer]
<input type="checkbox"/>	7	root	-16	-	0	16K	ptm		0:44	0.00%	[pf purge]
<input type="checkbox"/>	0	root	-16	-	0	256K	swpin		0:30	0.00%	[kernel[swapper]]
<input type="checkbox"/>	48171	root	20	0	17M	12M	kqread		0:21	0.00%	/usr/local/sbin/lighttpd f /var/etc/lightywebConfigurator.conf
<input type="checkbox"/>	42933	root	52	0	1034M	2984K	wait		0:19	0.00%	/bin/sh /var/db/rrd/updatedd.sh
<input type="checkbox"/>	89458	root	20	0	1038M	6M	select		0:12	0.00%	/usr/local/sbin/ntpd -g -c /var/etc/ntpd.conf -p /var/run/ntpd.pid(ntpd)

Показаны с 1 по 10 из 61 записей

Обновить

Рисунок 175 – Система: Диагностика: Активность

В таблице можно осуществлять поиск, выбирать, сколько записей отображать на странице, добавлять/убирать графы таблицы и отсортировать по колонкам таблицы, нажав соответствующие кнопки.

6.7.2 Категория «Службы»

Категория «Службы» позволяет просматривать настроенные службы. Эти службы можно остановить/запустить/перезагрузить, нажав на соответствующие кнопки напротив необходимой службы (Рисунок 176).

Система: Диагностика: Службы































Службы	Описание	Статус
configd	Демон настройки системы	  
dhcpcd	ДНCPv4-сервер	  
dhcpcd6	ДНCPv6-сервер	 
firewall	firewall	 
login	Пользователи и группы	 
ntpd	Демон сетевого времени	  
openssh	Демон SSH	  
pf	Фильтр пакетов	 
radvd	Демон объявления маршрутизатора	 
syslog-ng	Remote Syslog	  
syslogd	Системный журнал	  
webgui	WebGui	 

Рисунок 176 – Система: Диагностика: Службы

6.8 Подраздел «Конфигурация»

Подраздел «Конфигурация» позволяет экспортировать текущую конфигурацию на локальный хост и на удаленный FTP-сервер, восстановить конфигурацию, сбросить настройки системы до начальных, просматривать историю изменений (с возможностью отменить действия).

6.8.1 Категория «Резервные копии»

Процедура резервного копирования описана в Руководстве администратора в разделе 7, подразделе 7.3.

Также категория «Резервные копии» позволяет сохранять и восстанавливать конфигурацию системы, экспортировать наборы правил системы обнаружения вторжений, загруженных пользователями (Рисунок 177).

Система: Конфигурация: Резервные копии

Сохранение

☒ Не делать резервную копию базу данных RRD.
☐ Зашифровать этот файл конфигурации.

Сохранить конфигурацию

Нажмите, чтобы сохранить конфигурацию системы в формате XML.

Скачать наборы правил COV

Экспорт

Нажмите данную кнопку для скачивания загруженных пользователем наборов правил COV

Восстановить

Восстановить зону:
ВСЕ

Выберите файл Файл не выбран

☒ Перезагрузить после восстановления.
☐ Файл конфигурации зашифрован.

Восстановить конфигурацию

Откройте XML файл конфигурации и нажмите кнопку ниже, чтобы восстановить конфигурацию.

Рисунок 177 – Система: Конфигурация: Резервные копии

6.8.2 Категория «Значения по умолчанию»

Категория «Значения по умолчанию» позволяет сбросить все настройки до начальных:

- настройки установятся по умолчанию;
- IP-адрес локальной сети будет сброшен до 192.168.1.1;
- система будет настроена как DHCP-сервер на LAN-интерфейсе по умолчанию;
- WAN-интерфейс будет автоматически получать адрес от DHCP-сервера;

- имя и пароль администратора будут сброшены (имя — «root», пароль — «root»);
 - после внесения изменений система будет выключена.
- Для сброса настроек необходимо нажать на кнопку «Да» (Рисунок 178).



Рисунок 178 – Система: Конфигурация: Значения по умолчанию

6.8.3 Категория «История изменений»

Категория «История изменений» позволяет задать количество резервных копий конфигураций для хранения, сравнивать две конфигурации, а также просматривать конфигурации в виде таблицы. Выбрав одну из резервных копий, имеется возможность вернуться к ней либо просмотреть различия с текущим состоянием.

В группе настроек «Количество резервных копий» необходимо ввести количество конфигураций, которые будут храниться (Рисунок 179).

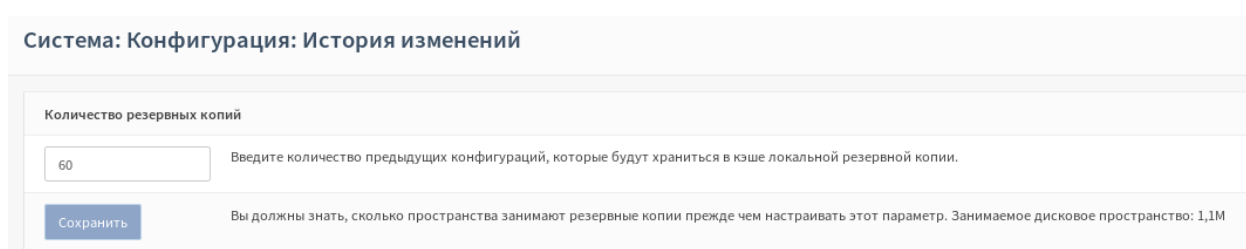


Рисунок 179 – Система: Конфигурация: История изменений (количество резервных копий)

После внесения изменений необходимо нажать на кнопку «Сохранить».

Группа настроек «История изменений» позволяет просматривать отличия конфигураций. Для этого необходимо нажать на флажок (столбец «Отличия») в таблице истории изменений на конфигурации, а затем нажать на кнопку «Просматривать отличия» (Рисунок 180).

Отличия конфигурации 04.07.20 10:31:32 от 04.07.20 10:31:37

```

--- /conf/backup/config-1593858697.2667.xml      2020-07-04 10:31:37.266945000 +0000
+++ /conf/config.xml      2020-07-04 10:31:37.271562000 +0000
@@ -450,8 +450,8 @@
</widgets>
<revision>
  <username>root@192.168.1.100</username>
  - <time>1593858692.7451</time>
  - <description>/api/ids/service/reconfigure &#x432;&#x430;&#x435;&#x441; &#x438;&#x437;&#x43C;&#x435;&#x43D;&#x438;&#x44F;</description>
  + <time>1593858697.2667</time>
  + <description>/api/ids/settings/set &#x432;&#x430;&#x435;&#x441; &#x438;&#x437;&#x43C;&#x435;&#x43D;&#x438;&#x44F;</description>
</revision>
<ca/>
<gateways>

```

История изменений

Просмотреть отличия

Чтобы просмотреть отличия между разными версиями конфигураций, выберите более раннюю версию в левом столбце, а более позднюю в правом и нажмите на

Отличия	Дата	Размер	Изменение конфигурации	
<input checked="" type="radio"/>	04.07.20 10:31:37	32 KB	root@192.168.1.100: /api/ids/settings/set внес изменения	Текущая
<input type="radio"/>	04.07.20 10:31:32	32 KB	root@192.168.1.100: /api/ids/service/reconfigure внес изменения	
<input type="radio"/>	04.07.20 10:31:32	32 KB	root@192.168.1.100: /api/ids/settings/set внес изменения	

Рисунок 180 – Система: Конфигурация: История изменений (История изменений)

Таблица истории изменений позволяет просматривать:

- дату/время изменения;
- размер изменения в конфигурации;
- идентификатор пользователя и описание совершенного действия.

А также скачать, вернуть и удалить (отменить действие) конфигурацию, нажав на соответствующие кнопки напротив изменения (Рисунок 181).

Отличия	Дата	Размер	Изменение конфигурации	
<input type="radio"/>	04.07.20 10:31:37	32 KB	root@192.168.1.100: /api/ids/settings/set внес изменения	Текущая
<input checked="" type="radio"/>	04.07.20 10:31:32	32 KB	root@192.168.1.100: /api/ids/service/reconfigure внес изменения	
<input type="radio"/>	04.07.20 10:31:32	32 KB	root@192.168.1.100: /api/ids/settings/set внес изменения	
<input type="radio"/>	03.07.20 22:31:39	31 KB	root@192.168.1.100: Enter CARP maintenance mode	
<input type="radio"/>	03.07.20 22:13:58	31 KB	root@192.168.1.100: /interfaces_groups_edit.php made changes	
<input type="radio"/>	03.07.20 21:12:07	31 KB	root@192.168.1.100: /firewall_nat_npt_edit.php made changes	
<input type="radio"/>	03.07.20 21:10:04	30 KB	root@192.168.1.100: /firewall_nat_out.php made changes	

Рисунок 181 – Система: Конфигурация: История изменений (История изменений: таблица)

6.8.4 Категория «Настройки экспорта»

Процедура настройки экспорта конфигурации по протоколу FTP/SMB описаны в Руководстве администратора в разделе 7, подразделе 7.4.

6.9 Подраздел «Доверенные сертификаты»

Подраздел «Доверенные сертификаты» позволяет настраивать Центр Сертификации, добавлять и импортировать сертификаты, а также отзывать сертификат. Для защищенного подключения графического интерфейса используется TLS протокол версии 1.2.

6.9.1 Категория «Полномочия»

Категория «Полномочия» позволяет настраивать Центр Сертификации. Все настроенные центры сертификации указаны в таблице, которая отображает следующие данные (Рисунок 182):

- название сертификата;

- является ли сертификат внутренним;
- эмитент;
- количество сертификатов;
- уникальное имя.

Также имеется возможность удалить, редактировать, экспортировать Центр Сертификации и экспортировать секретный ключ Центра Сертификации.

Система: Доверенные сертификаты: Полномочия + Добавить






Имя	Внутренний	Эмитент	Сертификаты	Уникальное имя	
TEST	ДА	самоподписанный	0	emailAddress=admin@mycompany.com, ST=Sachsen, O=My Company Inc, L=Leipzig, CN=internal-ca, C=AD	   
				<small>Действителен с:</small> Tue, 26 Mar 2019 21:18:48 +0000 <small>Действителен до:</small> Wed, 25 Mar 2020 21:18:48 +0000	


Рисунок 182 – Система: Доверенные сертификаты: Полномочия

Для того чтобы редактировать существующие Центры Сертификации, необходимо нажать на кнопку  напротив центра сертификации. Для того чтобы создать новый Центр Сертификации, необходимо нажать на кнопку + Добавить.

При редактировании центра сертификации поле «Название» необходимо ввести название Центра Сертификации. В поле «Метод» необходимо выбрать метод добавления центра сертификации (Рисунок 183).

Система: Доверенные сертификаты: Полномочия

Описательное имя

 Метод

Импортировать существующий центр сертификации ▼

Рисунок 183 – Система: Доверенные сертификаты: Полномочия (редактирование)

Если в поле «Метод» выбрать «Импортировать существующий центр сертификации», то появятся следующие поля. В поле «Данные сертификата» необходимо ввести данные сертификата X.509 в PEM формате. В поле «Секретный ключ сертификата» необходимо ввести секретный ключ для сертификата, указанного в поле «Данные сертификата». В поле «Серийный номер для следующего сертификата» необходимо ввести число, которое будет использоваться как серийный номер для следующего сертификата (Рисунок 184).

Существующий центр сертификации

Данные сертификата

```
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIBADANBgkqhkiG9w0BAQsFADC
BhTElMAkGA1UEBhMCQUQx
ETAPBgNVBAGMCCBTYWNo2VuMRAwDgYDVQQHDAd
MZWlwehmlnMRcwFQYDVQQKDA5N
eSBDdb21wYW55IEluYzEiMCAGCSqGSIb3DQEJARYTYW
RtaW5AbXlj21wYW55LmNv
-----
```

Секретный ключ сертификата
(необязательно)

