# **O** SOLAR

# Программный комплекс «Solar NGFW»

Версия 1.5

## Руководство администратора безопасности

Москва, 2025

## Содержание

Перечень терминов и сокращений	10
1. Введение	12
1.1. Область применения	12
2. Назначение и условия применения	13
2.1. Назначение Solar NGFW	13
2.2. Краткое описание возможностей	13
2.3. Условия применения	13
2.3.1. Требования к аппаратному обеспечению АРМ администратора	
безопасности	13
2.3.2. Требования к программному обеспечению АРМ администратора	
безопасности	14
2.3.3. Уровень подготовки администратора безопасности	14
2.3.4. Перечень эксплуатационной документации для ознакомления	15
3. Общие сведения о Solar NGFW	16
3.1. Принцип работы Solar NGFW	16
3.1.1. Принцип работы прокси-сервера в Solar NGFW	16
3.2. Политика безопасности доступа к веб-ресурсам	18
3.3. Принципы работы в интерфейсе Solar NGFW	19
3.3.1. Начало работы. Вход в систему	19
3.3.2. Описание основных элементов интерфейса	22
4. Рабочий стол: мониторинг работы системы	28
5. Досье: получение информации о пользователях	31
5.1. Общие сведения	31
5.2. Управление источниками данных и синхронизация Досье	32
5.3. Структурирование персон/групп персон	33
531 Общие свеления	33
5.3.2 Лействия с группами персон	33
5.3.3. Добавление и удаление персоны	35
5.4. Попучение информации о деятельности персон и групп персон	35
5.4.1. Попучение информации о деятельности порест и трупп персон	35
5.4.2. Попучение информации о деятельности конкретной персоны (карточка	00
о.ч.2. Получение информации о деятельности конкретной персоны (карточка персоны)	37
5.5. Операции с данными персон	Δ1
5.5.1. Перецень операций с данными персон	11
5.5.2. Поберление примечений комментериев и фейлов	11
5.5.2. Добавление примечании, комментариев и файлов	12
5.5.5. Гедактирование данных персоны	42
5.5.4. Объединение карточек персон	44
5.6. Поле «поиск персоны». оперативный доступ к данным о	45
Персоне/адресе	45
6.1. Одионика реализация политики ив	41
6.1. Описание элементов политики	47
6.2. Общий долодок изотройки долигии ИГ	50
6.3. Общий порядок настройки политики и в	5Z
6.4. Управление инструментами политики	54 54
6.4.1. Принципы работы со слоями правил политики	54
о.4.2. Принципы расоты с правилами и исключениями	58
о.4.3. Принципы расоты с инструментами политики	ю <i>3</i>
6.4.4. Экспорт и импорт политики и ее отдельных инструментов	00
о.э. инструменты политики	/1 •
6.5.1. Слои правил политики	71

	111
	116
	122
	122
6.5.6. Шаблоны заголовков и страниц	1/6
6.6. Приморы цеотройки попитики фильтрониц	140
0.0. Примеры настроики политики фильграции	150
6.6.2. Успользование межсетевого экрана в политике фильтрации	150
6.6.2. Иривление вео-сервисами и приложениями (пDPI)	157
о.о.э. исключение сигнатуры для правил системы предотвращения	150
вторжении	100
	109
6.6.5. Исключение вскрытия НТТРО-трафика пользователей	160
6.6.6. Блокировка загрузки ZIP-фаилов по протоколу HTTPS	103
6.6.7. Перенаправление трафика пользователей антивирусу	165
6.6.8. Управление фильтрациеи запросов пользователеи	167
6.6.9. Управление фильтрациеи ответов пользователеи	. 168
6.6.10. Блокировка загрузки содержимого черновиков в ОША в режиме	
обратного прокси	. 169
6.6.11. Блокировка загрузки писем с запрещенными файлами в ОWA в	
режиме обратного прокси	. 172
6.7. Отложенное скачивание	. 174
6.8. Управление базами категоризации	176
7. Статистика: получение сводных статистических отчетов	179
7.1. Общие сведения	179
7.2. Работа с отчетами	. 179
7.2.1. Общие сведения	179
7.2.2. Формирование отчета	180
7.2.3. Просмотр отчета	187
7.2.4. Редактирование отчета	190
7.2.5. Отправка копии отчета	191
7.2.6. Экспорт отчета в PDF	192
7.2.7. Удаление отчета	. 193
7.3. Работа с папками сохраненных отчетов	. 194
7.4. Примеры формирования отчетов	196
8. Пользователи: управление правами доступа пользователей	202
8.1. Роли: назначение прав доступа к функциям и разделам системы	202
8.1.1. Задание ролевой модели доступа	204
8.2. Пользователи: операции с учетными записями пользователей системы	212
8.2.1. Общие сведения	212
8.2.2. Создание учетной записи пользователя	213
8.2.3. Редактирование учетной записи пользователя	215
8.2.4. Блокировка/разблокировка учетной записи пользователя	217
8.2.5. Удаление учетной записи пользователя	217
8.3. LDAP операции с доменными группами	218
8.4. Выдача/отзыв прав доступа	219
Приложение А. Применение МІМЕ-типов для реализации политики безопасности	
доступа к веб-ресурсам в Solar NGFW	222
Приложение В. Язык описания регулярных выражений	224
Приложение С. Использование полстановочных символов	225
Приложение D. Метолы НТТР-протокопа	227
Приложение F. Матрица MЭ Solar NGEW	229
Приложение Е. Перечень фильтов для формирования отчетов	232
	202