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAg
EAAoIBAQC4HgJZJBAUSIWI
6qhbcjSlrhre8RPXYagpylmvpQDlx4CwO7fCg1BDrtLRK
ZYrIMFX+dLBPNglWBkT
ExXiRuHHrDvp0hTG79uP4gUcb8PIAjZ0E5dP+ZY6eKsl
53wQ2yWAA2ndHwZnf4WI
-----
```

Серийный номер для следующего
сертификата

1

Рисунок 184 – Система: Доверенные сертификаты: Полномочия (редактирование: Импортировать существующий центр сертификации)

Если в поле «Метод» выбрать «Создать внутренний Центр Сертификации», то появятся следующие поля. В поле «Длина ключа (бит)» необходимо выбрать длину ключа. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя (Рисунок 185).

Неверный внутренний Центр сертификации	
❗ Тип ключа	<input type="text" value="RSA"/>
❗ Длина ключа (бит)	<input type="text" value="2048"/>
❗ Алгоритм дайджеста	<input type="text" value="SHA256"/>
❗ Время существования (дни)	<input type="text" value="365"/>
Уникальное имя	
❗ Код страны :	<input type="text" value="RU (Russia)"/>
❗ Штат или область :	<input type="text" value="Moscow"/>
❗ Город :	<input type="text" value="Moscow"/>
❗ Организация :	<input type="text" value="My Company Inc"/>
❗ Эл. почта :	<input type="text" value="admin@mycompany.com"/>
❗ Стандартное имя :	<input type="text" value="internal-ca"/>
<input type="button" value="Сохранить"/>	

Рисунок 185 – Система: Доверенные сертификаты: Полномочия (редактирование: Создать внутренний Центр Сертификации)

Если в поле «Метод» выбрать «Создать промежуточный Центр Сертификации», то появятся следующие поля. В поле «Подписание Центра Сертификации» необходимо выбрать Центр Сертификации. В поле «Длина ключа (бит)» необходимо выбрать длину ключа в битах. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя (Рисунок 186).

Неверный внутренний Центр сертификации	
Подписание центра сертификации	Не выбрано
Key Type	RSA
Длина ключа (бит)	2048
Алгоритм дайджеста	SHA256
Время существования (д)	365
Уникальное имя	
Код страны :	AD (Andorra)
Штат или область :	Sachen
Город :	Leipzig
Организация :	My Company Inc
Эл. почта :	admin@mycompany.com
Стандартное имя :	internal-ca

Рисунок 186 – Система: Доверенные сертификаты: Полномочия (редактирование: Создать промежуточный Центр Сертификации)

После внесения изменений необходимо нажать на кнопку «Сохранить».

6.9.2 Категория «Сертификаты»

Субординированный Центр Сертификации позволяет выписывать различные end entity сертификаты для использования в следующих функциях:

- защищенный доступ к веб-интерфейсу;
- SSL Bump (перехват/дешифровка HTTPS-соединений).

Категория «Сертификаты» позволяет просматривать существующие сертификаты/просматривать информацию о них/удалить/создать сертификаты, а также экспортировать пользовательский ключ и пользовательский сертификат.

Все настроенные сертификаты указаны в таблице, которые отображает следующие данные (Рисунок 187):

- название сертификата;
- эмитент;
- уникальное имя (срок действия сертификата).

Система: Доверенные сертификаты: Сертификаты				Добавить
Имя	Эмитент	Уникальное имя	Используется	
Web GUI SSL certificate	самоподписанный	ST=Zuid-Holland, O=OPNsense, L=Middelharnis, C=NL	<div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	
CA: Yes, Сервер: No		Действителен с: Mon, 25 Mar 2019 16:13:20 +0000 Действителен до: Tue, 24 Mar 2020 16:13:20 +0000		
test	TEST	emailAddress=admin@mycompany.com, ST=Sachsen, O=My Company Inc, L=Leipzig, CN=test, C=AD	<div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>	
CA: No, Сервер: No		Действителен с: Wed, 27 Mar 2019 02:09:35 +0000 Действителен до: Thu, 26 Mar 2020 02:09:35 +0000		

Рисунок 187 – Система: Доверенные сертификаты: Сертификаты

Для того чтобы создать новый сертификат, необходимо нажать на кнопку

Добавить

При редактировании сертификата в поле «Метод» необходимо выбрать метод создания сертификата.

Если в поле «Метод» выбрать «Импортировать существующий сертификат», то появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Данные сертификата» необходимо ввести данные сертификата X.509 в PEM формате. В поле «Данные секретного ключа» необходимо ввести секретный ключ для сертификата, указанного в поле «Данные сертификата» (Рисунок 188).

Система: Доверенные сертификаты: Сертификаты

Метод

Импортировать существующий сертификат

Описательное имя

Импортировать сертификат

Данные сертификата

Данные секретного ключа

Сохранить

Рисунок 188 – Система: Доверенные сертификаты: Сертификаты (редактирование: Импортировать существующие сертификаты)

Если в поле «Метод» выбрать «Создать внутренний сертификат», то появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Центр сертификации» необходимо выбрать Центр Сертификации. В поле «Тип» необходимо выбрать тип сертификата для генерации, определяющий его условия. В поле «Длина ключа (бит)» необходимо выбрать длину ключа. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Расположение секретного ключа» необходимо выбрать, где необходимо сохранить секретный ключ. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя. В поле «Альтернативные имена» необходимо выбрать в поле «Тип» тип альтернативного имени и в поле «Значение» необходимо ввести его имя (Рисунок 189).

Система: Доверенные сертификаты: Сертификаты

Метод: Создать внутренний сертификат

Описание сертификата: Внутренний Сертификат

Центр сертификации: Внутренние центры сертификации неопределены. Вы должны добавить внутренний СА перед созданием внутреннего сертификата.

Тип: Сертификат клиента

Тип ключа: RSA

Длина ключа (бит): 2048

Алгоритм дайджеста: SHA256

Время существования (дни): 325

Расположение секретного ключа: Сохранить на этом компьютере

Уникальное имя

Код страны: AD (Andorra)

Штат или область:

Город:

Организация:

Эл. почта:

Стандартное имя:

Альтернативные имена

Тип	Значение
DNS	

Сохранить

Рисунок 189 – Система: Доверенные сертификаты: Сертификаты
(редактирование: Создать внутренний сертификат)

Если в поле «Метод» выбрать «Создать запрос на подпись сертификата», то появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Длина ключа (бит)» необходимо выбрать длину ключа. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация»

необходимо ввести название организации. В поле «Организационное подразделение» необходимо выбрать отдел организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя. В поле «Альтернативные имена» необходимо выбрать в поле «Тип» тип альтернативного имени и в поле «Значение» необходимо ввести его имя (Рисунок 190).

Запрос внешнего подписания		
Key Type	RSA	
Длина ключа (бит)	2048	
Алгоритм дайджеста	SHA256	
Уникальное имя		
Код страны :	AD (Andorra)	
Штат или область :	Sachen	
Город :	Leipzig	
Организация :	My Company Inc	
Организационное подразделение :		
Эл. почта :	admin@mycompany.com	
Стандартное имя :	internal-ca	
Альтернативные Имена		
Тип	Значение	
DNS		-
		+
<button>Сохранить</button>		

Рисунок 190 – Система: Доверенные сертификаты: Сертификаты (редактирование: Создать запрос на подпись сертификата)

Если в поле «Метод» выбрать «Создать запрос на получение сертификатов», то появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Центр сертификации» необходимо выбрать Центр сертификации. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «CSR файл» необходимо ввести CSR файл. CSR файл — это файл, который содержит в себе небольшой фрагмент зашифрованных данных о Вашем домене и компании, на который выдается сертификат (Рисунок 191).

Система: Доверенные сертификаты: Сертификаты

Метод	Создать запрос на получение сертификата
Описательное имя	
Запрос на получение сертификата	
Центр сертификации	
Алгоритм дайджеста	SHA256
Время существования (д)	365
CSR файл	
Показать подробнее	
Далее	

Рисунок 191 – Система: Доверенные сертификаты: Сертификаты
(редактирование: Создать запрос на получение сертификата)

Если нажать на кнопку «Показать подробнее» появятся следующие поля (Рисунок 192). В поле «Объект» можно просматривать информацию о сертификате. В поле «subjectAltName» необходимо ввести несколько доменных адресов сертификатов. В поле «basicConstraints» необходимо установить флажок напротив поля «Центр Сертификации» для возможности ввода максимального значения сертификатов. В поле «keyUsage» необходимо выбрать параметры для секретного ключа. В поле «extendedKeyUsage» необходимо выбрать параметры расширенного значения ключа.

Объект сертификации

Объект C=UA, ST=Kyivskay oblast, L=Kyiv, O=TEST, OU=IT, CN=test.com, emailAddress=test@mail.ru

subjectAltName

Тип	Значение
IP-адрес	192.168.1.1

basicConstraints

☒ Центр Сертификации

Максимальное значение сертификатов:

3

keyUsage

dataEncipherment


extendedKeyUsage

clientAuth, codeSigning, emailProtection, timeStamp

Сохранить

Рисунок 192 – Система: Доверенные сертификаты: Сертификаты (редактирование: Создать запрос на получение сертификата: Показать подробнее)

После внесения изменений необходимо нажать на кнопку «Сохранить».

При нажатии на кнопку  появляется всплывающее окно с отображением полной информацией о сертификате (Рисунок 193).

Сертификат

SHA256 Fingerprint=B3:E2:9C:30:CB:4A:4B:6A:40:05:50:EF:DD:78:5F:B8:42:48:3F:B7:4D:01:AD:C8:78:60:5B:E7:5C:6B:87:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

4d:81:0e:23:eb:c8:79:43:c3:5c:6d:83:33:ce:cf:96:65:fe:30:15

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, ST = Moscow, L = Moscow, O = InfoWatch LLC, OU = ICS Security, CN = armaif.ru

Validity

Not Before: Jul 2 10:24:35 2020 GMT

Not After : Oct 5 10:24:35 2022 GMT

Subject: C = RU, ST = Moscow, L = Moscow, O = InfoWatch LLC, OU = ICS Security, CN = armaif.ru

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (4096 bit)

Modulus:

00:bf:37:0f:ee:3b:cf:8c:69:a1:09:96:16:91:90:
 12:1a:27:86:7e:cb:a0:c1:d3:45:69:71:b1:3a:bd:
 10:47:b6:4f:8a:ea:f3:cb:f9:e3:89:cd:31:cf:fd:
 32:e7:56:25:9d:2b:91:89:e9:9a:44:a4:5d:2c:87:
 38:ea:bd:76:49:2d:c9:b6:46:46:13:d8:23:08:07:
 f0:75:f9:eb:55:ea:ef:40:90:3f:de:32:96:c4:72:
 73:38:f3:85:c4:3e:81:07:e7:87:5d:1d:c3:9b:1e:
 81:d1:ab:2f:8b:9e:f7:45:00:df:f2:34:ae:cd:42:
 6b:1f:7a:c8:4e:b5:5c:09:f9:02:1b:1f:36:03:bc:
 d2:50:67:a4:9e:3c:54:e4:a3:d3:b9:8c:89:c4:62:

Рисунок 193 – Система: Доверенные сертификаты: Сертификаты (подробная информация о сертификате)


6.9.3 Категория «Отзыв сертификатов»

Категория «Отзыв сертификатов» позволяет просматривать информацию о существующих списках отзыва сертификатов и добавить списки отзыва сертификатов существующих Центров Сертификации (Рисунок 194).

Система: Доверенные сертификаты: Отзыв сертификатов

Имя	Внутренний	Сертификаты	Используется	
TEST				+
test	ДА	1	НЕТ	⬇️ ⬆️ ⬇️
test1	НЕТ	Неизвестный (импортирован)	НЕТ	⬇️ ⬆️ ⬇️


Рисунок 194 – Система: Доверенные сертификаты: Отзыв сертификатов

Для добавления нового сертификата необходимо нажать на кнопку  напротив Центра Сертификации.


При добавлении сертификата в поле «Метод» необходимо выбрать способ выбора сертификата.

Если выбрать в поле «Метод» метод «Создать внутренний список сертификатов», появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Центр Сертификации» необходимо выбрать существующий Центр Сертификации. В поле «Время существования (д)» необходимо ввести срок действия сертификата в днях. В поле «Серийный номер» необходимо ввести серийный номер сертификата. После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 195).


Система: Доверенные сертификаты: Отзыв сертификатов

 Метод

Создать внутренний список отзыва сертификатов ▾


 Название

test


 Центр сертификации

TEST ▾

Внутренний список отзыва сертификатов

 Время существования (д)

9999

 Серийный номер

0

Сохранить

Рисунок 195 – Система: Доверенные сертификаты: Отзыв сертификатов

Если выбрать в поле «Метод» метод «Импортировать существующий список сертификатов», появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Центр Сертификации» необходимо выбрать существующий Центр Сертификации. В поле «Данные CRL» необходимо ввести список отзыва сертификата в формате X.509 CRL. Необходимо нажать на кнопку «Сохранить» (Рисунок 196).

Система: Доверенные сертификаты: Отзыв сертификатов

Метод	Импортировать существующий список отзыва серт...
Название	test2
Центр сертификации	TEST
Существующий список отзыва сертификатов	
Данные CRL	test
Сохранить	

Рисунок 196 – Система: Доверенные сертификаты: Отзыв сертификатов (редактирование: Импортировать существующий список сертификатов)

6.10 Подраздел «Мастер»

Подраздел «Мастер» позволяет пройти начальную настройку системы. Для этого необходимо нажать на кнопку «Далее» (Рисунок 197).

Система: Мастер: Общие настройки

Этот мастер проведёт вас через начальную настройку. Мастера можно прервать в любой момент нажатием на логотип вверху экрана.

Далее

Рисунок 197 – Система: Мастер

6.10.1 Мастер: шаг 1

На первом шаге система предложит настроить общие настройки. Подробнее заполнение всех полей приведено в подразделе 6.3.3 настоящего руководства. После настройки необходимо нажать на кнопку «Далее».

6.10.2 Мастер: шаг 2

На втором шаге начальной настройки система предложит настроить время (Рисунок 198). В поле «Имя сервера времени:» необходимо ввести полное имя сервера времени, с которым будет производиться синхронизация. В случае, если таких серверов несколько их необходимо вводить через запятую. В поле «Часовой пояс» необходимо выбрать часовой пояс и нажать на кнопку «Далее».

Система: Мастер: Настройка времени

Имя сервера времени:	<input type="text" value="0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2...."/>
Укажите полное имя сервера времени.	
Часовой пояс:	<input type="text" value="Etc/UTC"/>
<input type="button" value="Далее"/>	

Рисунок 198 – Система: Мастер: шаг 2

6.10.3 Мастер: шаг 3

На третьем шаге система предложит настроить WAN интерфейс. Подробнее заполнение всех полей приведено в подразделе 7.1 настоящего руководства. После настройки необходимо нажать на кнопку «Далее».

6.10.4 Мастер: шаг 4

На четвертом шаге система предложит настроить LAN интерфейс. Подробнее заполнение всех полей приведено в подразделе 7.1 настоящего руководства. После настройки необходимо нажать на кнопку «Далее».

6.10.5 Мастер: шаг 5

На пятом шаге начальной настройки система предложит настроить корневой пароль (Рисунок 199). В поле «Пароль пользователя root:» необходимо ввести пароль пользователя root. В поле «Подтверждение пароля пользователя root:» необходимо ввести пароль из поля «Пароль пользователя root:» повторно и нажать на кнопку «Далее».

Пароль пользователя root:	<input type="password"/>
(оставьте пустым для сохранения текущего значения)	
Подтверждение пароля пользователя root:	<input type="password"/>
<input type="button" value="Далее"/>	

Рисунок 199 – Система: Мастер: шаг 5

6.10.6 Мастер: шаг 6

На шестом шаге начальной настройки система предложит перезагрузиться для применения настроек (Рисунок 200). Необходимо нажать на кнопку «Перезагрузить».

Для применения изменений нажмите 'Перезагрузить'

[Перезагрузить](#)

Рисунок 200 – Система: Мастер: шаг 6

6.11 Подраздел «Журналы»

В подразделе «Журналы» отображается журнал Syslog (системный журнал реализован на базе Syslog), журнал событий конфигураций системы (реализован на базе configd), журнал событий веб-интерфейса (реализован на базе lighttpd), журнал системных событий, журнал событий безопасности, журнал действий пользователей.

6.11.1 Категория «Журнал Syslog»

Категория «Журнал Syslog» позволяет просматривать журнал Syslog в формате таблицы, где имеются данные о дате/времени события системы, а также сообщения о выполненном действии системы (Рисунок 201). В данном журнале приводятся все основные системные сообщения о работе системы и изменения в ней каких-либо параметров.

Система: Журналы: Журнал Syslog	
<div style="text-align: right;"> <input type="text" value="Поиск"/> <input type="button" value="↺"/> <input type="button" value="20"/> <input type="button" value="☰"/> </div>	
Дата	Сообщение
2020-07-21T06:42:53	dhclient[89086]: bound to 192.168.159.139 -- renewal in 900 seconds.
2020-07-21T06:42:53	dhclient: Creating resolv.conf
2020-07-21T06:42:53	dhclient[89086]: DHCPACK from 192.168.159.254
2020-07-21T06:42:53	dhclient[89086]: DHCPREQUEST on em2 to 192.168.159.254 port 67
2020-07-21T06:27:53	dhclient[89086]: bound to 192.168.159.139 -- renewal in 900 seconds.
2020-07-21T06:27:53	dhclient: Creating resolv.conf
2020-07-21T06:27:53	dhclient[89086]: DHCPACK from 192.168.159.254
2020-07-21T06:27:53	dhclient[89086]: DHCPREQUEST on em2 to 192.168.159.254 port 67
2020-07-21T06:12:57	kernel: pflg0: promiscuous mode enabled
2020-07-21T06:12:57	kernel: pflg0: promiscuous mode disabled
2020-07-21T06:12:56	armailf: plugins_configure dns (execute task : dnsmasq_configure_do())
2020-07-21T06:12:56	armailf: plugins_configure dns ()
2020-07-21T06:12:55	armailf: plugins_configure dhcp (execute task : dhcpd_dhcp_configure())
2020-07-21T06:12:55	armailf: plugins_configure dhcp ()
2020-07-21T06:12:55	armailf: plugins_configure ipsec (execute task : ipsec_configure_do(opt2))
2020-07-21T06:12:55	armailf: plugins_configure ipsec (.opt2)
2020-07-21T06:12:55	armailf: /usr/local/etc/rc.linkup: ROUTING: keeping current default gateway '192.168.159.2'
2020-07-21T06:12:55	armailf: /usr/local/etc/rc.linkup: ROUTING: setting IPv4 default route to 192.168.159.2
2020-07-21T06:12:55	armailf: /usr/local/etc/rc.linkup: ROUTING: IPv4 default gateway set to opt2

Рисунок 201 – Система: Журналы: Журнал Syslog

6.11.2 Категория «Backend журнал»

Категория «Backend журнал» позволяет просматривать журнал Backend, в котором отображается содержимое файла /var/log/configd.log. В журнале Backend отображаются все события, отправленные через веб-интерфейс, а также изменения всех параметров системы (изменения настроек ПК «InfoWatch ARMA Industrial Firewall», добавления правил, маршрутов и т.д.) в виде таблицы. В таблице отображаются данные о дате/времени события, а также сообщение о выполненном действии Backend журнала (Рисунок 202). В данном журнале

приводятся записи о результатах выполнения различных операций внутреннего конфигулятора сервера.

Система: Журналы: Backend журнал

Дата	Сообщение
2020-07-21T06:56:01	configd.py: [28b38118-b844-48bb-bf76-90a46d1d99c4] Show log
2020-07-21T06:55:09	configd.py: [06fbc88-f9ec-4bea-bc13-4a03d43e0160] Show log
2020-07-21T06:47:44	configd.py: [675910cf-820b-481e-a94e-80bc5d3fed7e] Show log
2020-07-21T06:46:26	configd.py: [41af1d38-1382-4c6e-ac96-cc8e9d9be337] list gateways
2020-07-21T06:45:27	configd.py: [7fee0bf9-7d0b-4abd-988f-ed67fcbaf3f8] Show log
2020-07-21T06:39:48	configd.py: [8f183588-da77-444f-8dca-d03e8f9de489] Show system activity
2020-07-21T06:15:12	configd.py: [77ced9b0-a1f7-4f59-9844-20ea8084874c] list systemhealth items
2020-07-21T06:15:07	configd.py: [ad88dde0-060f-437c-a5a5-5587667065f8] request prctt byte/packet counters
2020-07-21T06:15:00	configd.py: [5d58cc25-df93-49a0-be21-e3f4873d8ef9] request prctt byte/packet counters
2020-07-21T06:14:50	configd.py: [e443cb59-fef4-4b2e-9dd6-ed78804b5bdc] get suricata daemon status
2020-07-21T06:14:47	configd.py: [d0c6884f-c843-4602-a156-b2e81e4cc8cc] request pftop statistics
2020-07-21T06:14:44	configd.py: [a01c86b5-21bc-403f-ae0c-a0421eae610a] request pftop statistics
2020-07-21T06:14:42	configd.py: [de980614-77d2-4cf8-88e9-8ac45a8e6b19] request pftop statistics
2020-07-21T06:14:39	configd.py: [3d126f9-76dc-4118-8b3f-96b34287c847] request pftop statistics
2020-07-21T06:14:36	configd.py: [47076ed4-5c79-45ac-b2ec-6f99a6f59f60] request pftop statistics
2020-07-21T06:14:34	configd.py: [2bc29d92-6cfd-487f-9b30-810ae8f07a57] request pftop statistics
2020-07-21T06:14:31	configd.py: [6e47a429-a4f3-4f3f-b829-14ef14f8dc82] request pftop statistics
2020-07-21T06:14:28	configd.py: [8a558ea8-da8b-4b89-8595-9ec04592a514] request pftop statistics
2020-07-21T06:14:26	configd.py: [ac597727-162d-414e-82a3-98cb73d1ec34] request pftop statistics

Рисунок 202 – Система: Журналы: Backend журнал

6.11.3 Категория «Журнал веб-интерфейса»

Категория «Журнал веб-интерфейса» позволяет просматривать журнал веб-интерфейса в формате таблицы, где имеются данные о дате/времени события системы, а также сообщение о выполненном действии в веб-интерфейсе (Рисунок 203). В данном журнале представлены записи о событиях, связанных с веб-интерфейсом.

Система: Журналы: Журнал веб-интерфейса

Дата	Сообщение
2020-07-20T11:59:12	lighttpd[27635]: (connections.c.125) (warning) close: 11 Connection reset by peer
2020-07-20T11:51:33	lighttpd[27635]: (server.c.1488) server started (lighttpd/1.4.55)
2020-07-20T11:45:22	lighttpd[9579]: (server.c.1488) server started (lighttpd/1.4.55)
2020-07-20T11:40:20	lighttpd[16379]: (server.c.1488) server started (lighttpd/1.4.55)

Показаны с 1 по 4 из 4 записей

Очистить журнал

Рисунок 203 – Система: Журналы: Журнал веб-интерфейса

6.11.4 Категория «Журнал событий безопасности»



Категория «Журнал событий безопасности» позволяет просматривать журнал событий безопасности в формате таблицы. Таблица содержит следующие данные (Рисунок 204):

- дата;
- механизм;

- отправитель;
- получатель;
- действие;
- описание;
- имя пользователя;
- кнопка «Дополнительная информация».

В журнале событий безопасности отображаются следующие события:

- для системы обнаружения вторжений:
 - срабатывание сигнатур;
- для межсетевого экрана:
 - срабатывания правил межсетевого экрана;
- для arprwatch:
 - подключение несанкционированного устройства;
 - обнаружение конфликта IP-адресов;
 - обнаружение изменения IP, MAC адреса;
 - обнаружение подмены IP-адресов.
- для Портала авторизации:
 - удачная/неудачная авторизация пользователя.

В журнале событий безопасности с помощью сквозного поиска по всем полям осуществляется фильтрация. Для поиска по всем полям таблицы событий необходимо ввести строку совпадения в поле «Поиск» сверху таблицы и нажать на кнопку . Для поиска по определенному столбцу необходимо ввести строку совпадения в поле «Поиск» сверху столбца и нажать на кнопку .

Для экспорта журнала событий безопасности наверху страницы необходимо выбрать в раскрывающемся меню формат экспортируемого файла:

- CSV (экспортируется файл журнала в формате CSV с примененными фильтрами, со столбцом дополнительной информации);
- PDF расширенный (экспортируется файл журнала в формате PDF с примененными фильтрами, со столбцом дополнительной информации);
- PDF (экспортируется файл журнала в формате PDF с примененными фильтрами, без столбца дополнительной информации).

Нажать кнопку «Экспорт».

PDF Экспорт
 ↺ 20 ▢

Дата	Механизм	Отправитель	Получатель	Действие	Описание	Имя пользователя	Информация
30 августа 2019 г., 09:46	Межсетевой экран	192.168.1.4	192.168.1.6	разрешение (pass)	правило антиблокировки		0
30 августа 2019 г., 09:46	Межсетевой экран	192.168.1.4	192.168.1.6	разрешение (pass)	правило антиблокировки		0
30 августа 2019 г., 09:46	Межсетевой экран	127.0.0.1	127.0.0.1	разрешение (pass)	pass loopback		0
30 августа 2019 г., 09:46	Межсетевой экран	127.0.0.1	127.0.0.1	разрешение (pass)	let out anything from firewall host itself		0
30 августа 2019 г., 09:46	Межсетевой экран	192.168.1.6	192.168.1.1	разрешение (pass)	let out anything from firewall host itself		0
30 августа 2019 г., 09:46	Межсетевой экран	10.0.2.15	10.0.2.3	разрешение (pass)	let out anything from firewall host itself		0
30 августа 2019 г., 09:46	Межсетевой экран	127.0.0.1	127.0.0.1	разрешение (pass)	pass loopback		0
30 августа 2019 г., 09:46	Межсетевой экран	127.0.0.1	127.0.0.1	разрешение (pass)	let out anything from firewall host itself		0
30 августа 2019 г., 09:46	Межсетевой экран	10.0.2.15	10.0.2.3	разрешение (pass)	let out anything from firewall host itself		0
30 августа 2019 г., 09:46	Межсетевой экран	127.0.0.1	127.0.0.1	разрешение (pass)	pass loopback		0



Рисунок 204 – Система: Журналы: Журнал событий безопасности

6.11.5 Категория «Журнал системных событий»

Категория «Журнал системных событий» позволяет просматривать журнал системных событий в формате таблицы, где имеются данные о дате/времени события системы, а также сообщения о выполненном действии системы (Рисунок 205).

В журнале системных событий отображаются следующие события:

- запуск ntp-сервера;
- нет подключения к ntp-серверу;
- выключение ntp-сервера;
- изменение настроек ntp-сервера;
- сбой Портала авторизации (неуспешная попытка входа в Портал авторизации;
- сбой системы обнаружения вторжений;
- события контроля целостности;
- запуск веб-сервера;
- неуспешный доступ к странице графического интерфейса;
- загрузка системы.

В журнале системных событий с помощью сквозного поиска по всем полям осуществляется фильтрация. Для поиска по всем полям таблицы событий необходимо ввести строку совпадения в поле «Поиск» вверху таблицы и нажать на кнопку . Для поиска по определенному столбцу необходимо ввести строку совпадения в поле «Поиск» вверху столбца и нажать на кнопку .

Для экспорта журнала системных событий наверху страницы необходимо выбрать в раскрывающемся меню формат экспортируемого файла:

- CSV (экспортируется файл журнала в формате CSV с примененными фильтрами, со столбцом дополнительной информации);
- PDF расширенный (экспортируется файл журнала в формате PDF с примененными фильтрами, со столбцом дополнительной информации);

– PDF (экспортируется файл журнала в формате PDF с примененными фильтрами, без столбца дополнительной информации).

Нажать кнопку «Экспорт».

Система: Журналы: Журнал системных событий

PDF Экспорт

Поиск

20

Дата	Сообщение
20 июля 2020, 16:08	NTP-сервер версии 4 запущен
20 июля 2020, 16:08	Синхронизация с внешним ntp-сервером успешно выполнена
20 июля 2020, 16:07	NTP-сервер выключен
20 июля 2020, 15:53	NTP-сервер версии 4 запущен
20 июля 2020, 15:53	Синхронизация с внешним ntp-сервером успешно выполнена
20 июля 2020, 13:29	NTP-сервер выключен
20 июля 2020, 12:22	NTP-сервер версии 4 запущен
20 июля 2020, 12:22	Синхронизация с внешним ntp-сервером успешно выполнена
20 июля 2020, 12:21	NTP-сервер выключен
20 июля 2020, 11:52	NTP-сервер версии 4 запущен
20 июля 2020, 11:52	Синхронизация с внешним ntp-сервером успешно выполнена
20 июля 2020, 11:51	Система запущена
20 июля 2020, 11:50	Нет подключения к NTP-серверу по адресу 0.pool.ntp.org
20 июля 2020, 11:49	Нет подключения к NTP-серверу по адресу 3.pool.ntp.org
20 июля 2020, 11:48	Нет подключения к NTP-серверу по адресу 2.pool.ntp.org
20 июля 2020, 11:47	Нет подключения к NTP-серверу по адресу 1.pool.ntp.org
20 июля 2020, 11:46	Нет подключения к NTP-серверу по адресу 0.pool.ntp.org

Рисунок 205 – Система: Журналы: Журнал системных событий

6.11.6 Категория «Журнал действий пользователей»



Категория «Журнал действий пользователей» позволяет просматривать журнал действий пользователей в формате таблицы. Таблица содержит следующие данные (Рисунок 206):

- дата;
- имя пользователя;
- адрес;
- действия;
- успешно.

В журнале действий пользователей отображаются следующие события:

- включение и отключение межсетевого экрана;
- включение и отключение системы обнаружения вторжений;
- успешный/неуспешный доступ к страницам интерфейса;
- изменение/добавление/удаление правил межсетевого экрана;
- изменение настроек межсетевого экрана;
- изменение правил системы обнаружения вторжений;
- изменение настроек системы обнаружения вторжений;
- успешная/неуспешная авторизация в графическом и консольном интерфейсах;
- изменение размера записей в журнале веб-интерфейса;

- создание нового пользователя;
- включение «сложного» пароля;
- изменение настроек мониторинга состояния системы на странице анализа трафика, настроек `monit`;
- перезагрузка системы.

В журнале действий пользователей с помощью сквозного поиска по всем полям осуществляется фильтрация. Для поиска по всем полям таблицы событий необходимо ввести строку совпадения в поле «Поиск» вверху таблицы и нажать на кнопку . Для поиска по определенному столбцу необходимо ввести строку совпадения в поле «Поиск» вверху столбца и нажать на кнопку .

Для экспорта журнала действий пользователей наверху страницы необходимо выбрать в раскрывающемся меню формат экспортируемого файла:

- CSV (экспортируется файл журнала в формате CSV с примененными фильтрами, со столбцом дополнительной информации);
- PDF расширенный (экспортируется файл журнала в формате PDF с примененными фильтрами, со столбцом дополнительной информации);
- PDF (экспортируется файл журнала в формате PDF с примененными фильтрами, без столбца дополнительной информации).

Нажать кнопку «Экспорт».

Система: Журналы: Журнал действий пользователя

PDF
Экспорт
Поиск
20

Дата	Имя пользователя	Адрес	Действия	Статус
9 июля 2020, 17:43			Система обнаружения вторжений включена	
9 июля 2020, 17:43	root@192.168.1.100	192.168.1.100	root@192.168.1.100: изменил(а) настройки системы обнаружения вторжений Подробнее можно посмотреть по ссылке	Успешно
4 июля 2020, 10:31	root@192.168.1.100	192.168.1.100	root@192.168.1.100: изменил(а) настройки системы обнаружения вторжений Подробнее можно посмотреть по ссылке	Успешно
4 июля 2020, 10:31	root@192.168.1.100	192.168.1.100	root@192.168.1.100: изменил(а) настройки системы обнаружения вторжений Подробнее можно посмотреть по ссылке	Успешно
3 июля 2020, 18:39	root@192.168.1.100	192.168.1.100	root@192.168.1.100: было изменено правило межсетевого экрана на /firewall_rules_edit.php Подробнее можно посмотреть по ссылке	Успешно

« 1 »
Показаны с 1 по 5 из 5 записей

Рисунок 206 – Система: Журналы: Журнал действий пользователей

6.12 Подраздел «Питание»

Подраздел «Питание» позволяет перезагрузить/выключить систему, а также выйти из учетной записи пользователя.

6.12.1 Категория «Перезагрузка»

Категория «Перезагрузка» позволяет перезагрузить систему. Для этого необходимо нажать на кнопку «Да» после сообщения о перезагрузке (Рисунок 207).

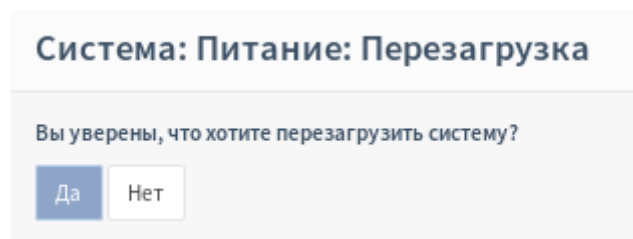


Рисунок 207 – Система: Питание: Перезагрузка

6.12.2 Категория «Выключение»

Категория «Выключение» позволяет выключить систему. Для этого необходимо нажать на кнопку «Да» после сообщения о выключении (Рисунок 208).

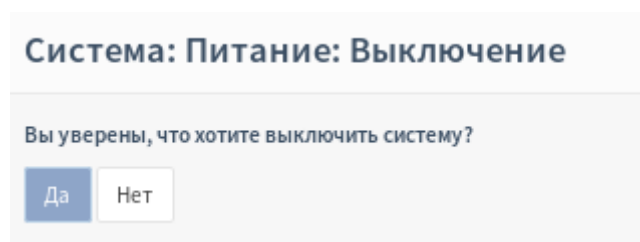


Рисунок 208 – Система: Питание: Выключение

6.12.3 Категория «Выход»

При переходе в категорию «Выход» произойдет моментальный выход из учетной записи пользователя и появится форма авторизации пользователя.

7 РАЗДЕЛ «ИНТЕРФЕЙСЫ»

Раздел «Интерфейсы» позволяет редактировать, добавлять, удалять сетевые интерфейсы, выгружать дампы трафика выбранного интерфейса, осуществлять трассировку маршрута через выбранный сетевой интерфейс, проверять «ping» с выбранного сетевого интерфейса.

7.1 Подраздел «[Название интерфейса]»

Категория «[Название интерфейса]» позволяет настраивать:


- общую конфигурацию интерфейса;
- конфигурацию статического IP-адреса;
- конфигурацию DHCP;
- конфигурацию PPP;
- конфигурацию PPPoE;
- конфигурацию PPTP;
- конфигурацию L2TP.

При редактировании [Название интерфейса] в поле «Включен» необходимо установить флажок для включения данного сетевого интерфейса. В поле «Блокировать» необходимо установить флажок для невозможности удаления данного интерфейса. В поле «Описание» необходимо ввести название интерфейса. В поле «Блокировать частные сети» необходимо установить флажок для блокирования трафика с IP-адресов, которые зарезервированы для частных сетей, в протоколе RFC 1918 (10/8, 172.16/12, 192.168/16), а также «зеркальных» (loopback) адресов (127/8). В настройке «Блокировать bogon сети» необходимо установить флажок для блокирования трафика от IP-адресов, которые зарезервированы или еще не присвоены IANA, не относящиеся к RFC 1918 (bogon — IP-адреса, которые не должны встречаться в таблицах маршрутизации в сети интернет или в качестве адреса отправителя получаемых пакетов). В полях «Тип конфигурации IPv4/IPv6» необходимо выбрать тип конфигурации. В поле «MAC-адрес» необходимо ввести адрес физического интерфейса, соответствующий редактируемому сетевому интерфейсу. В поле «Максимальный размер кадра» необходимо ввести расчетное значение. В поле «Скорость и двусторонний режим передачи данных» необходимо выбрать скорость и двусторонний режим передачи для редактируемого интерфейса. Если нет необходимости использовать интерфейс как шлюз, то в поле «Политика динамического шлюза» установить флажок при необходимости создавать динамические шлюзы без прямых целевых адресов (Рисунок 209).

Интерфейсы: [LAN]

Базовая конфигурация	
Включен	<input checked="" type="checkbox"/> Включить интерфейс
Блокировать	<input type="checkbox"/> Предотвращение удаления интерфейса
Устройство	em0
Описание	<input type="text" value="LAN"/>
Общая конфигурация	
Блокировать частные сети	<input checked="" type="checkbox"/>
Блокировать bogon сети	<input checked="" type="checkbox"/>
Тип конфигурации IPv4	Статический IPv4
Тип конфигурации IPv6	Отсутствует
MAC-адрес	<input type="text"/>
Максимальный размер кадра	<input type="text" value="1000"/>
Максимальный размер сегмента	<input type="text" value="42"/>
Скорость и двусторонний режим передачи данных	10baseT/UTP
Политика динамического шлюза	<input type="checkbox"/> Данному интерфейсу не нужны промежуточные системы для выполнения действий шлюза

Рисунок 209 – Интерфейсы: [Название интерфейса]: Общая конфигурация

При выборе в поле «Тип конфигурации IPv4/IPv6» тип конфигурации «Статический IPv4/IPv6» появится группа настроек «Конфигурация статического IPv4/IPv6-адреса». В поле «IPv4/IPv6-адрес» необходимо ввести IP-адрес и необходимо выбрать маску подсети. В поле «Публичный IPv4/IPv6-адрес шлюза» необходимо выбрать имеющийся шлюз из списка или добавить новый, нажав на . В группе настроек «Добавить новый шлюз» в поле «Шлюз по умолчанию» необходимо установить флажок для создания шлюза, который будет использоваться по умолчанию, в поле «Шлюз для Multy-WAN» необходимо установить флажок для включения шлюза для Multy-WAN, в поле «Имя шлюза» необходимо ввести название шлюза, в поле «IPv4/IPv6-адрес шлюза» необходимо ввести IP-адрес шлюза, в поле «Описание» необходимо ввести описание шлюза и необходимо нажать на кнопку «Сохранить». В поле «Использовать IPv4-подключение» необходимо установить флажок для использования IPv4-подключения (данное поле имеется только в поле «Конфигурация статического IPv6») (Рисунок 210).

Конфигурация DHCP-клиента		
Режим настройки	<div>Базовая</div> <div>Дополнительно</div> <div>Перезапись файла конфигурации</div>	
Псевдоним IPv4-адреса	192.168.1.3	32 ▼
Отклонить аренду IP-адресов от	192.168.1.5	
Имя хоста	test	
Переопределить MTU	<input checked="" type="checkbox"/>	

Рисунок 211 – Интерфейсы: [Название интерфейса]: Конфигурация DHCPv4 (Базовая)

Если в поле «Режим настройки» выбран пункт «Дополнительно», появятся следующие поля настройки. В поле «Отклонить аренду IP-адресов» необходимо ввести IP-адрес публичного DHCP-сервера, который необходимо игнорировать. В поле «Имя хоста» необходимо ввести идентификатор DHCP-клиента. В поле «Тайминг протокола» необходимо ввести в соответствующие поля время аренды IP-адресов в DHCP (возможно задать автоматически, нажав на кнопки «FreeBSD по умолчанию», «Очистить», «По умолчанию», «Сохраненный файл конфигурации»). В поле «Требования к аренде адресов» необходимо ввести опции DHCP, которые будут переданы серверу. В поле «Модификаторы параметра» необходимо ввести модификаторы параметров DHCP, которые будут применены для получения аренды DHCP (Рисунок 212).

Конфигурация DHCP-клиента

Режим настройки

Базовая

Дополнительно

Перезапись файла конфигурации

Отклонить аренду IP-адресов от

192.168.1.5

Имя хоста

test

Переопределить MTU

☒

Тайминг протокола

Тайм-аут:

60

Попробовать снова:

15

Выбрать тайм-аут:

0

Перезагрузка:

Отключение задержки:

Начальный интервал:

1

Предустановки:

FreeBSD по умолчанию

Очистить

По умолчанию

Сохраненный файл конфигурации

Требования к аренде адресов

Параметры отправки

Параметры Запроса

Требуемые параметры

Модификаторы параметра

Рисунок 212 – Интерфейсы: [Название интерфейса]: Конфигурация DHCPv4 (Дополнительно)

Если в поле «Режим настройки» выбран пункт «Перезапись файла конфигурации», появятся следующее поле «Перезапись файла конфигурации», в котором надо ввести полный абсолютный путь к файлу конфигурации DHCP (Рисунок 213).

Конфигурация DHCP-клиента

Режим настройки

Базовая

Дополнительно

Перезапись файла конфигурации

Перезапись файла конфигурации

/etc/dhcpd.conf.

Рисунок 213 – Интерфейсы: [Название интерфейса]: Конфигурация DHCPv4 (Перезапись файла конфигурации)

При выборе в поле «Тип конфигурации IPv6» тип конфигурации «DHCP» появится группа настроек «Конфигурация DHCPv6-клиента». В поле «Режим настройки» необходимо выбрать режим настройки.

Если в поле «Режим настройки» выбран пункт «Базовая», появятся следующие поля настройки. В поле «Запрашивается только префикс IPv6» необходимо установить флажок для того, чтобы запрашивать только префикс IPv6, но не его адрес. В поле «Размер делегирования префикса» необходимо выбрать значения делегируемого префикса. В поле «Отправить prefix-hint IPv6» необходимо установить флажок для отправки prefix-hint IPv6. В поле «Отправлять сообщение SOLOCIT» необходимо установить флажок для предотвращения бесконечного ожидания объявления маршрута. В поле «Предупреждение отправки» необходимо установить флажок для того, чтобы не отправлять сообщение о выходе клиента. В поле «Включить отладку» необходимо установить флажок для включения отладки для DHCPv6. В поле «Использовать IPv4-подключение» необходимо установить флажок для использования IPv4-подключения. В поле «Примените приоритет VLAN» необходимо выбрать приоритет VLAN (Рисунок 214).

The screenshot shows the 'DHCPv6 client configuration' window. At the top, there's a title bar 'Конфигурация DHCPv6-клиента'. Below it, a tabbed interface has three tabs: 'Режим настройки' (selected), 'Дополнительно', and 'Перезапись файла конфигурации'. The 'Режим настройки' tab contains several settings:

- 'Запрашивается только префикс IPv6': A checkbox that is currently unchecked.
- 'Размер делегирования префикса': A dropdown menu with '64' selected.
- 'Отправить хинт IPv6-префикса': A checkbox that is currently unchecked.
- 'Предупреждение отправки': A checkbox that is checked.
- 'Включить отладку': A checkbox that is checked.
- 'Использовать IPv4-подключение': A checkbox that is checked.
- 'Примените приоритет VLAN': A dropdown menu with 'Отключена' selected.

Рисунок 214 – Интерфейсы: [Название интерфейса]: Конфигурация DHCPv6 (Базовая)

Если в поле «Режим настройки» выбран пункт «Дополнительно», появятся следующие поля настройки. В поле «Отправлять сообщение SOLOCIT» необходимо установить флажок для предотвращения бесконечного ожидания объявления маршрута. В поле «Предупреждение отправки» необходимо установить флажок для того, чтобы не отправлять сообщение о выходе клиента. В поле «Включить отладку» необходимо установить флажок для включения отладки для DHCPv6. В поле «Использовать IPv4-подключение» необходимо установить флажок для использования IPv4-подключения. В поле «Примените приоритет VLAN» необходимо выбрать приоритет VLAN. В поле «Оператор Интерфейса» необходимо

установить флажок напротив поля «Только информация» для того, чтобы заменять параметры информационной конфигурации с серверами, в поле «Параметры отправки» необходимо ввести опции DHCP, передаваемые в ответ на запрос DHCP, в поле «Параметры Запроса» необходимо ввести опции DHCP, которые будут переданы на запрос DHCP, в поле «Сценарий» необходимо ввести абсолютный путь к скрипту. В поле «Объединение идентификации» необходимо установить флажок напротив поля «Постоянное выделение адресов» для постоянного выделения адресов и напротив поля «Делегирование префикса» для делегирования префикса. В полях в поле «Префикс интерфейса» необходимо ввести префикс и его длину в соответствующих полях. В полях «Аутентификация» необходимо ввести имя, по которому происходит авторизации, протокол, алгоритм, rdm. В полях «Информация о ключе» необходимо ввести в соответствующих полях имя ключа, realm (область авторизации), идентификатор ключа (32 битный идентификатор ключа), secret (значение ключа), окончание функции (время истечения срока действия ключа, если ключ бессрочен необходимо ввести «0») (Рисунок 215).

Конфигурация DHCPv6-клиента

1 Режим настройки	<div>Базовая</div> <div>Дополнительно</div> <div>Перезапись файла конфигурации</div>
1 Предупреждение отправки	<input type="checkbox"/>
1 Включить отладку	<input type="checkbox"/>
1 Использовать IPv4-подключение	<input type="checkbox"/>
1 Примените приоритет VLAN	Отключена
1 Оператор Интерфейса	<input type="checkbox"/> Только информация Параметры отправки Параметры Запроса Сценарий
1 Объединение идентификации	<input type="checkbox"/> Постоянное выделение адресов <input type="checkbox"/> Делегирование префикса
1 Префикс интерфейса	Префикс интерфейса, Длина слияния на уровне сайта
1 Аутентификация	authname test protocol Алгоритм idm
1 Информация о ключе	keyname test keyid test secret expire

Рисунок 215 – Интерфейсы: [Название интерфейса]: Конфигурация DHCPv6 (Дополнительно)

Если в поле «Режим настройки» выбран пункт «Перезапись файла конфигурации», появятся следующие настройки. В поле «Отправлять сообщение SOLOCIT» необходимо установить флажок для предотвращения бесконечного ожидания объявления маршрута. В поле «Предупреждение отправки» необходимо установить флажок для того, чтобы не отправлять сообщение о выходе клиента. В поле «Включить отладку» необходимо установить флажок для включения отладки для DHCPv6. В поле «Использовать IPv4-подключение» необходимо установить флажок для использования IPv4-подключения. В поле «Примените приоритет VLAN» необходимо выбрать приоритет VLAN. В поле «Перезапись файла

конфигурации» необходимо ввести полный абсолютный путь к файлу конфигурации DHCPv6 (Рисунок 216).

Конфигурация DHCPv6-клиента	
Режим настройки	Базовая Дополнительно Перезапись файла конфигурации
Предупреждение отправки	<input checked="" type="checkbox"/>
Включить отладку	<input checked="" type="checkbox"/>
Использовать IPv4-подключение	<input checked="" type="checkbox"/>
Примените приоритет VLAN	Отключена
Перезапись файла конфигурации	test

Рисунок 216 – Интерфейсы: [Название интерфейса]: Конфигурация DHCPv6 (Перезапись файла конфигурации)

При выборе в поле «Тип конфигурации IPv6» тип конфигурации «SLAAC» появится группа настроек «Конфигурация SLAAC». В поле «Использовать IPv4-подключение» необходимо установить флажок для включения IPv4-подключения (Рисунок 217).

Конфигурация SLAAC	
Использовать IPv4-подключение	<input checked="" type="checkbox"/>

Рисунок 217 – Интерфейсы: [Название интерфейса]: SLAAC

При выборе в поле «Тип конфигурации IPv6» тип конфигурации «Туннель 6RD» появится группа настроек «Конфигурация 6RD». В поле «Префикс 6RD» необходимо ввести IPv6-префикс 6RD-сегмента. В поле «Граничный передатчик 6RD» необходимо ввести IPv6-адрес 6RD-шлюза. В поле «Длина IPv6-префикса 6RD-сегмента» необходимо выбрать значение длины префикса 6RD-сегмента (Рисунок 218).

Быстрое развертывание 6RD	
Префикс 6RD	2001:db8::/32
Граничный передатчик 6rd	
Длина IPv6-префикса 6rd-сегмента	0 бит
6RD IPv4 префикс адреса	Автодетектирование

Рисунок 218 – Интерфейсы: [Название интерфейса]: 6RD

При выборе в поле «Тип конфигурации IPv6» тип конфигурации «Отслеживать состояние интерфейсов» появится группа настроек «Отслеживать IPv6-интерфейсы». В поле «IPv6-интерфейс» необходимо выбрать динамический IPv6-адрес WAN интерфейса, который будет отслеживаться для конфигурации. В поле «Идентификатор IPv6-префикса» необходимо ввести значение идентификатора IPv6-префикса. В поле «Ручное конфигурирование» необходимо установить флажок для включения ручной настройки DHCPv6 и маршрутизатора (Рисунок 219).

Отслеживать IPv6-интерфейсы	
IPv6-интерфейс	Не выбрано
Идентификатор IPv6-префикса	0x 0
Ручное конфигурирование	<input type="checkbox"/> Разрешить ручную настройку DHCPv6 и объявления маршрута

Рисунок 219 – Интерфейсы: [Название интерфейса]: Отслеживать состояние интерфейсов

После внесения изменений необходимо нажать на кнопку «Сохранить».

7.2 Подраздел «Назначение портов»

Подраздел «Назначение портов» позволяет настраивать соответствие между логическими и физическими сетевыми интерфейсами. Для этого необходимо выбрать в выпадающем списке напротив логического сетевого интерфейса соответствующий ему физический сетевой интерфейс. Для удаления сетевого интерфейса необходимо нажать на кнопку соответствующий значок напротив сетевого интерфейса (Рисунок 220). Для сохранения настроек необходимо нажать на кнопку «Сохранить».

Интерфейсы: Назначения портов






Интерфейс	Сетевой порт	
<u>LAN</u>	 em0 (00:0c:29:a2:e9:87) ▼	
Новый интерфейс:	 em1 (00:0c:29:a2:e9:91) ▼	
	Описание <input type="text"/>	
 Сохранить		

Рисунок 220 – Интерфейсы: Назначение портов

7.3 Подраздел «Обзор»

Подраздел «Обзор» позволяет просматривать следующую информацию о каждом настроенном сетевом интерфейсе (Рисунок 221):

- статус интерфейса;
- MAC-адрес интерфейса;
- IPv4-адрес;
- маску подсети IPv4;
- локальный IPv6-адрес канала;
- скорость и двусторонний режим передачи данных;
- количество входящих/исходящих пакетов (их суммарный размер);
- количество разрешенных входящих/исходящих пакетов (их суммарный размер);
- количество заблокированных входящих/исходящих пакетов (их суммарный размер);
- количество коллизий;
- прерывания.

Интерфейсы: Обзор

▼ LAN интерфейс (lan, em0)				
Статус	up			
MAC-адрес	00:0c:29:a2:e9:87 - VMware, Inc.			
Максимальный размер кадра	1500			
IPv4-адрес	192.168.1.1 / 24			
Локальный IPv6-адрес канала	fe80::20c:29ff:fea2:e987 / 64			
Медиа	1000baseT <full-duplex>			
Входящие/исходящие пакеты	745 / 1513 (79 KB / 1.81 MB)			
Входящие/исходящие пакеты (разрешить)	609 / 1513 (69 KB / 1.81 MB)			
Входящие/исходящие пакеты (блокировать)	9672 / 0 (136 bytes / 0 bytes)			
Входящие/исходящие ошибки	0/0			
Коллизии	0			
Прерывания	irq	устройство	всего	частота
	irq19	em0 em1	1047	0

Режим «Соединение по запросу» снова инициализирует соединение, если приходит пакет, предназначенный хосту, находящемуся в удаленной подсети. Примечание: разрыв соединения пользователем не предотвращает подключения к внешним хостам. Не используйте этот режим, если хотите убедиться, что линия

Рисунок 221 – Интерфейсы: Обзор

7.4 Подраздел «Настройки»

В подразделе «Настройки» приведены общие настройки интерфейсов.

В пункте «CRC аппаратного обеспечения» необходимо установить флажок напротив поля «Отключить сброс контрольной суммы аппаратного обеспечения» для отключения расчета контрольной суммы Ethernet-кадра средствами сетевой карты без участия ЦПУ. В поле «TSO аппаратного обеспечения» необходимо установить флажок напротив поля «Отключить сброс сегментации TCP аппаратного обеспечения» для отключения сброса сегментации TCP-пакета без участия ЦПУ с помощью аппаратных возможностей сетевой карты. В поле «LRO аппаратного обеспечения» необходимо установить флажок напротив поля «Отключить LRO аппаратного обеспечения» для отключения буферизации входящих пакетов и их передачи сетевому стеку в агрегированном виде с целью избежания неэффективной передачи каждого пакета в отдельности. В поле «Фильтрация аппаратного обеспечения VLAN» необходимо выбрать степень использования фильтра VLAN. В поле «Обработка ARP» необходимо установить флажок напротив поля «Блокировать ARP» для того, чтобы заблокировать сообщения в журнале регистрации ARP, если несколько сетевых интерфейсов хранятся на одном широкополосном домене. В поле «Уникальный идентификатор DHCP» необходимо ввести уникальный идентификатор DHCP (Рисунок 222). Необходимо нажать на кнопку «Сохранить» для сохранения настроек.

Интерфейсы: Другие типы: Сетевой мост

[+ Добавить](#)




Интерфейс	Участники	Описание	Link-local	
bridge0	LAN	test	Вкл.	 


Рисунок 223 – Интерфейсы: Другие типы: Сетевой мост

Для того чтобы редактировать существующие сетевые мосты, необходимо нажать на кнопку  напротив сетевого моста. Для того чтобы создать новый сетевой мост, необходимо нажать на кнопку [+ Добавить](#).

При редактировании сетевого моста в поле «Интерфейсы-участники» необходимо выбрать интерфейсы, соединенные с помощью этого моста. В поле «Описание» необходимо ввести описание сетевого моста (Рисунок 224).

Интерфейсы: Другие типы: Сетевой мост

Конфигурация сетевого моста

справка 

Интерфейсы-участники

LAN

Описание

Link-local адрес

☐ Включить link-local адрес

Показать дополнительные параметры

Сохранить

Отменить

Рисунок 224 – Интерфейсы: Другие типы: Сетевой мост (редактирование)

При нажатии кнопки «Показать дополнительные параметры» появятся следующие группы настроек.

В группе настроек «Протокол связующего дерева (RSTP/STP)» в поле «Включить» необходимо установить флажок для включения протокола связующего дерева (RSTP/STP) для этого моста. В поле «Протокол» необходимо выбрать протокол связующего дерева. В поле «STP-интерфейсы» необходимо выбрать интерфейс для работы протокола связующего дерева. В поле «Действительное время (с)» необходимо ввести время действия конфигурации протокола связующего дерева. В поле «Время приветствия (с)» необходимо ввести интервал времени между широковещательными конфигурационными сообщениями связующего дерева. В поле «Приоритет» необходимо ввести приоритет сетевого моста для связующего дерева. В поле «Счетчик задержки» необходимо ввести значение счетчика задержки для передачи по протоколу связующего дерева. В

полях в поле «Приоритет» необходимо установить приоритет для каждого интерфейса. В поле «Стоимость пути» необходимо ввести стоимость порта для каждого интерфейса. Каждый порт имеет свою стоимость (cost), обратно пропорциональную пропускной способности (bandwidth) порта и которую можно настраивать вручную (Рисунок 225).

Протокол остоного дерева (RSTP/STP)		
Включен	<input checked="" type="checkbox"/>	
Протокол	RSTP	
STP-интерфейсы:	Не выбрано	
Действительное время (секунды)	1	
Время смены состояний (секунды)	1	
Время приветствия (секунды)	2	
Приоритет	45	
Счетчик задержки	34	
Приоритет	Internet	
	LAN	2
	WAN	
Стоимость пути	Internet	
	LAN	2
	WAN	

Рисунок 225 – Интерфейсы: Другие типы: Сетевой мост (редактирование: Протокол связующего дерева (RSTP/STP))

В группе настроек «Дополнительные параметры» в поле «Размер кэша (записей)» необходимо ввести значение размера кэша адресов сетевого моста. В поле «Время жизни адреса в кэше (с)» необходимо ввести время нахождения записи адреса в кэше адресов в секундах. В поле «Порт SPAN» необходимо выбрать интерфейс, который будет использоваться в качестве SPAN порта на мосту. В поле «Пограничный порт» необходимо выбрать интерфейс, который будет использоваться в качестве пограничного порта. В поле «Автоопределение граничного порта» необходимо выбрать сетевой интерфейс, для которого будет определяться автоматически граничный порт. В поле «Фиксированные порты» необходимо выбрать интерфейсы, которые будут отмечены как «фиксированные» интерфейсы. В поле «Частные порты» необходимо выбрать интерфейс, который будет отмечен как «частный» (Рисунок 226).

Дополнительные параметры

i
Размер кэша (записей)

50

i
Время жизни адреса в кэше (с)

180

i
Порт SPAN

Отсутствует

i
Пограничный порт

LAN

i
Автоопределение граничного порта

Не выбрано

i
Фиксированные порты

Не выбрано

i
Частные порты

Не выбрано

Рисунок 226 – Интерфейсы: Другие типы: Сетевой мост (редактирование: Дополнительные параметры)

После внесения изменений необходимо нажать на кнопку «Сохранить».

7.5.2 Категория «LAGG»

Интерфейс LAGG используется для объединения нескольких сетевых интерфейсов в один виртуальный интерфейс для обеспечения аварийного переключения и агрегации каналов.

В категории «LAGG» отображаются настроенные интерфейсы LAGG в виде таблицы с возможностью удаления и редактирования, нажав на соответствующие кнопки напротив интерфейса LAGG. Таблица содержит следующие данные (Рисунок 227):

- название интерфейса LAGG;
- удаленный IP-адрес пира интерфейса LAGG;
- описание.


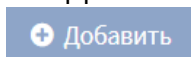
Интерфейсы: Другие типы: LAGG

Добавить

Интерфейс	Участники	Протокол	Описание
LAGG0	em0	LACP	test

LAGG позволяет агрегировать каналы, такое объединение позволяет увеличивать пропускную способность и надежность канала. Добавлять можно только неназначенные интерфейсы.

Рисунок 227 – Интерфейсы: Другие типы: LAGG

Для того чтобы редактировать существующие интерфейсы LAGG, необходимо нажать на кнопку  напротив интерфейса LAGG. Для того чтобы создать новый интерфейс LAGG, необходимо нажать на кнопку .

При редактировании интерфейса LAGG в поле «Родительский интерфейс» необходимо выбрать не назначенные интерфейсы, которые могут использоваться для агрегации каналов. В поле «Протокол LAG» необходимо выбрать протокол:

- FAILOVER (посылает и принимает трафик только через главный порт, если главный порт недоступен, используется следующий активный порт. Первый добавленный интерфейс является ведущим, все добавленные после ведущего интерфейсы используются в качестве аварийных и включаются в работу при обрыве соединения);
- FEC (поддерживает технологию Cisco EtherChannel);
- LACP (поддерживает протокол агрегирования каналов (LACP) и протокол маркирования, описанные в IEEE 802.3ad. LACP согласовывает набор агрегированных ссылок с узлом в одну или несколько групп агрегированных каналов (LAG));
- LOADBALANCE (балансирует трафик между активными портами на основе хешированной информации в заголовке протокола и принимает входящий трафик из любого активного порта);
- ROUNDROBIN (исходящий трафик распределяется циклическим планировщиком через все активные порты, а входящий трафик принимается с любого активного порта);
- NONE (этот протокол приостанавливает работу: отключает любой трафик без отключения самого LAGG-интерфейса).

В поле «Описание» необходимо ввести описание интерфейса (Рисунок 228).

Интерфейсы: Другие типы: LAGG






Конфигурация LAGG	
 Родительский интерфейс	Не выбрано
 Протокол LAG	LACP
 Описание	test
 Короткий тайм-аут	<input checked="" type="checkbox"/>
 Максимальный размер кадра	
<div>Сохранить Отменить</div>	

Рисунок 228 – Интерфейсы: Другие типы: LAGG (редактирование)

После внесения изменений необходимо нажать на кнопку «Сохранить».

7.5.3 Категория «Loopback»

В категории «Loopback» отображаются настроенные локальные интерфейсы (loopback интерфейсы) в виде таблицы с возможностью удаления и редактирования существующих интерфейсов, а также создания новых, нажав на соответствующие кнопки напротив интерфейса Loopback (Рисунок 229).

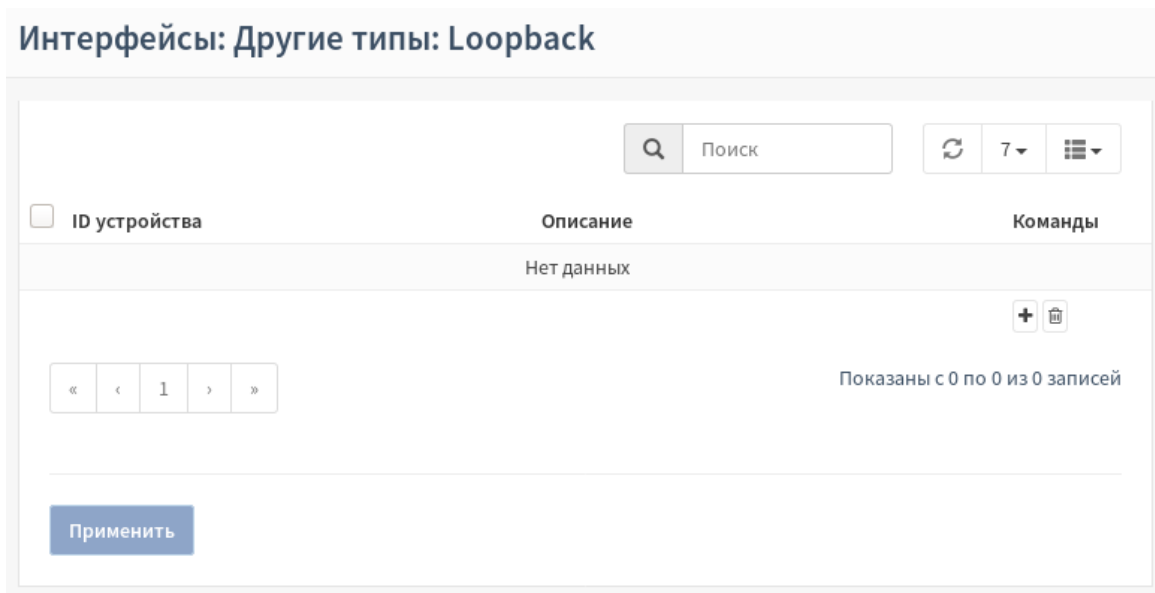




Рисунок 229 – Интерфейсы: Другие типы: Loopback

Для того чтобы редактировать существующие интерфейсы Loopback, необходимо нажать на кнопку  напротив интерфейса Loopback. Для того чтобы создать новый интерфейс Loopback необходимо нажать на кнопку .

ID устройства присваивается автоматически. В поле «Описание» необходимо добавить описание интерфейса (Рисунок 230).

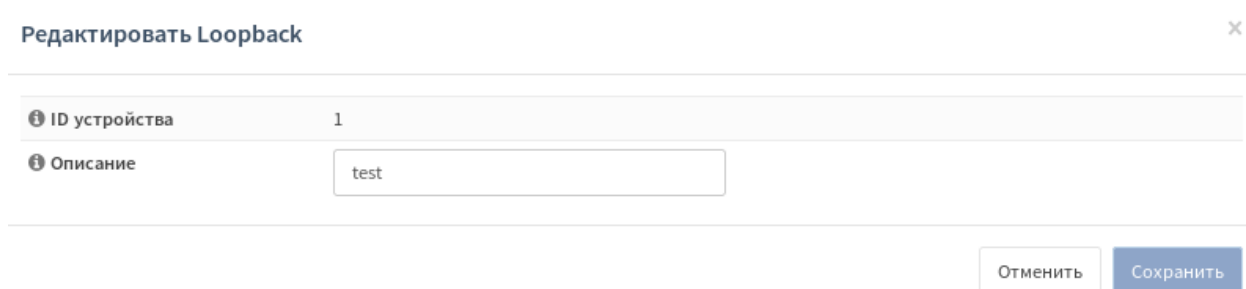


Рисунок 230 – Интерфейсы: Другие типы: Loopback (редактирование)

7.5.4 Категория «VLAN»



В категории «VLAN» отображаются настроенные интерфейсы VLAN в виде таблицы с возможностью удаления и редактирования существующих интерфейсов, а также создания новых, нажав на соответствующие кнопки напротив интерфейса VLAN. Таблица содержит следующие данные (Рисунок 231):

- название интерфейса VLAN;

- тег;
- приоритет;
- описание.


Интерфейсы: Другие типы: VLAN

[+ Добавить](#)

Интерфейс	Тег	PCP	Описание	
em0	1024	0	test	 

Не все драйверы/сетевые платы корректно поддерживают 802.1Q VLAN-тегирование. В таком случае VLAN-тегирование все равно будет работать, но уменьшенный MTU может вызвать проблемы.


Рисунок 231 – Интерфейсы: Другие типы: VLAN

Для того чтобы редактировать существующие интерфейсы VLAN, необходимо нажать на кнопку  напротив интерфейса VLAN. Для того чтобы создать новый интерфейс VLAN, необходимо нажать на кнопку [+ Добавить](#).

При редактировании интерфейса VLAN в поле «Родительский интерфейс» необходимо выбрать сетевые интерфейсы, которые будут использоваться для агрегации каналов. В поле «Тег VLAN» необходимо ввести тег VLAN. В поле «Приоритет VLAN» необходимо выбрать приоритет VLAN. В поле «Описание» необходимо ввести описание интерфейса (Рисунок 232).


Интерфейсы: Другие типы: VLAN

Редактировать VLAN-интерфейс




Родительский интерфейс

em0 (08:00:27:b4:d6:4e)




Тег VLAN

1024



Приоритет VLAN

Хорошая доставка (0, по-умолчанию)



Описание

test

Сохранить

Отменить

Рисунок 232 – Интерфейсы: Другие типы: VLAN (редактирование)

После внесения изменений необходимо нажать на кнопку «Сохранить».

7.5.5 Категория «VXLAN»

В категории «VXLAN» отображаются настроенные интерфейсы VXLAN в виде таблицы с возможностью удаления и редактирования существующих интерфейсов, а также создания новых, нажав на соответствующие кнопки напротив интерфейса VXLAN.

Интерфейсы: Другие типы: VXLAN

Поиск

7


<input type="checkbox"/> ID устройства	VNI	Отправитель	Команды
Нет данных			

« 1 »


Показаны с 0 по 0 из 0 записей







Применить

Рисунок 233 – Интерфейсы: Другие типы: VXLAN

Для добавления интерфейса VXLAN необходимо нажать на кнопку . В поле «ID-устройства» значение устанавливается по умолчанию. В поле «VNI» необходимо ввести VXLAN идентификатор сети. В поле «IP-адрес источника» необходимо указать адрес отправителя, используемый в инкапсулированном IPv4/IPv6. В поле «Удаленный шлюз» необходимо указать IP-адрес удаленного конца туннеля. В поле «Широковещательная группа» необходимо указать IP-адрес широковещательной группы, к которой присоединится интерфейс. В поле «Устройство» необходимо выбрать интерфейс (Рисунок 234).

Редактировать VxLan

справка 

 ID устройства	0
 VNI	
 IP-адрес источника	192.168.1.1
 Удаленный адрес	192.168.2.3
 Широковещательная группа	
 Устройство	WAN

Отменить Сохранить

Рисунок 234 – Интерфейсы: Другие типы: VXLAN (редактирование)

После внесения изменений необходимо нажать на кнопку «Сохранить».

7.6 Подраздел «Диагностика»

Подраздел «Диагностика» позволяет просматривать таблицу ARP, запускать сканирование ARP, просматривать таблицу DNS-записей, просматривать таблицу NDP-записей, экспортировать дампы трафика определенного сетевого интерфейса, выполнять и просматривать результаты команды «Ping», выполнять проверку порта (имеется ли на нем подключение), выполнять trace route.

7.6.1 Категория «ARP-таблица»

В категории «ARP-таблица» отображается ARP-таблица с возможностью удаления данных и обновления, нажав на соответствующие кнопки. Таблица содержит следующие данные (Рисунок 235):

- IP-адрес;
- MAC-адрес;
- производитель;
- название физического интерфейса;
- название сетевого интерфейса;
- имя хоста.

Интерфейсы: Диагностика: ARP-таблица

						<input type="text" value="Поиск"/> 10	
IP-адрес	MAC-адрес	Производитель	Интерфейс	Имя интерфейса	Имя хоста		
192.168.1.3	08:00:27:2c:28:85	PCS Systemtechnik GmbH	em3	OPT2			
172.16.0.2	08:00:27:e4:36:61	PCS Systemtechnik GmbH	em2	PFSYNC			
192.168.3.3	08:00:27:28:4d:38	PCS Systemtechnik GmbH	em1	lan			
192.168.3.34	08:00:27:74:f5:bf	PCS Systemtechnik GmbH	em1	lan			
192.168.3.254	0a:00:27:00:00:0c		em1	lan			

ПРИМЕЧАНИЕ: Локальные IPv6 пиры используют протокол NDP вместо ARP.

« < 1 > »

Показаны с 1 по 5 из 5 записей

Очистить Обновить

Рисунок 235 – Интерфейсы: Диагностика: ARP-таблица

7.6.2 Категория «Просмотр DNS-записей»

В категории «Просмотр DNS-записей» осуществляется поиск IP-адресов и записей, принадлежащих заданному имени хоста, а также отображается следующая информация (Рисунок 236):

- ответ (тип и IP-адрес);
- время разрешения сервером доменных имен и/или IP-адресов (сервер, время запроса);
- дополнительная информация).

Интерфейсы: Диагностика: Просмотр DNS-записей

Преобразовать DNS-имя или IP-адрес

Имя хоста или IP-адрес

Ответ

Тип

Адрес

192.168.3.34

Время разрешения сервером доменных имен и/или IP-адресов

Сервер

Время запроса

127.0.0.1

43 msec

Дополнительная информация:

Ping

Трассировка прохождения

ПРИМЕЧАНИЕ: следующие каналы к внешним службам могут быть ненадежными.

IP WHOIS @ DNS Stuff

IP Info @ DNS Stuff

Просмотр DNS-записей

Рисунок 236 – Интерфейсы: Диагностика: Просмотр DNS-записей

7.6.3 Категория «NDP-таблица»

В категории «NDP-таблица» отображается NDP-таблица, в которой перечислены локально подключенные узлы IPv6, с возможностью удаления данных и обновления, нажав на соответствующие кнопки. Таблица содержит следующие данные (Рисунок 237):

- IP-адрес;
- MAC-адрес;
- производитель;
- название физического интерфейса;
- название сетевого интерфейса.

Интерфейсы: Диагностика: NDP-таблица

Поиск

10

IPv6	MAC-адрес	Производитель	Интерфейс	Имя интерфейса
fe80::a00:27ff:feb4:d64e%em0_vlan1024	08:00:27:b4:d6:4e	PCS Systemtechnik GmbH	em0_vlan1024	
fe80::a00:27ff:feb4:d64e%lagg0	08:00:27:b4:d6:4e	PCS Systemtechnik GmbH	lagg0	
fe80::a00:27ff:fe2c:2885%em3	08:00:27:2c:28:85	PCS Systemtechnik GmbH	em3	OPT2
fe80::a00:27ff:fee4:3661%em2	08:00:27:e4:36:61	PCS Systemtechnik GmbH	em2	PFSYNC
fe80::a00:27ff:fe28:4d38%em1	08:00:27:28:4d:38	PCS Systemtechnik GmbH	em1	lan

Показаны с 1 по 5 из 5 записей

Обновить

Рисунок 237 – Интерфейсы: Диагностика: NDP-таблица

7.6.4 Категория «Netstat»

В категории «Netstat» отображается статистика работы с сетевыми интерфейсами в группированном виде (Рисунок 238):

- bpf-статистика;
- статистика по интерфейсам;
- mbuf-статистика;
- netisr;
- статистика по протоколам;

- статистика по сокетам.

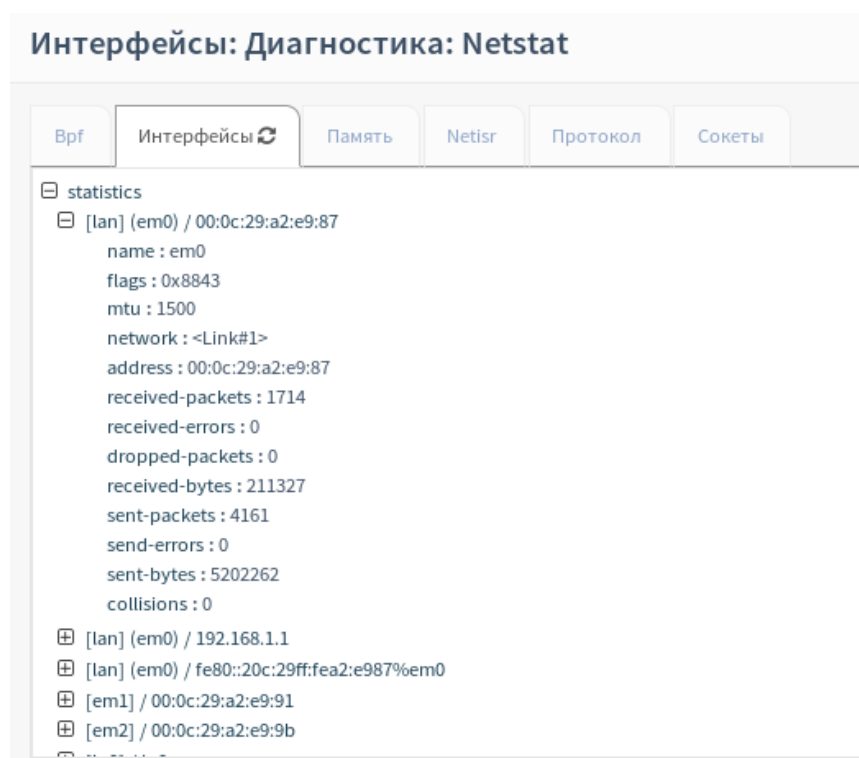


Рисунок 238 – Интерфейсы: Диагностика: Netstat

7.6.5 Категория «Захват пакетов»

Категория «Захват пакетов» позволяет запустить сканирование сети с возможностью дальнейшего экспорта по выбранному интерфейсу.

Для этого в группе настроек «Захват пакетов» в поле «Интерфейсы» необходимо выбрать интерфейсы для захвата трафика. В поле «Смешанный режим» необходимо установить флажок для того, чтобы принимать все пакеты, независимо от того, кому они адресованы. В поле «Семейство адресов» необходимо выбрать тип трафика для захвата. В поле «Протокол» необходимо выбрать протокол для захвата трафика. В поле «IP-адрес хоста» необходимо ввести IP-адрес источника. В поле «Порт» необходимо ввести порт. В поле «Длина пакета» необходимо ввести длину пакета (в битах). В поле «Количество» необходимо ввести количество пакетов, которые будут захватываться (Рисунок 239).

Интерфейсы: Диагностика: Захват пакетов

Захват пакетов	
<i>i</i> Интерфейс	LAN ▾
<i>i</i> Смешанный режим	<input type="checkbox"/>
<i>i</i> Семейство адресов	Только IPv4 ▾
<i>i</i> Протокол	Любой ▾
<i>i</i> IP-адрес хоста	<input type="text"/>
<i>i</i> Порт	<input type="text"/>
<i>i</i> Длина пакета	<input type="text"/>
<i>i</i> Количество	100

Рисунок 239 – Интерфейсы: Диагностика: Захват пакетов (настройка захвата пакетов)

В группе настроек «Просмотр настроек» в поле «Уровень детализации» необходимо выбрать уровень детализации информации о захваченных пакетах. В поле «Обратный запрос DNS» необходимо установить флажок для захвата пакетов, ассоциируемых со всеми IP-адресами обратного запроса DNS. Для начала захвата необходимо нажать на кнопку «Запустить». Для остановки захвата пакетов необходимо нажать на кнопку «Остановить». Для скачивания захваченных пакетов необходимо нажать на кнопку «Скачать захваченные пакеты». Для удаления захваченных пакетов необходимо нажать на кнопку «Удалить захваченные пакеты». Для просмотра захваченных пакетов необходимо нажать на кнопку «Просмотр захваченных пакетов», появится таблица с результатами захвата пакетов (Рисунок 240).

Просмотр настроек.

Уровень детализации: Нормальный

Обратный запрос DNS: ☐

Запустить Просмотр захваченных пакетов Удалить захваченные пакеты

Скачать захваченные пакеты

packetcapture_em0.cap

Интерфейс	Результат захвата пакетов
LAN em0	17:24:38.024789 IP 192.168.1.100.53376 > 192.168.1.1.443: tcp 541
LAN em0	17:24:38.024935 IP 192.168.1.1.443 > 192.168.1.100.53376: tcp 0
LAN em0	17:24:38.078975 IP 192.168.1.1.443 > 192.168.1.100.53376: tcp 1448
LAN em0	17:24:38.079184 IP 192.168.1.1.443 > 192.168.1.100.53376: tcp 1448
LAN em0	17:24:38.079329 IP 192.168.1.1.443 > 192.168.1.100.53376: tcp 1448

Рисунок 240 – Интерфейсы: Диагностика: Захват пакетов (настройка просмотра)

7.6.6 Категория «Ping»

Категория «Ping» позволяет выполнить команду «ping», чтобы проверить наличие доступа к устройству. Для этого в поле «Хост» необходимо ввести IP-адрес устройства, наличие доступа к которому надо проверить. В поле «Протокол IP» необходимо ввести версию протокола IP. В поле «IP-адрес источника» необходимо выбрать IP-адрес источника. В поле «Количество» необходимо выбрать количество отсылаемых пакетов. Необходимо нажать на кнопку «Ping» (Рисунок 241).

Интерфейсы: Диагностика: Ping

Хост	192.168.3.34
Протокол IP	IPv4
IP-адрес источника	По умолчанию.
Количество	3
Ping	

Рисунок 241 – Интерфейсы: Диагностика: Ping

Результат команды ping будет показан внизу страницы (Рисунок 242).

Результат команды ping

```
PING 192.168.3.34 (192.168.3.34): 56 data bytes
64 bytes from 192.168.3.34: icmp_seq=0 ttl=64 time=0.572 ms
64 bytes from 192.168.3.34: icmp_seq=1 ttl=64 time=0.337 ms
64 bytes from 192.168.3.34: icmp_seq=2 ttl=64 time=0.231 ms

--- 192.168.3.34 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.231/0.380/0.572/0.142 ms
```

Рисунок 242 – Интерфейсы: Диагностика: Ping (результаты работы команды)

7.6.7 Категория «Проверка порта»

Категория «Проверка порта» позволяет выполнить простой тест соединения TCP, чтобы определить, работает ли и принимает ли хост соединения на данном порте. Этот тест не работает для UDP, потому что нет никакого способа надежно определить, принимает ли порт UDP-соединение этим способом.

Для проверки порта поле «Хост» необходимо ввести адрес хоста. В поле «Порт» необходимо ввести порт. В поле «Протокол IP» необходимо выбрать версию протокола IP. В поле «IP-адрес источника» необходимо ввести IP-адрес источника и необходимо нажать на кнопку «Проверка». В поле «Порт источника» необходимо ввести порт источника. В поле «Показать текст с удаленного сервера» необходимо установить флажок для того, чтобы показать текст, полученный от сервера при попытке подключиться к порту (Рисунок 243).

Интерфейсы: Диагностика: Проверка порта

Эта веб-страница позволяет выполнить простой тест соединения TCP, чтобы определить, работает ли и принимает ли хост соединения на данном порте. Этот тест не работает для UDP, потому что нет никакого способа надежно определить, принимает ли порт UDP-соединение этим способом.

Цель этого теста — открыть соединение и отобразить возврат данных сервером (опционально), никакие данные удаленному хосту отправлены не будут.

Проверка порта		справка ⓘ
❗ Хост	<input type="text" value="192.168.3.34"/>	
❗ Порт	<input type="text" value="80"/>	
❗ Протокол IP	<input type="text" value="IPv4"/>	
❗ IP-адрес источника	<input type="text" value="По умолчанию"/>	
❗ Порт источника	<input type="text"/>	
❗ Показать текст с удаленного сервера	<input type="checkbox"/>	
<input type="button" value="Проверка"/>		

Рисунок 243 – Интерфейсы: Диагностика: Проверка порта

Результат проверки порта будет показан внизу страницы (Рисунок 244).

Результаты проверки порта

Connection to 192.168.3.34 80 port [tcp/http] succeeded!

Рисунок 244 – Интерфейсы: Диагностика: Проверка порта (результат)

7.6.8 Категория «Маршрут трассировки»

Категория «Маршрут трассировки» позволяет выполнить команду trace route. Для этого в поле «Хост» необходимо ввести хост. В поле «Протокол IP» необходимо выбрать версию протокола IP. В поле «IP-адрес источника» необходимо выбрать IP-адрес источника. В поле «Максимальное количество переходов» необходимо выбрать максимальное количество переходов. В поле «Обратное преобразование адресов» необходимо установить флажок для обратного преобразования адресов. В поле «Использовать ICMP» необходимо установить флажок для использования протокола ICMP. Необходимо нажать на кнопку «Трассировка прохождения» (Рисунок 245).

Интерфейсы: Диагностика: Маршрут трассировки

Хост	<input type="text" value="192.168.3.34"/>
Протокол IP	<input type="text" value="IPv4"/>
IP-адрес источника	<input type="text" value="По умолчанию."/>
Максимальное количество переходов	<input type="text" value="18"/>
Обратное преобразование адресов	<input type="checkbox"/>
Использовать ICMP	<input type="checkbox"/>
<input type="button" value="Трассировка прохождения"/>	

Рисунок 245 – Интерфейсы: Диагностика: Маршрут трассировки

Результат выполнения команды Trace Route будет показан внизу страницы (Рисунок 246).

Результат выполнения маршрутизации

```
tracert to 192.168.3.34 (192.168.3.34), 3 hops max, 48 byte packets
 1  192.168.3.34  1.593 ms  1.041 ms  1.544 ms
```

Рисунок 246 – Интерфейсы: Диагностика: Маршрут трассировки (результат)

8 РАЗДЕЛ «СЕТЬ»

Раздел «Сеть» позволяет анализировать дампы трафика на выбранных интерфейсах с помощью ПО TShark, просматривать доступные устройства с помощью ARPWatch для выбранных интерфейсов.

8.1 Подраздел «Обнаружение устройств»

Подраздел «Обнаружение устройств» позволяет просматривать таблицу подключенных устройств на выбранном сетевом интерфейсе.

8.1.1 Категория «Общие настройки»

Категория «Общие настройки» позволяет включить ARPwatch сервис и выбрать прослушиваемый сетевой интерфейс. Для включения ARPwatch сервиса необходимо поставить флажок напротив «Включен». В поле «Прослушиваемые интерфейсы» необходимо выбрать сетевые интерфейсы, которые необходимо прослушивать. Для сохранения настроек необходимо нажать кнопку «Сохранить» (Рисунок 247).

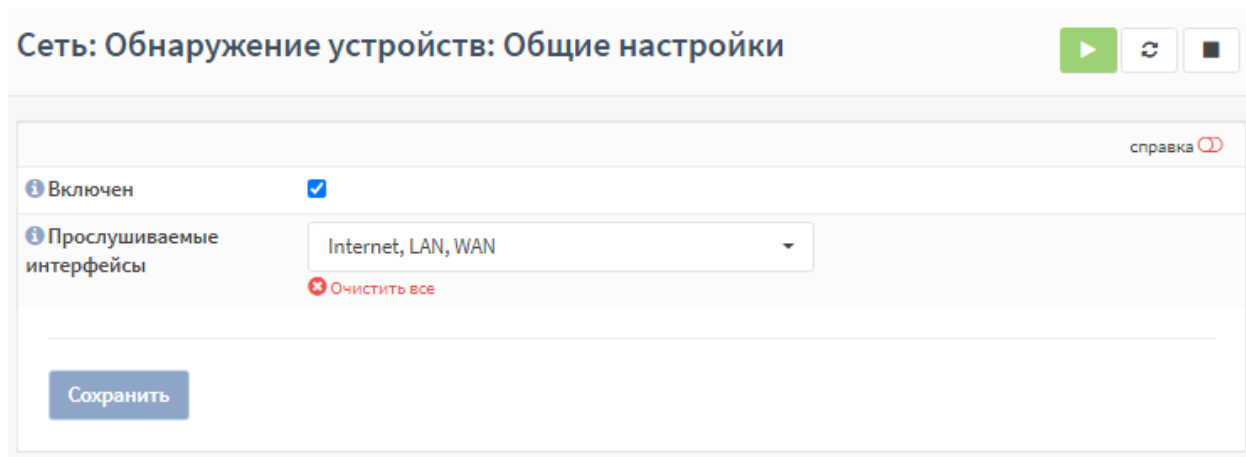


Рисунок 247 – Сеть: Обнаружение устройств: Общие настройки

8.1.2 Категория «Хосты»

В категории «Хосты» отображаются подключаемые устройства в виде таблицы на выбранном сетевом интерфейсе. Таблица содержит следующие данные (Рисунок 248):

- название физического интерфейса;
- MAC-адрес устройства;
- IP-адрес устройства;
- дата/время обнаружения устройства;
- состояние устройства (зарегистрировано/не зарегистрировано);
- тип;
- производитель;
- комментарий;
- хост;
- действия.

Сеть: Обнаружение устройств: Хосты



Записи не могут быть удалены, пока сервис работает


Интерфейс	MAC-адрес	IP-адрес	Дата	Зарегистрировано	Тип	Производитель	Комментарий	Хост	Действия
em1	00:50:56:EB:CE:9A	192.168.159.2	November 15, 2020 11:02 PM	<input type="checkbox"/>	Не определено	VMware, Inc.			
em1	00:0C29:69:DE:4D	192.168.159.140	November 15, 2020 11:02 PM	<input type="checkbox"/>	Не определено	VMware, Inc.			
em1	00:50:56:C0:00:08	192.168.159.1	November 15, 2020 11:01 PM	<input type="checkbox"/>	Не определено	VMware, Inc.			
em1	00:50:56:E1:8D:34	192.168.159.254	November 15, 2020 10:55 PM	<input type="checkbox"/>	Не определено	VMware, Inc.			
em0	00:0C29:FA:06:FB	192.168.1.200	November 15, 2020 11:03 PM	<input type="checkbox"/>	Не определено	VMware, Inc.			
em0	00:0C29:AB:82:C1	192.168.1.100	November 11, 2020 2:11 PM	<input type="checkbox"/>	Не определено	VMware, Inc.			
em0	00:0C29:69:DE:43	192.168.1.1	November 15, 2020 11:03 PM	<input type="checkbox"/>	Не определено	VMware, Inc.		атма	


Показаны с 1 по 7 из 7 записей

Рисунок 248 – Сеть: Обнаружение устройств: Хосты (при включенном ARPwatch сервисе)

Для редактирования/удаления устройства из таблицы необходимо отключить ARPwatch сервис. Для этого необходимо перейти в «Сеть» - «Обнаружение устройств» - «Общие настройки» и напротив поля «Включен» убрать флажок. Нажать кнопку «Сохранить» для сохранения внесенных изменений. На странице «Сеть» - «Обнаружение устройств» - «Хосты» появится возможность редактировать/удалять устройства.

Для удаления устройства необходимо нажать на кнопку  напротив устройства. Для удаления нескольких устройств необходимо поставить флажок напротив устройств в правом столбце таблицы и нажать кнопку  внизу таблицы.

Для удаления всех записей таблицы необходимо нажать кнопку  **Очистить все записи** внизу страницы.

Для редактирования устройства необходимо нажать на кнопку  напротив устройства. В окне редактирования хоста необходимо поставить флажок в «Зарегистрировано» для регистрации устройства. В поле «Комментарий» необходимо ввести описание устройства. Для сохранения необходимо нажать на кнопку «Сохранить».

8.2 Подраздел «Анализ трафика»

Подраздел «Анализ трафика» позволяет просматривать и анализировать входящие / исходящие пакеты по выбранному сетевому интерфейсу.


8.2.1 Категория «Журналирование»

Категория «Журналирование» позволяет просматривать захваченный трафик системой обнаружения вторжений в виде таблицы на выбранном интерфейсе, а именно следующую информацию (Рисунок 249):

- дата и время;
- IP-адрес отправителя;
- IP-адрес получателя;
- протокол;
- информация о пакете;
- дополнительная информация о трафике.

В поле «Файл не выбран» необходимо выбрать дамп трафика, захваченный системой обнаружения вторжений. Максимальное количество сохраняемых файлов – 20 файлов по 100 Мбайт каждый.

Для включения сбора дампов трафика необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Настройки». В поле «Включить» поставить флажок. В поле «Интерфейсы» выбрать прослушиваемые сетевые интерфейсы. Нажать кнопку «Сохранить».

Также поле «Фильтр отображения» позволяет осуществлять фильтрацию с помощью встроенных интерактивных фильтров. Для применения фильтра необходимо нажать кнопку .

Сеть: Анализ трафика: Журналирование

Нажмите кнопку обновления для обновления результатов после изменения фильтра

log.pcар.1576757973 ip.src==192.168.1.52

⌂ Все ▾

Дата	Отправитель	Получатель	Протокол	Содержание	Действия
19 декабря 2019, 12:19	192.168.1.52	192.168.1.20	TLSv1.2	436 Application Data	0
19 декабря 2019, 12:19	192.168.1.52	192.168.1.20	TCP	54 443 → 16471 [ACK] Seq=383 Ack=681 Win=507 Len=0	0
19 декабря 2019, 12:19	192.168.1.52	192.168.1.20	TCP	1514 [TCP segment of a reassembled PDU]	0
19 декабря 2019, 12:19	192.168.1.52	192.168.1.20	TCP	1514 443 → 16471 [ACK] Seq=1843 Ack=681 Win=513 Len=1460 [TCP segment of a reassembled PDU]	0
19 декабря 2019, 12:19	192.168.1.52	192.168.1.20	TCP	1514 443 → 16471 [ACK] Seq=3303 Ack=681 Win=513 Len=1460 [TCP segment of a reassembled PDU]	0
19 декабря 2019, 12:19	192.168.1.52	192.168.1.20	TCP	1514 443 → 16471 [ACK] Seq=4763 Ack=681 Win=513 Len=1460 [TCP segment of a reassembled PDU]	0

Рисунок 249 – Сеть: Анализ трафика: Журналирование

9 РАЗДЕЛ «МАРШРУТИЗАЦИЯ»

Раздел «Маршрутизация» позволяет настраивать динамическую маршрутизацию по следующим протоколам: RIP (v1, v2), OSPF, а также просматривать информацию о маршрутах по этим протоколам.

9.1 Подраздел «Общие настройки»

Подраздел «Общие настройки» позволяет изменять общие настройки динамической маршрутизации.

В пункте «Включен» необходимо установить флажок для включения динамической маршрутизации. В поле «Создание файла журнала» необходимо установить флажок для записи журнала на диск. В поле «Детализация журнала» необходимо выбрать уровень детализации журнала. В поле «Отправлять сообщения журнала в syslog» необходимо установить флажок для включения отправления событий журнала в syslog. В поле «Уровень системного журнала» необходимо выбрать уровень детализации журнала, который будет направлен в syslog (Рисунок 250).

Маршрутизация: Общие настройки

Включен	<input type="checkbox"/>
Создание файла журнала	<input type="checkbox"/>
Детализация журнала	INFORMATIONAL
Отправлять сообщения журнала в syslog	<input type="checkbox"/>
Уровень системного журнала	ALERTS

Сохранить

Рисунок 250 – Маршрутизация: Общие настройки

9.2 Подраздел «RIP»

Подраздел «RIP» позволяет настраивать динамическую маршрутизацию по протоколу RIP. В поле «Включен» необходимо установить флажок для включения динамической маршрутизации по протоколу RIP. В поле «Версия» необходимо выбрать версию протокола RIP. В поле «Пассивные интерфейсы» необходимо выбрать интерфейсы, которые не будут использоваться для поиска оптимального маршрута, в поле «Перераспределение маршрута» необходимо выбрать другие источники маршрутизации. В поле «Сети» необходимо ввести сети, которые должны быть известны при построении динамического маршрута. В поле

«Метрика по умолчанию» необходимо выставить метрику. После внесения изменений нажать на кнопку «Сохранить» (Рисунок 251).

Включить	<input checked="" type="checkbox"/>
Версия	2
Пассивные интерфейсы	LAN
Перераспределение маршрута	Протокол пограничного шлюза (BGP)
Сети	127.0.0.0/8
Метрика по умолчанию	5

Сохранить

Рисунок 251 – Маршрутизация: RIP

9.3 Подраздел «OSPF»

Подраздел «OSPF» позволяет настраивать динамическую маршрутизацию по протоколу OSPF, просматривать в виде таблицы настроенные сети, интерфейсы и список префиксов.

9.3.1 Категория «Общие настройки»

Категория «Общие настройки» позволяет настраивать протокол OSPF.

Для включения динамической маршрутизации по протоколу OSPF необходимо установить флажок в поле «Включен». В поле «Понижение CARP» необходимо установить флажок для отслеживания статуса CARP. В поле «ID роутера» необходимо ввести идентификатор маршрутизатора, если возникают пересечения с настройками CARP. В поле «Пассивные интерфейсы» необходимо выбрать интерфейсы, которые не будут использоваться для поиска оптимального маршрута, в поле «Перераспределение маршрута» необходимо выбрать другие источники маршрутизации. В поле «Карта распределения» необходимо выбрать карту для распределения. В поле «Объявлять шлюз по умолчанию» необходимо установить флажок для того, чтобы отправить информацию о том, что имеется шлюз по умолчанию. В поле «Всегда объявлять шлюз по умолчанию» необходимо установить флажок для того, чтобы транслировать шлюз по умолчанию. В поле

«Объявить метрику шлюза по умолчанию» необходимо ввести метрику шлюза по умолчанию (Рисунок 252).

Маршрутизация: OSPF

Общие настройки Сети Интерфейсы Списки префиксов Карты маршрутизации

☒ расширенный режим

Включен ☒

Понижение CARP ☐

ID роутера

Пассивные интерфейсы
 ☒ Очистить все

Перераспределение маршрута
 ☒ Очистить все

Карта распределения

Объявлять шлюз по умолчанию ☒

Всегда объявлять шлюз по умолчанию ☐

Объявить метрику шлюза по умолчанию

Рисунок 252 – Маршрутизация: OSPF: Общие настройки

9.3.2 Категория «Сети»

В категории «Сети» отображается таблица краткого обзора настроенных сетей. Таблица содержит следующие данные (Рисунок 253):

- состояние сети (включена/выключена);
- адрес сети;
- маска сети;
- область.

Общие настройки **Сети** Интерфейсы Списки префиксов



Включен	Адрес сети	Маска	Область	Команды
<input checked="" type="checkbox"/>	192.168.3.34	24	0.0.0.0	<input type="button" value="✎"/> <input type="button" value="📄"/> <input type="button" value="🗑"/>

Перезагрузка службы

1


Показаны с 1 по 1 из 1 записей

Рисунок 253 – Маршрутизация: OSPF: Сети

Для редактирования существующей сети необходимо нажать на кнопку  напротив сети. Для добавления новой сети необходимо нажать на кнопку .

Для включения сети необходимо установить флажок в поле «Включен». В поле «Адрес» необходимо ввести адрес сети. В поле «Маска сети» необходимо ввести маску сети (1-32). В поле «Область» необходимо ввести область сети (то есть, какие маршруты принадлежат к той же группе). В поле «Список входящих префиксов» необходимо выбрать список входящих префиксов сети. В поле «Список исходящих префиксов» необходимо выбрать список исходящих префиксов сети (Рисунок 254). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

Редактировать сеть ✕

справка 

Включен	<input checked="" type="checkbox"/>
Адрес сети	<input type="text" value="192.168.3.34"/>
Маска сети	<input type="text" value="24"/>
Область	<input type="text" value="0.0.0.0"/>
Область применения	<input type="text"/>
Список префиксов входящих	<input type="text" value="отсутствует"/>
Список префиксов исходящих	<input type="text" value="отсутствует"/>

Рисунок 254 – Маршрутизация: OSPF: Сети (редактирование)

9.3.3 Категория «Интерфейсы»

В категории «Интерфейсы» отображается таблица краткого обзора настроенных интерфейсов. Таблица содержит следующие данные (Рисунок 255):



- состояние интерфейса (включена/выключена);
- имя интерфейса;
- тип сети;
- тип аутентификации.

Общие настройки	Сети	Интерфейсы	Списки префиксов
-----------------	------	------------	------------------

Включен	Имя интерфейса	Тип сети	Тип аутентификации	Команды
<input checked="" type="checkbox"/>	LAN	Широковещательная сеть с множе...	MD5	<input type="button" value="✎"/> <input type="button" value="🗑"/> <input type="button" value="📄"/>

Показаны с 1 по 1 из 1 записей

Рисунок 255 – Маршрутизация: OSPF: Интерфейсы

Для редактирования существующего интерфейса необходимо нажать на кнопку  напротив интерфейса. Для добавления нового интерфейса необходимо нажать на кнопку .

Для включения интерфейса необходимо установить флажок в поле «Включен». В поле «Интерфейсы» необходимо выбрать интерфейс, в котором применить эти настройки. В поле «Тип аутентификации» необходимо выбрать тип аутентификации. В поле «Ключ аутентификации» необходимо ввести ключ аутентификации. В поле «Область» необходимо указать область. В поле «Стоимость» необходимо ввести стоимость интерфейса (используется для расчета маршрута). В поле «Интервал приветствия» необходимо ввести интервал, в течение которого отправляются пакеты приветствия. В поле «Мертвое время» необходимо ввести интервал времени, в течение которого интерфейс должен принять эти пакеты. В поле «Интервал повторной передачи» необходимо ввести интервал повторной передачи. В поле «Пауза повторной передачи» необходимо ввести интервал паузы повторной передачи. В поле «Приоритет» необходимо ввести приоритет интерфейса (чем больше приоритет, тем более вероятно, что этот интерфейс будет назначен в динамическом маршруте. В поле «Тип сети» необходимо выбрать тип сети (Рисунок 256). После внесенных изменений необходимо нажать на кнопку «Сохранить».

расширенный режим
справка

Включен
☒

Интерфейс

LAN

Тип аутентификации

MD5

Ключ аутентификации

test

Область

0.0.0.0

Стоимость

1

Интервал приветствия

2

Мертвое время

2

Интервал повторной передачи

2

Пауза повторной передачи

2

Приоритет

1

Тип сети

отсутствует, Широковещательная сеть с множес

Очистить все

Отменить

Сохранить

Рисунок 256 – Маршрутизация: OSPF: Интерфейсы (редактирование)



9.3.4 Категория «Список префиксов»

В категории «Список префиксов» отображается таблица краткого обзора настроенных списков префиксов. Таблица содержит следующие данные (Рисунок 257):

- состояние сети (включена/выключена);
- название списка префиксов;
- порядковый номер;
- действие;
- адрес сети.


Общие настройки	Сети	Интерфейсы	Списки префиксов	
<div> <div>Поиск</div> <div>7</div> </div>				
Включен	Имя	Номер последовательно...	Действие	Сеть
<input checked="" type="checkbox"/>	test	11	Разрешить	192.168.3.0
<div> <div>Перезагрузка службы</div> </div>				
<div> <div>Показаны с 1 по 1 из 1 записей</div> </div>				


Рисунок 257 – Маршрутизация: OSPF: Список префиксов

Для редактирования существующих списков префиксов необходимо нажать на кнопку  напротив списка. Для добавления нового списка необходимо нажать на кнопку .

Для включения списка префиксов необходимо установить флажок в поле «Включен». В поле «Имя» необходимо ввести название списка. В поле «Номер» необходимо ввести порядковый номер списка (10-99). В поле «Действие» необходимо выбрать действие для разрешения или блокирования правил. В поле «Сеть» необходимо ввести шаблон сети для поиска (Рисунок 258). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

Редактировать списки префиксов ×

справка 

Включен	<input checked="" type="checkbox"/>
Имя	<input type="text" value="test"/>
Номер	<input type="text" value="11"/>
Действие	<div>Разрешить </div> <div>✖ Очистить все</div>
Сеть	<input type="text" value="192.168.3.0"/>

Отменить Сохранить

Рисунок 258 – Маршрутизация: OSPF: Список префиксов (редактирование)

9.3.5 Категория «Карты маршрутизации»



В категории «Карты маршрутизации» отображается таблица краткого обзора настроенных карт маршрутизации. Таблица содержит следующие данные (Рисунок 259):

- состояние сети (включена/выключена);
- название карты маршрутизации;
- действие;
- ID карты маршрутов;
- список префиксов.

Маршрутизация: OSPF

Общие настройки Сети Интерфейсы Списки префиксов **Карты маршрутизации**

Поиск

 7 



Включен	Имя	Действие	ID	Список префиксов	Установить	Команды
Нет данных						

✚ Перезагрузка службы

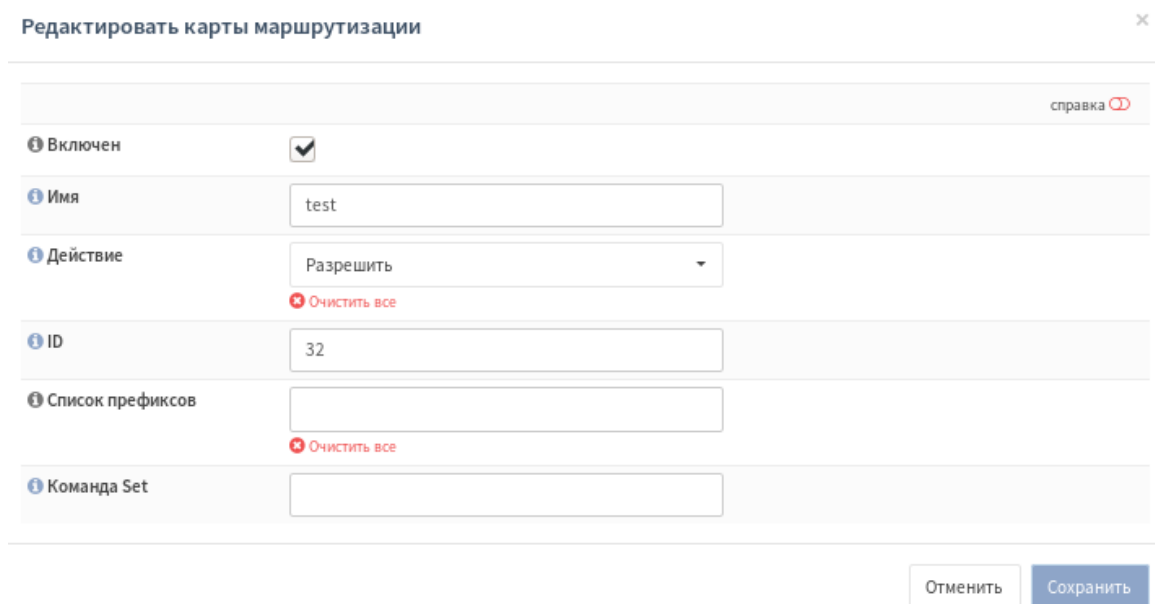
« « 1 » »

Показаны с 0 по 0 из 0 записей

Рисунок 259 – Маршрутизация: OSPF: Карты маршрутизации

Для редактирования существующих карт маршрутизации необходимо нажать на кнопку  напротив списка. Для добавления новой карты необходимо нажать на кнопку .

Для включения карты маршрутизации необходимо установить флажок в поле «Включен». В поле «Имя» необходимо ввести имя карты маршрутов. В поле «Действие» необходимо выбрать действие. В поле «ID» необходимо указать ID карты маршрутов. В поле «Список префиксов» необходимо выбрать список префиксов. В поле «Команда Set» необходимо ввести Set команду (Рисунок 260).



Редактировать карты маршрутизации	
справка	
Включен	<input checked="" type="checkbox"/>
Имя	<input type="text" value="test"/>
Действие	<div>Разрешить</div> <div>Очистить все</div>
ID	<input type="text" value="32"/>
Список префиксов	<div><input type="text"/></div> <div>Очистить все</div>
Команда Set	<input type="text"/>

Отменить Сохранить

Рисунок 260 – Маршрутизация: OSPF: Карты маршрутизации

9.4 Подраздел «Диагностика»

В подразделе «Диагностика» отображаются данные о настроенных динамических маршрутах по следующим протоколам:

- RIP (v1, v2);
- OSPF.

9.4.1 Категория «Общие настройки»


Категория «Общие настройки» позволяет просматривать данные о маршрутах IPv4 (Рисунок 261), IPv6 (Рисунок 262), а также общую конфигурацию настроенных динамических маршрутов (Рисунок 263).

Маршруты IPv4		Маршруты IPv6	Запущенная конфигурация		
Код	Сеть	Административная дистанция	Метрика	Интерфейс	Время
K> *	0.0.0.0/0			em3	
C> *	172.16.0.0/30			em2	
C> *	192.168.1.0/24			em3	
C> *	192.168.1.5/32			gif0	
*	192.168.1.222/32			em3	
C> *	192.168.1.222/32			gre0	
O	192.168.3.0/24	110	1	em1	00:03:10
C> *	192.168.3.0/24			em1	

Рисунок 261 – Маршрутизация: Диагностика: Общие настройки: Маршруты IPv4

Маршруты IPv4		Маршруты IPv6	Запущенная конфигурация		
Код	Сеть	Административная дистанция	Метрика	Интерфейс	Время
*	fe80::/64			em0_vlan1024	
*	fe80::/64			lagg0	
*	fe80::/64			gre0	
*	fe80::/64			gif0	
*	fe80::/64			lo0	
*	fe80::/64			em3	
*	fe80::/64			em2	
C> *	fe80::/64			em1	

Рисунок 262 – Маршрутизация: Диагностика: Общие настройки: Маршруты IPv6



```
Building configuration...

Current configuration:
!
frr version 3.0.3
frr defaults traditional
!
log file /var/log/frr.log notifications
!
log syslog notifications
!
interface em1
 ip ospf authentication message-digest
 ip ospf cost 1
 ip ospf dead-interval 2
 ip ospf hello-interval 2
 ip ospf message-digest-key 1 md5 test
!
router rip
 version 2
 redistribute connected
 redistribute bgp
 network 192.168.3.34/24
 passive-interface em1
!
router ospf
 redistribute static
 redistribute bgp
 passive-interface em1
 network 192.168.3.34/24 area 0.0.0.0
 area 0.0.0.0 filter-list prefix test in
 default-information originate
!
router ospf6
 router-id 192.168.1.1
 redistribute static
!
line vty
!
end
```

Рисунок 263 – Маршрутизация: Диагностика: Общие настройки: Запущенная конфигурация

9.4.2 Категория «OSPF»

Категория «OSPF» позволяет просматривать общие данные о настройке динамической маршрутизации по протоколу OSPF (Рисунок 264), таблицу маршрутизации сети/роутера, внешнюю таблицу маршрутизации (Рисунок 265), таблицы состояний связи (Рисунок 266), таблицу соседей (Рисунок 267), данные о настроенных интерфейсах (Рисунок 268).

Маршрутизация: Диагностика: OSPF

Обзор

Таблица маршрутизации

База данных

Соседи

Интерфейс

Общие настройки

Соответствие RFC2328	<input checked="" type="checkbox"/>
ASBR	<input checked="" type="checkbox"/>
ID роутера	192.168.3.3
Совместимость с RFC1583	<input type="checkbox"/>
Скрытая возможность	<input type="checkbox"/>
Начальная задержка планирования SPF	0
Минимальное время удержания	50 Миллисекунды
Максимальное время удержания	5000 Миллисекунды
Текущее время удержания	2
SPF таймер	inactive
Обновить таймер	10
Подсчет прикрепленных областей	1

Область состояния связи

	Количество	Контрольная сумма
Внешний LSA	1	0x00001445
Невыявленный LSA	0	0x00000000

Области

Рисунок 264 – Маршрутизация: Диагностика: OSPF: Обзор

Обзор

Таблица маршрутизации

База данных

Соседи

Интерфейс

Таблица маршрутизации сети

Поиск

10

Тип	Сеть	Стоимость	Область	Через	Через интерфейс
N	192.168.3.0/24	1	N/A	Подключённые напрямую	em1

<

<

1

>

>

Показаны с 1 по 1 из 1 записей

Таблица маршрутизации маршрутизатора

Поиск

10

Тип	Стоимость	Область	ASBR	Через	Через интерфейс
Нет данных					

<

<

1

>

>

Показаны с 0 по 0 из 0 записей

Внешняя таблица маршрутизации

Поиск

10

Тип	Сеть	Стоимость	Тег	Через	Через интерфейс
Нет данных					

<

<

1

>

>

Показаны с 0 по 0 из 0 записей

Рисунок 265 – Маршрутизация: Диагностика: OSPF: Таблица маршрутизации

Маршрутизация: Диагностика: OSPF								
<div>Обзор</div> <div>Таблица маршрутизации</div> <div>База данных</div> <div>Соседи</div> <div>Интерфейс</div>								
ID маршрутизатора 192.168.3.3								
Область состояния связи маршрутизатора								
Area 0.0.0.0								
ID связи	Маршрутизатор ADU	Возраст	Номер последовательности	Контрольная сумма	Счётчик соединений			
192.168.3.3	192.168.3.3	476	0x80000003	0xb0a2	1			
Показаны с 1 по 2 из 2 записей								
Сетевая область состояния связи								
Внешние состояния								
ID связи	Маршрутизатор ADU	Возраст	Номер последовательности	Контрольная сумма	Маршрут			
0.0.0.0	192.168.3.3	478	0x80000001	0xc445	E2 0.0.0.0 [Red]			
Показаны с 1 по 3 из 3 записей								

Рисунок 266 – Маршрутизация: Диагностика: OSPF: База данных

Обзор	Таблица маршрутизации	База данных	Соседи	Интерфейс					
ID соседней связи	Приоритет	Состояние	Тайм-аут	Адрес	Интерфейс	RxmtL	RxgtL	DBmtL	
Нет данных									
Показаны с 0 по 0 из 0 записей									

Рисунок 267 – Маршрутизация: Диагностика: OSPF: Соседи

Маршрутизация: Диагностика: OSPF	
Обзор	Таблица маршрутизации
База данных	Соседи
Интерфейс	
em1	
Включен	<input checked="" type="checkbox"/>
Адрес	192.168.3.3/24
Вещание	192.168.3.255
Область	0.0.0.0
Обнаружено несовпадение MTU	<input checked="" type="checkbox"/>
ID роутера	192.168.3.3
Тип сети	BROADCAST
Стоимость	1
Задержка передачи	1
Состояние	DR
Приоритет	1
Резервный назначенный маршрутизатор	
Члены многоадресной группы	<None>
Интервалы	Интервал приветствия: 2 Интервал молчания: 2 Интервал ожидания: 2 Интервал ретрансляции: 5
unparsed	No Hellos (Passive interface)
Подсчет соседних связей	0
Подсчет примыкающих соседних связей	0

Рисунок 268 – Маршрутизация: Диагностика: OSPF: Интерфейс

9.4.3 Категория «Журналирование»

Категория «Журналирование» позволяет просматривать журнал событий динамических маршрутов (Рисунок 269), реализованных по следующим протоколам:

- RIP (v1, v2);
- OSPF.

Маршрутизация: Диагностика: Журналирование

Дата	Время	Службы	Сообщение
27.03.2019	12:27:59	ZEBRA	zebra 3.0.3 starting: vty@2601
27.03.2019	12:39:01	ZEBRA	Terminating on signal
27.03.2019	12:39:03	ZEBRA	zebra 3.0.3 starting: vty@2601
27.03.2019	12:39:03	RIP	ripd 3.0.3 starting: vty@2602
27.03.2019	12:39:03	ZEBRA	client 16 says hello and bids fair to announce only rip routes
27.03.2019	12:55:48	RIP	Terminating on signal
27.03.2019	12:55:48	ZEBRA	client 16 disconnected. 0 rip routes removed from the rib
27.03.2019	12:55:48	ZEBRA	Terminating on signal
27.03.2019	12:55:50	ZEBRA	zebra 3.0.3 starting: vty@2601
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for em1
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for em1
27.03.2019	12:55:50	OSPF	ospfd 3.0.3 starting: vty@2604
27.03.2019	12:55:50	ZEBRA	client 16 says hello and bids fair to announce only ospf routes
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for bridge0
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for bridge1
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for em0
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for em0_vlan1024

Рисунок 269 – Маршрутизация: Диагностика: Журналирование

10 РАЗДЕЛ «СЛУЖБЫ»

Раздел «Службы» позволяет настраивать следующие службы:

- Портал авторизации;
- DHCPv4;
- DHCPv6;
- Monit;
- сетевое время;
- веб-прокси.

10.1 Подраздел «Портал авторизации»

Подраздел «Портал авторизации» позволяет просматривать, создавать, редактировать зоны, создавать шаблоны начальных страниц, просматривать сессии Портала авторизации по интерфейсам, просматривать / создать / ограничить срок действия ваучеров, просматривать журнал событий Портал авторизации.

10.1.1 Категория «Администрирование»

Категория «Администрирование» вкладка «Зоны» позволяет просматривать существующие зоны Портала авторизации в виде таблицы (Рисунок 270). В таблице представлены следующие данные:

- состояние зоны (включена/выключена);
- идентификатор зоны;
- номер зоны;
- описание зоны.

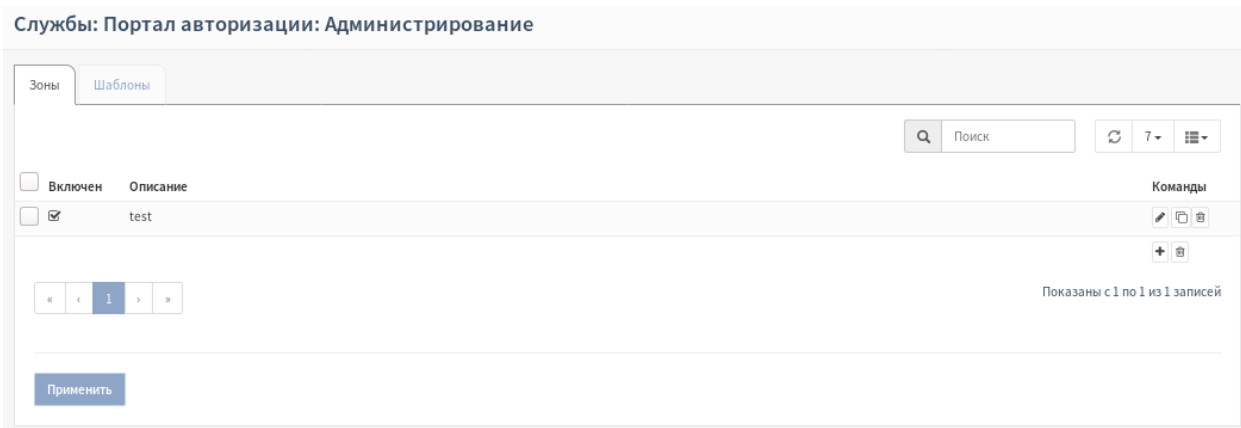




Рисунок 270 – Службы: Портал авторизации: Администрирование: Зоны

Для редактирования существующей зоны необходимо нажать на кнопку  напротив зоны. Для создания новой зоны необходимо нажать на кнопку .

При редактировании зоны в поле «Включен» необходимо установить флажок для включения этой зоны. В поле «Интерфейсы» необходимо выбрать интерфейсы, для которых будет включен Портал авторизации. В поле «Аутентификация через» необходимо выбрать сервер аутентификации. Для того чтобы пакеты «Accounting Request» отсылались постоянно, а не только, когда это обязательно (например, по истечению дневного лимита) в поле «Постоянно

посылать пакеты «Accounting Request» необходимо установить флажок. В поле «Принудительно использовать локальную группу» необходимо выбрать группу, которой будет ограничен доступ. В поле «Значение тайм-аута бездействия (в минутах)» необходимо ввести время, через которое пользователь принудительно выйдет из системы, в случае его бездействия. В поле «Значение тайм-аута сеанса (в минутах)» необходимо ввести значение, через которое пользователь принудительно выйдет из системы. В поле «Множественный вход пользователя в систему» необходимо установить флажок для подключения нескольких устройств, используя один логин. В поле «Сертификат SSL» необходимо выбрать сертификаты. В поле «Имя хоста» необходимо ввести IP-адрес, куда будет перенаправляться пользователь со страницы авторизации. В поле «Разрешенные адреса» необходимо ввести IP-адреса, которым разрешен доступ без авторизации. В поле «Разрешенные MAC-адреса» необходимо ввести MAC-адреса, которым разрешен доступ без авторизации. В поле «Прозрачный прокси (HTTP)» необходимо установить флажок для переадресации HTTP-трафика на прозрачный прокси. В поле «Прозрачный прокси (HTTPS)» необходимо установить флажок для переадресации HTTPS-трафика на прозрачный прокси. В поле «Пользовательский шаблон» необходимо выбрать пользовательский шаблон входа в систему. В поле «Описание» необходимо ввести описание (Рисунок 271). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

Отменить Сохранить

(редактирование)

авторизации (Рисунок 272).

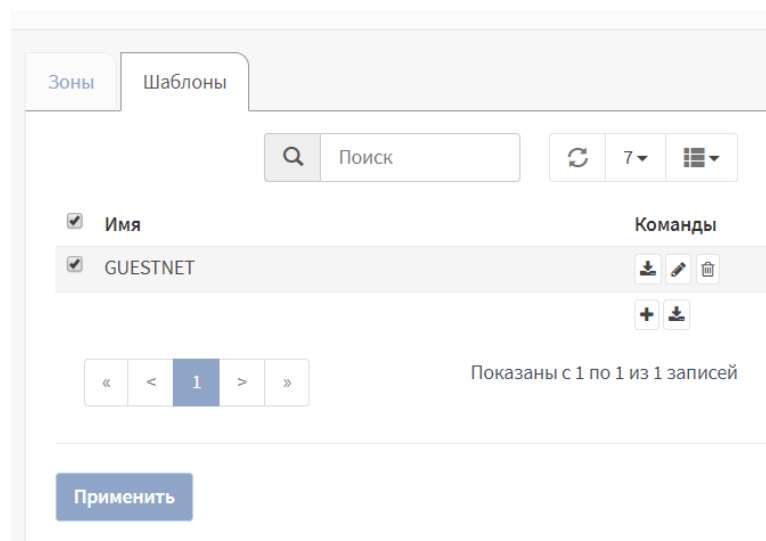


Рисунок 272 – Службы: Портал авторизации: Администрирование: Шаблоны

Также раздел позволяет экспортировать существующий шаблон и импортировать новый шаблон, нажав соответствующие кнопки. При нажатии на кнопку «Импортировать» появится всплывающее окно со следующими полями. В поле «Имя шаблона» необходимо ввести имя шаблона. Необходимо нажать на кнопку «Необходимо выбрать файл» для локального выбора файла шаблона и необходимо нажать на кнопку «Загрузка» (Рисунок 273).

Загрузить файл

Имя шаблона

Имя

Ввод из файла

Выберите файл

Файл не выбран

Загрузка

Рисунок 273 – Службы: Портал авторизации: Администрирование: Шаблоны (импорт шаблона)

10.1.2 Категория «Сессии»

В категории «Сессии» отображается информация о запущенных сессиях Портала авторизации в виде таблицы (Рисунок 274). Таблица содержит следующие данные:

- идентификатор сессии;
- имя пользователя;
- MAC-адрес пользователя;
- IP-адрес пользователя;
- дата/время сессии.

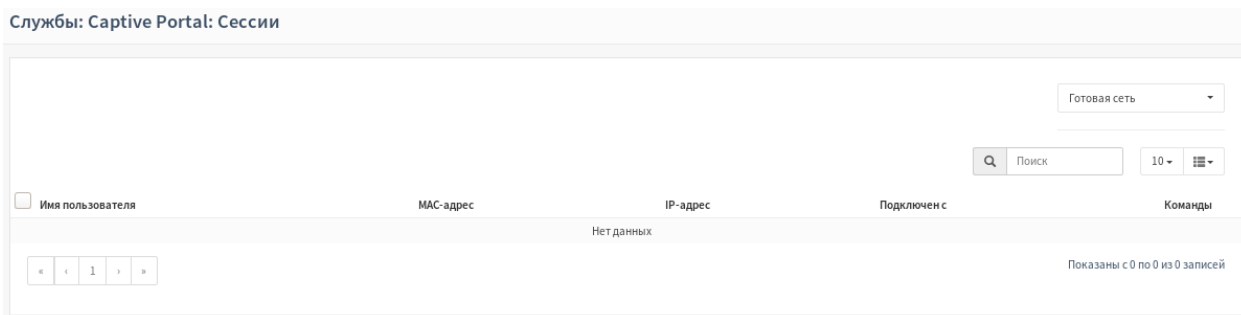


Рисунок 274 – Службы: Портал авторизации: Сессии

10.1.3 Категория «Ваучеры»

В категории «Ваучеры» отображаются все ваучеры выбранного Ваучер-сервера в виде таблицы (Рисунок 275).

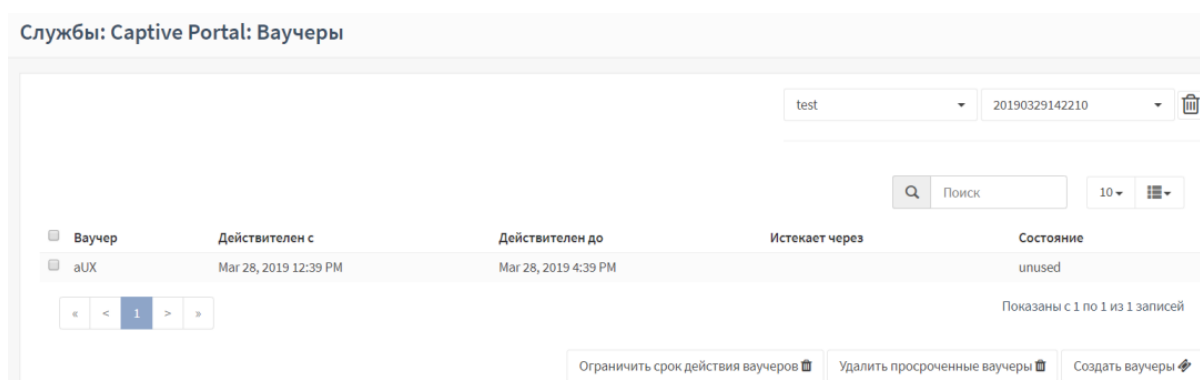


Рисунок 275 – Службы: Портал авторизации: Ваучеры

Раздел позволяет ограничить срок действия ваучеров, для этого необходимо выбрать ваучеры и нажать на кнопку «Ограничить срок действия ваучеров».

Также раздел позволяет удалить просроченные ваучеры, нажав соответствующую кнопку.

Для создания нового ваучера необходимо нажать на кнопку «Создать ваучеры» (Рисунок 276). В появившемся всплывающем окне в поле «Достоверность» необходимо выбрать срок действия ваучера (то есть срок действия одного сеанса использования этого ваучера). В поле «Истекает после» необходимо выбрать через сколько ваучер истекает. В поле «Количество ваучеров» необходимо выбрать количество добавляемых ваучеров. В поле «Имя группы» необходимо выбрать имя группы ваучеров и необходимо нажать на кнопку «Сгенерировать». После этого созданный (-ные) ваучер (-ы) будут автоматически экспортированы в локальную систему в формате «*.csv».

×

Сгенерировать ваучеры

Настройка	Значение
Достоверность	4 часа ▾
Истекает после	никогда ▾
Количество ваучеров	1 ▾
Имя группы	<input type="text" value="20200714100232"/>

Сгенерировать
Заккрыть

Рисунок 276 – Службы: Портал авторизации: Ваучеры (создание ваучеров)

10.1.4 Категория «Журнал»

В категории «Журнал» отображается журнал событий Портала авторизации (Рисунок 277).

Службы: Портал авторизации: Журнал

↺ 20 ▾

Дата	Сообщение
2020-07-22T06:55:09	api[94793]: session expired
2020-07-20T11:50:43	config[91645]: failed migrating from version 0.0.0 to 1.0.4 in OPNsense\Quagga\OSPF (skipping step)
2020-07-20T11:50:43	config[91645]: #2 (main)
2020-07-20T11:50:43	config[91645]: #1 /usr/local/opsense/mvc/script/run_migrations.php(57): OPNsense\Base(BaseModel->runMigrations())
2020-07-20T11:50:43	config[91645]: #0 /usr/local/opsense/mvc/app/models/OPNsense/Base/BaseModel.php(686): OPNsense\Base(BaseModel->serializeToConfig())
2020-07-20T11:50:43	config[91645]: Stack trace:
2020-07-20T11:50:43	config[91645]: in /usr/local/opsense/mvc/app/models/OPNsense/Base/BaseModel.php:575
2020-07-20T11:50:43	config[91645]: Model OPNsense\Quagga\OSPF6 can't be saved, skip (Phalcon\Validation\Exception: [OPNsense\Quagga\OSPF6:routerid] The field is required
2020-07-20T11:50:43	config[91645]: [OPNsense\Quagga\OSPF6:routerid] The field is required
2020-07-20T11:50:43	config[91645]: #2 (main)
2020-07-20T11:50:43	config[91645]: #1 /usr/local/opsense/mvc/script/run_migrations.php(57): OPNsense\Base(BaseModel->runMigrations())
2020-07-20T11:50:43	config[91645]: #0 /usr/local/opsense/mvc/app/models/OPNsense/Base/BaseModel.php(686): OPNsense\Base(BaseModel->serializeToConfig())
2020-07-20T11:50:43	config[91645]: Stack trace:
2020-07-20T11:50:43	config[91645]: in /usr/local/opsense/mvc/app/models/OPNsense/Base/BaseModel.php:575
2020-07-20T11:50:43	config[91645]: Model OPNsense\Quagga\RIP can't be saved, skip (Phalcon\Validation\Exception: [OPNsense\Quagga\RIP:networks] The field is required
2020-07-20T11:50:43	config[91645]: [OPNsense\Quagga\RIP:networks] The field is required
2020-07-20T11:50:43	config[91645]: #2 (main)
2020-07-20T11:50:43	config[91645]: #1 /usr/local/opsense/mvc/script/run_migrations.php(57): OPNsense\Base(BaseModel->runMigrations())
2020-07-20T11:50:43	config[91645]: #0 /usr/local/opsense/mvc/app/models/OPNsense/Base/BaseModel.php(686): OPNsense\Base(BaseModel->serializeToConfig())
2020-07-20T11:50:43	config[91645]: Stack trace:

Показаны с 1 по 20 из 21 записей
Очистить журнал

Рисунок 277 – Службы: Портал авторизации: Журнал

10.2 Подраздел «DHCPv4»

Подраздел «DHCPv4» позволяет настраивать DHCPv4-сервер.

10.2.1 Категория «[Название интерфейса]»

Категория [Название интерфейса] позволяет настраивать DHCPv4-сервер для интерфейса.

В пункте «Включен» необходимо установить флажок для включения DHCPv4-сервера. В поле «Блокировать неизвестных клиентов» необходимо установить флажок для разрешения получения IP-адресов только клиентам из выбранного далее диапазона. В поле «Диапазон» необходимо ввести диапазон IP-адресов, входящий в доступный диапазон, указанный в поле «Доступный диапазон». В поле «Дополнительные пулы» необходимо ввести дополнительные пулы адресов внутри подсети, которые не входят в доступный диапазон, указанный в поле «Доступный диапазон». В поле «WINS-серверы» необходимо ввести WINS-сервера. В поле «DNS-серверы» необходимо ввести DNS-серверы. В поле «Имя домена» необходимо ввести доменное имя. В поле «Список поиска доменов» необходимо ввести список поиска домена. В поле «Время аренды по умолчанию (секунд)» необходимо ввести время аренды для клиентов, которые не запрашивают конкретное время аренды. В поле «Максимальное время аренды (с)» необходимо ввести максимальное время аренды для клиентов, которые не запрашивают точное время. В поле «MTU интерфейса» необходимо ввести указание на MTU на этом интерфейсе. В поле «IP-адрес участника для аварийного переключения» необходимо ввести IP-адрес интерфейса на другом устройстве для аварийного переключения. В поле «Статический ARP» необходимо установить флажок для включения статического ARP. В поле «Изменить формат даты» необходимо установить флажок для изменения отображения времени аренды DHCP с UTC на местное время (Рисунок 278).

Рисунок 278 – Службы: DHCPv4: [Название интерфейса]

В пункте «Динамический DNS» при нажатии на кнопку «Дополнительно» в поле «Включить регистрацию имен DHCP-клиентов в DNS» необходимо установить флажок для включения регистрации имен DHCP-клиентов DNS и в первом поле необходимо ввести IP-адрес основного сервера доменных имен, во втором поле необходимо ввести имя доменного ключа, в третьем поле необходимо ввести секретный ключ домена. В пункте «Контроль доступа по MAC-адресам» при нажатии на кнопку «Дополнительно» в первом поле необходимо ввести список разрешенных MAC-адресов, во втором поле необходимо ввести список блокируемых MAC-адресов. В пункте «NTP-серверы» при нажатии на кнопку

«Дополнительно» в поле необходимо ввести NTP-серверы. В пункте «TFTP-сервер» при нажатии на кнопку «Дополнительно» в поле необходимо ввести TFTP-сервер. В пункте «LDAP URI» при нажатии на кнопку «Дополнительно» в поле необходимо ввести полный URL для LDAP-сервера (Рисунок 279).

<p>③ Динамический DNS</p>	<p><input checked="" type="checkbox"/> Включить регистрацию имен DHCP-клиентов в DNS. Введите доменное имя динамического DNS, которое будет использоваться для регистрации имен клиентов на DNS-сервере. Примечание: оставьте поле пустым, чтобы отключить регистрацию динамического 192.168.1.99 Введите IP-адрес основного сервера доменных имен для системы динамических доменных имен. 192.168.1.98 Введите имя доменного ключа динамического DNS, которое будет использоваться для регистрации имен клиентов на DNS-сервере. 192.168.1.97 Введите секретный ключ домена динамического DNS, который будет использоваться для регистрации имен клиентов на DNS-сервере. Выберите алгоритм ключа динамического домена DNS. hmac-md5</p>
<p>③ Контроль доступа по MAC-адресам</p>	<p>Введите список разрешенных MAC-адресов через запятую и без пробелов, например 00:00:00,01:E5:FF 00:00:00,01:E5:FF Введите список блокируемых MAC-адресов через запятую и без пробелов, например 00:00:00,01:E5:FF 00:00:00,01:E5:FA</p>
<p>③ NTP-серверы</p>	<p>192.168.1.222</p>
<p>③ TFTP-сервер</p>	<p>Установка имени узла TFTP 192.168.1.33 Установка загрузочного файла Оставьте пустым, чтобы отключить. Введите полное имя хоста или IP-адрес TFTP-сервера и полный путь к загрузочному файлу (опционально).</p>
<p>③ LDAP URI</p>	<p>ldap://ldap.example.com/dc=example,dc=com Оставьте поле пустым, чтобы отключить. Введите полный URL для LDAP-сервера в формате ldap://ldap.example.com/dc=example,dc=com</p>

Рисунок 279 – Службы: DHCPv4: [Название интерфейса] (дополнительно, часть 1)

В пункте «Включить загрузку по сети» при нажатии на кнопку «Дополнительно» необходимо установить флажок напротив поля «Включить загрузку по сети» для включения загрузки по сети. В первом поле необходимо ввести IP-адрес следующего сервера, во втором поле необходимо ввести имя файла BIOS, в третьем поле необходимо ввести имя файла UEFI 32bit, в четвертом поле необходимо ввести имя файла UEFI 64bit, в пятом поле необходимо ввести корневой путь. В пункте «WPAD» при нажатии на кнопку «Дополнительно» необходимо установить флажок напротив поля «Включить автоматическую настройку прокси-сервера» для включения автоматической настройки прокси-сервера. При необходимости включить OMAPI необходимо установить флажок напротив «Включить OMAPI» и в соответствующих полях ввести порт, ключ и алгоритм ключа OMAPI. В пункте «Дополнительные параметры» при нажатии на кнопку «Дополнительно» необходимо ввести дополнительные параметры, которые необходимо включить в информацию об аренде DHCP (Рисунок 280).

Включить загрузку по сети

☐ Включить загрузку по сети.

Указать IP-адрес следующего сервера

Указать имя файла BIOS по умолчанию

Указать имя файла UEFI 32bit

Указать имя файла UEFI 64bit

Примечание: чтобы это работало, необходимо иметь файлы и настроенный сервер. Вам нужны все три имени файлов и настроенный сервер загрузки для работы UEFI.

Указать корневой путь

Примечание: формат строки bios(имясервера)(протокол)(порт)(UUID).

DHCP

☐ Включить автоматическую настройку пренес-сервера

Enable OMAPI

☐ Enable OMAPI

OMAPI port

key algorithm


OMAPI key

Дополнительные параметры

Номер	Тип	Значение
-	Текстовый	
+		

Сохранить

Рисунок 280 – Службы: DHCPv4: [Название интерфейса] (дополнительно, часть 2)

Также в категории «[Название интерфейса]» можно настроить статическую маршрутизацию через DHCP для определенного интерфейса. Для этого необходимо нажать на  в пункте «Статическая маршрутизация через DHCP для этого интерфейса».

В поле «MAC-адрес» ввести или скопировать MAC-адрес. В поле «Идентификатор клиента» указать идентификатор клиента. В поле «IP-адрес» ввести IP-адрес. В поле «Имя хоста» ввести имя хоста без доменной части. В поле «Описание» ввести описание ссылки. Для создания статических записей в таблице ARP необходимо установить флажок напротив «Статические записи в таблице ARP». В поле «WINS-серверы» ввести адреса WINS-серверов. В поле «DNS-серверы» ввести адреса DNS-серверов. В поле «Шлюз» можно оставить шлюз по умолчанию или указать альтернативный. В поле «Имя домена» можно оставить по умолчанию или указать альтернативный. В поле «Список поиска доменов» при необходимости ввести дополнительный список поиска доменов. В поле «Время аренды по умолчанию (с)» указать время аренды или оставить по умолчанию (7200 секунд). В поле «Максимальное время аренды (с)» указать максимальное время аренды или оставить по умолчанию (86400 секунд) (Рисунок 281).

Статическая маршрутизация через DHCP	
① MAC-адрес	<input type="text"/> Скопировать мой MAC-адрес
① Идентификатор клиента	<input type="text"/>
① IP-адрес	<input type="text"/>
① Имя хоста	<input type="text"/>
① Описание	<input type="text"/>
① Статические записи в таблице ARP	<input type="checkbox"/>
① WINS-серверы	<input type="text"/> <input type="text"/>
① DNS-серверы	<input type="text"/> <input type="text"/>
① Шлюз	<input type="text"/>
① Имя домена	<input type="text"/>
① Список поиска доменов	<input type="text"/>
① Время аренды по умолчанию (с)	<input type="text"/>
① Максимальное время аренды (с)	<input type="text"/>

Рисунок 281 – Службы: DHCPv4: [Название интерфейса] (Настройка статической маршрутизации через DHCP, часть 1)

В пункте «Динамический DNS» при нажатии на кнопку «Дополнительно» в поле «Включить регистрацию имен DHCP-клиентов в DNS» необходимо установить флажок для включения регистрации имен DHCP-клиентов DNS и в первом поле необходимо ввести IP-адрес основного сервера доменных имен. В пункте «NTP-серверы» при нажатии на кнопку «Дополнительно» в поле необходимо ввести NTP-серверы. В пункте «TFTP-сервер» при нажатии на кнопку «Дополнительно» в поле необходимо ввести имя хоста или IP-адрес TFTP-сервера и полный путь к загрузочному файлу (Рисунок 282).

Рисунок 282 – Службы: DHCPv4: [Название интерфейса] (Настройка статической маршрутизации через DHCP, часть 2)

После внесения изменений необходимо нажать на кнопку «Сохранить».

10.2.2 Категория «Ретрансляция»

Категория «Ретрансляция» позволяет настраивать ретрансляцию DHCPv4. При ретрансляции запросы DHCP могут быть «перенаправлены» на другой сервер.

Для включения DHCP-ретрансляции необходимо установить флажок в пункте «Включен». В поле «Интерфейсы» необходимо выбрать интерфейсы, для которых необходимо настроить DHCP-ретранслятор. В поле «Добавлять идентификатор канала» необходимо установить флажок для добавления идентификатора канала и агента в запросы. В поле «Серверы назначения» необходимо ввести IP-адреса серверов, на которые будут перенаправляться DHCP запросы (Рисунок 283). После внесения изменений необходимо нажать на кнопку «Сохранить».

Рисунок 283 – Службы: DHCPv4: Ретрансляция

10.2.3 Категория «Аренда адресов»

Категория «Аренда адресов» позволяет просматривать все IP-адреса, которые раздаются клиентам (Рисунок 284). Позволяет просматривать все активные и все настроенные аренды, нажав соответствующие кнопки.

Службы: DHCPv4: Аренда адресов (0)								
Интерфейс	IP-адрес	MAC-адрес	Имя хоста	Описание	Начало	Окончание	Статус	Тип аренды
Показать все настроенные файлы аренды								

Рисунок 284 – Службы: DHCPv4: Аренда адресов

10.2.4 Категория «Журнал»

Категория «Журнал» позволяет просматривать журнал DHCPv4-сервера (Рисунок 285).

Службы: DHCPv4: Журнал	
<div> <input type="text" value="Поиск"/> 20 </div>	
Дата	Сообщение
2020-07-21T06:12:56	dhcpcd: Server starting service.
2020-07-21T06:12:56	dhcpcd: Sending on Socket/fallback/fallback-net
2020-07-21T06:12:56	dhcpcd: Sending on BPF/em0/00:0c:29:a2:e9:87/192.168.1.0/24
2020-07-21T06:12:56	dhcpcd: Listening on BPF/em0/00:0c:29:a2:e9:87/192.168.1.0/24
2020-07-21T06:12:56	dhcpcd: Wrote 0 leases to leases file.
2020-07-21T06:12:56	dhcpcd: For info, please visit https://www.isc.org/software/dhcp/
2020-07-21T06:12:56	dhcpcd: All rights reserved.
2020-07-21T06:12:56	dhcpcd: Copyright 2004-2020 Internet Systems Consortium.
2020-07-21T06:12:56	dhcpcd: Internet Systems Consortium DHCP Server 4.4.2
2020-07-21T06:12:56	dhcpcd: PID file: /var/run/dhcpcd.pid
2020-07-21T06:12:56	dhcpcd: Database file: /var/db/dhcpcd.leases
2020-07-21T06:12:55	dhcpcd: Config file: /etc/dhcpcd.conf
2020-07-21T06:12:55	dhcpcd: For info, please visit https://www.isc.org/software/dhcp/
2020-07-21T06:12:55	dhcpcd: All rights reserved.
2020-07-21T06:12:55	dhcpcd: Copyright 2004-2020 Internet Systems Consortium.
2020-07-21T06:12:55	dhcpcd: Internet Systems Consortium DHCP Server 4.4.2
2020-07-20T17:40:49	dhcpcd: Server starting service.
2020-07-20T17:40:49	dhcpcd: Sending on Socket/fallback/fallback-net
2020-07-20T17:40:49	dhcpcd: Sending on BPF/em0/00:0c:29:a2:e9:87/192.168.1.0/24
2020-07-20T17:40:49	dhcpcd: Listening on BPF/em0/00:0c:29:a2:e9:87/192.168.1.0/24
<div> « 1 2 » </div> <div>Показаны с 1 по 20 из 21 записей</div> <div>Очистить журнал</div>	

Рисунок 285 – Службы: DHCPv4: Журнал

10.3 Подраздел «DHCPv6»

Подраздел «DHCPv6» позволяет настраивать DHCPv6-сервер.

10.3.1 Категория «[Название интерфейса]»

Категория [Название интерфейса] позволяет настраивать DHCPv6-сервер для интерфейса.

В пункте «Включен» необходимо установить флажок для включения DHCPv4-сервера. В поле «Диапазон» необходимо ввести диапазон IP-адресов, входящий в доступный диапазон, указанный в поле «Доступный диапазон». В поле «Дополнительные делегируемые префиксы» необходимо ввести дополнительные делегируемые префиксы адресов внутри подсети, которые не входят в доступный диапазон, указанный в поле «Доступный диапазон». В поле «DNS-серверы» необходимо ввести DNS-серверы. В поле «Имя домена» необходимо ввести

доменное имя. В поле «Список поиска доменов» необходимо ввести список поиска домена. В поле «Время аренды по умолчанию (секунд)» необходимо ввести время аренды для клиентов, которые не запрашивают конкретное время аренды. В поле «Максимальное время аренды (с)» необходимо ввести максимальное время аренды для клиентов, которые не запрашивают точное время. В поле «Изменить формат даты» необходимо установить флажок для изменения отображения времени аренды DHCP с UTC на местное время.

10.4 Подраздел «Monit»

Сервис «Monit» является встроенным пакетом в систему. Это небольшая утилита с открытым исходным кодом для мониторинга Unix-систем с возможностью выполнения скриптов в качестве реакции на заданное событие.

Сервис «Monit» выполняет следующее:

- отслеживает состояния серверов (доступность, потребление ресурсов);
- производит мониторинг сервисов (состояние, потребляемые ресурсы, количество child-process и многое другое);
- производит мониторинг сетевых сервисов (возможность подключения и корректность ответа);
- производит выполнение встроенных или собственных (с помощью скриптов) действий при достижении определенных событий;
- производит отправку уведомлений на E-mail или в централизованный web-интерфейс M/Monit (коммерческая надстройка над «Monit»).

10.4.1 Категория «Настройки»

В пункте «Настройки» осуществляется настройка сервиса «Monit».

В категории «Основные настройки» необходимо установить флажок напротив «Включить monit», чтобы включить «Monit». В поле «Интервал опроса» необходимо ввести интервал опроса в секундах. В поле «Задержка старта» необходимо ввести задержку старта системы, чтобы пакет «Monit» запустил контролируемые сервисы. В поле «Почтовый сервер» необходимо ввести список SMNT серверов. В поле «Порт почтового сервера» необходимо ввести порт почтового сервера. В поле «Имя пользователя» необходимо ввести имя пользователя для аутентификации. В поле «Пароль» необходимо ввести пароль для аутентификации пользователя. В поле «Защищенное соединение» необходимо установить флажок для включения шифрования. В поле «SSL Version» необходимо выбрать версию SSL. Для включения верификации SSL сертификатов необходимо установить флажок напротив «Верификация SSL сертификатов». В поле «Журнал» необходимо ввести журнал процесса «Monit». В поле «Файл состояния» необходимо ввести файл состояния процесса «Monit». В поле «Путь к очереди событий» необходимо ввести путь к каталогу очередей событий. В поле «Слоты очереди событий» необходимо ввести количество слотов событий. В поле «Включите HTTPD» необходимо установить флажок для запуска «Monit» сервиса HTTPD (Рисунок 286).

Основные настройки	Настройки сообщений	Настройки службы	Настройки тестов служб
<div> <div></div> <div>расширенный режим</div> </div>			
Включить monit		<input checked="" type="checkbox"/>	
Интервал опроса		<input type="text" value="120"/>	
Задержка старта		<input type="text" value="120"/>	
Почтовый сервер		<input type="text" value="127.0.0.1"/> <div>✖</div> <div>✖ Очистить все</div>	
Порт почтового сервера		<input type="text" value="25"/>	
Имя пользователя		<input type="text" value="root"/>	
Пароль		<input type="password" value="****"/>	
Защищённое соединение		<input checked="" type="checkbox"/>	
SSL Version		<input type="text" value="AUTO"/>	
Верификация SSL сертификатов		<input checked="" type="checkbox"/>	
Журнал		<input type="text" value="syslog facility log_daemon"/>	
Файл состояния		<input type="text"/>	
Путь к очереди событий		<input type="text"/>	
Слоты очереди событий		<input type="text"/>	
Включите HTTPD		<input checked="" type="checkbox"/>	
Отслеживание порта HTTPD		<input type="text" value="2812"/>	
Список отслеживания доступа к HTTPD		<input type="text" value="user:password, @group..."/> <div>Для окончания ввода используйте TAB.</div> <div>✖ Очистить все</div>	
URL M/Monit		<input type="text"/>	
Тайм-аут M / Monit		<input type="text" value="5"/>	
Регистрация учетных данных M / Monit		<input checked="" type="checkbox"/>	

Рисунок 286 – Службы: «Monit»: Настройки: Основные настройки

Категория «Настройки сообщений» позволяет просматривать в виде таблицы настроенные предупреждения (Рисунок 287). Таблица содержит следующие данные:

- состояние (включено/выключено);
- получатель;
- событие;
- описание.

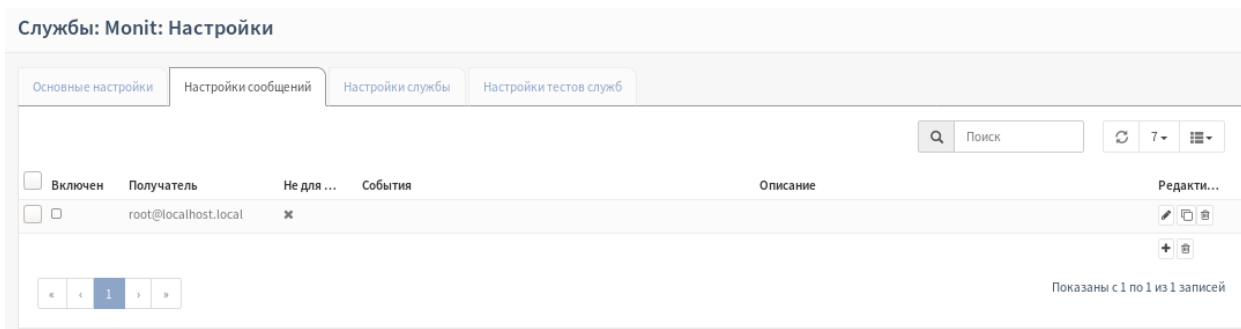





Рисунок 287 – Службы: «Monit»: Настройки: Настройки сообщений

Для редактирования существующего сообщения необходимо нажать на кнопку  напротив сообщения. Для создания нового сообщения необходимо нажать на кнопку .

При редактировании предупреждения (Рисунок 288) в поле «Включить сообщения» необходимо установить флажок для включения предупреждения. В поле «Получатель» необходимо ввести e-mail получателя. В поле «Не для следующих» необходимо установить флажок для отключения отправки предупреждения для следующих событий. В пункте «Формат почты» необходимо ввести формат сообщения:

- `$ EVENT` (добавляет описание произошедшего событие);
- `$ SERVICE` (добавляет название сервиса);
- `$ DATE` (добавляет текущее время и дату (стиль даты RFC 822));
- `$ HOST` (добавляет имя хоста, на котором работает «Monit»);
- `$ ACTION` (добавляет название действия, которое было сделано «Monit»);
- `$ ОПИСАНИЕ` (добавляет описание состояния ошибки).

В пункте «Напоминание» необходимо ввести через сколько циклов присылать напоминание. В пункте «Описание» необходимо ввести описание, например, «Оповещение по e-mail» и необходимо нажать на кнопку «Сохранить изменения».

справка 

Включить сообщения
☒

Получатель

Не для следующих
☒

События

Download bytes exceeded, Execution failed, Ping fa ▾

✖ Очистить все

Формат почты

\$ SERVICE

Напоминание

Описание

Отменить

Сохранить















Рисунок 288 – Службы: «Monit»: Настройки: Настройки сообщений: редактирование

В категории «Настройки службы» показаны настроенные проверяемые сервисы в виде таблицы (Рисунок 289). Таблица содержит следующие данные:

- состояние сервиса (включено/выключено);
- имя сервиса;
- идентификатор сервиса.



Службы: Monit: Настройки

Основная настройка
Настройка сообщения
Настройка службы
Настройка тестов службы

<input type="checkbox"/>	Включен	Имя	Редакти...
<input checked="" type="checkbox"/>	✓	\$HOST	  
<input checked="" type="checkbox"/>	✓	RootFs	  
<input type="checkbox"/>	□	carp_status_change	  
<input type="checkbox"/>	□	gateway_alert	  
			 


Показаны с 1 по 4 из 4 записей

Рисунок 289 – Службы: «Monit»: Настройки: Настройки службы

Для редактирования существующего сервиса необходимо нажать на кнопку  напротив сервиса. Для создания нового сервиса необходимо нажать на кнопку .

При редактировании сервиса в поле «Включить проверки служб» необходимо установить флажок для включения проверки сервисов. В поле «Имя» необходимо ввести имя сервиса. В поле «Тип» необходимо выбрать тип проверки сервиса. В поле «PID файл» необходимо ввести PID-файл процесса. В поле «Совпадение» необходимо ввести шаблон совпадения. В поле «Запустить» необходимо ввести скрипт запуска сервиса. В поле «Остановить» необходимо ввести скрипт остановки сервиса. В поле «Тесты» необходимо выбрать список тестов сервисов. В поле «Зависит от» необходимо выбрать сервис (-ы), от которых зависит данный сервис. В поле «Описание» необходимо ввести описание и необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (Рисунок 290).

Редактировать сервис ✕

☒ расширенный режим справка 

Включить проверки служб ☐

Имя

Тип Процесс ▾

PID файл

Совпадение

Запустить

Остановить

Тесты Не выбрано ▾
✖ Очистить все

Зависит от Не выбрано ▾
✖ Очистить все

Описание

Отменить Сохранить

Рисунок 290 – Службы: «Monit»: Настройки: Настройки службы (редактирование)

Категория «Настройка тестов служб» позволяет просматривать таблицу тестов служб (Рисунок 291). Таблица содержит следующие данные:

- название теста;
- условие для срабатывания тестов служб;
- действие, которое будет выполнено при срабатывании условия.

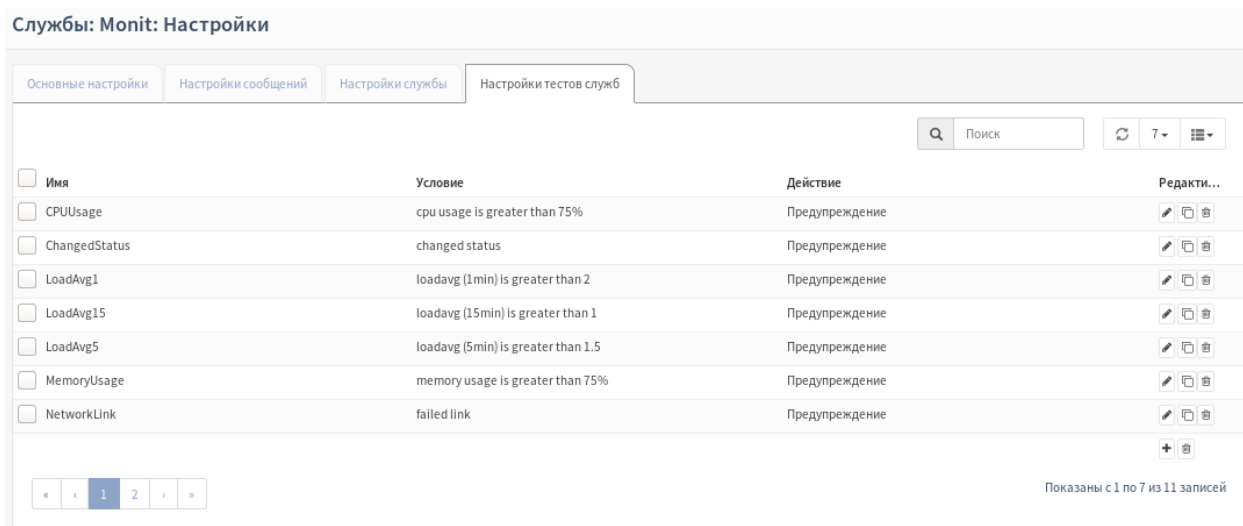


Рисунок 291 – Службы: «Monit»: Настройки: Настройка тестов служб

Для редактирования существующего теста служб необходимо нажать на кнопку напротив теста. Для создания нового теста необходимо нажать на кнопку .

При редактировании в поле «Имя» необходимо ввести название теста. В поле «Условие» необходимо ввести условие срабатывания теста. В поле «Действие» необходимо выбрать действие, которое будет выполнено при срабатывании условия (Рисунок 292).

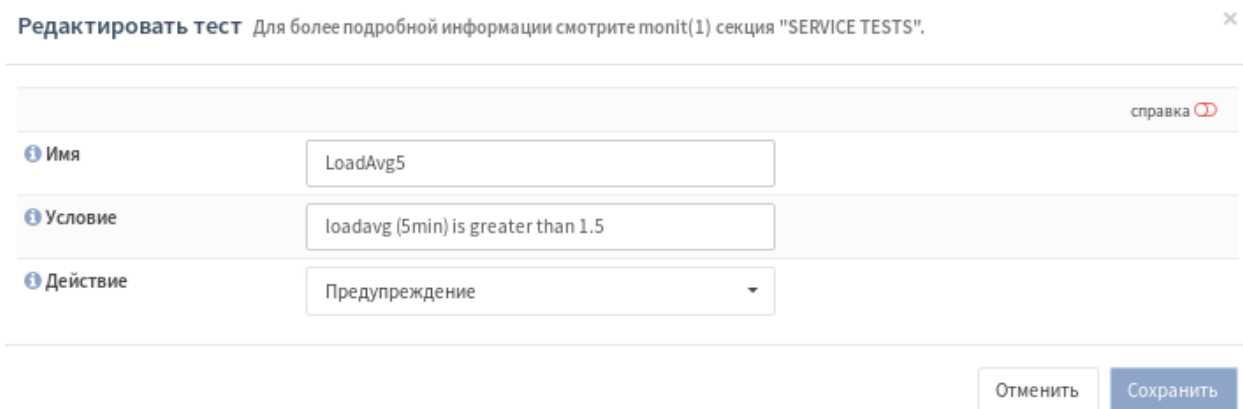


Рисунок 292 – Службы: «Monit»: Настройки: Настройка тестов служб (редактирование)

10.4.2 Категория «Статус»

Категория «Статус» позволяет просматривать информацию о «Monit» (Рисунок 293).

```
Either the file /var/run/monit.sock does not exists or it is not a unix socket.  
Please check if the Monit service is running.  
  
If you have started Monit recently, wait for StartDelay seconds and refresh this page.
```

Рисунок 293 – Службы: «Monit»: Статус

10.5 Подраздел «Сетевое время»

Подраздел «Сетевое время» позволяет производить общие настройки синхронизации времени, настраивать GPS-приемник, PPS, просматривать статус и журнал NTP.

10.5.1 Категория «Общие настройки»

Категория «Общие настройки» позволяет отредактировать конфигурацию NTP-сервера.

В поле «Интерфейсы» необходимо выбрать интерфейсы, которые будут прослушиваться. В поле «Серверы времени» необходимо ввести серверы времени и указать их приоритет. В поле «Автономный режим» необходимо ввести число, указывающее на приоритет автономного режима. Который позволяет использовать системные часы при недоступности остальных. В поле «Графики NTP» необходимо установить флажок для включения RRD-графиков статистики NTP. В поле «Системное журналирование» необходимо установить флажок напротив поля «Включить журналирование сообщений узлов (по умолчанию: отключено)» для включения журналирования сообщений узлов и напротив поля «Включить журналирование системных сообщений (по умолчанию: отключено)» для включения журналирования системных сообщений. В поле «Журналирование статистики» необходимо установить флажок (-и) для включения необходимых параметров. В поле «Ограничения доступа» необходимо установить флажок (-и) при необходимости выполнения выбранных параметров. В поле «Секунды координации» необходимо ввести настройки секунд, добавляемых к всемирному координированному времени для согласования его со средним солнечным временем. Настройки дополнительной секунды вводится в виде текста и загружается с помощью файла нажатием на кнопку «Выбрать файл». В поле «Дополнительно» необходимо ввести дополнительные параметры и нажать на кнопку «Сохранить» для сохранения внесенных изменений (Рисунок 294, Рисунок 295).

Службы: Сетевое время: Общие настройки

Конфигурация NTP-сервера

Интерфейс (-ы): Не выбрано

Серверы времени

Сеть	Предпочитать	Не использовать
0.pool.ntp.org	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>
2.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>
3.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>

Автономный режим

Графики NTP ☐ Включить RRD графики NTP статистики (по умолчанию: выключено).

Системное журналирование ☐ Включить журналирование сообщений узлов (по умолчанию: отключено).
☐ Включить журналирование системных сообщений (по умолчанию: отключено).

Журналирование статистики Эти параметры создают сохраняемые ежедневные журналы в /var/log/ntp.
☐ Включить журналирование статистики задающего тактового генератора (по умолчанию: отключено).
☐ Включить журналирование статистики высокостабильного тактового генератора (по умолчанию: отключено).
☐ Включить журналирование статистики NTP-узла (по умолчанию: отключено).

Рисунок 294 – Службы: Сетевое время: Общие настройки (часть 1)

Ограничения доступа Данные опции контролируют доступ к NTP из WAN.

☒ Включить пакеты «Kiss-o'-death» (по умолчанию: отключено).
☒ Блокировать изменение состояния (т.е. конфигурация времени прогона) с помощью ntpq и ntpdc (по умолчанию: включено).
☐ Отключить запросы ntpq и ntpdc (по умолчанию: отключено).
☐ Отключить все запросы, кроме ntpq и ntpdc (по умолчанию: отключено).
☒ Блокировать пакеты, которые пытаются ассоциироваться с узлом (по умолчанию: отключено).
☒ Блокировать службу контроля сообщений о ловушке в режиме 6 (по умолчанию: отключено).

Секунды координации Файл секунды координации позволяет NTP анонсировать последнее добавление или вычитание секунды координации. Как правило, это件 полезно только в том случае, если данный сервер является первичным сервером времени.

Введите настройки секунды синхронизации в виде текста:

Или, выберите файл для загрузки: Файл не выбран

Дополнительно

Дополнительно

Введите здесь любые дополнительные параметры, которые вы хотели бы добавить к конфигурации сетевого времени, через пробел или перенос строки.

Рисунок 295 – Службы: Сетевое время: Общие настройки (часть 2)

10.5.2 Категория «GPS-приемник»

Категория «GPS-приемник» позволяет настраивать GPS-приемник, подключенный к ПК. GPS-приемник, подключенный через порт последовательного ввода-вывода, может использоваться в качестве системных часов для NTP. Кроме того, если GPS-приемник поддерживает PPS, правильно настроен и подключен, то он может также использоваться в качестве системных часов для PPS.

В поле «GPS-приемник» необходимо выбрать предварительно заданную конфигурацию. В поле «Предложения NMEA» необходимо выбрать одно или несколько предложений NMEA. В поле «Fudge time 1 (секунды)» необходимо выбрать смещение сигнала GPS PPS. В поле «Fudge time 2 (секунды)» необходимо выбрать смещение времени GPS. В поле «Часовой слой» необходимо ввести значение для изменения приоритета. В поле «Флажки» необходимо поставить флажки напротив нужных параметров. В поле «Идентификатор часов» необходимо ввести идентификатор GPS. В поле «Инициализация GPS-приемника» в поле необходимо ввести команды GPS-приемнику. В поле «Вычисление контрольной суммы» необходимо ввести текст между "\$" и "*" и нажать «Подсчитать». Необходимо нажать на кнопку «Сохранить» (Рисунок 296, Рисунок 297).

Службы: Сетевое время: GPS-приемник

Конфигурация NTP GPS-приемника справка

GPS-приемник Универсальный

Предложения NMEA Все

Fudge time 1 (секунды)

Fudge time 2 (секунды)

Часовой слой

Флажки

Как правило, нет необходимости менять значения по умолчанию для данных

- ☒ NTP должен использовать данный тактовый генератор (по умолчанию: включено).
- ☐ Протокол NTP не должен использовать данные часы, они будут отображаться только для справки (по умолчанию: отключено).
- ☒ Включить обработку сигнала PPS (по умолчанию: включено).
- ☐ Включить обработку отрицательного перепада сигнала PPS (по умолчанию: положительный перепад).
- ☒ Включить тактовую синхронизацию PPS ядра (по умолчанию: включено).
- ☐ Скрыть местоположение во временной метке (по умолчанию: открыто).
- ☐ Логировать доли секунды в получаемых значениях времени (по-умолчанию: Не логируется).

Идентификатор часов

Рисунок 296 – Службы: Сетевое время: GPS-приемник (часть 1)

Инициализация GPS-приемника

```

$SDDBT,41.620,0.0,0.0,M
$SDDBT,41.604,0.0,0.0,M
$SDDBT,41.200,0.0,0.0,M
$SDDBT,41.016,0.0,0.0,M
$SDDBT,41.620,0.0,0.0,M
$SDDBT,41.604,0.0,0.0,M
$SDDBT,41.604,0.0,0.0,M
$SDDBT,41.016,0.0,0.0,M

```

Примечание: вводимые здесь команды будут отправлены GPS-приемнику во время инициализации. Ознакомьтесь с документацией GPS-приемника перед внесением каких-либо изменений.

Вычислитель контрольной суммы NMEA

Введите текст между "\$" и "*" в командной строке NMEA

Контрольная сумма: 00

GPS-приемник, подключенный через порт последовательного ввода/вывода, может использоваться в качестве системных часов для NTP. Кроме того, если GPS-приемник поддерживает PPS, правильно настроен и подключен, то он может также использоваться в качестве системных часов для PPS. ПРИМЕЧАНИЕ: USB GPS-приемник может использоваться, но не рекомендуется из-за синхронизации USB.

Для лучших результатов, NTP должен иметь хотя бы три источника времени. Также образом лучше всего сконфигурировать как минимум два сервера в Службы: Сетевое время чтобы минимизировать расхождение часов если данные GPS-приемник станут неверными со временем. Иначе ntpd может только использовать значения из несинхронизированных локальных часов когда предоставляется значения времени клиентом.

Рисунок 297 – Службы: Сетевое время: GPS-приемник (часть 2)

10.5.3 Категория «PPS»

Категория «PPS» позволяет настраивать сетевое время с сигналами PPS.

В поле «Время коррекции (с)» необходимо задать время смещения сигнала PPS. В поле «Часовой слой» задать часовой слой тактового генератора PPS (0-16) или оставить значение по умолчанию (0). В поле «Флажки» при необходимости изменить значения по умолчанию необходимо установить флажки напротив соответствующих полей. В поле «Идентификатор часов» задать идентификатор тактового генератора PPS (Рисунок 298).

Службы: Сетевое время: PPS

Конфигурация NTP PPS справка

Время коррекции (с)

Часовой слой

Флажки

- ☐ Включить обработку отрицательного перепада сигнала PPS (по умолчанию: положительный перепад).
- ☐ Включить порядок главных часов PPS (по умолчанию: отключено).
- ☐ Записать временную метку один раз для каждой секунды, используется для построения графиков отклонения Аллана (по умолчанию: отключено).

Идентификатор часов

Сохранить

Устройства с PPS выходом, такие как радиоприемники, которые принимают временной сигнал от DCF77 (DE), JJY (JP), MSF (GB) или WWVB (US), могут использоваться в качестве PPS-источника для NTP. Также можно использовать GPS-приемник с последовательным интерфейсом, но, как правило, лучше использовать драйвер GPS. Сигнал синхронизации PPS вырабатывается только в момент перехода с одной секунды на другую, так что требуется по меньшей мере еще один источник для подсчета секунд.

Примечание: Необходимо настроить по меньшей мере 3 дополнительных источника времени на странице: «Службы. NTP», чтобы надежно выдавать время каждого импульса PPS.

Рисунок 298 – Службы: Сетевое время: PPS

10.5.4 Категория «Статус»

Категория «Статус» позволяет просматривать таблицу состояний синхронизации времени. В таблице отображаются следующие данные (Рисунок 299):

- статус сервера сетевого времени;
- IP-адрес сервера;
- идентификатор источника;
- приоритет сервера сетевого времени;
- тип;
- начальное время;
- интервал опроса;
- задержка;
- смещение;
- неустойчивость.

Статус протокола сетевого времени

Статус	Сервер	Ref ID	Часовой слой	Тип	Когда	Опрос	Охват	Задержка	Смещение	Неустойчивость
Активный пир	188.225.9.167	194.190.168.1	2	u	341	512	377	12.139	+2.748	0.551
Резко отклоняющееся значение	77.51.199.214	.PPS.	1	u	219	512	377	7.214	+2.947	0.401
Кандидат	80.240.216.155	89.109.251.23	2	u	80	512	377	5.557	+3.195	0.242
Кандидат	85.21.78.23	194.58.202.20	2	u	139	512	377	24.197	-6.718	0.631

Рисунок 299 – Службы: Сетевое время: Статус

10.5.5 Категория «Журнал»

Категория «Журнал» позволяет просматривать журнал NTP (Рисунок 300).

Дата	Сообщение
2020-07-21T06:14:04	ntpd[61826]: kernel reports TIME_ERROR: 0x2041: Clock Unsynchronized
2020-07-21T06:14:04	ntpd[61826]: kernel reports TIME_ERROR: 0x2041: Clock Unsynchronized
2020-07-21T06:14:04	ntpd[61826]: Listening on routing socket on fd #30 for interface updates
2020-07-21T06:14:04	ntpd[61826]: Listen normally on 9 lo0 127.0.0.1:123
2020-07-21T06:14:04	ntpd[61826]: Listen normally on 8 lo0 [fe80::1%4]:123
2020-07-21T06:14:04	ntpd[61826]: Listen normally on 7 lo0 [-:]:123
2020-07-21T06:14:04	ntpd[61826]: Listen normally on 6 em2 192.168.159.139:123
2020-07-21T06:14:04	ntpd[61826]: Listen normally on 5 em2 [fe80::20c29ff:fea2e99b%3]:123
2020-07-21T06:14:04	ntpd[61826]: Listen normally on 4 em1 [fe80::20c29ff:fea2e991%2]:123
2020-07-21T06:14:04	ntpd[61826]: Listen normally on 3 em1 192.168.2.1:123
2020-07-21T06:14:04	ntpd[61826]: Listen normally on 2 em0 192.168.1.1:123
2020-07-21T06:14:04	ntpd[61826]: Listen and drop on 1 v4wildcard 0.0.0.0:123
2020-07-21T06:14:04	ntpd[61826]: Listen and drop on 0 v6wildcard [::]:123
2020-07-21T06:14:04	ntpd[61826]: restrict: 'monitor' cannot be disabled while 'limited' is enabled
2020-07-21T06:14:04	ntpd[61826]: gps base set to 2020-06-07 (week 2109)
2020-07-21T06:14:04	ntpd[61826]: basedate set to 2020-06-05
2020-07-21T06:14:04	ntpd[61826]: proto: precision = 0.189 usec (-22)
2020-07-21T06:14:04	ntpd[83693]: -----
2020-07-21T06:14:04	ntpd[83693]: available at https://www.nwttime.org/support
2020-07-21T06:14:04	ntpd[83693]: corporation. Support and training for ntp-4 are

« < 1 2 > »

Показаны с 1 по 20 из 21 записей

[Очистить журнал](#)

Рисунок 300 – Службы: Сетевое время: Журнал

10.6 Подраздел «Веб-прокси»

Подраздел «Веб-прокси» позволяет настраивать прокси-сервер, перенаправляющий прокси-сервер, а также создавать списки контроля доступа.

Веб-прокси Squid (кэширующий прокси) поддерживает широкие возможности фильтрации по различным критериям:

- фильтрация по IP-адресам;
- фильтрация по портам назначения;
- фильтрация по типу браузера;
- фильтрация по типу контента (по MIME-типам);
- фильтрация по общим белым и черным спискам;

– фильтрация по скачиваемым спискам.

Прокси-сервер поддерживает работу в прозрачном режиме (прозрачный HTTP-прокси). Смысл прозрачного проксирования заключается в том, что пользователи не имеют явных настроек на веб-прокси, тем не менее, их трафик все равно будет перехвачен и попадет на веб-прокси.

FTP-прокси обрабатывает только незашифрованный FTP-трафик.

Перенаправляющий прокси-сервер работает за счет использования правил межсетевого экрана («Межсетевой экран» - «NAT» - «Переадресация портов»).

10.6.1 Категория «Администрирование»

Вкладка «Основные настройки прокси»

В элементе «Основные настройки прокси» вкладки «Основные настройки прокси» осуществляются основные настройки прокси-сервера.

В пункте «Включить прокси» необходимо установить флажок для включения прокси-сервера. В поле «Порт ICP» необходимо ввести номер порта, на который сервис Squid будет посылать и принимать ICP-запросы. В поле «Включить ведение журнала обращения» необходимо установить флажок для включения ведения журнала запросов клиентов. В поле «Журналировать получателей» необходимо выбрать журнал, данные которого необходимо отправить адресату. В поле «Игнорировать хосты в журнале access.log» необходимо ввести подсети/адреса, которые необходимо игнорировать для записи в журнал access.log. В поле «Использовать альтернативные DNS-серверы» необходимо ввести IP-адреса альтернативных DNS-серверов. В поле «Включить сначала DNSv4» необходимо установить флажок при необходимости, чтобы сервис Squid сначала связывался с веб-сайтами с двумя стеками через IPv4. В поле «Использовать заголовок Via» необходимо установить флажок при необходимости, чтобы сервис Squid добавлял Via заголовок в запросы и ответы. В поле «Обработка заголовков X-Forwarded-For» необходимо выбрать действие с заголовком X-Forwarded-For. В поле «Имя хоста, которое будет отображаться в сообщениях об ошибках» необходимо ввести имя хоста, которое будет отображаться в сообщениях об ошибках прокси-сервера. В поле «Почта администратора» необходимо ввести почту администратора системы. В поле «Блокировать строку с версией» необходимо установить флажок для блокирования выдачи версии сервиса Squid в HTTP-заголовках и HTML-страницах об ошибках. В поле «Обработка пробелов для URI» необходимо выбрать, что делать с URI, который содержит пробелы. Необходимо нажать на кнопку «Применить» для сохранения настроек (Рисунок 301).

Службы: Веб-прокси: Администрирование

Основные настройки прокси ▾	Перенаправляющий прокси ▾	Автонастройки прокси-сервера ▾
<input checked="" type="checkbox"/> расширенный режим		
Включить прокси	<input checked="" type="checkbox"/>	
Порт ICP	<input type="text"/>	
Включить ведение журнала обращений	<input checked="" type="checkbox"/>	
Журналировать получателей	<input type="text" value="Файл"/>	
Включить ведение журнала действий с кэшем	<input checked="" type="checkbox"/>	
Игнорировать хосты в журнале access.log	<input type="text" value="192.168.2.0"/> <input type="button" value="x"/>	
	<input checked="" type="button" value="Очистить все"/>	
Использовать альтернативные DNS-серверы	<input type="text" value="192.168.3.4"/> <input type="button" value="x"/>	
	<input checked="" type="button" value="Очистить все"/>	
Включить сначала DNS v4	<input type="checkbox"/>	
Использовать заголовок Via	<input checked="" type="checkbox"/>	
Обработка заголовков X-Forwarded-For	<input type="text" value="Добавить IP-адрес клиента (вкл)"/>	
Имя хоста, которое будет отображаться в сообщениях об ошибках	<input type="text"/>	
Почта администратора	<input type="text" value="admin@localhost.local"/>	
Блокировать строку с версией	<input checked="" type="checkbox"/>	
Обработка пробелов для URI	<input type="text" value="Удалить пробелы"/>	
<input type="button" value="Применить"/>		

Рисунок 301 – Службы: Веб-прокси: Администрирование (Основные настройки прокси)

В элементе «Настройки локального кэша» вкладки «Основные настройки» осуществляются основные настройки локального кэша.

В поле «Размер кэш памяти (в Мб)» необходимо ввести размер памяти кэша. В поле «Включить локальный кэш» необходимо установить флажок для включения локального кэша. В поле «Размер кэша (в Мб)» необходимо ввести количество дискового пространства для хранения локального кэша. В поле «Расположение директории кэша» необходимо ввести расположение директории для локального кэша. В поле «Число подкаталогов первого уровня» необходимо ввести количество подкаталогов первого уровня, которые будут созданы в директории для хранения

локального кэша. В поле «Число подкаталогов второго уровня» необходимо ввести количество подкаталогов второго уровня, которые будут созданы в директории для хранения локального кэша. В поле «Максимальный размер объектов (Кб)» необходимо ввести максимальный размер объекта. В поле «Включите кэш-пакет Linux» необходимо установить флажок для включения кэширования пакетов для дистрибутивов Linux. В поле «Включите кэш обновления Windows» необходимо установить флажок для включения кэширования обновлений Windows. Необходимо нажать на кнопку «Применить» (Рисунок 302).

Службы: Веб-прокси: Администрирование

Основные настройки прокси ▾ Перенаправляющий прокси ▾ Автонастройки прокси-сервера ▾

☒ расширенный режим

Размер кэш-памяти (в Мб)	256
Включите локальный кэш	<input type="checkbox"/>
Размер кэша (в Мб)	100
Расположение директории кэша	/var/squid/cache
Число подкаталогов первого уровня	16
Число подкаталогов второго уровня	256
Максимальный размер объектов (Кб)	
Включите кэш-пакет Linux	<input checked="" type="checkbox"/>
Включите кэш обновления Windows	<input checked="" type="checkbox"/>

Применить

Рисунок 302 – Службы: Веб-прокси: Администрирование (Настройки локального кэша)

В элементе «Настройки управления трафиком» вкладки «Основные настройки прокси» осуществляются основные настройки управления трафиком.

В пункте «Включить управление трафиком» необходимо установить флажок для включения управления трафиком. В поле «Максимальный размер скачиваемых файлов (Кб)» необходимо ввести максимальный размер скачиваемых файлов. В поле «Максимальный размер загружаемых файлов (Кб)» необходимо ввести максимальный размер загружаемых файлов. В поле «Регулирование общей пропускной способности (Кбит/с)» необходимо ввести допустимую общую пропускную способность. В поле «Регулирование общей пропускной способности для хоста (Кбит/с)» необходимо ввести допустимую пропускную способность для хоста. Необходимо нажать на кнопку «Применить» (Рисунок 303).

Службы: Веб-прокси: Администрирование

Основные настройки прокси - Перенаправляющий прокси - Автонастройки прокси-сервера - Удаленные

Включить управление трафиком. ☐

Максимальный размер скачиваемых файлов (КБ) 2048

Максимальный размер загружаемых файлов (КБ) 1024

Регулирование общей пропускной способности (Кбит/с) 1024

Регулирование общей пропускной для хоста (Кбит/с) 256

Применить

Рисунок 303 – Службы: Веб-прокси: Администрирование (Настройки управления трафиком)

В элементе «Настройки родительского прокси» вкладки «Основные настройки прокси» осуществляются настройки родительского прокси.

Для включения родительского прокси необходимо установить флажок в пункте «Включить». В поле «Хост» необходимо ввести IP-адрес или хост родительского прокси. В поле «Порт» необходимо ввести порт родительского прокси. Для включения аутентификации родительского прокси необходимо установить флажок напротив пункта «Включить аутентификацию». В поле «Имя пользователя» необходимо задать имя пользователя. В поле «Пароль» необходимо задать пароль пользователя. В поле «Локальные домены» необходимо ввести список доменов, не отправляемых через родительский прокси. В поле «Локальные IP-адреса» необходимо ввести список IP-адресов, не отправляемых через родительский прокси (Рисунок 304).

Службы: Веб-прокси: Администрирование

Основные настройки прокси - **Перенаправляющий прокси** - Автонастройки прокси-сервера - Удаленны

Включить ☐

Хост

Порт

Включить аутентификацию ☐

Имя пользователя

Пароль

Локальные домены

Очистить все

Локальные IP-адреса

Очистить все

Применить

Рисунок 304 – Службы: Веб-прокси: Администрирование (Настройки родительского прокси)

Вкладка «Перенаправляющий прокси»

В элементе «Перенаправляющий прокси» вкладки «Перенаправляющий прокси» осуществляются основные настройки перенаправляющего прокси.

В поле «Интерфейсы» необходимо выбрать сетевые интерфейсы, к которым будет привязан перенаправляющий прокси-сервер. В поле «Номер порта прокси-сервера» необходимо ввести порт, который перенаправляющий прокси-сервер будет прослушивать. В поле «Включить прозрачный HTTP-прокси» необходимо установить флажок для включения прозрачного режима прокси-сервера. В поле «Включить проверку SSL» необходимо установить флажок для включения режима проверки SSL, который позволяет регистрировать информацию о соединениях HTTPS. В поле «Протоколировать только информацию SNI» необходимо установить флажок для журналирования запрошенных доменов и IP-адресов. В поле «Порт SSL прокси» необходимо ввести порт, который сервис SSL-прокси будет прослушивать. В поле «Использовать Центр Сертификации» необходимо выбрать Центр Сертификации, который необходимо использовать. В поле «SSL no bump sites» необходимо ввести список сайтов, которые не будут проверяться. В поле «Размер кэша SSL» необходимо ввести максимальный размер для сертификатов SSL. В поле «SSL cert workers» необходимо ввести количество используемых сертификатов SSL. В поле «Разрешить подсети на интерфейсе» необходимо установить флажок для добавления подсетей интерфейсов в список с правами доступа. Необходимо нажать на кнопку «Применить» (Рисунок 305).

Службы: Веб-прокси: Администрирование

Основные настройки прокси ▾ | **Перенаправляющий прокси ▾** | Автонастройки прокси-сервера ▾

☒ расширенный режим

Интерфейсы прокси	LAN ▾ <small>✖ Очистить все</small>
Номер порта прокси-сервера	3128
Включить прозрачный HTTP-прокси	<input checked="" type="checkbox"/>
Включить проверку SSL	<input checked="" type="checkbox"/>
Протоколировать только информацию SNI	<input type="checkbox"/>
Порт SSL прокси	3129
Использовать центр сертификации	Не выбрано ▾
SSL no bump sites	 <small>✖ Очистить все</small>
Размер кэша SSL	4
SSL cert workers	5
Разрешить подсети на интерфейсе	<input checked="" type="checkbox"/>

Применить

Рисунок 305 – Службы: Веб-прокси: Администрирование: Перенаправляющий прокси

В элементе «Настройки FTP-прокси» вкладки «Перенаправляющий прокси» осуществляются основные настройки FTP-прокси.

В поле «Интерфейсы FTP-прокси» необходимо выбрать интерфейсы, к которым будет привязан прокси-сервер FTP. В поле «Порт FTP-прокси» необходимо ввести порт, который прокси-сервер будет прослушивать. В поле «Включить прозрачный режим» необходимо установить флажок для включения прозрачного режима FTP-прокси. Необходимо нажать на кнопку «Применить» (Рисунок 306).

Службы: Веб-прокси: Администрирование

Основные настройки прокси ▾ Перенаправляющий прокси ▾ Автонастройки прокси-сервера ▾

❗ Интерфейсы FTP-прокси Не выбрано ▾

✖ Очистить все

❗ Порт FTP-прокси 2121

❗ Включить прозрачный режим ☒

Применить

Рисунок 306 – Службы: Веб-прокси: Администрирование: Настройки FTP-прокси

В элементе «Список управления доступом» вкладки «Перенаправляющий прокси» осуществляются основные настройки списка управления доступом.

В поле «Разрешенные подсети» необходимо ввести адреса подсетей, которым будет разрешен доступ к прокси-серверу. В поле «IP-адреса без ограничений» необходимо ввести IP-адреса, которым будет разрешен доступ к прокси-серверу. В поле «Заблокированные IP-адреса хоста» необходимо ввести IP-адреса, которым будет запрещен доступ к прокси-серверу. В поле «Белый список» необходимо ввести доменные адреса, которым будет разрешен доступ к прокси-серверу. В поле «Черный список» необходимо ввести доменные имена, которым будет запрещен доступ. В поле «Блокировать browser/user-agent строки» необходимо ввести user-agent строки, которые будут заблокированы. В поле «Блокировать ответ с конкретным MIME-типом» необходимо ввести ответы MIME-тип, которые будут блокироваться. В поле «Разрешенные TCP-порты» необходимо ввести TCP-порты источника, которым будет разрешен доступ. В поле «Разрешенные SSL-порты» необходимо ввести порты SSL, которым будет разрешен доступ (Рисунок 307). Необходимо нажать на кнопку «Применить».

Службы: Веб-прокси: Администрирование

Основные настройки прокси ▾ Перенаправляющий прокси ▾ Автонастройки прокси-сервера ▾ Удаленные списки контроля до

☒ расширенный режим

Разрешенные подсети	192.168.2.0 ×	✖ Очистить все
IP-адреса без ограничений	192.168.1.200 ×	✖ Очистить все
Заблокированные IP-адреса хоста	192.168.1.100 ×	✖ Очистить все
Белый список	https?:\V\/([a-zA-Z]+\.)mydomain\, ×	✖ Очистить все
Черный список	https?:\V\/([a-zA-Z]+\.)mydomain\, ×	✖ Очистить все
Блокировать browser/user-agent строки	^(.)+Macintosh(.)+Firefox/37\,0 ×	✖ Очистить все
Блокировать ответы с конкретным MIME-типом	video /flv ×	✖ Очистить все
Разрешенные TCP-порты назначения	80:http × 21:ftp × 443:https × 70:gopher × 210:wais × 1025-65535:unregistered ports × 280:http-mgmt × 488:gss-http × 591:filemaker × 777:multiling http ×	✖ Очистить все
Разрешенные SSL-порты	443:https ×	✖ Очистить все

Применить

Рисунок 307 – Службы: Веб-прокси: Администрирование: Список управления доступом

В элементе «Настройки ICAP» вкладки «Перенаправляющий прокси» осуществляются основные настройки ICAP.

Протокол ICAP (Internet Content Adaptation Protocol) необходим для осуществления интеграции Squid с сторонними СЗИ.

В пункте «Включить ICAP» необходимо установить флажок для включения ICAP-сервера. В поле «Запрос на изменение URL» необходимо ввести URL, на который должны посылааться REQMOD запросы. В поле «Ответ на изменение URL» необходимо ввести URL, на который должны посылааться REQMOD ответы. В поле «TTL параметры по умолчанию» необходимо ввести TTL параметры. В поле «Отправить IP-адрес по умолчанию» необходимо установить флажок для отправки IP-адреса на ICAP-сервер. В поле «Отправить имя пользователя» необходимо установить флажок для того, чтобы отправить имя пользователя на ICAP-сервер. В поле «Закодировать имя пользователя» необходимо установить флажок для кодировать имена пользователей. В поле «Заголовок имени пользователя» необходимо ввести заголовок, который должен использоваться для отправки имени пользователя. В поле «Включите предпросмотр» необходимо установить

флажок для включения предпросмотра. В поле «Размер в режиме предпросмотра» необходимо ввести размер превью, которое отправится на ICAP сервер. В поле «Список исключений» необходимо ввести целевые домены списка исключений. Необходимо нажать на кнопку «Применить» (Рисунок 308).

Службы: Веб-прокси: Администрирование

Основные настройки прокси ▾
Перенаправляющий прокси ▾
Автонастройки прокси-сервера ▾

●
расширенный режим

Включить ICAP ☒

REQMOD URL

RESPMOD URL

TTL параметров по умолчанию

Отправить IP-адрес клиента ☒

Отправить имя пользователя ☐

Закодировать имя пользователя ☐

Заголовок имени пользователя

Включить предпросмотр ☒

Размер в режиме предпросмотра

Список исключений

✖ Очистить все

Применить

Рисунок 308 – Службы: Веб-прокси: Администрирование: Настройки ICAP

В элементе «Настройки аутентификации» вкладки «Перенаправляющий прокси» осуществляются основные настройки аутентификации.

В поле «Метод аутентификации» необходимо выбрать сервер аутентификации. В поле «Принудительно использовать локальную группу» необходимо выбрать группы, которые будут иметь доступ. В поле «Подсказка» необходимо ввести подсказку при аутентификации. В поле «TTL аутентификации (часов)» необходимо ввести срок действия TTL. В поле «Процесс аутентификации» необходимо ввести число процессов аутентификации, которые могут быть запущены одновременно. Необходимо нажать на кнопку «Применить» (Рисунок 309).

Службы: Веб-прокси: Администрирование

Основные настройки прокси ▾	Перенаправляющий прокси ▾	Автонастройки прокси-сервера ▾	Удаленные списки ▾
<hr/>			
Метод аутентификации	Local Database ▾ Очистить все		
Принудительно использовать локальную группу	Не выбрано ▾ Очистить все <small>Restrict access to users in the selected (local) group. NOTE: please be aware that users (or vouchers) which aren't administered locally will be denied when using this option.</small>		
Подсказка	ARMA proxy authentication		
TTL аутентификации (часов)	2		
Процесс аутентификации	5		
Применить			

Рисунок 309 – Службы: Веб-прокси: Администрирование: Настройки аутентификации

В элементе «Настройки агента SNMP» вкладки «Перенаправляющий прокси» осуществляются основные настройки агента SNMP.

В пункте «Включение SNMP» необходимо установить флажок для включения агента SNMP. В поле «Порт SNMP» необходимо ввести порт, который Squid будет прослушивать SNMP-запросы. В поле «Пароль SNMP» необходимо ввести пароль доступа к SNMP. Необходимо нажать на кнопку «Применить» (Рисунок 310).

Службы: Веб-прокси: Администрирование			
Основные настройки прокси ▾	Перенаправляющий прокси ▾	Автонастройки прокси-сервера ▾	Удаленные списки ▾
<hr/>			
Включить	<input checked="" type="checkbox"/>		
Порт SNMP	3401		
Пароль SNMP	public		
Применить			



Рисунок 310 – Службы: Веб-прокси: Администрирование: Настройки агента SNMP

Вкладка «Автонастройки прокси-сервера»

Категория «Автонастройки прокси-сервера» позволяет настраивать правила прокси-сервера, добавлять несколько прокси-серверов с разными настройками, а также добавлять шаблоны совпадения.


Во вкладке «Правила» отображается таблица правил прокси-сервера со следующей информацией:

- статус правила (включено/выключено);
- описание правила;
- действие правила.

Для редактирования созданного правила необходимо нажать на кнопку  напротив правила. Для создания нового правила необходимо нажать на кнопку .

При редактировании правила в поле «Включен» необходимо установить флажок для включения правила. В поле «Описание» необходимо ввести описание правила. В поле «Шаблон совпадения» необходимо выбрать шаблон совпадения. В поле «Тип объединения» необходимо выбрать тип объединения шаблонов совпадения. Поле «Или», если при любом совпадении правило работает, «И», если при всех совпадениях правила работает. В поле «Тип совпадения» необходимо выбрать «Если», если необходимо, чтобы правило работало при соответствии шаблона совпадения, или «Иначе» в противном случае. В поле «Прокси-сервера» необходимо выбрать прокси-сервер, к которому будет применено правило. Для сохранения необходимо нажать на кнопку «Сохранить» (Рисунок 311).

Редактировать правило ×

справка 

Включен

☒

Описание

Шаблон совпадения

Очистить все

Тип объединения

И

▼

Тип совпадения

Если

▼

Прокси-сервера

Очистить все



Отменить

Сохранить

Рисунок 311 – Службы: Веб-прокси: Администрирование: Автонастройки прокси-сервера (Правила)

Во вкладке «Прокси-сервера» отображается таблица прокси-серверов со следующей информацией:

- имя прокси-сервера;
- тип;
- URL;
- описание.

Для редактирования созданного прокси-сервера необходимо нажать на кнопку  напротив прокси-сервера. Для создания нового прокси-сервера необходимо нажать на кнопку .

При редактировании прокси-сервера в поле «Имя» необходимо ввести имя прокси-сервера. В поле «Описание» необходимо ввести описание прокси-сервера. В поле «Тип прокси-сервера» необходимо выбрать тип прокси-сервера. В поле «URL» необходимо ввести URL-адрес прокси-сервера. Для сохранения необходимо нажать на кнопку «Сохранить» (Рисунок 312).

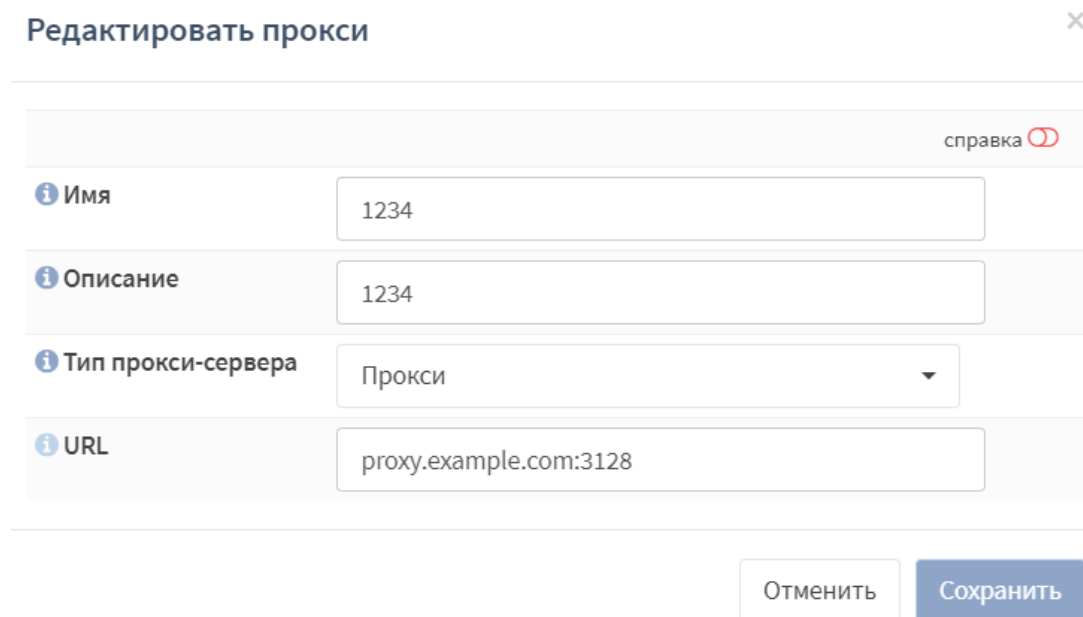




Рисунок 312 – Службы: Веб-прокси: Администрирование: Автонастройки прокси-сервера (Прокси-сервера)

Во вкладке «Шаблон совпадения» отображается таблица шаблонов совпадения со следующей информацией:

- имя шаблона совпадения;
- описание;
- тип совпадения.

Для редактирования созданного шаблона совпадения необходимо нажать на кнопку  напротив шаблона совпадения. Для создания нового шаблона совпадения необходимо нажать на кнопку .

При редактировании шаблона совпадения в поле «Имя» необходимо ввести имя шаблона совпадения. В поле «Описание» необходимо ввести описание шаблона совпадения. В поле «Отрицание» необходимо установить флажок для отрицания шаблона совпадения. В поле «Тип шаблона совпадения» необходимо выбрать тип шаблона совпадения. В поле «Сеть» необходимо ввести сетевой адрес для шаблона совпадения. В поле «Хост шаблона» необходимо ввести хост паттерна. В поле «Шаблон URL» необходимо ввести URL-адрес паттерна. В поле «Уровень домена с» необходимо ввести минимальный уровень домена, для которого действует шаблон совпадения. В поле «Уровень домена до» необходимо ввести максимальный уровень домена, для которого действует шаблон совпадения. В

поле «Время начала (час)» необходимо ввести начальное время действия шаблона совпадения. В поле «Время окончания (час)» необходимо ввести время окончания действия шаблона совпадения. В поле «Начало» необходимо ввести месяц начала действия шаблона совпадения. В поле «Окончание» необходимо ввести месяц окончания действия шаблона совпадения. В поле «Начало» необходимо ввести день недели начала действия шаблона совпадения. В поле «Окончание» необходимо ввести день недели окончания действия шаблона совпадения. После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 313).

Добавление шаблона совпадения ×

справка ⓘ

Имя	<input type="text"/>
Описание	<input type="text"/>
Отрицание	<input type="checkbox"/>
Тип совпадения	Шаблон совпадения URL ▾
Сеть	<input type="text"/>
Хост шаблона	<input type="text"/>
Шаблон URL	<input type="text"/>
Уровень домена с	<input type="text" value="0"/>
Уровень домена до	<input type="text" value="0"/>
Время начала (час)	<input type="text" value="0"/>
Время окончания (час)	<input type="text" value="0"/>
Месяц начала	Январь ▾
Месяц окончания	Январь ▾
День начала	Понедельник ▾
День окончания	Понедельник ▾



Рисунок 313 – Службы: Веб-прокси: Администрирование: Автонастройки прокси-сервера (Шаблон совпадения)

Вкладка «Удаленные списки контроля доступа»

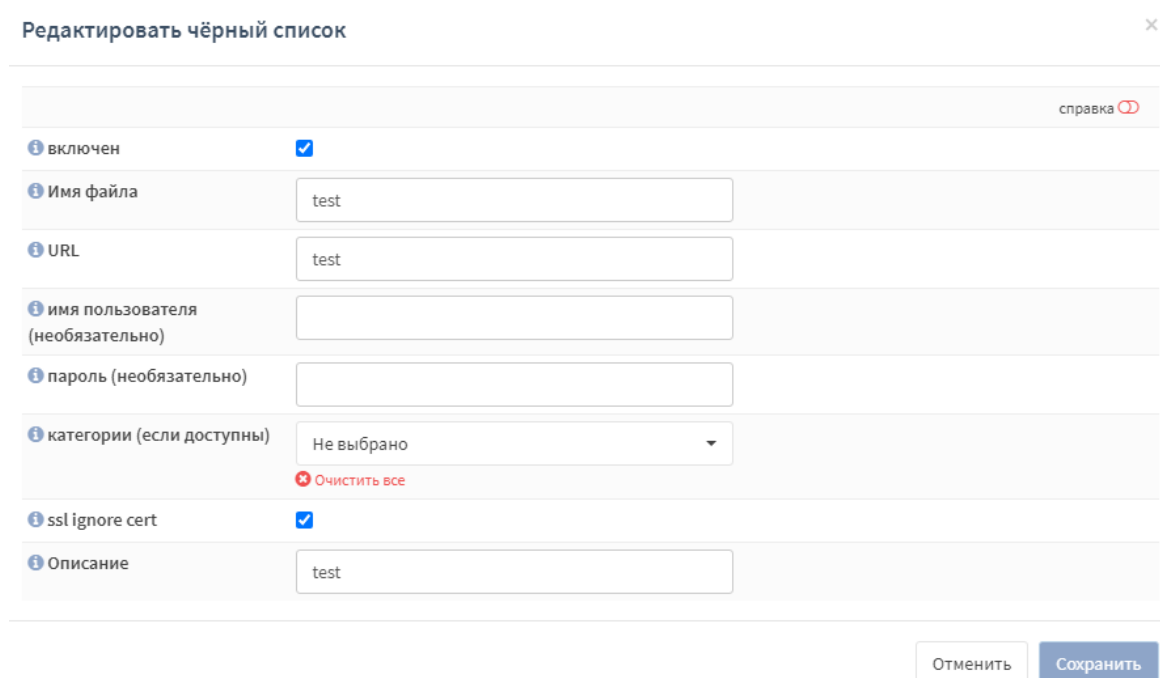
В категории «Удаленные списки контроля доступа» отображаются списки доступа в виде таблицы. Таблица содержит следующие данные:

- состояние списка (включен/выключен);
- имя списка;
- URL;
- описание.

Также раздел позволяет создать новый список доступа и удалить/редактировать существующие списки. Для редактирования существующего

необходимо нажать на кнопку  напротив списка. Для создания нового списка необходимо нажать на кнопку .

При редактировании списка в поле «Включен» необходимо установить флажок для включения списка. В поле «Имя файла» необходимо ввести название списка. В поле «URL» необходимо ввести URL для загрузки черного списка. В поле «Имя пользователя (необязательно)» необходимо ввести имя пользователя. В поле «Пароль (необязательно)» необходимо ввести пароль пользователя. В поле «Категория (если доступны)» необходимо выбрать категории списков. В поле «ssl ignore cert» необходимо установить флажок для игнорирования проверки SSL-сертификата. В поле «Описание» необходимо ввести описание списка и необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (Рисунок 314).



The screenshot shows a web interface titled "Редактировать чёрный список" (Edit Blacklist) with a close button (X) in the top right corner. The form contains several fields:

- Включен** (Included): A checkbox that is checked.
- Имя файла** (File name): A text input field containing "test".
- URL**: A text input field containing "test".
- Имя пользователя (необязательно)** (Username (optional)): An empty text input field.
- Пароль (необязательно)** (Password (optional)): An empty text input field.
- Категории (если доступны)** (Categories (if available)): A dropdown menu showing "Не выбрано" (Not selected). Below it is a red button labeled "Очистить все" (Clear all).
- ssl ignore cert**: A checkbox that is checked.
- Описание** (Description): A text input field containing "test".

At the bottom right of the form are two buttons: "Отменить" (Cancel) and "Сохранить" (Save).

Рисунок 314 – Службы: Веб-прокси: Администрирование: Удаленные списки контроля доступа

Также раздел позволяет скачать списки контроля доступа, скачать и применить списки контроля доступа, запланировать с помощью планировщика Cron работы списков контроля доступа и применить добавленные списки, нажав на соответствующие кнопки.

Вкладка «Помощь»

Категория «Помощь» позволяет сбросить все сгенерированные данные и перезапустить прокси (Рисунок 315).

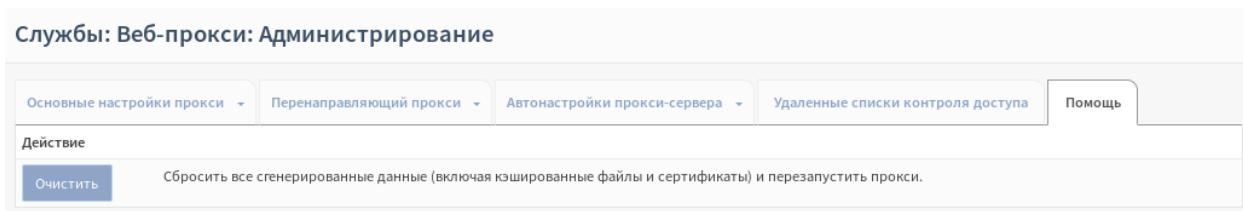


Рисунок 315 – Службы: Веб-прокси: Администрирование: Помощь

10.6.2 Категория «Журнал кэша»

Категория «Журнал кэша» позволяет просматривать журнал кэша в формате таблицы (Рисунок 316).

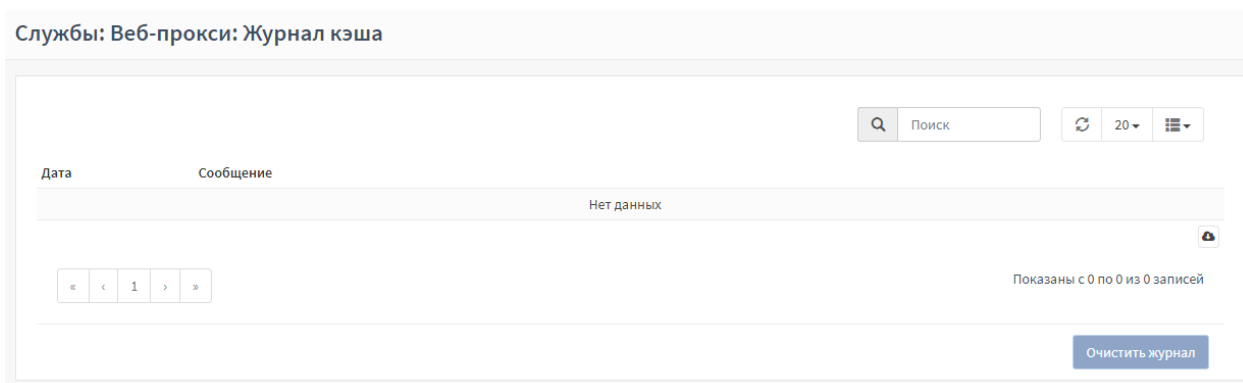


Рисунок 316 – Службы: Веб-прокси: Журнал кэша

10.6.3 Категория «Журнал доступа»

Категория «Журнал доступа» позволяет просматривать журнал доступа в формате таблицы (Рисунок 317).



Рисунок 317 – Службы: Веб-прокси: Журнал доступа

10.6.4 Категория «Журнал хранения»

Категория «Журнал хранения» позволяет просматривать журнал хранения в формате таблицы (Рисунок 318).

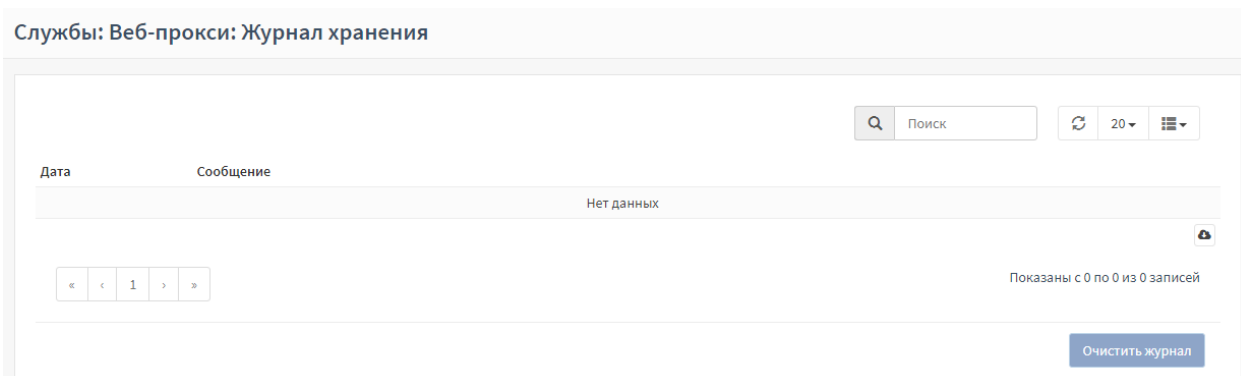


Рисунок 318 – Службы: Веб-прокси: Журнал хранения

11 РАЗДЕЛ VPN

11.1 Подраздел «IPsec»

Режим IPsec предполагает использование ISAKMP/IKEv2 для установления ассоциаций безопасности (security association).

11.1.1 Категория «Настройки туннеля»

Категория «Настройки туннеля» позволяет настраивать VPN-туннель.

Для добавления VPN-туннеля необходимо нажать на кнопку .

В пункте «Общая информация» при необходимости отключить фазу 1, не удаляя ее из списка, необходимо установить флажок напротив «Отключить эту запись фазы 1». В поле «Метод подключения» необходимо выбрать логику соединения. В поле «Версия обмена ключами» необходимо выбрать версию KeyExchange-протокола. В поле «Протокол интернета» необходимо выбрать семейство протоколов Интернета. В поле «Интерфейс» необходимо указать интерфейс для локальной конечной точки создаваемой записи фазы 1. В поле «Удаленный шлюз» необходимо ввести публичный IP-адрес или имя хоста удаленного шлюза. Для динамических IP-адресов рекомендуется установить флажок напротив «Позволить подключения с любого шлюза» в поле «Динамический шлюз». В поле «Описание» необходимо ввести описание (Рисунок 319).

VPN: IPsec: Настройки туннеля









Общая информация	
 Отключена	<input type="checkbox"/> Отключить эту запись фазы 1 Включите этот параметр, чтобы отключить фазу 1, не удаляя ее из списка.
 Метод подключения	<div>по умолчанию</div> <div>Выберите логику соединения. Если вы используете CARP, вы, возможно, захотите использовать параметр «Только ответ» (ожидать подключения другой стороны).</div>
 Версия Обмена ключами	<div>V2</div> <div>Выберите версию KeyExchange-протокола, которая должна использоваться. Она обычно известна как IKEv1 или IKEv2.</div>
 Протокол Интернета	<div>IPv4</div> <div>Выделите семейство Протоколов Интернета из этого выпадающего списка.</div>
 Интерфейс	<div>Internet</div> <div>Выберите интерфейс для локальной конечной точки этой записи phase1.</div>
 Удаленный шлюз	<div>192.168.2.20</div> <div>Введите публичный IP адрес или имя хоста удаленного шлюза.</div>
 Динамический шлюз	<input type="checkbox"/> Позволить подключения с любого шлюза Рекомендуется для динамических IP-адресов, которые могут быть разрешены DynDNS при запуске или обновлении IPsec.
 Описание	<div></div> <div>Вы можете ввести здесь описание ссылки (не обработано).</div>

Рисунок 319 – VPN: IPsec: Настройки туннеля (Общая информация)

В пункте «Предложение Phase 1 (Аутентификация)» в поле «Метод аутентификации» необходимо выбрать метод аутентификации. В поле «Мой идентификатор» необходимо выбрать идентификатор. В поле «Идентификатор пира» необходимо выбрать идентификатор пира. В поле «Предварительно

выданный ключ» необходимо ввести строку предварительного ключа (Рисунок 320).

The screenshot shows a configuration window titled "Предложение Phase 1 (Аутентификация)". It contains four rows of settings, each with an information icon (i) on the left and a dropdown or text field on the right:

- Метод аутентификации: Mutual PSK
- Мой идентификатор: Локальный IP-адрес
- Идентификатор пира: IP-адрес пира
- Предварительно выданный ключ: (empty text field)

Рисунок 320 – VPN: IPsec: Настройки туннеля (Предложение Phase 1 (Аутентификация)) (1)

При выборе Mutual RSA в поле «Метод аутентификация» появятся дополнительные поля. В поле «Мой сертификат» необходимо выбрать сертификат, ранее сконфигурированный с Управлением сертификатами. В поле «Мой центр сертификации» необходимо выбрать центр сертификации (Рисунок 321).

The screenshot shows a configuration window titled "Предложение Phase 1 (Аутентификация)". It contains five rows of settings, each with an information icon (i) on the left and a dropdown or text field on the right:

- Метод аутентификации: Mutual RSA
- Мой идентификатор: Локальный IP-адрес
- Идентификатор пира: IP-адрес пира
- Мой Сертификат: Web GUI SSL certificate
- Мой центр сертификации: test

Рисунок 321 – VPN: IPsec: Настройки туннеля (Предложение Phase 1 (Аутентификация)) (2)

При выборе Mutual Public Key в поле «Метод аутентификация» появятся дополнительные поля. В поле «Локальная пара ключей» необходимо ввести пару локальных ключей, предварительно настроенную в «IPsec» – «Пары ключей RSA». В поле «Пара ключей пира» необходимо ввести пару ключей пира, предварительно настроенную в «IPsec» – «Пары ключей RSA» (Рисунок 322).

Предложение Phase 1 (Аутентификация)	
Метод аутентификации	Mutual Public Key
Мой идентификатор	Локальный IP-адрес
Идентификатор пира	IP-адрес пира
Локальная пара ключей	
Пара ключей пира	

Рисунок 322 – VPN: IPsec: Настройки туннеля (Предложение Phase 1 (Аутентификация)) (3)

В пункте «Предложения Phase 1 (Алгоритмы)» в поле «Алгоритм шифрования» необходимо выбрать алгоритм шифрования. В поле «Алгоритм хеша» необходимо выбрать алгоритм хеширования. В поле «Группа ключей DH» необходимо выбрать соответствующую группу ключей. В поле «Время существования» необходимо задать время или оставить по умолчанию (28800) (Рисунок 323).

Предложение Phase 1 (Алгоритмы)	
Алгоритм шифрования	AES
	128
Алгоритм хеша	SHA256
Группа ключей DH	14 (2048 bits)
Время существования	28800

Рисунок 323 – VPN: IPsec: Настройки туннеля (Предложение Phase 1 (Алгоритмы))

В пункте «Дополнительные параметры» при использовании режима на основе маршрута (VTI) необходимо установить флажок напротив «Политика установки». В поле «Ключ отключения» необходимо установить флажок, если требуется переустановить соединение. В поле «Отключить повторную аутентификацию» необходимо установить флажок, если не требуется повторное подтверждение пира. Для поддержки взаимодействия по протоколу IKEv2 необходимо установить флажок напротив «Изоляция туннеля». Для включения использования NAT-T в поле «Обход контура NAT» необходимо выбрать

настройку. Для отключения протокола IKEv2 MOBIKE необходимо установить флажок напротив «Отключить MOBIKE». Для включения DPD необходимо установить флажок напротив «Обнаружение недоступных пиров». В поле «Тайм-аут неактивности» необходимо указать время до закрытия. В поле «Margintime» необходимо ввести время до старта переполучения ключей SA. В поле «Rekeyfuzz» необходимо ввести процент, на который случайно увеличивается margintime (Рисунок 324).

Дополнительные параметры	
Политика установки	<input checked="" type="checkbox"/>
Ключ отключения	<input type="checkbox"/>
Отключить повторную аутентификацию	<input type="checkbox"/>
Изоляция туннеля	<input type="checkbox"/>
Обход контура NAT	Включен
Отключить MOBIKE	<input type="checkbox"/>
Обнаружение недоступных пиров	<input type="checkbox"/>
Таймаут неактивности	125
Margintime	500
Rekeyfuzz	
<input type="button" value="Сохранить"/>	

Рисунок 324 – VPN: IPsec: Настройки туннеля (Дополнительные параметры)

После внесения изменений необходимо нажать на кнопку «Сохранить».

11.1.2 Категория «Мобильные клиенты»

Категория «Мобильные клиенты» позволяет настраивать IPsec на сервере.

Для включения поддержки мобильных клиентов IPsec необходимо установить флажок напротив «Включен». В пункте «Расширенная аутентификация (Xauth)» в поле «Сервер для аутентификации» необходимо выбрать сервер. В поле «Принудительно использовать группу» при необходимости ограничения доступа пользователям выбрать локальную группу. В пункте «Конфигурация клиента (modecfg)» в поле «Пул виртуальных адресов IPv4/IPv6» необходимо установить флажок в «Предоставление виртуальных IP-адресов клиентам» и в окне ниже указать сеть или IP-адрес, которой будут выдаваться VPN-клиентам. В поле «Список сети» при необходимости установить флажок в «Предоставьте список доступных сетей».

клиентам». В поле «Сохранить пароль Xauth» необходимо установить флажок, чтобы разрешить клиентам сохранять Xauth пароли. При необходимости предоставления клиентам доменного имени по умолчанию установить флажок в поле «Домен DNS по умолчанию» и написать имя. В поле «Разделить DNS». При необходимости предоставления клиентам список NTP-серверов установить флажки в соответствующих полях «DNS-серверы» и «WINS-серверы». В поле «Группа phase 2 PFS» необходимо указать группу phase 2 PFS. В поле «Баннер при входе» при необходимости установить флажок напротив «Предоставить клиентам баннер при входе» (Рисунок 325).

VPN: IPsec: Мобильные клиенты

Расширения IKE	
Включен	<input checked="" type="checkbox"/> Включить поддержку мобильных клиентов IPsec
Расширенная аутентификация (Xauth)	
Сервер для аутентификации	Локальная база данных
Принудительно использовать локальную группу	(отсутствует)
Конфигурация клиента (mode-cfg)	
Пул виртуальных IPv4 адресов	<input checked="" type="checkbox"/> Укажите виртуальный IPv4 адрес клиентам 192.168.0.0 24
Пул виртуальных IPv6 адресов	<input type="checkbox"/> Укажите виртуальный IPv6 адрес клиентам 64
Список сети	<input type="checkbox"/> Предоставьте список доступных сетей клиентам
Сохранить пароль Xauth	<input type="checkbox"/> Разрешить клиентам сохранять Xauth пароли (Только для клиентов Cisco VPN)
Домен DNS по умолчанию	<input type="checkbox"/> Предоставить клиентам доменное имя по умолчанию
Разделить DNS	<input type="checkbox"/> Предоставьте список разделенных DNS имен доменов клиентам
DNS-серверы	<input type="checkbox"/> Предоставить клиенту список DNS-серверов
WINS-серверы	<input type="checkbox"/> Предоставить клиенту список WINS-серверов
Группа phase 2 PFS	выкл.
Баннер при входе	<input type="checkbox"/> Предоставить клиентам баннер при входе
<input type="button" value="Сохранить"/>	

Рисунок 325 – VPN: IPsec: Мобильные клиенты

После внесения изменений необходимо нажать на кнопку «Сохранить».

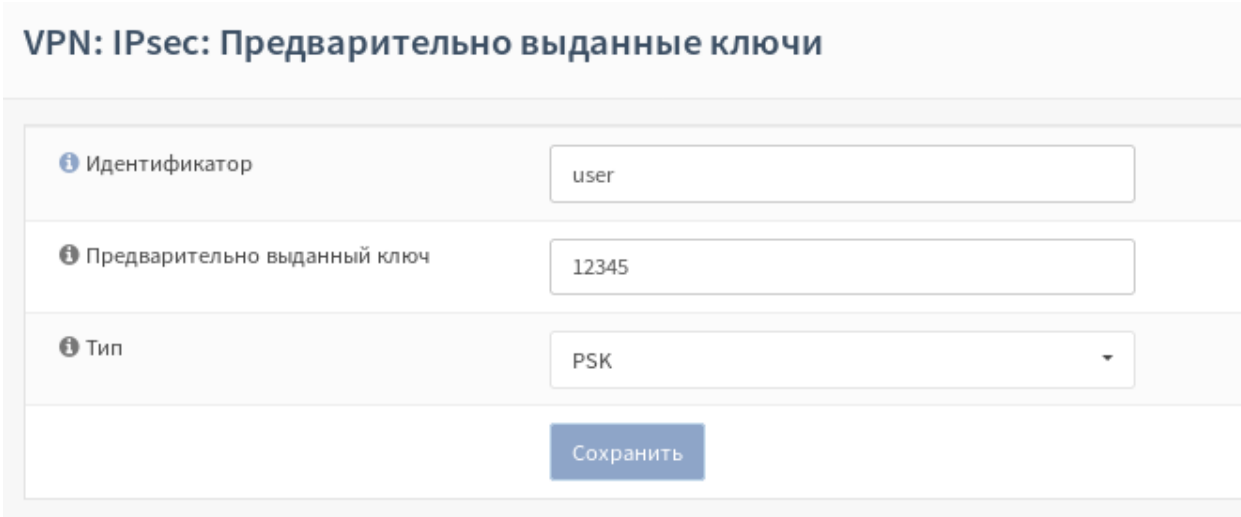
11.1.3 Категория «Предварительно выданные ключи»

Категория «Предварительно выданные ключи» позволяет создавать ключ, который будет использоваться для аутентификации устройства связи.

Для того чтобы создать ключ необходимо нажать на кнопку



В поле «Идентификатор» необходимо указать IP-адрес, полностью определенное имя домена или адрес электронной почты. В поле «Предварительно выданный ключ» необходимо задать ключ. В поле «Тип» выбрать тип ключа и нажать на кнопку «Сохранить» (Рисунок 326).



VPN: IPsec: Предварительно выданные ключи

Идентификатор	<input type="text" value="user"/>
Предварительно выданный ключ	<input type="text" value="12345"/>
Тип	<input type="text" value="PSK"/>

Рисунок 326 – VPN: IPsec: Предварительно выданные ключи

11.1.4 Категория «Пары ключей RSA»

Категория «Пары ключей RSA» позволяет создавать пары ключей RSA для аутентификации в сетях IPsec VPN.

Для добавления необходимо нажать на кнопку .

В поле «Имя» необходимо ввести имя для пары ключей. В поле «Тип» необходимо выбрать тип пары ключей. В поле «Открытый ключ» необходимо вставить открытый ключ выбранного типа. В поле «Секретный ключ» необходимо вставить опциональный закрытый ключ соответствующий открытому ключу (Рисунок 327).

Редактировать пару ключей

справка

Имя

user

Тип ключа

RSA

Открытый ключ

Секретный ключ

Отменить

Сохранить

Рисунок 327 – VPN: IPsec: Пары ключей RSA

11.1.5 Категория «Дополнительные настройки»

Категория «Дополнительные настройки» позволяет задавать дополнительные настройки IPsec.

Для отключения автоматического добавления правил VPN необходимо установить флажок в «Отключить все автоматически добавленные правила VPN». В поле «Ассоциации безопасности» необходимо установить флажок при необходимости всегда предпочитать старые SA новым. В поле «Сквозные сети» при необходимости добавить свою локальную сеть (-и). Для предотвращения автоматического добавления маршрутов необходимо установить флажок напротив «Не устанавливать маршруты автоматически» (Рисунок 328).

VPN: IPsec: Дополнительные настройки

Дополнительные настройки IPsec

Отключить автоматически добавленные правила VPN

☐ Отключить все автоматически добавленные правила VPN.

Ассоциации безопасности

☒ Предпочесть более старый IPsec SAs

Сквозные сети

Не устанавливать маршруты

☐ Не устанавливать маршруты автоматически

Рисунок 328 – VPN: IPsec: Дополнительные настройки (часть 1)

В поле «Отладка IPsec» необходимо выбрать разделы, на основании которых будет запущен IPsec (Рисунок 329).

Отладка IPsec

Запустить IPsec в режиме на основе выбранных разделов
Низкоуровневое кодирование/декодирование (ASN.1, X.509 и т.д.)

Базовая

Управление конфигурацией и плагинами

Базовая

CHILD_SA/IPsec SA

Базовая

Основной демон настройки/очистки/обработки сигналов

Базовая

Кодирование/декодирование пакетов, операции шифрования/дешифрования

Базовая

Сообщения библиотеки libipsec

Базовая

IKE_SA/ISAKMP SA

Базовая

Integrity Measurement Collector

Базовая

Integrity Measurement Verifier

Базовая

Работы с очередями/обработка и управление пулом потоков

Базовая

IPsec / Сетевой интерфейс ядра

Базовая

Сообщения библиотеки libstrongswan

Базовая

IKE_SA, обрабатывающий синхронизацию для доступа IKE_SA

Базовая

Сетевое взаимодействие IKE

Базовая

Служба доверенной платформы

Базовая

Сообщения библиотеки libtls

Базовая

Доверенное сетевое подключение

Базовая

Запустить IPsec в режиме отладки, чтобы генерировались более подробные журналы в целях устранения неисправностей.

Рисунок 329 – VPN: IPsec: Дополнительные настройки (часть 2)

11.1.6 Категория «Информация о статусе»

В категории «Информация о статусе» отображается информация о статусе соединений IPsec (Рисунок 330).

VPN: IPsec: Информация о статусе

Соединение	Версия	Локальный идентификатор	Локальный IP-адрес	Удаленный идентификатор	Удаленный IP-адрес	Локальная аутентификация	Удаленная аутентификация	Статус
------------	--------	-------------------------	--------------------	-------------------------	--------------------	--------------------------	--------------------------	--------

Рисунок 330 – VPN: IPsec: Информация о статусе

11.1.7 Категория «Статус аренды адресов»

В категории «Статус аренды адресов» отображается информация о статусе аренды адресов (Рисунок 331).

VPN: IPsec: Статус аренды адресов

Нет пулов IPsec.

Рисунок 331 – VPN: IPsec: Статус аренды адресов

11.1.8 Категория «База данных безопасных ассоциаций (SAD)»

В категории «База данных безопасных ассоциаций (SAD)» отображается база данных безопасных ассоциаций (Рисунок 332).

VPN: IPsec: База данных безопасных ассоциаций (SAD)

Нет безопасных ассоциаций IPsec.

Рисунок 332 – VPN: IPsec: База данных безопасных ассоциаций (SAD)

11.1.9 Категория «База данных политик безопасности (SPD)»

В категории «База данных политик безопасности (SPD)» отображается база данных политик безопасности (Рисунок 333).

VPN: IPsec: База данных политик безопасности (SPD)

Нет политик безопасности IPsec.

Рисунок 333 – VPN: IPsec: База данных политик безопасности (SPD)

11.1.10 Категория «Журнал»

В категории «Журнал» отображаются сообщения о настроенных VPN-туннелях (Рисунок 334).

VPN: IPsec: Журнал

Поиск

20

Дата	Сообщение
Нет данных	

« < 1 > »

Показаны с 0 по 0 из 0 записей

Очистить журнал


Рисунок 334 – VPN: IPsec: Журнал

11.2 Подраздел «OpenVPN»

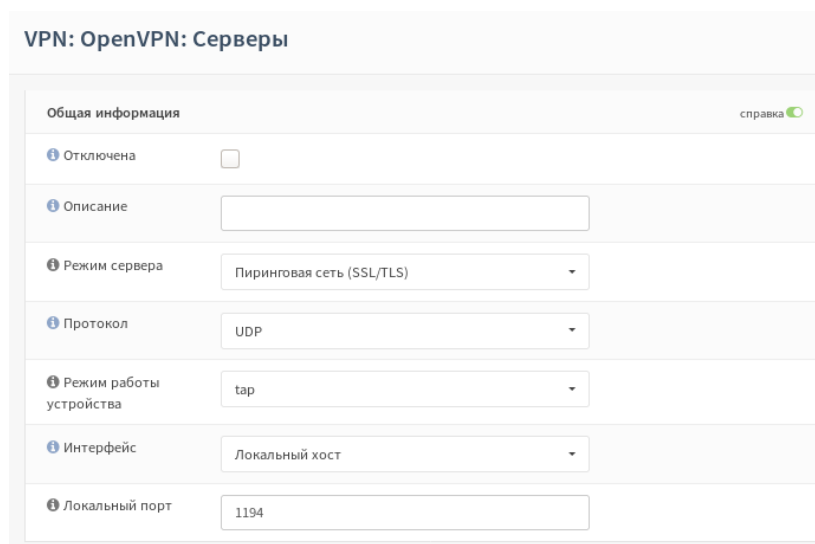
OpenVPN – это реализация VPN, которая использует SSL/TLS для защиты туннелируемого трафика. Такой подход становится возможным благодаря механизму TUN/TAP, реализованному в виде загружаемого драйвера ядра. OpenVPN поддерживает работу в режиме «сеть» - «сеть» и «узел» - «сеть».

11.2.1 Категория «Серверы»

Категория «Серверы» позволяет настраивать OpenVPN сервер.

Для добавления сервера необходимо нажать на кнопку .

В пункте «Общая информация» при необходимости отключить сервер, не удаляя его из списка, необходимо установить флажок напротив «Отключена». В поле «Описание» необходимо ввести описание ссылки. В поле «Режим сервера» необходимо выбрать из выпадающего списка режим сервера. В поле «Протокол» необходимо выбрать семейство протоколов для использования. В поле «Режим работы устройства» необходимо выбрать виртуальный сетевой драйвер ядра системы. В поле «Интерфейс» необходимо выбрать интерфейс. В поле «Локальный порт» необходимо указать локальный порт (Рисунок 335).




The screenshot shows a web interface for configuring an OpenVPN server. The title is 'VPN: OpenVPN: Серверы'. Below it is a tabbed interface with the 'Общая информация' tab selected. To the right of the tab is a 'справка' (help) icon. The form contains several fields:

- Отключена:** A checkbox that is currently unchecked.
- Описание:** A text input field.
- Режим сервера:** A dropdown menu with 'Пиринговая сеть (SSL/TLS)' selected.
- Протокол:** A dropdown menu with 'UDP' selected.
- Режим работы устройства:** A dropdown menu with 'tap' selected.
- Интерфейс:** A dropdown menu with 'Локальный хост' selected.
- Локальный порт:** A text input field containing the value '1194'.

Рисунок 335 – VPN: OpenVPN: Серверы (Общая информация)

При выборе режима сервера «Удаленный доступ (аутентификация пользователя)» и «Удаленный доступ (SSL/TLS+аутентификация пользователя)» появится дополнительное окно «Сервер для аутентификации», в котором необходимо указать сервер для аутентификации (Рисунок 336).

VPN: OpenVPN: Серверы

Общая информация справка 

Отключена ☐

Описание

Режим сервера

Сервер для аутентификации

Принудительно использовать локальную группу
 Ограничить доступ пользователями выбранной локальной группы. Пожалуйста убедитесь что другие механизмы аутентификации отказывают в аутентификации когда используете эту опцию.

Протокол

Режим работы устройства

Интерфейс

Локальный порт

Рисунок 336 – VPN: OpenVPN: Серверы (режим «Удаленный доступ (SSL/TLS+аутентификация пользователя)»)

В пункте «Криптографические установки» для включения аутентификации пакетов TLS и автоматического генерирования совместно использующего ключа аутентификации TLS необходимо установить флажки напротив нужных пунктов в поле «Аутентификация TLS». В поле «Центр сертификации пиров» необходимо выбрать центр сертификации пиров. В поле «Список отзыва сертификатов узлов» необходимо выбрать список, если такой создан или создать его в разделе «Система» - «Доверенные сертификаты» - «Отзыв сертификатов». В поле «Сертификат сервера» необходимо выбрать сертификат сервера. В поле «Длина параметров DH» необходимо выбрать формат параметра DH. В поле «Алгоритм шифрования» необходимо выбрать алгоритм шифрования. В поле «Дайджест-алгоритм аутентификации» необходимо выбрать дайджест-алгоритм аутентификации, если клиенты не поддерживают установленный по умолчанию алгоритм хеширования SHA1. В поле «Аппаратные средства криптозащиты» необходимо выбрать средство криптозащиты. В поле «Уровень сертификата» необходимо указать уровень сертификата (Рисунок 337).

Криптографические установки	
1 Аутентификация TLS	<input checked="" type="checkbox"/> Включить аутентификацию пакетов TLS. <input checked="" type="checkbox"/> Автоматически генерировать совместно используемый ключ аутентификации TLS.
1 Центр сертификации пиров	Не выбрано ▲
1 Список отзыва сертификатов узлов	Списки отзыва сертификатов (CRL) не определены. Создать под Система: сертификаты .
1 Сертификат сервера	Web GUI SSL certificate *In Use ▲
1 Длина параметров DH	2048 бит ▲
1 Алгоритм шифрования	AES-128-CBC (128 bit key, 128 bit block) ▲
1 Дайджест-алгоритм аутентификации	SHA1 (160-bit) ▲
1 Аппаратные средства криптозащиты	Без аппаратного ускорения криптоалгоритмов ▲
1 Уровень сертификата	Один (клиент+сервер) ▲

Рисунок 337 – VPN: OpenVPN: Серверы (Криптографические установки)

В пункте «Настройки туннеля» в полях «Туннельная сеть IPv4» и «Туннельная сеть IPv6» необходимо указать адрес сети виртуального сервера. В поле «Перенаправление шлюза» необходимо установить флажок для того, чтобы передавать весь трафик клиента через туннель. При необходимости добавлять маршруты к локальной сети через туннель на удаленном компьютере указать адрес сетей IPv4 и IPv6 в полях «Локальная сеть IPv4» и «Локальная сеть IPv6». Для VPN-соединения между двумя пунктами необходимо ввести адрес удаленной сети LAN в полях «Удаленная сеть IPv4» и «Удаленная сеть IPv6». В поле «Число одновременных подключений» необходимо указать максимальное количество клиентов, которым разрешено одновременно подключаться к серверу. В поле «Сжатие» необходимо выбрать алгоритм сжатия туннельных пакетов. Для совпадения IP заголовка туннельного пакета со значением инкапсулированного пакета необходимо установить флажок напротив поля «Тип сервиса». Для разрешения нескольких одновременных подключений от клиентов в поле «Резервные соединения» необходимо установить флажок. При необходимости не переадресовывать IPv6-трафик необходимо установить флажок напротив поля «Отключить IPv6» (Рисунок 338).

Настройки туннеля	
Туннельная сеть IPv4	192.168.2.22
Туннельная сеть IPv6	
Перенаправление шлюза	<input checked="" type="checkbox"/>
Удаленная сеть IPv4	192.168.1.20
Удаленная сеть IPv6	
Число одновременных подключений	5
Сжатие	Включено с использованием адаптивного сжатия ▼
Тип сервиса	<input type="checkbox"/>
Резервные соединения	<input checked="" type="checkbox"/>
Отключить IPv6	<input type="checkbox"/>

Рисунок 338 – VPN: OpenVPN: Серверы (Настройки туннеля)

В пункте «Настройки клиента» в поле «Динамический IP-адрес» необходимо установить флажок для разрешения подключенным клиентам сохранять соединения, если их IP-адрес изменился. В поле «Пул IP-адресов» для предоставления клиентам IP-адрес виртуального адаптера необходимо установить флажок. В поле «Топология сети» при необходимости выделить только один IP-адрес для клиента необходимо установить флажок. Для предоставления клиентам доменного имени по умолчанию необходимо установить флажок напротив поля «Домен DNS по умолчанию». Для принудительного обновления кэша DNS необходимо установить флажок напротив поля «Принудительное обновление кэша DNS». При необходимости предоставлять клиенту список NTP-серверов необходимо установить флажок напротив поля «NTP-серверы» и указать серверы в полях ниже. Для включения NetBIOS через TCP/IP необходимо установить флажок напротив поля «Параметры NetBIOS». В поле «Порт управления клиентами» необходимо установить флажок, если используется другой порт управления на клиентах и в соответствующем поле указать порт (Рисунок 339).

Настройки клиента	
<i>i</i> Динамический IP-адрес	<input type="checkbox"/>
<i>i</i> Пул IP-адресов	<input checked="" type="checkbox"/>
<i>i</i> Топология сети	<input type="checkbox"/>
<i>i</i> Домен DNS по умолчанию	<input type="checkbox"/>
<i>i</i> DNS-серверы	<input type="checkbox"/>
<i>i</i> Принудительное обновление кэша DNS	<input type="checkbox"/>
<i>i</i> NTP-серверы	<input checked="" type="checkbox"/> Сервер №1: <input type="text" value="192.168.1.50"/> Сервер №2: <input type="text"/>
<i>i</i> Параметры NetBIOS	<input type="checkbox"/>
<i>i</i> Порт управления клиентами	<input checked="" type="checkbox"/> <input type="text" value="198"/>

Рисунок 339 – VPN: OpenVPN: Серверы (Настройки клиента)


В пункте «Дополнительная конфигурация» в поле «Дополнительно» при необходимости ввести любые дополнительные параметры. В поле «Уровень детальности сообщений» необходимо выбрать уровень из выпадающего списка. При необходимости использовать имя пользователя вместо общего имени для проверки совпадения переопределенных значений необходимо установить флажок напротив поля «Принудительно принимать логин их переопределенных значений клиента» (Рисунок 340).

Рисунок 340 – VPN: OpenVPN: Серверы (Дополнительная конфигурация)

После внесения изменений необходимо нажать на кнопку «Сохранить».

11.2.2 Категория «Клиенты»

Категория «Клиенты» позволяет настраивать OpenVPN клиента.

Для добавления клиента необходимо нажать на кнопку .

В пункте «Общая информация» при необходимости отключить сервер, не удаляя его из списка, необходимо установить флажок напротив «Отключена». В поле «Описание» необходимо ввести описание ссылки. В поле «Режим сервера» необходимо выбрать из выпадающего списка режим сервера. В поле «Протокол» необходимо выбрать семейство протоколов для использования. В поле «Режим работы устройства» необходимо выбрать виртуальный сетевой драйвер ядра системы. В поле «Интерфейс» необходимо выбрать интерфейс. В поле «Удаленный сервер» необходимо ввести адрес удаленного сервера или выбрать его случайным образом, установив флажок в поле «Выбрать удаленный сервер случайным образом». Для неограниченного разрешения удаленного сервера необходимо установить флажок напротив поля «Установите повторно разрешение DNS». В поле «Хост или адрес Прокси» необходимо ввести хост или адрес прокси. В поле «Номер порта прокси-сервера» необходимо указать порт прокси-сервера. В поле «Дополнительные опции аутентификации прокси» необходимо выбрать метод аутентификации и в полях «Имя пользователя» и «Пароль» необходимо ввести имя и пароль. При необходимости привязаться к определенному порту в поле «Локальный порт» необходимо ввести значение порта (Рисунок 341).

VPN: OpenVPN: Клиенты

Общая информация		
Отключена	<input type="checkbox"/>	
Описание	<input type="text"/>	
Режим сервера	Пиринговая сеть (SSL/TLS)	
Протокол	UDP	
Режим работы устройства	tun	
Интерфейс	любой	
Удаленный сервер	Хост или адрес	Порт
	<input type="text"/>	<input type="text"/>
	<input checked="" type="checkbox"/> Выбрать удаленный сервер случайным образом	
Установите повторно разрешение DNS	<input type="checkbox"/> Неограниченное разрешение удаленного сервера	
Хост или адрес Прокси	<input type="text"/>	
Номер порта прокси-сервера	<input type="text"/>	
Дополнительные опции аутентификации прокси	Метод аутентификации базовый Имя пользователя root Пароль ****	

Рисунок 341 – VPN: OpenVPN: Клиенты (Общая информация)

В пункте «Настройки аутентификации пользователей» в поле «Имя пользователя/пароль» необходимо ввести имя и пароль пользователя, если не требуется оставить пустым. В поле «Время пересогласования» необходимо ввести время пересогласования ключа канала данных в секундах (Рисунок 342).

Настройки Аутентификации пользователей	
Имя пользователя/пароль	Имя пользователя <input type="text"/> Пароль <input type="text"/> Оставьте пустым, когда не требуется имя пользователя и пароль.
Время пересогласования	4500

Рисунок 342 – VPN: OpenVPN: Клиенты (Настройки аутентификации пользователей)

В пункте «Криптографические установки» для включения аутентификации пакетов TLS и автоматического генерирования совместно использующего ключа аутентификации TLS необходимо установить флажки напротив нужных пунктов в поле «Аутентификация TLS». В поле «Центр сертификации пиров» необходимо выбрать центр сертификации пиров. В поле «Сертификат клиента» необходимо выбрать сертификат клиента. В поле «Алгоритм шифрования» необходимо выбрать алгоритм шифрования. В поле «Дайджест-алгоритм аутентификации» необходимо

выбрать дайджест-алгоритм аутентификации, если клиенты не поддерживают установленный по умолчанию алгоритм хеширования SHA1. В поле «Аппаратные средства криптозащиты» необходимо выбрать средство криптозащиты (Рисунок 343).

Криптографические установки	
1 Аутентификация TLS	<input checked="" type="checkbox"/> Включить аутентификацию пакетов TLS. <input checked="" type="checkbox"/> Автоматически генерировать совместно используемый ключ аутентификации TLS.
1 Центр сертификации пиров	<input type="text"/>
1 Сертификат клиента	Отсутствует (Требуется имя пользователя и паро...)
1 Алгоритм шифрования	AES-128-CBC (128 bit key, 128 bit block)
1 Дайджест-алгоритм аутентификации	SHA1 (160-bit)
1 Аппаратные средства криптозащиты	Без аппаратного ускорения криптоалгоритмов

Рисунок 343 – VPN: OpenVPN: Клиенты (Криптографические настройки)

В пункте «Настройки туннеля» в полях «Туннельная сеть IPv4» и «Туннельная сеть IPv6» необходимо указать адрес сети виртуального сервера. Для VPN-соединения между двумя пунктами необходимо ввести адрес удаленной сети LAN в полях «Удаленная сеть IPv4» и «Удаленная сеть IPv6». В поле «Ограничить исходящую пропускную способность» необходимо указать максимальную исходящую пропускную способность для туннеля. В поле «Сжатие» необходимо выбрать алгоритм сжатия туннельных пакетов. Для совпадения IP заголовка туннельного пакета со значением инкапсулированного пакета необходимо установить флажок напротив поля «Тип сервиса». При необходимости не переадресовывать IPv6-трафик необходимо установить флажок напротив поля «Отключить IPv6». Для того чтобы запретить серверу добавлять маршруты в таблицу маршрутизации клиента необходимо установить флажок напротив поля «Не получать маршруты». В поле «Не добавлять/удалять маршруты» необходимо установить флажок, чтобы не добавлять и не удалять маршруты автоматически (Рисунок 344).

Настройки туннеля	
Туннельная сеть IPv4	192.168.2.23
Туннельная сеть IPv6	
Удаленная сеть IPv4	192.168.1.40
Удаленная сеть IPv6	
Ограничить исходящую пропускную способность	350
Сжатие	Включено с использованием адаптивного сжатия
Тип сервиса	<input checked="" type="checkbox"/>
Отключить IPv6	<input type="checkbox"/>
Не получать маршруты	<input type="checkbox"/>
Не добавлять/удалять маршруты	<input checked="" type="checkbox"/>

Рисунок 344 – VPN: OpenVPN: Клиенты (Настройки туннеля)

В пункте «Дополнительная конфигурация» в поле «Дополнительно» при необходимости ввести любые дополнительные параметры. В поле «Уровень детальности сообщений» необходимо выбрать уровень из выпадающего списка (Рисунок 345).

Дополнительная конфигурация	
Дополнительно	<div></div>
Уровень детальности сообщений	<div>1 (по умолчанию)</div> <p>Каждый уровень показывает всю информацию из предыдущих уровней. Рекомендуется использовать уровень 3, если вам необходима подробная сводка того, что происходит, без лишнего вывода</p> <p>none — нет результатов, кроме фатальных ошибок. default-4 — диапазон обычного использования. 5 — вывод символов R и W в консоль для каждого прочитанного и записанного пакета, верхний регистр используется для пакетов TCP/UDP, а нижний регистр для пакетов TUN/TAP. 6-11 — диапазон отладочной информации.</p>
<div>Сохранить</div>	

Рисунок 345 – VPN: OpenVPN: Клиенты (Дополнительная конфигурация)

После внесения изменений необходимо нажать на кнопку «Сохранить».

11.2.3 Категория «Переопределение значений для конкретного клиента»

В пункте «Общая информация» при необходимости отключить переопределение для конкретного клиента, не удаляя его из списка, необходимо установить флажок напротив «Отключена». В поле «Серверы» необходимо выбрать сервер OpenVPN. В поле «Стандартное имя» необходимо ввести имя клиента. В поле «Блокировка соединений» необходимо установить флажок для блокирования соединения клиента на основании его стандартного имени (Рисунок 346).

VPN: OpenVPN: Переопределение значений для конкретного клиента

Общая информация	
Отключена	<input checked="" type="checkbox"/>
Серверы	Не выбрано
Стандартное имя	<input type="text"/>
Описание	<input type="text"/>
Блокировка соединений	<input checked="" type="checkbox"/>

Рисунок 346 – VPN: OpenVPN: Переопределение значений конкретного клиента (Общая информация)

В пункте «Настройки туннеля» в полях «Туннельная сеть IPv4» и «Туннельная сеть IPv6» необходимо указать адрес сети виртуального сервера. При необходимости добавлять маршруты к локальной сети через туннель на удаленном компьютере указать адрес сетей IPv4 и IPv6 в полях «Локальная сеть IPv4» и «Локальная сеть IPv6». Для VPN-соединения между двумя пунктами необходимо ввести адрес удаленной сети LAN в полях «Удаленная сеть IPv4» и «Удаленная сеть IPv6». В поле «Перенаправление шлюза» необходимо установить флажок для того, чтобы передавать весь трафик клиента через туннель (Рисунок 347).

Настройки туннеля	
Туннельная сеть IPv4	192.168.2.21
Туннельная сеть IPv6	
Локальная сеть IPv4	192.168.1.55
Локальная сеть IPv6	
Удаленная сеть IPv4	
Удаленная сеть IPv6	
Перенаправление шлюза	<input checked="" type="checkbox"/>

Рисунок 347 – VPN: OpenVPN: Переопределение значений конкретного клиента (Настройки туннеля)

В пункте «Настройки клиента» в поле «Определение сервера» необходимо установить флажок для предотвращения получения клиентом каких-либо клиентских настроек, определенных сервером. Для предоставления клиентам доменного имени по умолчанию необходимо установить флажок напротив поля «Домен DNS по умолчанию». При необходимости предоставлять клиенту список NTP-серверов необходимо установить флажок напротив поля «NTP-серверы» и указать серверы в полях ниже. Для включения NetBIOS через TCP/IP необходимо установить флажок напротив поля «Параметры NetBIOS». В поле «Дополнительно» необходимо ввести любые дополнительные параметры (Рисунок 348).

Настройки клиента	
Определения сервера	<input checked="" type="checkbox"/>
Домен DNS по умолчанию	<input type="checkbox"/>
DNS-серверы	<input type="checkbox"/>
NTP-серверы	<input type="checkbox"/>
Параметры NetBIOS	<input type="checkbox"/>
Дополнительно	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div>
<div style="background-color: #4a7ebb; color: white; padding: 5px 15px; display: inline-block;">Сохранить</div>	

Рисунок 348 – VPN: OpenVPN: Переопределение значений конкретного клиента (Настройки клиента)

После внесения изменений необходимо нажать на кнопку «Сохранить».

11.2.4 Категория «Экспорт настроек клиента»

Категория «Экспорт настроек клиента» позволяет настроить экспорт профилей клиентов.

В поле «Сервер удаленного доступа» необходимо выбрать OpenVPN-сервер для экспорта профилей. В поле «Тип экспорта» необходимо выбрать формат файла для экспорта. В поле «Имя хоста» необходимо ввести адрес (-а) или имя (имена) хостов. В поле «Порт» необходимо указать прослушиваемый порт OpenVPN. При необходимости использовать случайный локальный порт источника для трафика от клиента в поле «Использовать случайный локальный порт» установить флажок. В поле «P12 Пароль/Подтверждение пароля» необходимо ввести пароль для защиты содержимого файла pkcs12. Для включения проверки имени сервера сертификата при подключении клиента необходимо установить флажок напротив поля «Проверка сервера». В поле «Windows Certificate System Store» необходимо установить флажок для загрузки сертификата и закрытого ключа из Windows Certificate System Store. Для того чтобы не сохранять пароль в памяти необходимо установить флажок напротив поля «Не сохранять пароль». В поле «Пользовательская конфигурация» необходимо ввести конфигурацию, которая будет возвращена в файле вывода без изменений (Рисунок 349).

VPN: OpenVPN: Экспорт настроек клиента

Сервер удаленного доступа	Не выбрано
Тип экспорта	Не выбрано
Имя хоста	
Порт	
Использовать случайный локальный порт	<input checked="" type="checkbox"/>
Проверка сервера	<input checked="" type="checkbox"/>
Windows Certificate System Store	<input checked="" type="checkbox"/>
Не сохранять пароль	<input type="checkbox"/>
Пользовательская конфигурация	

Учетные записи / сертификаты

Сертификат	Пользователи
------------	--------------

Рисунок 349 – VPN: OpenVPN: Экспорт настроек клиента

11.2.5 Категория «Статус соединения»

В категории «Статус соединения» отображаются статусы всех запросов OpenVPN (Рисунок 350).

VPN: OpenVPN: Статус соединения

Статус OpenVPN
Не определено запросов OpenVPN

Рисунок 350 – VPN: OpenVPN: Статус соединения

11.2.6 Категория «Журнал»

В категории «Журнал» отображаются сообщения о настроенных OpenVPN серверов и клиентах (Рисунок 351).

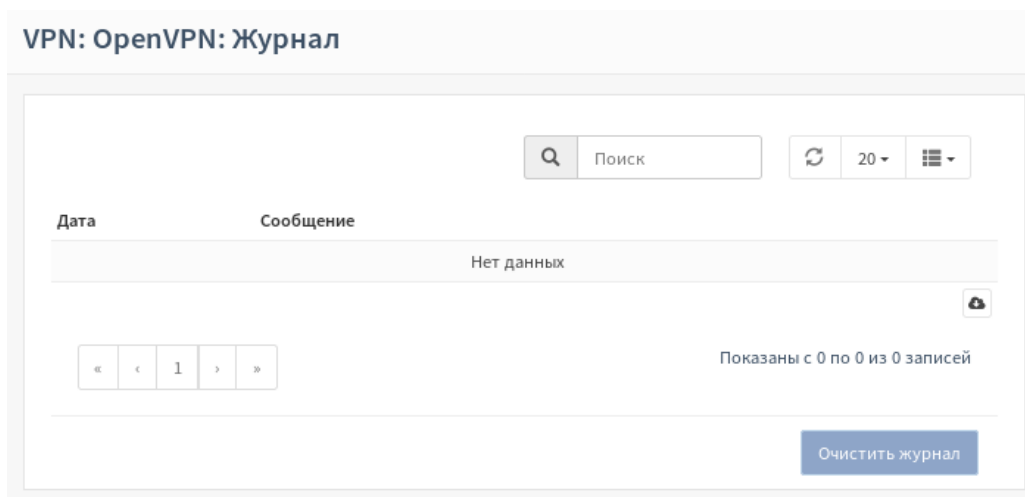


Рисунок 351 – VPN: OpenVPN: Журнал

12 ПОЛЬЗОВАТЕЛЬСКИЕ СЦЕНАРИИ

12.1 Настройка Netflow

Для настройки Netflow необходимо перейти в раздел «Создание отчетов» - «Netflow» (Рисунок 352).

Создание отчетов: NetFlow

Захват Кэш

☒ расширенный режим

Прослушиваемые интерфейсы LAN Очистить все

Интерфейсы WAN Не выбрано Очистить все

Захватывать внутренний трафик ☒

Версия v9

Получатели 192.168.0.1:2550 Очистить все

Таймаут активности 1800

Таймаут неактивности 15

Применить

Рисунок 352 – Настройка Netflow

В поле «LAN интерфейс» необходимо выбрать все интерфейсы, из которых необходимо собирать данные. В поле «WAN интерфейс» необходимо выбрать все интерфейсы, из которых необходимо экспортировать данные. Для анализа локального трафика необходимо поставить «галочку» напротив поля «Захватывать внутренний трафик». В зависимости от протокола, необходимо выбрать «v5» или «v9» в поле «Версия» («v5» не поддерживает IPv6).

В поле «Получатели» необходимо добавить получателей в формате [IP-адрес: порт]. Внутренний IP-адрес будет добавлен автоматически, если выбрано «Захватывать внутренний трафик». Необходимо нажать на кнопку «Применить».

Необходимо подождать сбор трафика Netflow в зависимости от активности трафика. На удаленном компьютере появится статистика, собранная Netflow (Рисунок 353).


```
user@user-VirtualBox:~$ flow-cat /var/log/flow/ft-v05.2019-11-14.161501+0300|flow-print -f5
```

Start	End	Sif	SrcIPaddress	SrcP	Dif	DstIPaddress	DstP	P	Fl	Pkts	Octets
1114.16:12:07.516	1114.16:12:07.516	0	192.168.1.1	56531	1	192.168.1.99	2550	17	0	1	1492
1114.16:12:09.516	1114.16:12:09.516	1	192.168.1.99	43434	3	192.168.1.1	2550	17	0	1	100
1114.16:12:43.516	1114.16:12:46.516	1	192.168.1.201	10168	1	192.168.1.52	80	6	2	2	104
1114.16:12:43.516	1114.16:12:46.516	1	192.168.1.201	10169	1	192.168.1.52	80	6	2	2	104
1114.16:12:54.516	1114.16:12:54.516	1	192.168.1.99	43434	3	192.168.1.1	2550	17	0	1	148
1114.16:13:13.516	1114.16:13:13.516	1	192.168.1.99	44922	3	192.168.1.1	2550	17	0	1	100
1114.16:13:14.516	1114.16:13:14.516	1	192.168.1.99	43434	3	192.168.1.1	2550	17	0	1	100
1114.16:13:45.516	1114.16:13:48.516	1	192.168.1.201	60424	3	239.255.255.250	1900	17	0	4	804
1114.16:14:23.516	1114.16:14:23.516	1	192.168.1.99	44922	3	192.168.1.1	2550	17	0	1	148
1114.16:14:19.516	1114.16:14:24.516	1	192.168.1.99	43434	3	192.168.1.1	2550	17	0	2	200
1114.16:14:47.516	1114.16:14:47.516	1	192.168.1.99	44922	3	192.168.1.1	2550	17	0	1	292
1114.16:14:47.516	1114.16:14:47.516	1	192.168.1.99	43434	3	192.168.1.1	2550	17	0	1	292
1114.16:15:00.516	1114.16:15:09.516	1	192.168.1.201	10182	3	192.168.1.1	22	6	2	3	156
1114.16:15:14.516	1114.16:15:14.516	1	192.168.1.201	54241	3	224.0.0.252	5355	17	0	1	50
1114.16:14:29.516	1114.16:15:43.516	0	192.168.1.1	80	1	192.168.1.201	10179	6	3	561	807611
1114.16:15:45.516	1114.16:15:48.516	1	192.168.1.201	56393	1	239.255.255.250	1900	17	0	4	804
1114.16:15:57.516	1114.16:15:57.516	1	192.168.1.99	44922	3	192.168.1.1	2550	17	0	1	148
1114.16:15:57.516	1114.16:15:57.516	1	192.168.1.99	43434	3	192.168.1.1	2550	17	0	1	148
1114.16:16:22.516	1114.16:16:22.516	1	192.168.1.99	44922	3	192.168.1.1	2550	17	0	1	148
1114.16:16:22.516	1114.16:16:22.516	1	192.168.1.99	43434	3	192.168.1.1	2550	17	0	1	148
1114.16:16:28.516	1114.16:16:28.516	0	192.168.1.1	80	1	192.168.1.201	10179	6	0	1	40
1114.16:16:42.516	1114.16:16:57.516	1	192.168.1.99	44922	3	192.168.1.1	2550	17	0	2	200
1114.16:16:42.516	1114.16:16:57.516	1	192.168.1.99	43434	3	192.168.1.1	2550	17	0	2	200
1114.16:14:29.516	1114.16:17:26.516	1	192.168.1.201	10179	3	192.168.1.1	80	6	3	115	12827
1114.16:17:13.516	1114.16:17:26.516	0	192.168.1.1	80	1	192.168.1.201	10179	6	0	2	80
1114.16:17:43.516	1114.16:17:43.516	0	192.168.1.1	0	1	192.168.1.201	0	1	0	1	60
1114.16:17:43.516	1114.16:17:43.516	1	192.168.1.201	0	3	192.168.1.1	0	1	0	1	60
1114.16:17:26.516	1114.16:18:00.516	1	192.168.1.201	10198	3	192.168.1.1	80	6	3	46	7909
1114.16:17:26.516	1114.16:18:00.516	1	192.168.1.201	10196	3	192.168.1.1	80	6	3	110	11678
1114.16:17:26.516	1114.16:18:00.516	0	192.168.1.1	80	1	192.168.1.201	10198	6	3	185	251388
1114.16:17:26.582	1114.16:18:00.582	1	192.168.1.201	10197	3	192.168.1.1	80	6	3	7	1679
1114.16:17:26.582	1114.16:18:00.582	1	192.168.1.201	10195	3	192.168.1.1	80	6	3	7	1678
1114.16:17:26.582	1114.16:18:00.582	0	192.168.1.1	80	1	192.168.1.201	10196	6	3	500	719513
1114.16:17:26.582	1114.16:18:00.582	1	192.168.1.201	10193	3	192.168.1.1	80	6	3	33	3870
1114.16:17:26.582	1114.16:18:00.582	0	192.168.1.1	80	1	192.168.1.201	10197	6	3	7	944
1114.16:17:26.582	1114.16:18:00.582	1	192.168.1.201	10194	3	192.168.1.1	80	6	3	18	4416
1114.16:17:26.582	1114.16:18:00.582	0	192.168.1.1	80	1	192.168.1.201	10195	6	3	7	944
1114.16:17:26.582	1114.16:18:00.582	0	192.168.1.1	80	1	192.168.1.201	10193	6	3	147	206308

Рисунок 353 – Экспорт данных Netflow

12.2 Кэширующий прокси (Squid)

12.2.1 Кэширующий прокси: установка

Включение/отключение

Для включения прокси-сервера необходимо зайти в поле «Службы» - «Веб-прокси» - «Администрирование», установить флажок «Включить прокси» и нажать «Применить». По умолчанию используется прокси-сервер с пользовательской аутентификацией на основе локальной базы данных пользователей и выполняется на порту 3128 интерфейса LAN.

Изменение прокси-интерфейсов

Для изменения интерфейсов (подсетей) необходимо перейти во вкладку «Перенаправляющий прокси» и добавить/удалить интерфейсы в поле «Интерфейсы прокси». После добавления необходимо нажать на кнопку «Применить».

Изменение порта для прослушивания

По умолчанию прокси-сервер будет прослушивать порт 3128. Для того чтобы изменить порт для прослушивания необходимо перейти во вкладку «Перенаправляющий прокси». Далее необходимо ввести значение порта в поле «Порт SSL прокси». После внесения изменений необходимо нажать на кнопку «Применить».

Включение кэша

Для включения кэширования необходимо нажать на стрелку около вкладки «Основные настройки прокси» и в выпадающем списке выбрать «Настройки локального кэша» (Рисунок 354).

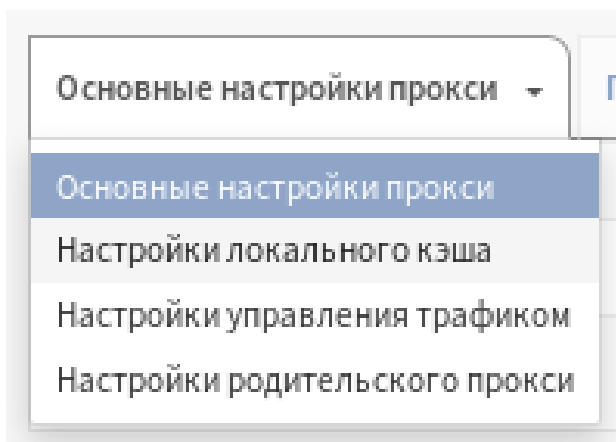



Рисунок 354 – Включение кэша

Необходимо установить флажок напротив поля «Включить локальный кэш» и нажать «Применить».

Поскольку кэш не создается по умолчанию, необходимо остановить и запустить службу в разделе «Система» - «Диагностика» - «Службы». Для этого необходимо нажать  напротив squid, это обеспечит правильное создание кэша.

Изменение метода проверки подлинности

Для изменения метода проверки подлинности необходимо нажать на стрелку около вкладки «Перенаправляющий прокси» и в выпадающем списке выбрать «Настройки аутентификации». Затем необходимо выбрать требуемый (-ые) аутентификатор (-ы) в поле «Метод аутентификации» или нажать «Очистить все», если не используется аутентификация.

В зависимости от серверов проверки подлинности, которые настроены в разделе «Система» - «Доступ» - «Серверы», возможно выбрать один или несколько из следующих параметров:

- нет аутентификации (оставить поле пустым);
- локальная база данных пользователей;
- LDAP;
- Radius.

FTP-прокси

Для включения FTP-прокси необходимо нажать на стрелку около вкладки «Перенаправляющий прокси» и в выпадающем списке выбрать «Настройка FTP-прокси». Далее выбрать один или несколько интерфейсов в поле «Интерфейсы FTP-прокси» и нажать «Применить».

Список контроля доступа

Для настройки списка управления доступом необходимо нажать на стрелку около вкладки «Перенаправляющий прокси» и в выпадающем списке выбрать «Список управления доступом». Эта вкладка позволяет:

- настроить список разрешенных подсетей в поле «Разрешенные подсети» (по умолчанию допускаются интерфейсы прокси);
- добавить IP-адреса для ограничения доступа в поле «IP-адреса без ограничений» (отсутствие аутентификации и черного списка для этих IP-адресов);
- добавить IP-адрес заблокированных хостов в поле «Заблокированные IP-адреса хоста» (запрещает клиенту использовать прокси-сервер);
- выбрать белый список в поле «Белый список» (необходимо нажать на кнопку (i), чтобы увидеть примеры, белый список преобладает над черным списком);
- выбрать черный список в поле «Черный список» (если этого нет в белом списке, блокирует трафик, основанный на регулярном выражении).

Правило межсетевого экрана: подключение через прокси-сервер

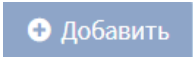
Для подключения через прокси-сервер, необходимо добавить правило межсетевого экрана. Для этого необходимо перейти в раздел «Межсетевой экран» - «Правила» - «LAN» (если пользователи и прокси-сервер находятся в локальной) и нажать кнопку . Необходимо добавить правило в соответствии с таблицей (Таблица 11) в начало списка правил. Для сохранения и применения внесенных изменений необходимо нажать на кнопку «Сохранить», а затем на кнопку «Применить изменения».

Таблица 11 – Правило межсетевого экрана

Настройки	Значения
Действие	Блокирование
Интерфейс	LAN
Протокол	TCP/UDP
Отправитель	LAN сеть
Диапазон портов назначения	HTTP
Категория	Подключение прокси-сервера
Описание	Блокировать HTTP-запрос

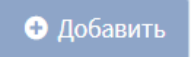
Далее необходимо добавить еще одно правило, которое будет блокировать доступ к HTTPS. Для этого необходимо нажать на кнопку  и заполнить поля в соответствии с таблицей (Таблица 12). Для сохранения и применения внесенных изменений необходимо нажать на кнопку «Сохранить», а затем на кнопку «Применить изменения».

Таблица 12 – Правило блокирования доступа к HTTPS

Настройки	Значения
Действие	Блокирование
Интерфейс	LAN
Протокол	TCP/UDP
Отправитель	LAN сеть
Диапазон портов назначения	HTTPS
Категория	Подключение прокси-сервера
Описание	Блокировать HTTPS-запрос

Настройка веб-браузера (Firefox)

Для настройки веб-браузера, чтобы использовать его с прокси-сервером, необходимо перейти к настройкам сети и настроить прокси-сервер в веб-браузере, например, Firefox (Рисунок 355). В группе настроек «Configure Proxies to Access the Internet» необходимо выбрать «Manual proxy Configuration» и ввести в поле «HTTP Proxy» значение IP-адреса ПК «InfoWatch ARMA Industrial Firewall» (например, 192.168.1.1, в поле «Port» необходимо ввести порт ПК «InfoWatch ARMA Industrial Firewall» (например, 3128). В поле «No Proxy for» необходимо ввести подсети, которые будут не проксироваться, например, ввести «Localhost, 127.0.0.1, 192.168.1.0/24».

Для других браузеров необходимо воспользоваться документацией к браузерам для настройки прокси сервера. Значения необходимо подставлять, руководствуясь установленным при настройке прокси на ПК «InfoWatch ARMA Industrial Firewall».

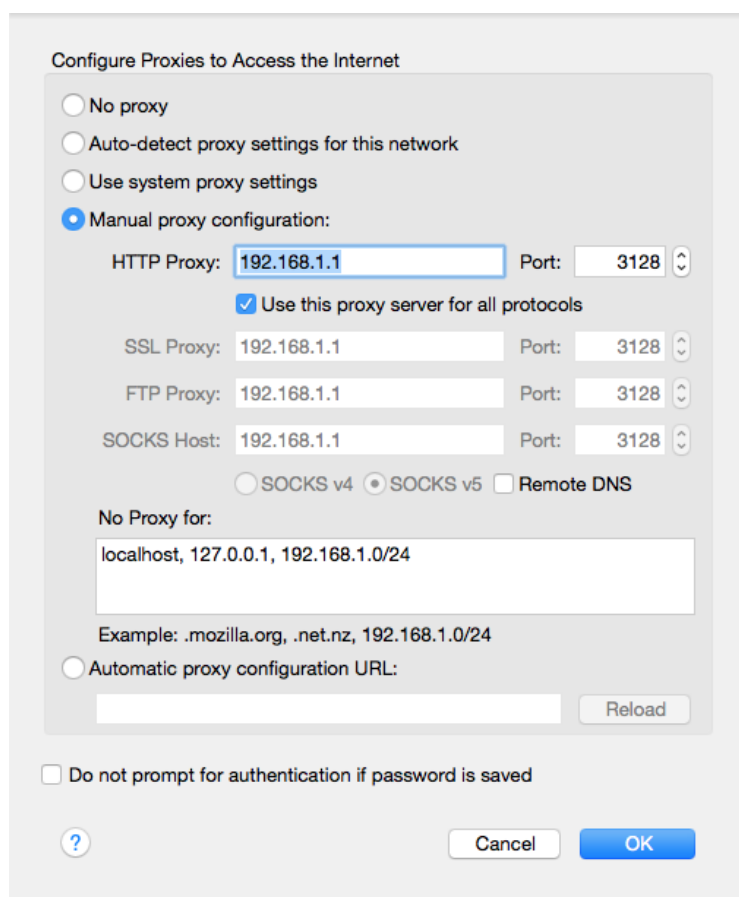


Рисунок 355 – Настройки браузера


12.2.2 Настройка веб-фильтрации

Веб-фильтрация на основе категорий в ПК «InfoWatch ARMA Industrial Firewall» выполняется с использованием встроенного прокси-сервера и одного из свободно доступных черных списков.

Отключение аутентификации

Для отключения аутентификации необходимо перейти в поле «Служба» - «Веб-прокси» - «Администрирование» - «Перенаправляющий прокси» - «Настройки аутентификации». В поле «Метод аутентификации» необходимо нажать на кнопку «Очистить все», чтобы отключить аутентификацию пользователя и нажать «Применить», чтобы сохранить изменения.

Настройка черного списка

Для настройки черного списка необходимо нажать на вкладку «Списки удаленного контроля доступа». Затем нажать на , чтобы добавить новый список.

Появится экран, в который необходимо ввести следующие данные в соответствии с таблицей (Таблица 13).

Таблица 13 – Настройка черного списка

Настройки	Значения	Комментарий
Включено	Включено	Включить выключить

Настройки	Значения	Комментарий
Имя файла	UT1	Необходимо выбрать уникальное имя файла
URL	(скопируйте/вставьте URL-адрес)	URL-адрес черного списка
Категории	(Оставить пустым)	Если оставить пустым, будет выбран полный список
Описание	Веб фильтр UT1	Ваше описание

Для сохранения изменений необходимо нажать на кнопку «Сохранить изменения».

Загрузка категорий

Далее необходимо нажать на кнопку «Скачать списки контроля доступа». Стоит учитывать, что для успешного выполнения данного шага необходимо, чтобы в ПК «InfoWatch ARMA Industrial Firewall» был настроенным порт WAN с доступом в Интернет.

Включение прокси

Для включения прокси-сервера, необходимо перейти в поле «Прокси» - «Администрирование» и установить флажок напротив поля «Включить прокси», далее нажать «Применить». Прокси-сервер будет привязан к локальной сети и порту 3128.

Включение прокси-сервера может занять некоторое время.

Отключение прокси-сервера

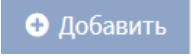
Для подключения через прокси-сервер, необходимо добавить правило межсетевого экрана. Для этого необходимо перейти в раздел «Межсетевой экран» - «Правила» - «LAN», нажать  и заполнить поля в соответствии с таблицей (Таблица 14).

Таблица 14 – Добавление правила

Настройки	Значения
Действие	Блокирование
Интерфейс	LAN
Протокол	TCP/UDP
Отправитель	LAN сеть
Диапазон портов назначения	HTTP
Категория	Подключение прокси-сервера

Настройки	Значения
Описание	Блокировать HTTP-запрос

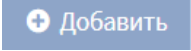
Необходимо добавить еще одно правило, которое будет блокировать доступ к HTTPS. Для этого необходимо нажать на кнопку  и заполнить поля в соответствии с таблицей (Таблица 15). Для сохранения и применения внесенных изменений необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения».

Таблица 15 – Блокирование доступа к HTTPS

Настройки	Значения
Действие	Блокирование
Интерфейс	LAN
Протокол	TCP/UDP
Отправитель	LAN сеть
Диапазон портов назначения	HTTPS
Категория	Подключение прокси-сервера
Описание	Блокировать HTTPS-запрос

12.3 Встроенная система предотвращения вторжений

12.3.1 Настройка системы обнаружения вторжений в режиме IDS

Чтобы включить IDS, необходимо перейти в разделе «Сеть» - «Обнаружение устройств» - «Администрирование» и установить флажок напротив поля «Включен». В примере используется интерфейс WAN, руководствуясь тем, что ПК будет связан с подключением к внешней сети (Рисунок 356).

Обнаружение вторжений: Администрирование

Настройки
Сохранение
Правила
Предупреждения (Alerts)
Расписание

☒ расширенный режим

Включен	<input checked="" type="checkbox"/>
Режим IPS	<input type="checkbox"/>
Смешанный режим	<input type="checkbox"/>
Передавать предупреждения (alerts) в syslog	<input checked="" type="checkbox"/>
Активировать eve логирование в syslog	<input checked="" type="checkbox"/>
Сравнение маршрутов	Aho-Corasick
Интерфейсы	WAN
	<input checked="" type="button" value="Очистить все"/>
Домашние сети (SHOME_NET)	192.168.0.0/16 × 10.0.0.0/8 × 172.16.0.0/12 ×
	<input checked="" type="button" value="Очистить все"/>
размер пакета по-умолчанию	
Архивировать журнал	Еженедельно
Сохранить журналы	4
Содержимое пакета для журнала	<input type="checkbox"/>

Рисунок 356 – Настройка обнаружения вторжений в режиме IDS

Необходимо нажать на кнопку «Применить».

12.3.2 Настройка системы предотвращения вторжений в режиме IPS

Чтобы включить IPS, необходимо перейти в поле «Обнаружение вторжений» - «Администрирование» и установить флажок напротив поля «Включен» и «Режим IPS». В примере используется интерфейс WAN, руководствуясь тем, что ПК будет связан с подключением к внешней сети (Рисунок 357).

расширенный режим

Включен	<input checked="" type="checkbox"/>
Режим IPS	<input checked="" type="checkbox"/>
Смешанный режим	<input type="checkbox"/>
Передавать предупреждения (alerts) в syslog	<input type="checkbox"/>
Активировать eve логирование в syslog	<input type="checkbox"/>
Сравнение маршрутов	Aho-Corasick
Интерфейсы	WAN
	✖ Очистить все
Архивировать журнал	Еженедельно
Сохранить журналы	4

Применить

Рисунок 357 – Настройка обнаружения вторжений в режиме IPS

Необходимо нажать на кнопку «Применить».

Для выбора правил необходимо перейти в поле «Обнаружение вторжений» - «Администрирование» - «Правила». Для включения правила необходимо нажать на флажок напротив выбранного правила в поле таблицы «Информация/Включен» (Рисунок 358).

<input checked="" type="checkbox"/>	1	Предупреждение	files.rules	##none##	FILEEXT JPG file claimed		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	3	Предупреждение	files.rules	##none##	FILEEXT BMP file claimed		<input type="checkbox"/>
<input checked="" type="checkbox"/>	6	Предупреждение	files.rules	##none##	FILESTORE jpg		<input type="checkbox"/>
<input checked="" type="checkbox"/>	8	Предупреждение	files.rules	##none##	FILESTORE pdf		<input type="checkbox"/>
<input checked="" type="checkbox"/>	9	Предупреждение	files.rules	##none##	FILEMAGIC pdf		<input type="checkbox"/>
<input checked="" type="checkbox"/>	10	Предупреждение	files.rules	##none##	FILEMAGIC jpg(1)		<input type="checkbox"/>
<input checked="" type="checkbox"/>	11	Предупреждение	files.rules	##none##	FILEMAGIC jpg(2)		<input type="checkbox"/>
<input checked="" type="checkbox"/>	12	Предупреждение	files.rules	##none##	FILEMAGIC short		<input type="checkbox"/>
<input checked="" type="checkbox"/>	15	Предупреждение	files.rules	##none##	FILE store all		<input type="checkbox"/>

Рисунок 358 – Правила

12.4 Задание и синхронизация времени по протоколу NTP

Для задания и синхронизации времени по протоколу NTP необходимо из веб-интерфейса в разделе «Службы» - «Сетевое время» - «Общие настройки» задать в поле «Серверы времени» по крайней мере один NTP сервер. Для сохранения конфигурации необходимо нажать на кнопку «Сохранить» (Рисунок 359).

Службы: Сетевое время: Общие настройки

Конфигурация NTP-сервера

Интерфейс (-ы): Не выбрано

Серверы времени

Сеть	Предпочитать	Не использовать
0.pool.ntp.org	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>
2.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>
3.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>

Автономный режим:

Графики NTP: ☐ Включить RRD графики NTP статистики (по умолчанию: включено).

Системное журналирование: ☐ Включить журналирование сообщений узлов (по умолчанию: отключено).
☐ Включить журналирование системных сообщений (по умолчанию: отключено).

Журналирование статистики: Дополнительно - Показать параметры журналирования статистики

Ограничения доступа: Дополнительно - Показать параметры ограничения доступа

Секунды координации: Дополнительно - Показать настройки секунды координации

Дополнительно: Дополнительно - Показать дополнительные параметры


Рисунок 359 – Задание и синхронизация времени по протоколу NTP

В результате, время системы должно синхронизироваться с временем на NTP сервере. Поддерживается только NTP версии 4.

12.5 Настройки экспорта событий по SYSLOG (интеграция с SIEM-системами)

Настройка экспорта событий по SYSLOG (интеграция с SIEM-системами) описана в подразделе 6.3.1 настоящего руководства.

12.6 Изменение возможностей (прав) пользователей

Для редактирования прав группы пользователей необходимо перейти в раздел «Система» - «Доступ» - «Группы». Для редактирования группы нажать на кнопку  и указать необходимые привилегии в поле «Присвоенные привилегии» (Рисунок 360).

Система: Доступ: Группы

Определен

Имя группы

test

Описание

Членство в группе

Не член

Член

root

→

←

Присвоенные привилегии

Тип	Имя
Веб-интерфейс	Вход / Выход из системы / Инструментальная панель
Веб-интерфейс	Все страницы


✎

Сохранить

Отменить

Рисунок 360 – Изменение возможностей (прав) пользователей

12.7 Создание нового пользователя

Для создания нового пользователя необходимо перейти в разделе «Система» - «Пользователи» и нажать кнопку . В появившемся меню заполняются данные для нового пользователя. Обязательные поля для заполнения:

- «Имя пользователя» (необходимо ввести имя пользователя);
- «Пароль» (необходимо ввести пароль для входа в учетную запись пользователя в первом поле и повторить этот пароль во втором поле).

После внесения изменений необходимо нажать на кнопку «Сохранить» (Рисунок 361).

Определен	USER	справка
Отключена	<input type="checkbox"/>	
Имя пользователя	<input type="text" value="root"/>	
Пароль	<input type="password" value="••••"/> <input type="text"/> (подтверждение) <input type="checkbox"/> Сгенерировать закодированный пароль для предотвращения локального входа для этого пользователя.	
Полное имя	<input type="text"/>	
Электронная почта	<input type="text"/>	
Комментарий	<input type="text"/>	
Предпочтительная целевая страница	<input type="text"/>	
Язык	По умолчанию.	
Оболочка входа	<input type="text" value="/sbin/nologin"/>	
Дата окончания срока действия	<input type="text"/>	

Рисунок 361 – Создание нового пользователя

12.8 Выбор совокупности регистрируемых событий

Для выбора регистрируемых событий для журналирования межсетевого экрана необходимо перейти в раздел «Система» - «Настройки» - «Журналирование» (Рисунок 362).

Локальные опции записи	
Обратный порядок отображения	<input checked="" type="checkbox"/>
Размер журнала (байт)	<input type="text"/>
События межсетевого экрана по умолчанию	<input checked="" type="checkbox"/> Журналировать пакеты, соответствующие правилам блокировки по умолчанию из набора правил <input checked="" type="checkbox"/> Журналировать пакеты, соответствующие правилам разрешения по умолчанию из набора правил <input checked="" type="checkbox"/> Журналировать пакеты, блокированные правилом «Блокировать bogon сети» <input checked="" type="checkbox"/> Журналировать пакеты, блокированные правилом «Блокировать частные сети»
Журнал веб-сервера	<input checked="" type="checkbox"/> Ошибка записи из-за сбоя сервера
Локальные записи	<input type="checkbox"/> Выключить запись журнала на локальный диск
Сброс записей	<input type="button" value="Очистить файлы журналов"/>
<input type="button" value="Сохранить"/>	

Рисунок 362 – Выбор регистрируемых событий

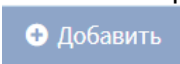
Данная категория позволяет выбрать события, которые необходимо журналировать, генерируемые межсетевым экраном, такие как:

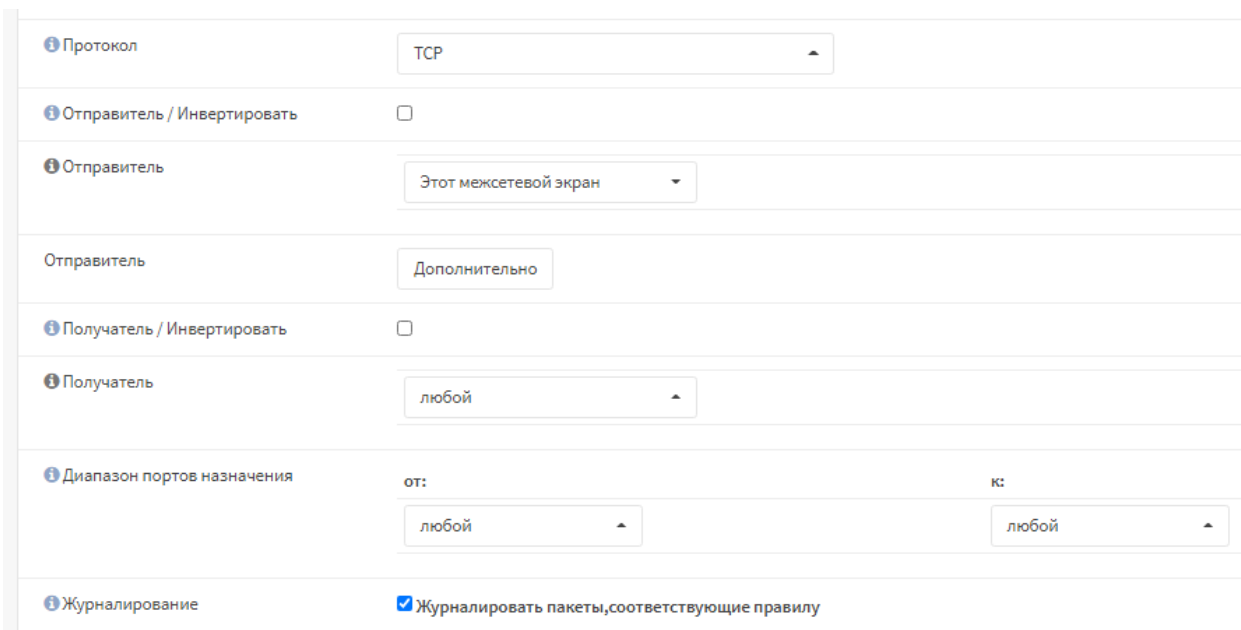
- журналировать пакеты, соответствующие правилам блокировки по умолчанию из набора правил;
- журналировать пакеты, соответствующие правилам разрешения по умолчанию из набора правил;
- журналировать пакеты, заблокированные правилом «Блокировать bogon сети»;
- журналировать пакеты, заблокированные правилом «Блокировать частные сети».

Для выбора событий для журналирования необходимо установить флажок напротив и нажать кнопку «Сохранить».

Для настройки журналирования пакетов, соответствующих правилам разрешения по умолчанию из набора правил, необходимо оставить изначальный (после установки) список правил межсетевого экранирования.

Дополнительно предусмотрена возможность журналировать пакеты, соответствующие правилам межсетевого экранирования. Для этого необходимо создать правило в поле «Межсетевой экран» - «Правила» - «WAN» и добавить

правило, нажав на кнопку . В настройках правила обязательно необходимо задать поля «Отправитель», «Действие», «Протокол» и установить флажок напротив поля «Журналировать пакеты, соответствующие правилу». Для сохранения и применения внесенных изменений необходимо нажать на кнопку «Сохранить», а затем на кнопку «Применить изменения» (Рисунок 363).



Протокол	TCP	
Отправитель / Инvertировать	<input type="checkbox"/>	
Отправитель	Этот межсетевой экран	
Отправитель	Дополнительно	
Получатель / Инvertировать	<input type="checkbox"/>	
Получатель	любой	
Диапазон портов назначения	от: любой	к: любой
Журналирование	<input checked="" type="checkbox"/> Журналировать пакеты, соответствующие правилу	

Рисунок 363 – Добавление правила МЭ

Для включения журналирования действий пользователей необходимо перейти в «Система» - «Настройки» - «Администрирование» и поставить флажок в поле «Журнал доступа». Для сохранения изменений необходимо нажать кнопку «Сохранить».

12.9 Фильтрация промышленных протоколов АСУ ТП

ПК «InfoWatch ARMA Industrial Firewall» позволяет производить анализ промышленных протоколов АСУ ТП, осуществлять разбор по функциям и полям этих протоколов, отображать собранную информацию. В текущей версии ПК «InfoWatch ARMA Industrial Firewall» имеется возможность создания правил обнаружения или блокирования пакетов следующих промышленных протоколов:

- Modbus;
- IEC 104;
- S7comm;
- OPC UA;
- OPC DA;
- UMAS;
- MMS;
- GOOSE.

12.9.1 Настройка протокола Modbus

Описание настройки параметров правила по протоколу Modbus TCP описано в подразделе 5.2.1 настоящего руководства.

12.9.2 Настройка протокола IEC 104

Описание настройки параметров правила по протоколу IEC 104 описано в подразделе 5.2.2 настоящего руководства.

12.9.3 Настройка протокола S7comm

Описание настройки параметров правила по протоколу S7comm описано в подразделе 5.2.3 настоящего руководства.

12.9.4 Настройка протокола OPC UA

Описание настройки параметров правила по протоколу OPC UA описано в подразделе 5.2.4 настоящего руководства.

12.9.5 Настройка протокола OPC DA

Описание настройки параметров правила по протоколу OPC DA описано в подразделе 5.2.5 настоящего руководства.

12.9.6 Настройка протокола UMAS

Описание настройки параметров правила по протоколу UMAS описано в подразделе 5.2.6 настоящего руководства.

12.9.7 Настройка протокола MMS

Описание настройки параметров правила по протоколу MMS описано в подразделе 5.2.7 настоящего руководства.

12.9.8 Настройка протокола GOOSE

Описание настройки параметров правила по протоколу GOOSE описано в подразделе 5.2.8 настоящего руководства.

12.10 Импорт пользовательских решающих правил в формате Snort

Для импорта пользовательских решающих правил в формате Snort необходимо загрузить правила обнаружения вторжений в текстовом формате (текстовый файл с набором правил в формате Snort с расширением «.rules»). Для этого необходимо перейти в раздел «Обнаружение вторжений» - «Администрирование» - «Сохранение». Для загрузки локальных правил необходимо нажать на кнопку «Загрузить новый локальный набор правил». После этого появится всплывающее окно об успешном загрузке правил (Рисунок 115).

Затем необходимо убедиться, что правила были добавлены в список (Рисунок 364).

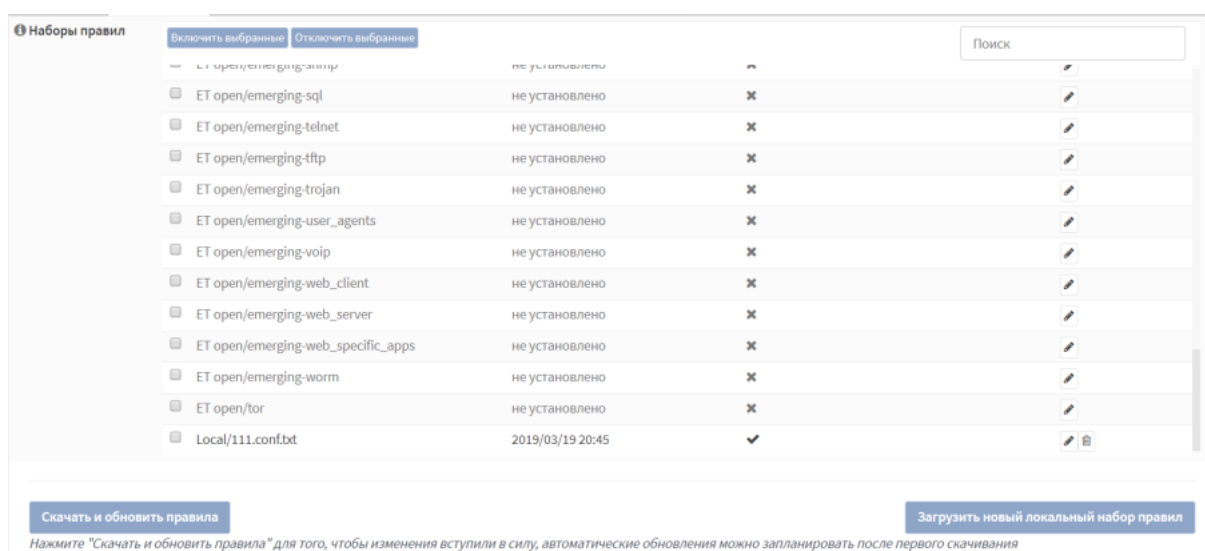


Рисунок 364 – Список импортированных правил

Для активации выбранных настроек необходимо нажать на кнопку «Скачать и обновить правила».

12.11 Экспорт пользовательских решающих правил

Для экспорта пользовательских решающих правил через консольный интерфейс необходимо настроить доступ по SSH. Для этого необходимо перейти в раздел меню «Система» - «Настройки» - «Администрирование» и найдите на этой странице «SSH».

В разделе «SSH-сервер» необходимо установить флажок напротив поля «Включить SSH», в поле «Группа логина» необходимо выбрать все группы, доступ к которым необходимо разрешить через SSH, в поле «Вход суперпользователей (root) в учетную запись» установить флажок напротив поля «Разрешить вход пользователей (root) в учетную запись», в поле «Метод аутентификации» установить флажок напротив поля «Разрешить парольный вход в учетную запись». В поле «Порт SSH» необходимо выбрать порт (по умолчанию 22), в поле «Прослушиваемые интерфейсы» выбрать интерфейс, через который необходимо

подключиться по SSH и нажать кнопку «Сохранить» в конце страницы (Рисунок 365).

SSH	
SSH-сервер	<input checked="" type="checkbox"/> Включите безопасный shell
Группа логина	wheel, admins
Вход суперпользователей в учетную запись	<input checked="" type="checkbox"/> Разрешите вход суперпользователей в учетную запись
Метод аутентификации	<input type="checkbox"/> Разрешите парольный вход в учётную запись
Порт SSH	22
Прослушиваемые интерфейсы	Все (рекомендуется)

Рисунок 365 – Доступ по SSH

Далее подключиться с помощью утилиты «Winscp» к системе и скачать пользовательские правила из директории «/usr/local/etc/suricata/rules».

Для экспорта загруженных пользователем наборов правил системы обнаружения вторжений через веб-интерфейс необходимо перейти в раздел «Система» - «Конфигурация» - «Резервные копии» и в группе настроек «Скачать наборы правил COB» нажать кнопку «Сохранение» (Рисунок 366).

Скачать наборы правил COB

Экспорт

Нажмите данную кнопку для скачивания загруженных пользователем наборов правил COB

Рисунок 366 – Экспорт правил

12.12 Динамическая маршрутизация

Для примера приведена настройка динамической маршрутизации на трех ПК «InfoWatch ARMA Industrial Firewall». Общая конфигурация представлена на рисунке (Рисунок 367).

Необходимо настроить интерфейсы ПК «InfoWatch ARMA Industrial Firewall» в соответствии с рисунком (Рисунок 367).

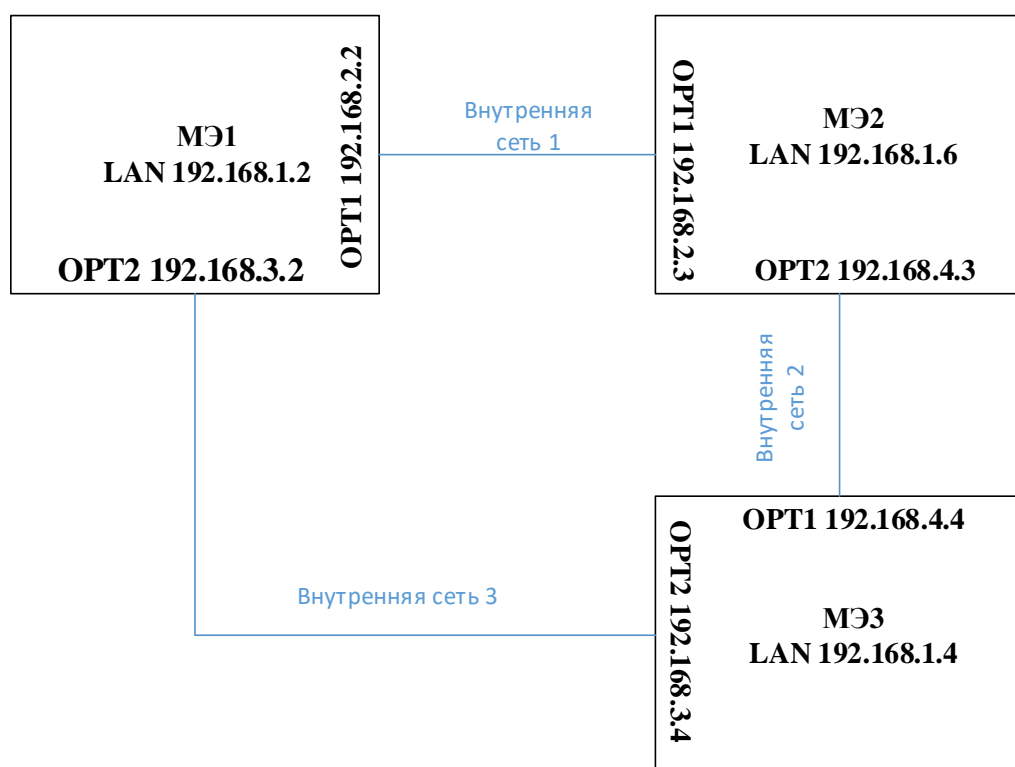
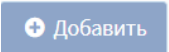


Рисунок 367 – Конфигурация МЭ для примера динамической маршрутизации


Изначально ПК «InfoWatch ARMA Industrial Firewall» пропускает пакеты только на интерфейсах WAN и LAN, а на других блокирует. Поэтому необходимо создать правило, которое будет пропускать пакеты на интерфейсы OPT1 и OPT2. Для этого во всех ПК «InfoWatch ARMA Industrial Firewall» необходимо перейти в поле «Межсетевой экран» - «Правила» - «OPT1» и нажать на кнопку . В поле «Действие» необходимо выбрать «Разрешение», в поле «Интерфейс» выбрать «OPT1», в поле «Версия TCP/IP» выбрать «IPv4», в поле «Описание» ввести описание правила, например, «Default allow OPT1 to any rule». Необходимо нажать на кнопку «Сохранить» (Рисунок 368, Рисунок 369).

Действие	Разрешение	
Отключена	<input type="checkbox"/> Отключить это правило	
Интерфейс	OPT1	
Версии TCP/IP	IPv4	
Протокол	any	
Отправитель / Инвертировать	<input type="checkbox"/>	
Отправитель	любой	
Диапазон портов источника	от: любой	к: любой
Получатель / Инвертировать	<input type="checkbox"/>	
Получатель	любой	

Рисунок 368 – Настройка правила для OPT1 (часть 1)

Получатель	любой	
Диапазон портов назначения	от: любой	к: любой
Журналирование	<input type="checkbox"/> Журналировать пакеты, соответствующие правилу	
Категория		
Описание	Default allow OPT1 to any rule	
дополнительные возможности		
ОС источника	Любой	
Нет XMLRPC Sync	<input type="checkbox"/>	
Расписание	отсутствует	
Шлюз	по умолчанию	

Рисунок 369 – Настройка правила для OPT1 (часть 2)

Для настройки правила OPT2, во всех ПК «InfoWatch ARMA Industrial Firewall» необходимо перейти в поле «Межсетевой экран» - «Правила» - «OPT2» и нажать на кнопку . В поле «Действие» необходимо выбрать «Разрешение», в поле «Интерфейс» выбрать «OPT2», в поле «Версия TCP/IP» выбрать «IPv4», в поле «Описание» ввести описание правила, например, «Default allow OPT2 to any rule». Необходимо нажать на кнопку «Сохранить» (Рисунок 370, Рисунок 371).

Действие	Разрешение
Отключена	<input type="checkbox"/> Отключить это правило
Интерфейс	OPT2
Версии TCP/IP	IPv4
Протокол	any
Отправитель / Инвертировать	<input type="checkbox"/>
Отправитель	любой
Отправитель	Дополнительно
Получатель / Инвертировать	<input type="checkbox"/>
Получатель	любой

Рисунок 370 – Настройка правила для OPT2 (часть 1)

гипермаркет

Получатель	любой	
Диапазон портов назначения	от: любой	к: любой
Журналирование	<input type="checkbox"/> Журналировать пакеты, соответствующие правилу	
Категория		
Описание	Default allow OPT2 to any rule	
дополнительные возможности		
ОС источника	Любой	
Нет XMLRPC Sync	<input type="checkbox"/>	
Расписание	отсутствует	
Шлюз	по умолчанию	


lumerang (c) 2019 Tehiz


Рисунок 371 – Настройка правила для OPT2 (часть 2)


После проверки корректности настройки правил во всех ПК «InfoWatch ARMA Industrial Firewall» необходимо отправить ping от МЭ 1 к МЭ 3:

– Ping 192.168.3.4.

Наличие ответа на запрос ping означает, что имеется подключение МЭ 1 и МЭ 3.

В МЭ 1 необходимо перейти в раздел «Маршрутизация» - «Общие настройки» и установить флажок напротив поля «Включен». Для настройки динамического маршрута необходимо перейти в поле «Маршрутизация» - «RIP». Необходимо установить флажок напротив поля «Включить», в поле «Версия» выбрать 2, в поле «Пассивные интерфейсы» выбрать «LAN», в поле «Перераспределение маршрута» выбрать «Перераспределение маршрута», в поле «Сети» ввести «192.168.2.0/24» и нажать кнопку «Сохранить», а затем нажать  в верхнем правом углу.

В МЭ 2 необходимо перейти в раздел «Маршрутизация» - «Общие настройки» и установить флажок напротив поля «Включен». Для настройки динамического маршрута необходимо перейти в поле «Маршрутизация» - «RIP». Необходимо установить флажок напротив поля «Включить», в поле «Версия» выбрать 2, в поле «Пассивные интерфейсы» выбрать «LAN», «WAN», в поле «Перераспределение маршрута» выбрать «Перераспределение маршрута», в поле «Сети» ввести «192.168.2.0/24», «192.168.4.0/24» и нажать кнопку «Сохранить», а затем нажать  в верхнем правом углу.

В МЭ 3 необходимо перейти в раздел «Маршрутизация» - «Общие настройки» и установить флажок напротив поля «Включен». Для настройки динамического маршрута необходимо перейти в поле «Маршрутизация» - «RIP». Необходимо установить флажок напротив поля «Включить», в поле «Версия» выбрать 2, в поле «Пассивные интерфейсы» выбрать «LAN», «WAN», в поле «Перераспределение маршрута» выбрать «Перераспределение маршрута», в поле «Сети» ввести «192.168.4.0/24» и нажать кнопку «Сохранить», а затем нажать  в верхнем правом углу.

12.13 Настройки для работы на уровне L2

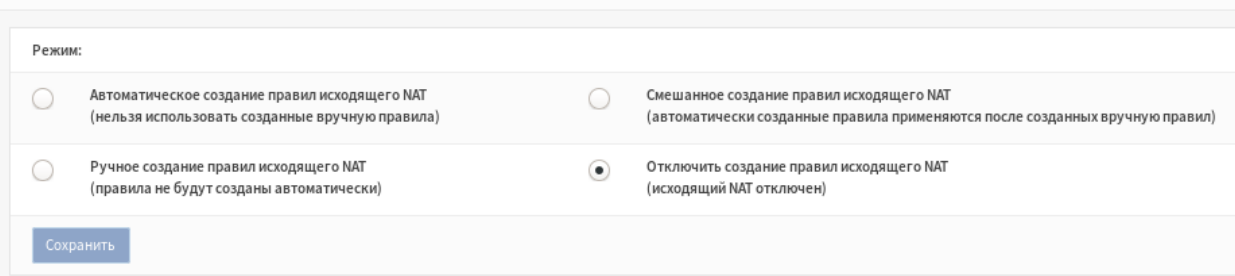
Для перехода в режим работы на уровне L2 (по умолчанию ПК «InfoWatch ARMA Industrial Firewall» работает на уровне L3) необходимо создать мост между двумя сетевыми интерфейсами.

Переход на уровень L2 может быть использован для создания прозрачного режима, не требующего создания подсетей.

12.13.1 Отключение исходящего NAT

Для отключения исходящего NAT необходимо перейти в раздел «Межсетевой экран» - «NAT» - «Исходящий» и отключить NAT путем установки флажка на значение «Отключить создание правил исходящего NAT (исходящий NAT отключен)» (Рисунок 372).

Межсетевой экран: NAT: Исходящий



Режим:	
<input type="radio"/> Автоматическое создание правил исходящего NAT (нельзя использовать созданные вручную правила)	<input type="radio"/> Смешанное создание правил исходящего NAT (автоматически созданные правила применяются после созданных вручную правил)
<input type="radio"/> Ручное создание правил исходящего NAT (правила не будут созданы автоматически)	<input checked="" type="radio"/> Отключить создание правил исходящего NAT (исходящий NAT отключен)

Рисунок 372 – Отключение исходящего NAT

12.13.2 Изменение системных параметров

Необходимо включить мост путем изменения системного параметра (net.link.bridge.pfil_bridge) со значения «default» на «1» в разделе меню «Система» - «Настройки» - «Параметры» и нажать кнопку «Сохранить» (Рисунок 373).

Система: Настройки: Параметры

Редактировать параметры системы

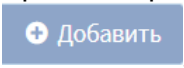
Параметр	net.link.bridge.pfil_bridge
Описание	Set to 1 to enable filtering on the bridge interface
Значение	1

Сохранить Отменить

Рисунок 373 – Изменение системных параметров

Аналогичным образом изменить значения параметра (net.link.bridge.pfil_member) со значения «default» на «0» и нажать кнопку «Применить изменения».

12.13.3 Создание моста

Для создания моста необходимо перейти в раздел «Интерфейсы» - «Другие типы» - «Сетевой мост» и нажать кнопку . В меню необходимо выбрать несколько интерфейсов, которые будут добавлены в сетевой мост и нажать кнопку «Сохранить» (Рисунок 374).







Интерфейс	Участники	Описание
BRIDGE0	LAN, WAN	 

Рисунок 374 – Создание моста

12.13.4 Назначение управляющего интерфейса

Для того чтобы обеспечить возможность управления ПК, необходимо задать новый управляющий (manage) интерфейс. В разделе «Интерфейсы» - «Назначение портов» и необходимо нажать на кнопку  напротив моста (Рисунок 375).

Интерфейсы: Назначения портов

Интерфейс	Сетевой порт	
<u>LAN</u>	em0 (08:00:27:e0:97:bb)	
<u>WAN</u>	em1 (08:00:27:df:ed:44)	
Новый интерфейс:	bridge0 ()	

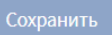


Рисунок 375 – Назначение управляющего интерфейса

После этого необходимо перейти в настройки вновь созданного интерфейса в разделе «Интерфейсы» - «OPT1», включить его, в поле «Тип конфигурации» необходимо выбрать «Статический IPv4» и установить IP- адрес. Нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

12.13.5 Отключение частных сетей и Bogon

В разделе «Интерфейсы» - «WAN» необходимо отключить поля «Блокировать частные сети» и «Блокировать Bogon сети» нажать кнопку «Сохранить», затем кнопку «Применить изменения».

12.13.6 Отключение DHCP сервера на LAN

Для отключения DHCP сервера необходимо перейти в раздел «Службы» - «DHCPv4» - «LAN» и отключить функцию «Включить DHCP-сервер на LAN интерфейсе».

12.13.7 Отключение интерфейсов LAN и WAN

После конфигурации моста, необходимо отключить обработку трафика на уровне L3. Для этого необходимо перейти в раздел «Интерфейсы» - «LAN» и в раздел «Интерфейсы» - «WAN», в каждом в поле «Тип конфигурации IPv4» установить значение «Отсутствует» и нажать кнопку «Сохранить».

12.14 Настройки режима отказоустойчивого кластера (высокой доступности)

Для настройки кластера необходимо настроить параметры в разделе «Система» - «Высокий уровень доступности» - «Настройки» (Рисунок 376).

Система: Высокий уровень доступности: Настройки

Синхронизация состояния

1 Синхронизировать состояния ☐

1 Отключить упреждение ☐

1 Синхронизировать интерфейс LAN

1 Синхронизировать IP-адрес пира 224.0.0.240

Настройки синхронизации конфигурации (XMLRPC Sync) [Perform synchronization](#)

1 Синхронизировать конфигурацию с IP-адресом

1 Имя пользователя удаленной системы root

1 Пароль удаленной системы

1 Инструментальная панель ☐

1 Пользователи и группы ☐

1 Серверы аутентификации ☐

1 Сертификаты ☐

Рисунок 376 – Выбор регистрируемых событий

В примере описывается настройка кластера на основе двух сетей. 192.168.1.0/24 будет использоваться для внутренней сети, а 172.8.0.0/24 будет использоваться для маршрутизации трафика в Интернет.

При использовании CARP все интерфейсы должны иметь выделенный IP-адрес, который будет объединен с одним общим виртуальным IP-адресом для связи с обеими сетями.

12.14.1 Установка интерфейсов и основные правила межсетевого экрана

В примере используются три интерфейса, все имеют базовую настройку.

Необходимо перейти в раздел «Интерфейсы», необходимо убедиться, что имеется все три интерфейса и назначены адреса и подсети в соответствии с таблицей (Таблица 16).

Таблица 16 – Интерфейсы

Название интерфейса	IP-адрес
LAN	192.168.1.10/24
WAN	172.18.0.101/24
PFSYNC	10.0.0.1

Затем необходимо убедиться, что соответствующие протоколы могут использоваться на разных интерфейсах. Для этого необходимо перейти в «Межсетевой экран» - «Правила» и убедиться, что LAN и WAN принимают CARP-пакеты.

Необходимо задать IP-адреса на резервном устройстве в соответствии с таблицей (Таблица 17).

Таблица 17 – Сервер резервного копирования

Название интерфейса	IP-адрес
LAN	192.168.1.20/24
WAN	172.18.0.102/24
PFSYNC	10.0.0.2

12.14.2 Настройка виртуальных IP-адресов

Необходимо перейти в поле «Межсетевой экран» - «Виртуальные IP-адреса» - «Настройки» и добавить новый виртуальный IP-адрес в соответствии с таблицей (Таблица 18).

Таблица 18 – Настройка виртуальных IP-адресов

Название	Значение
Тип	CARP
Интерфейс	WAN
IP-адрес	172.18.0.100/24
Виртуальный пароль	root
Группа VHID	1
Частота синхронизации	Base 1/Skew 0
Описание	VIP WAN

12.14.3 Настройка исходящего NAT

Когда трафик выходит из межсетевого экрана, он также должен использовать виртуальный IP-адрес. По умолчанию для ПК «InfoWatch ARMA Industrial Firewall» используется IP-адрес интерфейсов (в примере иначе).

Необходимо перейти в поле «Межсетевой экран» - «NAT» и выбрать «Исходящий». Необходимо выбрать «Ручное создание правил исходящего NAT» на этой странице и изменить правила, исходящие из сети 192.168.1.0/24, чтобы использовать виртуальный интерфейс CARP (172.18.0.100).

12.14.4 Настройка синхронизации XMLRPC SYNC

Для настройки синхронизации высокого уровня доступности используя XMLRPC SYNC необходимо включить «pfSync», используя выделенный интерфейс и

межсетевой экран. Для этого необходимо перейти в раздел «Система» - «Высокая доступность» - «Настройки», включить «Синхронизовать состояния» и выбрать сетевой интерфейс в «Синхронизовать интерфейс», используемый для «pfSync». Затем настроить пир IP-адреса в поле «Синхронизовать пир IP-адреса» ввести адрес: 10.0.0.2.

Затем необходимо настроить параметры, которые будут дублироваться на сервер резервного копирования, используя опцию «Настройка синхронизации конфигурации (XMLRPC SYNC)». Поставить флажок напротив:

- «Правила межсетевого экрана»;
- «NAT»;
- «DHCPD»;
- «Виртуальные IP-адреса».

12.14.5 Настройка тестирования

Чтобы проверить настройку, необходимо подключить пользователя к локальной сети и открыть SSH-соединение с хостом обоих межсетевых экранов. Теперь при подключении необходимо просматривать таблицу состояний на обоих межсетевых экранах («Создание отчетов» - «Состояние»). Таблицы состояний должны быть одинаковы.

12.15 Создание правил МЭ

Для удобства, в веб-интерфейсе правила межсетевого экрана задаются отдельно для каждого из сетевых интерфейсов, настроенных в ПК «InfoWatch ARMA Industrial Firewall». Правила располагаются в виде списка с приоритетом от верхнего к нижнему. Иными словами, сетевой пакет проверяется на совпадение с критериями правил по порядку, сверху вниз.

Если сетевой пакет удовлетворяет критериям правила, то к пакету применяется действие, заданное в правиле. Если к пакету уже применено правило, то обработка пакета сетевым экраном прекращается. Такой пакет далее не будет сверяться с оставшимися правилами в списке.

Действия «блокировать (block)» и «отклонить (reject)» предполагают блокирование пакета межсетевым экраном (причем в первом случае, удаленная сторона никак не оповещается о свершившейся блокировке). Действие пропустить (pass) разрешает прохождение пакета через межсетевой экран и приводит к созданию состояния.

Если сетевой пакет не удовлетворяет критериям ни одного правила, то пакет блокируется (т.е. отбрасывается без индикации удаленной стороне).

12.15.1 Создание правил МЭ для всех сетевых интерфейсов

Создание правила МЭ для определенного сетевого интерфейса описано в подразделе 4.2.1.

12.15.2 Создание правил МЭ для определенного сетевого интерфейса

Создание правила МЭ для определенного сетевого интерфейса описано в подразделе 4.2.2.

12.16 Создание правил NAT

Создание правила NAT «Переадресация портов» описано в подразделе 4.3.1 настоящего руководства.

Создание правила NAT «Один к одному» описано в подразделе 4.3.2 настоящего руководства.

Создание правила NAT «Исходящий» описано в подразделе 4.3.3 настоящего руководства.

12.17 Настройка прокси-сервера для взаимодействия с внешним антивирусом на удаленном хосте по протоколу ICAP

Антивирусная проверка – это проверка на уровне шлюза, которая обеспечивает:

- защиту от опасных веб-сайтов;
- защиту от зараженных файлов.

Для того чтобы осуществлялась антивирусная проверка, трафик от клиентских машин должен попадать на прокси-сервер устройства ПК «InfoWatch ARMA Industrial Firewall». Подробное описание настроек прокси представлено в п. 10.6.1 настоящего руководства.

Далее приведены настройки прокси-сервера, которые обеспечат попадание HTTP и HTTPS трафика на прокси-сервер.

12.17.1 Настройка HTTP-прокси

Для включения HTTP-прокси необходимо перейти в «Службы» - «Веб-прокси» - «Администрирование» - «Основные настройки прокси» и поставить флажок напротив «Включен».

Далее необходимо перейти во вкладку «Перенаправляющий прокси» - «Основные настройки перенаправления». В поле «Включен» необходимо поставить флажок. В поле «Интерфейсы» необходимо выбрать сетевой интерфейс, к которому будет привязан прокси-сервер. В поле «Номер порта прокси сервера» необходимо ввести номер порта, который прокси-сервер будет прослушивать. В поле «Включить прозрачный HTTP-прокси» необходимо поставить флажок для включения проксирования. Нажать кнопку «Применить» (Рисунок 377).

Службы: Веб-прокси: Администрирование

Основная настройки прокси
Перенаправляющий прокси
Автонастройки прокси-сервера

☒ расширенный режим

i Интерфейсы прокси

LAN

Очистить все

i Номер порта прокси-сервера

3128

i Включить прозрачный HTTP-прокси

☒

i Включить проверку SSL

☒

i Протоколировать только информацию SNI

☐

i Порт SSL прокси

3129

i Использовать центр сертификации

Не выбрано

i SSL no bump sites

Очистить все

i Размер кэша SSL

4

i SSL cert workers

5

i Разрешить подсети на интерфейсе

☒

Применить

Рисунок 377 – Службы: Веб-прокси: Администрирование (настройка HTTP-прокси)

Следующим шагом необходимо создать правило переадресации NAT. Для этого необходимо нажать на ссылку «Добавление нового правила межсетевого экрана» в описании поля «Включить прозрачный HTTP-прокси» (Рисунок 378).

i Включить прозрачный HTTP-прокси

☒

Включить прозрачный режим прокси-сервера. Для пересылки трафика с межсетевого экрана на прокси-сервер потребуется правило межсетевого экрана.
Добавление нового правила межсетевого экрана

Рисунок 378 – Службы: Веб-прокси: Администрирование (настройка HTTP-прокси: Создание правила NAT)

Затем необходимо заполнить поля правила в соответствии с таблицей 19, нажать кнопку «Сохранить», а затем «Применить изменения».

Таблица 19 – Создание NAT правила для настройки HTTP-прокси

Название поля	Значение
Интерфейс	LAN [Сетевой интерфейс, выбранный в поле «Интерфейсы» на странице «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси»]
Протокол	TCP

336

arma.infowatch.ru

Название поля	Значение
Источник	LAN сеть
Диапазон портов источника	Любой - любой
Назначение	Любой
Диапазон портов назначения	HTTP - HTTP
Адрес перенаправления	127.0.0.1
Порт перенаправления	3128
Описание	Перенаправление трафика на прокси
Зеркальный NAT	Включить
Связные правила фильтрации	Добавить связанное правило фильтрации

Необходимо подключить по внутренней сети устройство. На устройстве в качестве шлюза по умолчанию ввести IP-адрес сетевого интерфейса из поля «Интерфейсы» на странице «Службы» - «Веб-прокси» - «Администрирование» - «Основные настройки прокси». Затем необходимо ввести DNS-сервер на устройстве: «8.8.8.8». Это необходимо для возможности перехода на веб-сайт по доменному имени сайта. На удаленном устройстве необходимо открыть в веб-браузере сайт ([http](http://o-site.spb.ru/), например: <http://o-site.spb.ru/>). В случае успешного подключения к сети Интернет отобразиться страница сайта.

12.17.2 Настройка HTTPS-прокси

Для включения HTTPS-прокси необходимо перейти в «Службы» - «Веб-прокси» - «Администрирование» - «Основные настройки прокси» и поставить флажок напротив «Включен». Далее необходимо перейти во вкладку «Перенаправляющий прокси» - «Основные настройки перенаправления». В поле «Интерфейсы прокси» необходимо выбрать сетевой интерфейс, к которому будет привязан прокси-сервер. В поле «Номер порта прокси сервера» необходимо ввести номер порта, который прокси-сервер (HTTP) будет прослушивать. В поле «Включить прозрачный HTTP-прокси» необходимо поставить флажок для включения проксирования. В поле «Включить проверку SSL» необходимо поставить флажок для включения возможности подключения через HTTPS протокол. В поле «Порт SSL прокси» необходимо ввести номер порта, который SSL прокси-сервер будет прослушивать. Нажать кнопку «Применить» (Рисунок 379).

Службы: Веб-прокси: Администрирование

Основные настройки прокси ▾ Перенаправляющий прокси ▾ Автонастройки прокси-сервера ▾ Удаленные списки

☒ расширенный режим

Интерфейсы прокси LAN ✖ Очистить все

Номер порта прокси-сервера 3128

Включить прозрачный HTTP-прокси ☒

Включить проверку SSL ☒

Протоколировать только информацию SNI ☐

Порт SSL прокси 3129

Использовать центр сертификации Не выбрано

SSL no bump sites ✖ Очистить все

Размер кэша SSL 4

SSL cert workers 5

Разрешить подсети на интерфейсе ☒

Применить

Рисунок 379 – Службы: Веб-прокси: Администрирование (настройка HTTPS-прокси)

Следующим шагом необходимо создать правило переадресации NAT. Для этого необходимо нажать на ссылку «Включить проверку SSL» в описании «Добавление нового правила natfirewall rule» (Рисунок 380).

Включить проверку SSL ☒

Включите проверку SSL, которая позволяет регистрировать информацию о соединениях HTTPS, такую как запрошенный URL, и/или работать прокси-серверу, направляя трафик из внешней сети во внутреннюю и наоборот. Если вы планируете использовать прозрачный режим HTTPS, вам нужно добавить правила nat, чтобы отразить ваш трафик. [Добавление нового правила natfirewall rule](#)

Рисунок 380 – Службы: Веб-прокси: Администрирование (настройка HTTPS-прокси: создание NAT правила)

Далее необходимо заполнить поля правила в соответствии с таблицей 20, нажать кнопку «Сохранить», а затем «Применить изменения».

Таблица 20 – Создание NAT правила для настройки HTTPS-прокси

Название поля	Значение
Интерфейс	LAN [Сетевой интерфейс, выбранный в поле «Интерфейсы» на странице «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси»]
Протокол	TCP
Источник	LAN сеть

Название поля	Значение
Диапазон портов источника	Любой - любой
Назначение	Любой
Диапазон портов назначения	HTTPS - HTTPS
Адрес перенаправления	127.0.0.1
Порт перенаправления	3129
Описание	Перенаправление трафика на прокси
Зеркальный NAT	Включить
Связные правила фильтрации	Добавить связанное правило фильтрации


Следующим шагом необходимо создать сертификат. Для этого необходимо перейти в «Система» - «Доверенные сертификаты» - «Полномочия» и нажать кнопку . Далее необходимо заполнить поля в соответствии с таблицей 21.

Таблица 21 – Создание сертификата

Поле	Значение
Описание	ARMA CA
Метод	Создать внутренний ЦС
Длина ключа (биты)	2048
Digest алгоритм	SHA256
Срок жизни (дней)	356
Код страны	RU (Россия)
Область	МО
Город	Москва
Организация	InfoWatch
Email адрес	admin@infowatch.ru
Простое имя	arma-ca

Для сохранения необходимо нажать кнопку «Сохранить».

Для скачивания сертификата необходимо перейти в «Система» - «Доверенные сертификаты» - «Полномочия» и нажать кнопку «Экспорт сертификата CA» напротив созданного сертификата. Скаченный сертификат необходимо переместить на устройство, которое необходимо подключить к SSL прокси-серверу.

Затем необходимо подключить по внутренней сети устройство. На устройстве в качестве шлюза по умолчанию ввести IP-адрес сетевого интерфейса из поля «Интерфейсы» на странице «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси». Затем необходимо ввести DNS-сервер на устройстве: «8.8.8.8». Это необходимо для возможности перехода на веб-сайт по доменному имени сайта.

На устройстве необходимо настроить веб-браузера. Далее описан пример добавления сертификата для веб-браузера FireFox.

Для добавления сертификата необходимо открыть веб-браузер FireFox, перейти в раздел «Приватность» - «Защита» - «Сертификаты» и нажать кнопку «Просмотр сертификатов» (Рисунок 381).

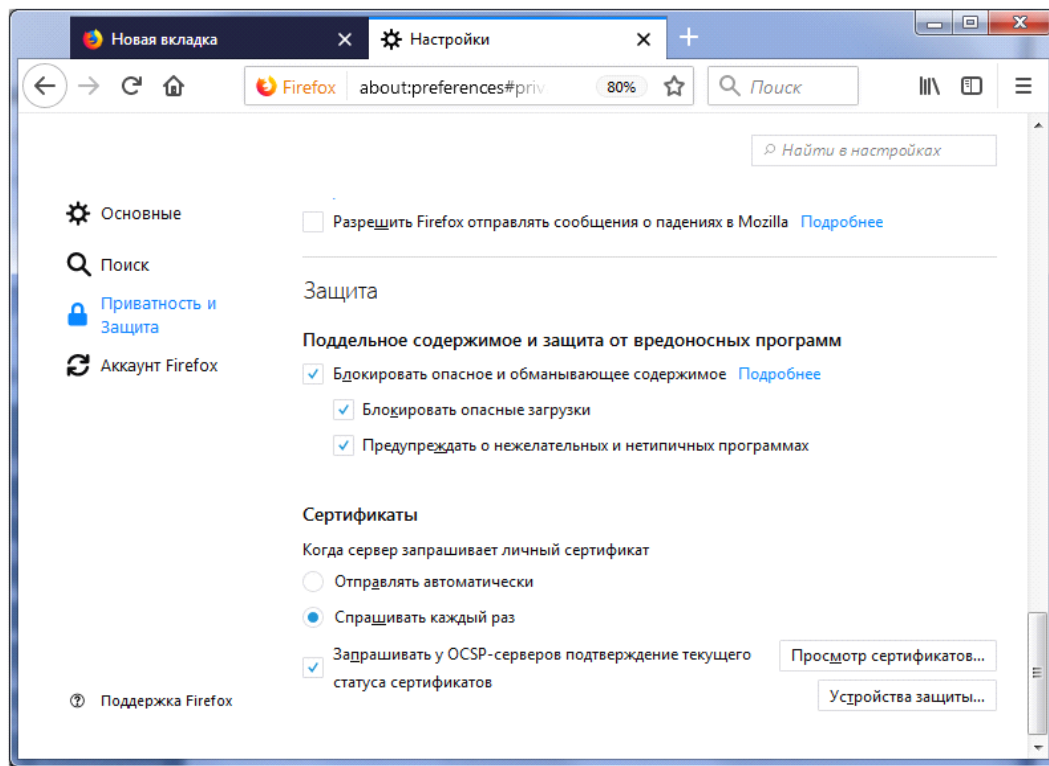


Рисунок 381 – Добавление сертификата (часть 1)

В окне необходимо выбрать вкладку «Центры сертификации» и нажать кнопку «Импортировать...» (Рисунок 382).

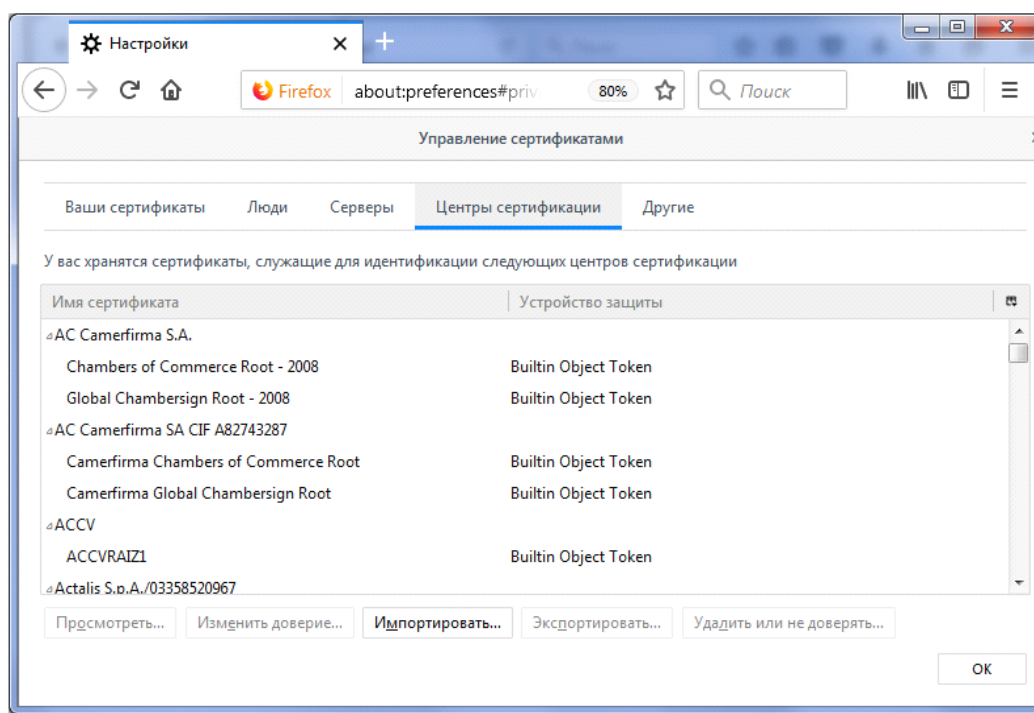


Рисунок 382 – Добавление сертификата (часть 2)

Необходимо найти на жестком диске сохраненный файл сертификата и нажать кнопку «Открыть» (Рисунок 383).

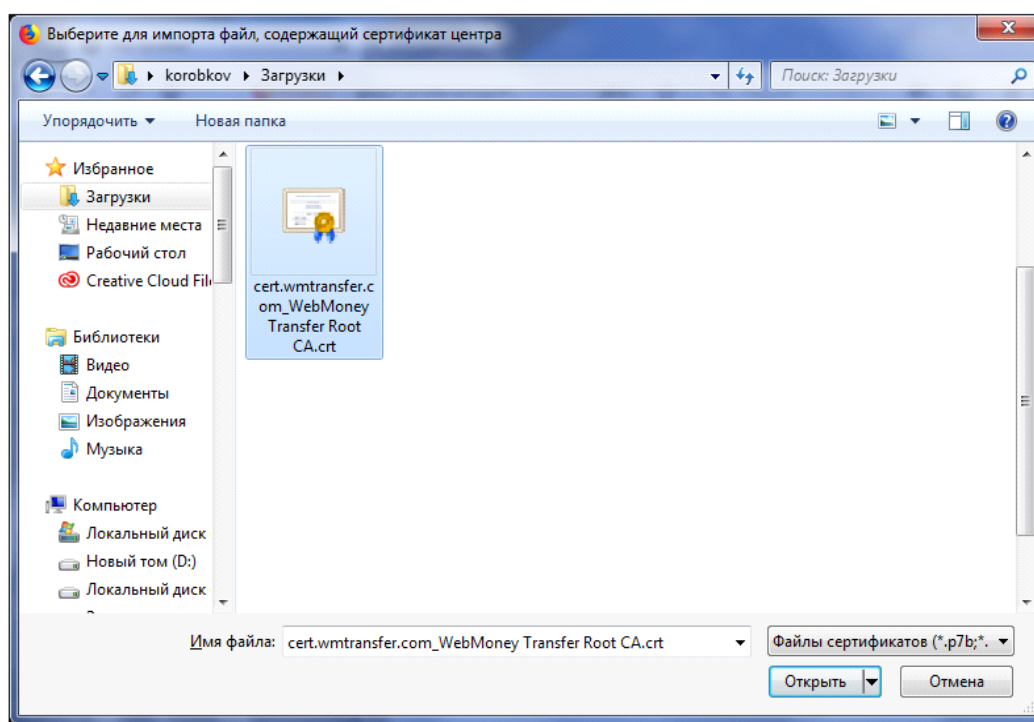


Рисунок 383 – Добавление сертификата (часть 3)

В окне «Загрузка сертификата» необходимо выбрать цели, для которых импортируется сертификат (Рисунок 384).

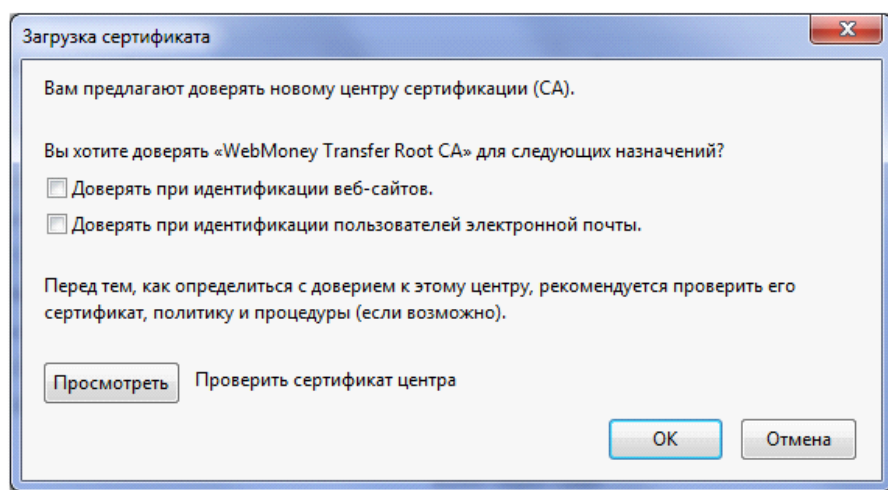


Рисунок 384 – Добавление сертификата (часть 4)

Необходимо выбрать все предложенные варианты, отметив их флажками, после чего нажать кнопку «ОК» (Рисунок 385).

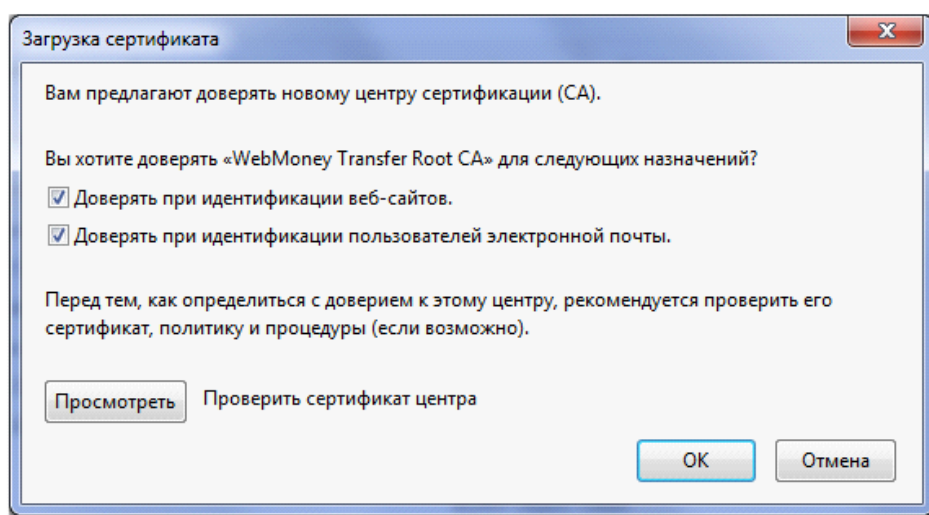


Рисунок 385 – Добавление сертификата (часть 5)

Для контроля правильности проделанных операций необходимо открыть вкладку «Центры сертификации» и в конце списка найти установленный корневой сертификат.

Далее на удаленном устройстве необходимо открыть в веб-браузере сайт ([https](https://vk.com), например: <https://vk.com>). В случае успешного подключения к сети Интернет отобразится страница сайта.

12.17.3 Настройка внешнего антивируса

Настройка антивирусов сторонних производителей выходит за рамки данной инструкции. Необходимо обратиться к документации производителя антивируса для его настройки.

12.17.4 Настройка ПК «InfoWatch ARMA Industrial Firewall» для взаимодействия с внешним антивирусом

Прокси-сервер поддерживает взаимодействие с антивирусом, выполняемом на отдельном внешнем хосте, посредством протокола ICAP.

В данном разделе освещаются настройки на стороне ПК «InfoWatch ARMA Industrial Firewall» для взаимодействия с внешним антивирусом.

Необходимо подключить сервер, на котором выполняется антивирус, к шлюзу ПК «InfoWatch ARMA Industrial Firewall» через свитч или напрямую с помощью отдельного сетевого кабеля. Также, для безопасной передачи ICAP-трафика, ПК «InfoWatch ARMA Industrial Firewall» и внешний антивирус можно разместить в отдельном VLAN.


Далее необходимо указать в свойствах прокси-сервера как он будет взаимодействовать по ICAP с внешним антивирусом. Для этого необходимо перейти в «Службы» - «Прокси» - «Администрирование» - «Перенаправляющий прокси» - «Настройки ICAP». В «Включить» необходимо поставить флажок. В «Запрос на изменение URL» необходимо ввести URL, идентифицирующие ICAP-сервис (антивирус). Любой ICAP-сервис может поддерживать работу в двух режимах — Request Modification и Response Modification — поэтому задается не один, а два URL-идентификатора. Каждый URL-идентификатор, таким образом, обозначает не столько ICAP-сервис как таковой, а ICAP-сервис + режим работы.

Для проверки функционала антивирусной защиты удобно использовать ресурс: «<http://www.eicar.org>». EICAR — безвредный тестовый вирус, применяемый для простой проверки - работает ли антивирус.

На странице «<http://2016.eicar.org/85-0-Download.html>» скачать вирус EICAR по протоколу HTTP, HTTPS, в виде архивного ZIP-файла и т.п.

Проверку необходимо осуществлять с конечного компьютера пользователя.

12.18 Настройка портала авторизации

Для настройки Портала авторизации необходимо добавить новый интерфейс, через который пользователи из внутренней сети получают доступ к Порталу авторизации. Для этого необходимо перейти в раздел «Интерфейсы» - «Назначения портов», нажать  для добавления нового интерфейса и нажать кнопку «Сохранить». Далее необходимо перейти в «Интерфейсы» - «OPT1»,

поставить флажок в поле «Включен» и заполнить настройки интерфейса в соответствии с таблицей 22.

Таблица 22 – Настройка интерфейса

Поле	Значение
Описание	GUESTNET
Блокировать	Не выбрано
Блокировать частные сети	Не выбрано
Блокировать bogon сети	Не выбрано
Тип конфигурации IPv4	Статический IPv4
Тип конфигурации IPv6	Отсутствует
MAC-адрес	(Оставить пустым)
Максимальный размер кадра	(Оставить пустым)
Максимальный размер сегмента	(Оставить пустым)
Скорость и двусторонний режим передачи данных	По умолчанию
Статический адрес IPv4	192.168.200.1/24
Публичный IPv4-адрес шлюз	Автодетектирование

Далее необходимо нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

Для настройки DHCP-сервера необходимо перейти в раздел «Службы» - «DHCPv4» - «GUESTNET» и заполнить поля в соответствии с таблицей 23.

Таблица 23 – Настройка DHCP-сервера

Поле	Значение
Включен	Включен
Диапазон	192.168.200.100 - 192.168.200.200
DNS-серверы	192.168.200.1
Шлюз	192.168.200.1

Необходимо нажать кнопку «Сохранить».

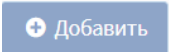
Далее необходимо добавить два разрешающих правила. Для добавления первого разрешающего правила межсетевого экрана необходимо перейти в раздел «Межсетевой экран» - «Правила» - «GUESTNET» и нажать . И заполнить поля в соответствии с таблицей 24.

Таблица 24 – Разрешение входа в Портал авторизации

Поле	Значение
Действие	Разрешить
Интерфейс	GUESTNET
Протокол	TCP
Отправитель	GUESTNET сеть
Получатель	GUESTNET адрес

Поле	Значение
Диапазон портов назначения	(Другое) 8000 / (Другое) 10000
Категория	Общие правила GuestNet
Описание	Разрешить вход в Портал авторизации

Необходимо нажать кнопку «Сохранить».

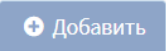


Для добавления второго разрешающего правила межсетевого экрана необходимо перейти в раздел «Межсетевой экран» - «Правила» - «GUESTNET» и нажать . И заполнить поля в соответствии с таблицей 25.

Таблица 25 – Разрешение внутренней сети

Поле	Значение
Действие	Разрешить
Интерфейс	GUESTNET
Протокол	Any
Отправитель	GUESTNET сеть
Получатель	Любой
Диапазон портов получателя	Любой
Категория	Общие правила GUESTNET
Описание	Разрешить GUESTNET

Необходимо нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

Далее необходимо загрузить шаблон страницы авторизации для пользователей Портала авторизации. Для этого необходимо перейти в «Службы» - «Портал авторизации» - «Администрирование» - «Шаблоны» и нажать на  внизу таблицы для скачивания шаблона страницы авторизации пользователей. Далее отредактировать скаченный шаблон при необходимости. Затем нажать на , ввести в поле «Имя шаблона» название шаблона, например, «Test», выбрать скаченный шаблон, нажав на кнопку «Выберите файл» и нажать «Загрузить», а затем кнопку «Применить».


Для создания новой зоны авторизации необходимо перейти в раздел «Службы» - «Портал авторизации» - «Администрирование» и нажать . Необходимо заполнить поля редактирования зоны авторизации в соответствии с таблицей 26.

Таблица 26 – Настройки зоны авторизации

Поле	Значение
Включено	Выбрано
Интерфейсы	GUESTNET
Аутентификация через	Локальная база данных
Значение тайм-аута бездействия	0

Поле	Значение
Значение тайм-аута сеанса	0
Множественный вход пользователя в систему	Не выбрано
Сертификат SSL	Отсутствует
Имя хоста	(оставить пустым)
Разрешенные адреса	(оставить пустым)
Пользовательский шаблон	Test [шаблон созданный в «Службы» - «Портал авторизации» - «Шаблоны»]
Описание	Гостевая

Нажать кнопку «Сохранить», а затем кнопку «Применить».

Далее для авторизации пользователя в портале авторизации необходимо подключиться по локальной сети к ПК «InfoWatch ARMA Industrial Firewall». Открыть на внешнем устройстве любой веб-браузер и ввести запрос: «8.8.8.8». При успешной настройке портала авторизации появится форма входа. Необходимо ввести аутентификационные данные и нажать кнопку «Вход». При успешной авторизации в Портале авторизации отобразится страница «8.8.8.8» в веб-браузере.

При необходимости в выходе из Портала авторизации необходимо перейти на страницу «[IP-адрес графического веб-интерфейса]:8000» и нажать кнопку «Выход».

12.19 Создание Custom правил COB

Создание Custom правил COB описано в подразделе 5.2.9 настоящего руководства.

12.20 Настройка записи дампов трафика

Настройка записи дампов трафика описана в подразделе 7.6.5 настоящего руководства.

12.21 Настройка Active Directory сервера аутентификации (импорт пользователей)

Настройка Active Directory сервера аутентификации (импорт пользователей) описана в подразделе 4.1.3 руководства администратора.

12.22 Добавление правил МЭ и COB для пользователей сервера аутентификации Active Directory

Для добавления пользователей внешнего сервера аутентификации Active Directory необходимо настроить Active Directory сервер аутентификации в соответствии с разделом 12.21 настоящего руководства.

Далее необходимо настроить Портал авторизации, через который пользователи сервера аутентификации Active Directory получают доступ к ПК «InfoWatch ARMA Industrial Firewall».

Перед началом настройки Портала авторизации в ПК «InfoWatch ARMA

Industrial Firewall» должны быть установлены интерфейсы WAN (с доступом в Интернет) и LAN.

Для настройки Портала авторизации необходимо добавить новый интерфейс, через который пользователи из внутренней сети получают доступ к Порталу авторизации. Для этого необходимо перейти в раздел «Интерфейсы» - «Назначения портов», нажать «+» для добавления нового интерфейса и нажать кнопку «Сохранить». Далее необходимо перейти в «Интерфейсы» - «OPT1», поставить флажок в «Включен» и заполнить настройки интерфейса в соответствии с таблицей 27.

Таблица 27 – Настройка интерфейса

Поле	Значение
Описание	GUESTNET
Блокировать	Не выбрано
Блокировать частные сети	Не выбрано
Блокировать bogon сети	Не выбрано
Тип конфигурации IPv4	Статический IPv4
Тип конфигурации IPv6	Отсутствует
MAC-адрес	(Оставить пустым)
Максимальный размер кадра	(Оставить пустым)
Максимальный размер сегмента	(Оставить пустым)
Скорость и двусторонний режим передачи данных	По умолчанию
Статический адрес IPv4	192.168.200.1/24
Публичный IPv4-адрес шлюз	Автодетектирование

Далее необходимо нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

Для настройки DHCP-сервера необходимо перейти в раздел «Службы» - «DHCPv4» - «GUESTNET» и заполнить поля в соответствии с таблицей 28.

Таблица 28 – Настройки DHCP-сервера

Поле	Значение
Включить	Включен
Диапазон	192.168.200.100 - 192.168.200.200
DNS-серверы	192.168.200.1
Шлюз	192.168.200.1

Необходимо нажать кнопку «Сохранить».

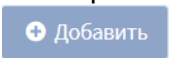
Далее необходимо добавить два разрешающих правила. Для добавления первого разрешающего правила межсетевого экрана необходимо перейти в раздел «Межсетевой экран» - «Правила» - «GUESTNET» и нажать . И заполнить поля в соответствии с таблицей 29.

Таблица 29 – Разрешить вход в Портал авторизации

Поле	Значение
Действие	Разрешить
Интерфейс	GUESTNET
Протокол	TCP
Отправитель	GUESTNET сеть
Получатель	GUESTNET адрес
Диапазон портов назначения	(Другое) 8000 / (Другое) 10000
Категория	Общие правила GuestNet
Описание	Разрешить вход в Портал авторизации

Необходимо нажать кнопку «Сохранить».

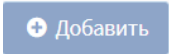

Для добавления второго разрешающего правила межсетевого экрана необходимо перейти в раздел «Межсетевой экран» - «Правила» - «GUESTNET» и нажать . И заполнить поля в соответствии с таблицей 30.

Таблица 30 – Разрешить гостевые сети

Поле	Значение
Действие	Разрешить
Интерфейс	GUESTNET
Протокол	Any
Отправитель	GUESTNET сеть
Получатель	Любой
Диапазон портов получателя	Любой
Категория	Общие правила GuestNet
Описание	Разрешить гостевую сеть

Необходимо нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

Далее необходимо загрузить шаблон страницы авторизации для пользователей Портала авторизации. Для этого необходимо перейти в «Службы» - «Портал авторизации» - «Шаблоны» и нажать на  внизу таблицы для скачивания шаблона страницы авторизации пользователей. Далее нажать на «+», ввести в «Имя шаблона» название шаблона «Test», выбрать скаченный шаблон, нажав на кнопку «Выберите файл» и нажать «Загрузить», а затем кнопку «Применить».

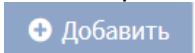
Для создания новой зоны авторизации необходимо перейти в раздел «Службы» - «Портал авторизации» - «Администрирование» и нажать «+». Необходимо заполнить поля редактирования зоны авторизации в соответствии с таблицей 31.

Таблица 31 – Настройки зоны авторизации

Поле	Значение
Включено	Выбрано
Интерфейсы	GUESTNET
Аутентификация через	Active Directory сервер
Значение тайм-аута бездействия	0
Значение тайм-аута сеанса	0
Множественный вход пользователя в систему	Не выбрано
Сертификат SSL	Отсутствует
Имя хоста	(оставить пустым)
Разрешенные адреса	(оставить пустым)
Разрешенные MAC-адреса	(оставить пустым)
Пользовательский шаблон	Test [шаблон созданный в «Службы» - «Портал авторизации» - «Шаблоны»]
Описание	Гостевая


Нажать кнопку «Сохранить», а затем кнопку «Применить».

Открыть на внешнем устройстве любой браузер и ввести запрос: «8.8.8.8». В окне авторизации необходимо ввести аутентификационные данные пользователя сервера аутентификации Active Directory и нажать кнопку «Войти».

Для добавления правила межсетевого экрана, которое будет распространяться на пользователей сервера аутентификации Active Directory необходимо перейти в раздел «Межсетевой экран» - «Правила» - «OPT1» и нажать кнопку .

При создании правила в поле «Отправитель» необходимо выбрать «OPT1 сеть». Заполнение остальных полей описано в подразделе 12.15.2 настоящего руководства.

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

Для добавления правила системы обнаружения вторжений, которое будет распространяться на пользователей сервера аутентификации Active Directory необходимо перейти в раздел «Обнаружение вторжений» - «Контроль уровня приложений» и нажать на кнопку  для создания нового правила.

В поле «IP-адрес отправителя» необходимо ввести подсеть сетевого интерфейса OPT1 (например, 192.168.2.0/24). Заполнение остальных полей описано в подразделах 12.9, 12.19 настоящего руководства. Для сохранения внесенных изменений необходимо нажать на кнопку «Сохранить изменения».

12.23 Ограничение пропускной способности для пользователей сервера аутентификации Active Directory

Для ограничения пропускной способности пользователей сервера аутентификации Active Directory необходимо добавить сервер аутентификации Active Directory. Добавление и настройка сервера аутентификации Active Directory

описано в подразделе 12.21 настоящего руководства. Далее необходимо настроить Портал авторизации. Настройка Портала авторизации подробнее описана в подразделе 12.22 настоящего руководства.

Добавление канала с заданной пропускной способностью описано в подразделе 4.4.2 настоящего руководства.

Добавление правила, которое будет применяться к настроенному каналу для пользователей сервера аутентификации Active Directory, описано в подразделе 4.4.3 настоящего руководства.

12.24 Импорт правил COB по SMB

12.24.1 Импорт правил COB по SMB по запросу пользователя

Для импорта базы решающих правил по запросу пользователя по протоколу SMB необходимо убедиться в наличии архива с правилами, а затем настроить импорт правил.

Для просмотра архива баз решающих правил на удаленном компьютере необходимо перейти в папку формата armaif_[версия ПК «InfoWatch ARMA Industrial Firewall»], например, armaif_3.0. В папке найти архив наборов решающих правил формата «tar.gz». Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz», например, rulesets_3.0_1.1.2.tar.gz. При импорте правил выбирается файл правил с наиболее новой версией.

Далее необходимо настроить импорт правил в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо перейти в «Обнаружение вторжений» - «Настройка импорта правил» - «Настройки». В поле «Включен» поставить флажок. В поле «Протокол» выбрать «SMB». В поле «Адрес» ввести IP-адрес удаленного компьютера. В поле «Samba сервис» необходимо ввести название samba сервиса. В поле «Логин», «Пароль» необходимо ввести учетные данные для подключения к samba серверу. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах). Нажать кнопку «Выполнить».

Перейти в разделе «Обнаружение вторжений» - «Администрирование» - «Обновления» и нажать кнопку «Скачать и обновить правила».

По завершении настройки импорта необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Правила» и найти импортируемые правила (Рисунок 386).

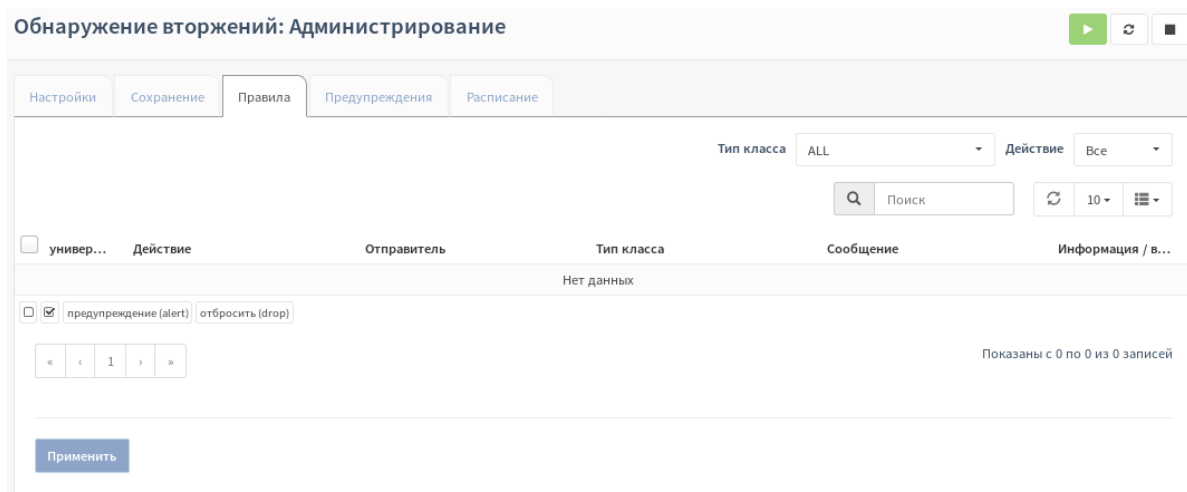


Рисунок 386 – Список правил COB (импорт по запросу пользователя)

12.24.2 Импорт правил COB по SMB по расписанию

Для настройки импорта базы решающих правил по расписанию пользователя по протоколу SMB необходимо убедиться в наличии архива с правилами, а затем настроить импорт правил, расписание для импорта правил.

Для просмотра архива баз решающих правил на удаленном компьютере необходимо перейти в папку формата armaif_[версия ПК «InfoWatch ARMA Industrial Firewall»], например, armaif_3.0. В папке найти архив наборов решающих правил формата «tar.gz». Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz», например, rulesets_3.0_1.1.2.tar.gz. При импорте правил выбирается файл правил с наиболее новой версией.

Далее необходимо настроить импорт правил в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо перейти в «Обнаружение вторжений» - «Настройка импорта правил» - «Настройки». В поле «Включен» поставить флажок. В поле «Протокол» выбрать «SMB». В поле «Адрес» ввести IP-адрес удаленного компьютера. В поле «Samba сервис» необходимо ввести название samba сервиса. В поле «Логин», «Пароль» необходимо ввести учетные данные для подключения к samba серверу. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах). Нажать кнопку «Применить».

Для импорта наборов правил COB по расписанию необходимо создать расписание. Для этого необходимо перейти в раздел «Обнаружение вторжений» - «Администрирование» - «Расписание». В правилах задается периодичность запуска задачи, а не конкретное время запуска задачи.

При редактировании задачи Cron в поле «Включен» необходимо установить флажок для разрешения выполнения задачи Cron. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле «Ч» необходимо выбрать время в часах, когда будет запущена задача. В поле «День месяца» необходимо выбрать день месяца, когда будет запущена задача. В поле «Месяцы» необходимо выбрать месяцы, когда будет запущена задача. В поле «День недели»

необходимо выбрать день недели, когда будет запущена задача. В поле «Команда» необходимо выбрать команду «Импорт правил COB». В поле «Параметры» ввести параметры. В поле «Описание» необходимо ввести описание задачи.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения задачи Cron.

Далее необходимо подождать заданный промежуток времени.

Перейти в раздел «Обнаружение вторжений» - «Администрирование» - «Сохранение» и нажать кнопку «Скачать и обновить правила».

По завершении настройки импорта необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Правила» и найти импортируемые правила (Рисунок 387).

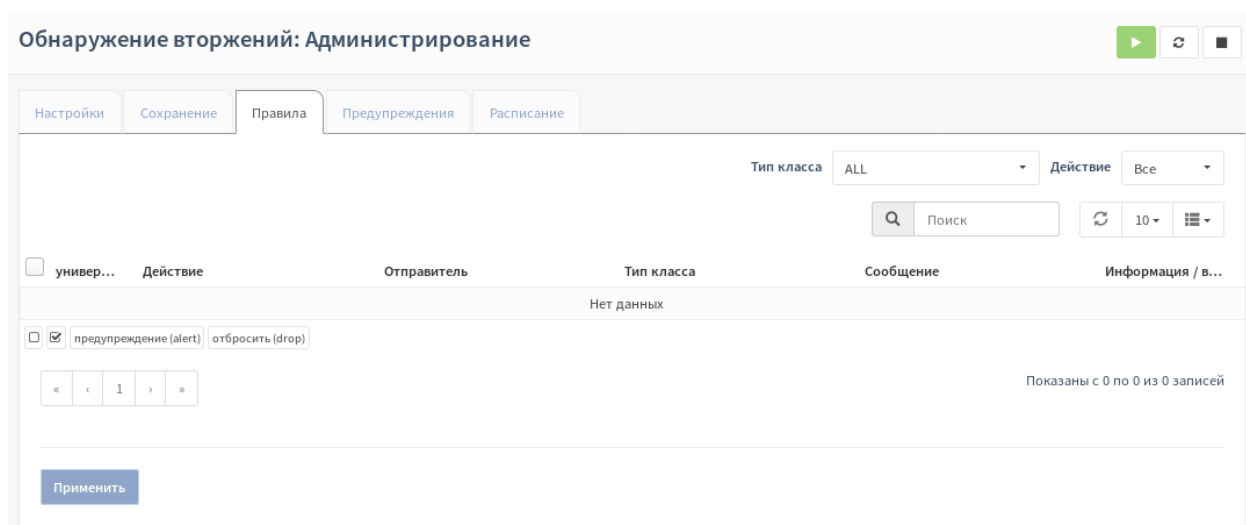


Рисунок 387 – Список правил COB (импорт по расписанию)

12.25 Импорт правил COB по FTP

12.25.1 Импорт правил COB по FTP по запросу пользователя

Для импорта базы решающих правил по запросу пользователя по протоколу FTP необходимо убедиться в наличии архива с правилами, а затем настроить импорт правил.

Для просмотра архива баз решающих правил на удаленном компьютере необходимо перейти в папку формата armaif_[версия ПК «InfoWatch ARMA Industrial Firewall»], например, armaif_3.0. В папке найти архив наборов решающих правил формата «tar.gz». Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz», например, rulesets_3.0_1.1.2.tar.gz. При импорте правил выбирается файл правил с наиболее новой версией.

Далее необходимо настроить импорт правил в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо перейти в «Обнаружение вторжений» - «Настройка импорта правил» - «Настройки». В поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения к FTP серверу. В поле «Путь к корневой папке»

необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах). Нажать кнопку «Выполнить».

Перейти в разделе «Обнаружение вторжений» - «Администрирование» - «Сохранение» и нажать кнопку «Скачать и обновить правила».

По завершении настройки импорта необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Правила» и найти импортируемые правила (Рисунок 386).

12.25.2 Импорт правил COB по FTP по расписанию

Для настройки импорта базы решающих правил по расписанию пользователя по протоколу FTP необходимо убедиться в наличии архива с правилами, а затем настроить импорт правил, расписание для импорта правил.

Для просмотра архива баз решающих правил на удаленном компьютере необходимо перейти в папку формата armaif_[версия ПК «InfoWatch ARMA Industrial Firewall»], например, armaif_3.0. В папке найти архив наборов решающих правил формата «tar.gz». Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz», например, rulesets_3.0_1.1.2.tar.gz. При импорте правил выбирается файл правил с наиболее новой версией.

Далее необходимо настроить импорт правил в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо перейти в «Обнаружение вторжений» - «Настройка импорта правил» - «Настройки». В поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения к FTP серверу. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах). Нажать кнопку «Применить».

Для импорта наборов правил COB по расписанию необходимо создать расписание. Для этого необходимо перейти в раздел «Обнаружение вторжений» - «Настройка импорта правил» - «Расписание». В правилах задается периодичность запуска задачи, а не конкретное время запуска задачи.

При редактировании задачи Cron в поле «Включен» необходимо установить флажок для разрешения выполнения задачи Cron. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле «Ч» необходимо выбрать время в часах, когда будет запущена задача. В поле «День месяца» необходимо выбрать день месяца, когда будет запущена задача. В поле «Месяцы» необходимо выбрать месяцы, когда будет запущена задача. В поле «День недели» необходимо выбрать день недели, когда будет запущена задача. В поле «Команда» необходимо выбрать команду «Импорт правил COB». В поле «Параметры» ввести параметры. В поле «Описание» необходимо ввести описание задачи.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения задачи Cron.

Далее необходимо подождать заданный промежуток времени.

Перейти в разделе «Обнаружение вторжений» - «Администрирование» - «Сохранение» и нажать кнопку «Скачать и обновить правила».

По завершении настройки импорта необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Правила» и найти импортируемые правила (Рисунок 387).

12.26 Экспорт конфигурации по SMB

12.26.1 Экспорт конфигурации по SMB запросу пользователя

Экспорт конфигурации по SMB по запросу пользователя описан в подразделе 7.4 руководства администратора.

Далее на удаленной машине необходимо перейти в настроенную папку и убедиться в наличие экспортируемой конфигурации. Конфигурация ПК «InfoWatch ARMA Industrial Firewall» экспортируются в архиве формата «tar».

12.26.2 Экспорт конфигурации по SMB по расписанию

Экспорт конфигурации и по SMB по расписанию описан в подразделе 6.3.8 настоящего руководства.

Далее на удаленной машине необходимо перейти в настроенную папку и убедиться в наличие экспортируемой конфигурации. Конфигурация ПК «InfoWatch ARMA Industrial Firewall» экспортируются в архиве формата «tar».

12.27 Экспорт конфигурации по FTP

12.27.1 Экспорт конфигурации по FTP по запросу пользователя

Экспорт конфигурации по FTP по запросу пользователя описан в подразделе 7.4 руководства администратора.

Далее на удаленной машине необходимо перейти в настроенную папку и убедиться в наличие экспортируемой конфигурации. Конфигурация ПК «InfoWatch ARMA Industrial Firewall» экспортируются в архиве формата «tar».

12.27.2 Экспорт конфигурации по FTP по расписанию

Экспорт конфигурации и по FTP по расписанию описан в подразделе 6.3.8 настоящего руководства.

Далее на удаленной машине необходимо перейти в настроенную папку и убедиться в наличие экспортируемой конфигурации. Конфигурация ПК «InfoWatch ARMA Industrial Firewall» экспортируются в архиве формата «tar».

12.28 Настройка DHCP-сервера

Настройка DHCP-сервера описана в подразделе 10.2.1 настоящего руководства.

12.29 Настройка DHCP клиента

Для настройки DHCP-клиента необходимо в графическом интерфейсе перейти в «Интерфейсы» - «[Название интерфейса, на котором настраивается

DHCP клиент]». В поле «Тип конфигурации IPv4»/ «Тип конфигурации IPv6» необходимо выбрать «DHCP». Остальные поля оставить по умолчанию. Нажать кнопку «Сохранить».

В консольном меню необходимо ввести команду «8», а затем «ping [IP-адрес DHCP-сервера]».

Убедиться, в наличие IP-адреса на выбранном интерфейсе в диапазоне DHCP-сервера.

12.30 Настройка динамической маршрутизации RIP

Настройка динамической маршрутизации RIP описана в подразделе 9.2 настоящего руководства.

12.31 Настройка динамической маршрутизации OSPF

Настройка динамической маршрутизации OSPF описана в подразделе 9.3 настоящего руководства.

12.32 Настройка блокирования сеанса доступа пользователя при неактивности

Для настройки блокирования сеанса доступа пользователя при неактивности необходимо перейти в «Система» - «Настройки» - «Администрирование» и в поле «Тайм-аут сессии» ввести количество минут, через которое сеанс доступа будет заблокирован при неактивности пользователя. Для сохранения настроек необходимо нажать кнопку «Сохранить».

12.33 Просмотр и фильтрация пакетов, прошедших через ПК «InfoWatch ARMA Industrial Firewall»


Для просмотра дампов трафика пакетов, прошедших через ПК «InfoWatch ARMA Industrial Firewall» необходимо включить систему обнаружения вторжений.

Перед включением необходимо убедиться, что отключен режим Hardware Offloading. Для выключения режима Hardware Offloading необходимо перейти в «Интерфейсы» - «Настройки» и поставить флажки напротив «CRC аппаратного обеспечения», «TSO аппаратного обеспечения», «LRO аппаратного обеспечения». Нажать кнопку «Сохранить» внизу страницы.

Для включения системы обнаружения вторжений необходимо установить флажок напротив поля «Включен». В поле «Сравнение шаблонов» необходимо выбрать используемый алгоритм поиска подстроки при обработке пакетов:

- по умолчанию (используется алгоритм Aho-Corasick);
- Aho-Corasick (алгоритм сопоставления со «словарем», который находит подстроки из «словаря» в пакетах);
- Hyperscan (высокопроизводительная библиотека сопоставления регулярных выражений от Intel).

В поле «Интерфейсы» необходимо выбрать интерфейсы, которые будут использоваться системой обнаружения и предотвращения вторжений. Для сохранения настроек необходимо нажать на кнопку «Применить»

Для просмотра собранных дампов трафика необходимо перейти в «Сеть» - «Анализ трафика» - «Журналирование» и выбрать дамп трафика для анализа. Максимальное количество сохраняемых файлов – 20 файлов по 100 Мбайт каждый. В поле «Фильтр отображения» позволяет осуществлять фильтрацию с помощью встроенных интерактивных фильтров. Для применения фильтра необходимо нажать кнопку .

12.34 Настройка мониторинга по SNMP (v1, v2)


Для настройки мониторинга по протоколу SNMP v1, v2 необходимо перейти в раздел «Система» - «Настройки» - «SNMP» - «Общие настройки» и выполнить следующие действия:

- установить флажок напротив «Включен»;
- установить значение в «Community String» (например, «custom»);
- нажать кнопку «Сохранить».

Настройка завершена. Для подключения к ПК «InfoWatch ARMA Industrial Firewall» необходимо использовать IP-адрес, через который будет осуществляться мониторинг. В качестве Community String необходимо использовать значение, введенное в поле «Community String».

12.35 Настройка мониторинга по SNMPv3

Для настройки мониторинга по протоколу SNMP v3 необходимо перейти в раздел «Система» - «Настройки» - «SNMP» - «Общие настройки» и выполнить следующие действия:

- во вкладке «Общие настройки»:
 - установить флажок напротив «Включен»;
 - оставить поле «Community String» пустым;
 - нажать «Сохранить».
- во вкладке «SNMPv3» создать пользователя:
 - нажать на  для создания пользователя;
 - установить флажок напротив «Включен»;
 - ввести имя пользователя в поле «Имя пользователя»;
 - ввести пароль в поле «Пароль»;
 - ввести ключ шифрования в поле «Ключ шифрования»;
 - нажать «Сохранить».

Настройка завершена. Для подключения к ПК «InfoWatch ARMA Industrial Firewall» необходимо использовать IP-адрес, через который будет осуществляться мониторинг, и учетные данные созданного пользователя.

12.36 Создание сертификата

Создание сертификата описано в подразделе 6.9.1 настоящего руководства.

Для того чтобы скачать созданный сертификат необходимо перейти в «Система» - «Доверенные сертификаты» - «Сертификаты».

Затем необходимо добавить сертификат в список доверенных сертификатов в веб-браузере. Далее расписан пример добавления сертификата для веб-браузера Google Chrome.

В веб-браузере Google Chrome необходимо перейти в меню «Настройки» - «Дополнительные настройки» и нажать кнопку «Настроить сертификаты».

Для установки сертификата необходимо перейти во вкладку «Доверенные корневые центры сертификации» и нажать кнопку «Импорт...». В открывшемся окне необходимо нажать кнопку «Далее >».

Для выбора файла сертификата необходимо нажать кнопку «Обзор..» и выбрать файл сертификата. Нажать кнопку «Открыть», а затем кнопку «Далее >».

Предлагаемое по умолчанию хранилище сертификатов должно совпадать с тем, куда следует поместить корневой сертификат. Если импорт был инициирован из другого раздела хранилища сертификатов, то необходимо выбрать по кнопке «Обзор..» хранилище «Доверенные корневые центры сертификации» и нажать кнопку «Далее >».

Затем следует подтвердить завершение работы мастера, нажав кнопку «Готово», затем кнопку «Да» и кнопку «ОК».

Для контроля правильности проделанных операций в «Сертификаты» - «Доверенные корневые центры сертификации» в конце списка необходимо найти установленный ранее корневой сертификат.

Затем необходимо перезагрузить веб-браузер.

12.37 Настройка статической маршрутизации

Для настройки статической маршрутизации необходимо перейти в «Система» - «Шлюзы» - «Единичный» и нажать кнопку «+». В поле «Имя» ввести название шлюза. В поле «Интерфейс» выбрать сетевой интерфейс, через который будет проходить маршрут. В поле «Семейство адресов» выбрать версию протокола IP. В поле «IP-адрес» ввести IP-адрес шлюза. Нажать кнопку «Сохранить».

Затем перейти в «Система» - «Маршруты» - «Конфигурация» и нажать кнопку «+». В поле «Адрес сети» необходимо ввести адрес сети (в формате [адрес сети]/[маска сети]) конечной точки маршрута. В поле «Шлюз» выбрать созданный шлюз. В поле «Описание» ввести описание маршрута. Нажать кнопку «Сохранить изменения».

12.38 Настройка OpenVPN в режиме «сеть – сеть»

Для того чтобы настроить OpenVPN в режиме «сеть - сеть» используется следующая топология (Рисунок 388).

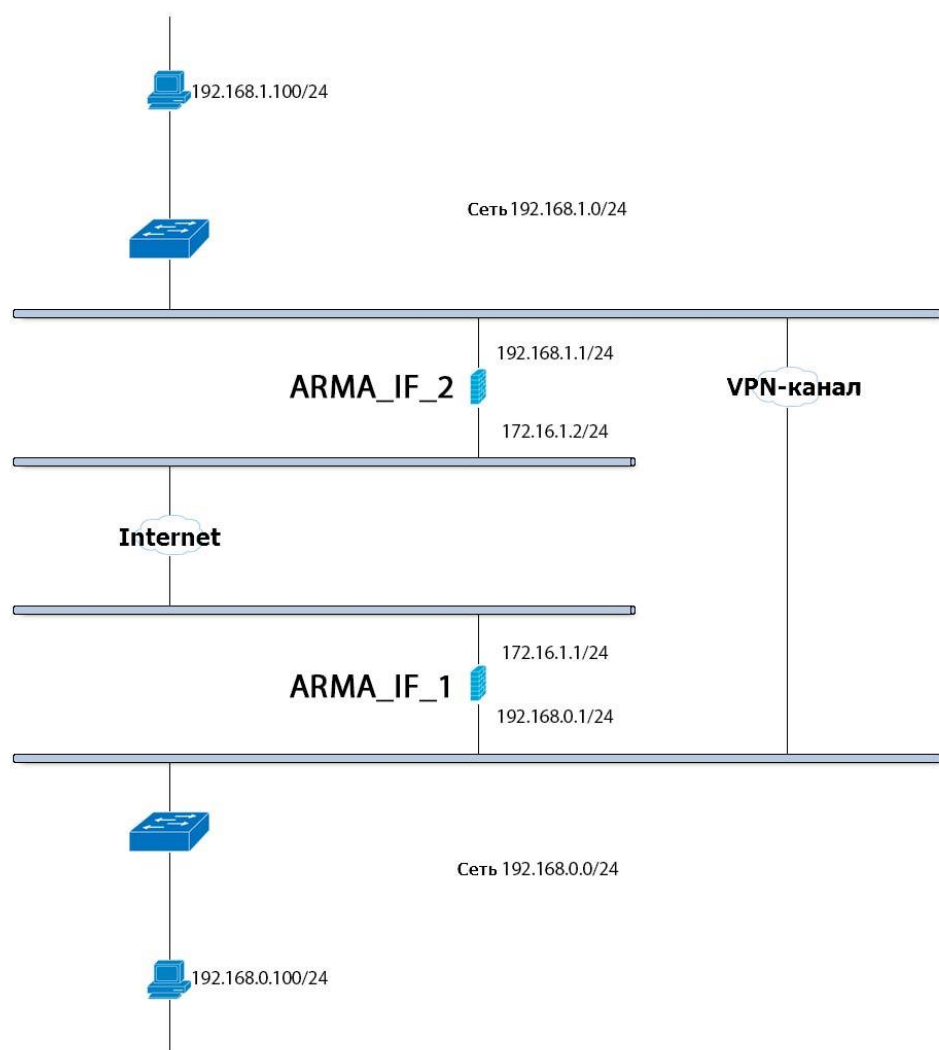


Рисунок 388 – Топология сети для настройки OpenVPN в режиме «сеть - сеть»

Маршрутизатор ARMA_IF_1

Имя хоста	ARMA_IF_1
WAN IP	172.16.1.1/24
LAN IP	192.168.0.1/24

Маршрутизатор ARMA_IF_2

Имя хоста	ARMA_IF_2
WAN IP	172.16.1.2/24
LAN IP	192.168.1.1/24

Убедитесь, что маршрутизаторы ARMA_IF_1 и ARMA_IF_2 имеют адекватные сетевые настройки. В частности, WAN-адаптерам должны быть присвоены валидные «белые» либо доступные друг другу (с одного МЭ можно получить ответ на команду ping по адресу интерфейса WAN другого МЭ) IP-адреса - в нашем примере, это адреса 172.16.1.1 и 172.16.1.2.

На обоих маршрутизаторах, в разделе «Межсетевой экран» - «Правила» на вкладке WAN, создайте правило для разрешения ICMP-трафика в тестовых. С

каждого из маршрутизаторов, из раздела «Интерфейсы» - «Диагностика» - «Ping», осуществите пропинговку IP-адреса WAN-адаптера противоположного маршрутизатора. Тем самым, проверяем, что передача трафика между маршрутизаторами через сеть Интернет (либо любую другую изолированную) возможна и ей ничего не препятствует.

LAN-сегмент, располагающийся за каждым из маршрутизаторов, должен использовать уникальную IP-сеть. В нашем примере, это условие выполняется – за маршрутизатором ARMA_IF_1 располагается IP-сеть 192.168.0.0/24, за маршрутизатором ARMA_IF_2 располагается IP-сеть 192.168.1.0/24.

12.38.1 Настройка VPN на маршрутизаторе ARMA_IF_1

Для настройки VPN на маршрутизаторе ARMA_IF_1 необходимо перейти в «VPN» - «OpenVPN» - «Серверы» и нажать на кнопку «Добавить» в верхнем правом углу формы. Используйте следующие настройки (настройки, которые мы опускаем, должны остаться по умолчанию):

Режим сервера	Пиринговая сеть (общий ключ)
Протокол	UDP
Режим работы устройства	tun
Интерфейс	WAN
Локальный порт	1194
Описание	OpenVPN peer 1
Совместно используемый ключ	Установите флажок для генерации нового ключа
Алгоритм шифрования	AES-256-CBC (256-bit)
Дайджест-алгоритм аутентификации	SHA512 (512-bit)
Hardware Crypto	Без аппаратного ускорения криптоалгоритмов
Туннельная сеть IPv4	10.10.0.0/24
Локальная сеть/сети IPv4	192.168.0.0/24
Удаленная сеть/сети IPv4	192.168.1.0/24
Сжатие	Включено с использованием адаптивного сжатия

Для применения настроек необходимо нажать на кнопку «Сохранить».

12.38.2 Копирование ключа

После создания нового сервера, в его настройках генерируется ключ, который необходимо также прописать на противоположной стороне туннеля (на маршрутизаторе ARMA_IF_2). Для копирования ключа, щелкните на иконку «карандаш» напротив ранее созданного VPN-сервера.

Пример того, как выглядит ключ:

```
#  
# 2048 bit OpenVPN static key  
#  
-----BEGIN OpenVPN Static key V1-----  
0d6db17250aa5a20afc8952a367e86f1  
71605721f1519a3827945b426879c1c9  
b3bf75fb9c910a1eb0252eaf62d9f944  
2123776554e569ce8b52043a3668ea43  
9cafa790e07245775550c81f91c46f73  
b500fcdcf7b86edac1e885c6a8e6a794  
75b868b4ad5d8cd468a53d05853da91e  
e43a3ae58f56f50daddb7b884b9336e7  
519e3530a27853c9da3eb7bf24fde79a  
0b0b4b8bbaf3296240ebfa069afc5d42  
84baeed3307ef8973697bc10b20d27b8  
1416876456514534379e2b823d67aaa4  
4662b130e1d5114bf8f1992a638f098b  
3bc55085d1277faa6e7fd6110080796f  
ce6e3758a9092c5543455e248ac129fb  
60c321ac395bb23abbd567560f1888b1  
-----END OpenVPN Static key V1-----
```

12.38.3 Настройка VPN на маршрутизаторе ARMA_IF_2

Для настройки VPN на маршрутизаторе ARMA_IF_2 необходимо перейти в раздел «**VPN**» - «**OpenVPN**» - «**Клиенты**» и нажать на кнопку «Добавить» в верхнем правом углу формы.

Используйте следующие настройки (настройки, которые мы опускаем, должны остаться по умолчанию):

Режим сервера	Пиринговая сеть (общий ключ)
Протокол	UDP
Режим работы устройства	tun

Интерфейс	WAN
Адрес сервера	172.16.1.1
Порт сервера	1194
Описание	OpenVPN peer 2
Совместно используемый ключ	Уберите флажок и вставьте ключ, скопированный с маршрутизатора ARMA_IF_1
Encryption algorithm	AES-256-CBC (256-bit)
Auth Digest Algorithm	SHA512 (512-bit)
Hardware Crypto	Без аппаратного ускорения криптоалгоритмов
Туннельная сеть IPv4	10.10.0.0/24
Удаленная сеть/сети IPv4	192.168.0.0/24
Сжатие	Включено с использованием адаптивного сжатия

Для применения настроек необходимо нажать на кнопку «Сохранить».

Как видно из настроек, VPN будет обладать следующими характеристиками:

SSL/TLS используется

Туннелируемый трафик инкапсулируется в UDP-пакеты

OpenVPN демон будет обрабатывать подключения только на IP-адрес, присвоенный WAN-адаптеру

Сертификаты не используются

Аутентификация по логину/паролю не используется

Аутентификация TLS не используется

Сжатие данных используется

12.38.4 Создание правил межсетевого экрана

На маршрутизаторе, который настраивался как VPN-сервер (маршрутизатор ARMA_IF_1), в разделе «Межсетевой экран» - «Правила» во вкладке WAN, создайте правило для разрешения OpenVPN-трафика. По умолчанию, OpenVPN использует протокол UDP и порт 1194 ().

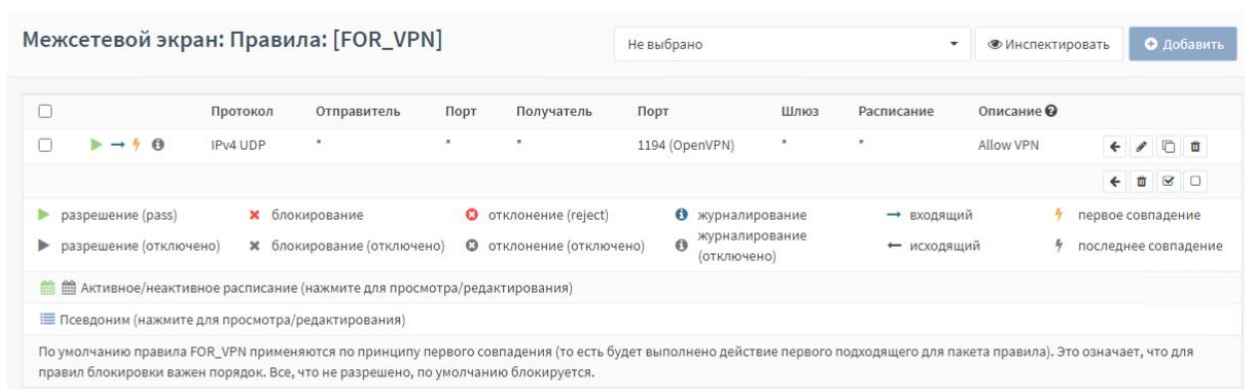


Рисунок 389 – Правило МЭ на маршрутизаторе ARMA_IF_1 (1)

Для того чтобы трафик мог передаваться между сетями 192.168.1.0/24 и 192.168.2.0/24 по туннелю, в разделе «Межсетевой экран» - «Правила» во вкладке OpenVPN, создайте следующие правила:

На маршрутизаторе ARMA_IF_1 – правило для разрешения трафика из IP-сети 192.168.1.0/24.

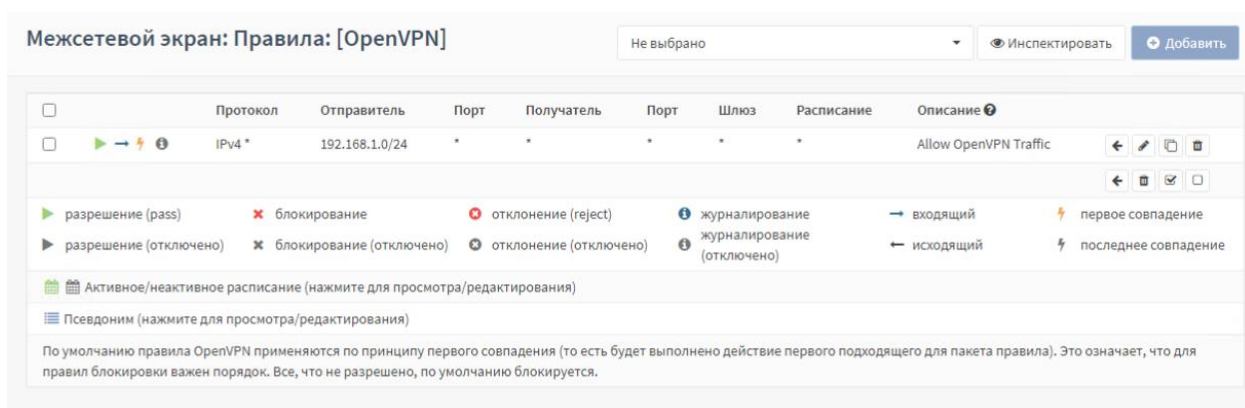


Рисунок 390 – Правило МЭ на маршрутизаторе ARMA_IF_1 (2)

На маршрутизаторе ARMA_IF_2 – правило для разрешения трафика из IP-сети 192.168.0.0/24.

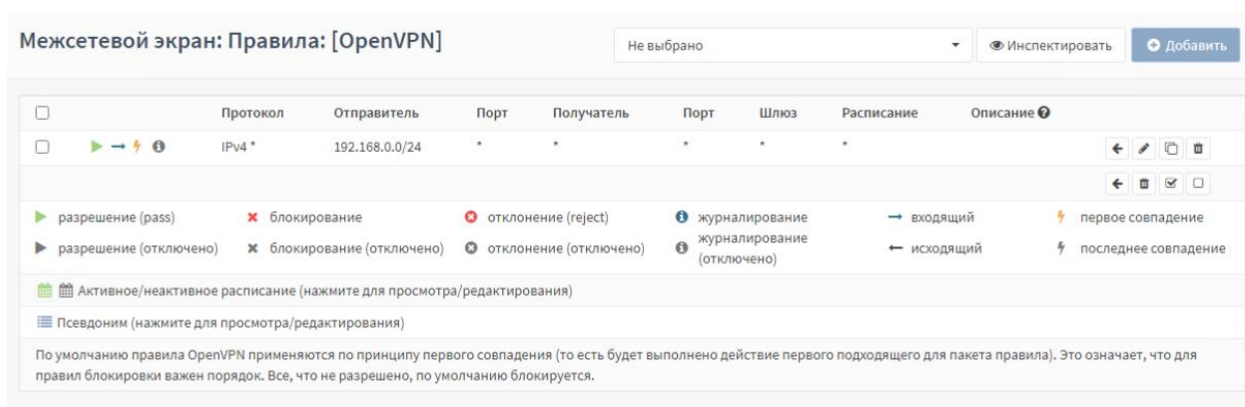


Рисунок 391 – Правило МЭ на маршрутизаторе ARMA_IF_2

Для применения настроек необходимо нажать на кнопку «Применить изменения».

Подключенных к VPN-серверу клиентов можно посмотреть в разделе «VPN» - «OpenVPN» - «Статус соединения» (Рисунок 392).




VPN: OpenVPN: Статус соединения						
Статистика запросов клиента						
Имя	Удаленный хост	Виртуальный адрес	Подключен с	Отправлено байт	Получено байт	Статус
ssl vpn client UDP	172.16.1.1	10.10.0.2	2020-12-04 11:46:07	26 KB	25 KB	up   

Рисунок 392 – VPN. OpenVPN. Статус соединения

13 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

13.1 Неправильный ввод в системе

При неправильном вводе в системе возникает ошибка «ошибка на стороне сервера (Рисунок 393).

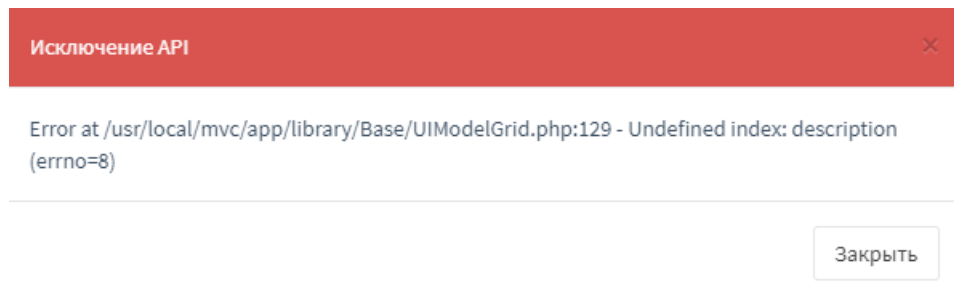


Рисунок 393 – Ошибка на стороне сервера

13.2 Предупреждение об удалении

При любом удалении появляется всплывающее предупреждение (Рисунок 394).

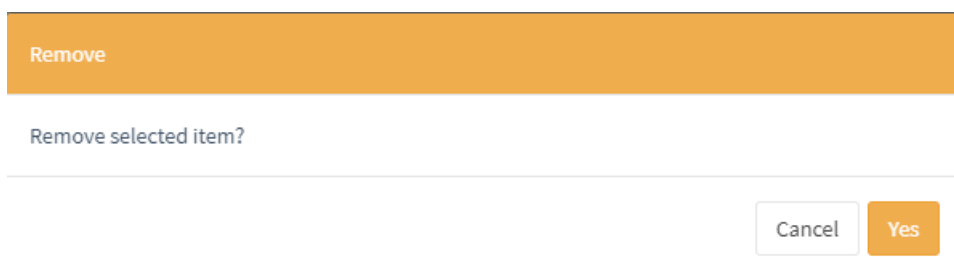


Рисунок 394 – Удаление

13.3 Неправильный ввод в поле

При любом неправильном вводе в поля появляется предупреждение вверху страницы (Рисунок 395) или напротив полей (Рисунок 396).

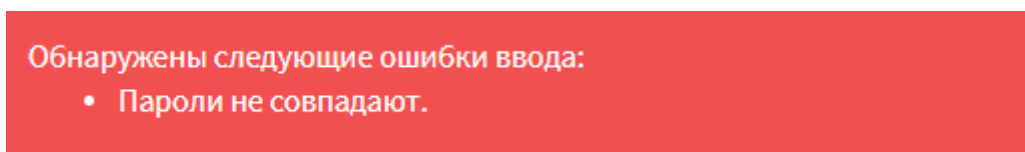


Рисунок 395 – Предупреждение о неправильном вводе (вид 1)

Размер кэша (в МБ)

100укапаку

Specify a positive cache size. (number of MB's)

Рисунок 396 – Предупреждение о неправильном вводе (вид 2)

13.4 Предупреждение при применении настроек

При применении настроек появляется предупреждение вверху страницы (Рисунок 397).

Настройки применены, правила перезагружаются в фоновом режиме

Рисунок 397 – Применено изменение

13.5 Импорт файла с некорректными правилами

При импорте файла с некорректными правилами системы обнаружения вторжений в формате Snort в разделе меню «Обнаружение вторжений» - «Администрирование» - «Сохранение» правила не будут добавлены. Запись об этом появится в «Обнаружение вторжений» - «Журнал» (Рисунок 398).

Обнаружение вторжений: Журнал

<div><div>🔍</div><div>Искать конкретное сообщение...</div></div>	
Дата	Сообщение
Aug 9 16:49:44	suricata: [100126] <Notice> -- rule reload complete
Aug 9 16:49:44	suricata: [100142] <Error> -- [ERRCODE: SC_ERR_PCAP_DISPATCH(20)] - error code -2
Aug 9 16:49:44	suricata: [100126] <Error> -- [ERRCODE: SC_ERR_INVALID_SIGNATURE(39)] - error parsing signature "alert tcp any any -> " from file /usr/local/etc/suricata/opsense.rules/userlocal.rules at line 1

Рисунок 398 – Некорректный файл правил COB