Лист контроля версий	
----------------------	--

# Список иллюстраций

3.1. Solar NGFW в архитектуре защиты сети	16
3.2. Пример проверки данных информационного обмена с помощью Solar NGFW	18
3.3. Авторизация	20
3.4. Уведомление об отсутствии лицензии	20
3.5. Окно лицензии	21
3.6. Рабочий стол	22
3.7. Главное меню Solar NGFW	24
3.8. Меню пользователя	25
3.9. Выбор раздела «Политика > Справочники > Ключевые слова»	26
3.10. Примеры меню действий	27
4.1. Раздел «Рабочий стол»	28
42 Выбор периода обновления данных на рабочем стопе	28
4.3. Разлеп «Рабочий стоп»: просмотр статистики системы	29
4.4. Раздел «Рабочий стол»: сужение временного диапазона	29
4.5. Раздел «Рабочий стол»: озжение временного дианазона	30
4.0.1 аздел «Гассчий стол», расширение временного дианазона	31
5.2 Раздел «Досье»: Видадиа «Настройки»	32
	33
5.5. Синхронизация досье	24
5.4. Кнопки для дооавления раздела, труппы или персоны	34 24
5.5. Меню деиствии струппои персон	34 25
5.6. Удаление персоны из группы	30
5.7. Раздел «досье». Получение информации о группе персон	30
5.8. Раздел «досье». Получение информации о группе персон. Вкладка «Статистика	~7
запросов»	37
5.9. Получение информации о группе персон. Вкладка «Статистика запросов»:	~ 7
экспорт данных в CSV	37
5.10. Раздел «Досье», список персон. Краткая карточка персоны	38
5.11. Полная карточка персоны (вкладка «Основное»)	38
5.12. Полная карточка персоны (вкладка «Трафик»)	39
5.13. Полная карточка персоны (вкладка «Типы данных»)	40
5.14. Полная карточка персоны (вкладка «Журнал»)	40
5.15. Полная карточка персоны (вкладки «Трафик», »Типы данных» и »Журнал»)	41
5.16. Полная карточка персоны: добавление, просмотр и удаление примечаний	42
5.17. Полная карточка персоны. Режим редактирования данных	43
5.18. Режим редактирования данных: примеры окон для редактирования сведений	
о персоне	43
5.19. Объединение карточек персон	45
5.20. Особенности поиска персон: поиск ведется одновременно по нескольким	
атрибутам персоны	46
5.21. Оперативное получение данных о сотруднике	46
6.1. Раздел «Политика»	49
6.2. Раздел «Политика»: распространяемая политика	50
6.3. Приоритет правила	51
6.4. Окно «Применить политику»	52
6.5. Окно «Настройка» в разделе «Политика»	53
6.6. Справка в слое "Доступ без аутентификации"	54
6.7. Меню действий со слоем	55
6.8. Скопированный слой	56
6.9. Включение/отключение слоя	57
6.10. Раздел «Политика»: список правил и исключений	58

6.11       Строка с правилом       58         6.12       Раздел «Политика»: настройка отображения колонок таблицы       59         6.13. Поиск по атрибутам правил и исключения       60         6.14. Формирование правила и/или исключения       62         6.15. Колпурование значений       62         6.16. Включение/отключение правила или исключения       63         6.17. Кнопки для экспорта и импорта политики       67         6.18. Экспорт турлпы инструментов политики       67         6.19. Экспорт турлпы инструментов политики       61         6.20. Импорт инструментов политики       71         6.21. Окно «Загрузить данные из файла»       71         6.22. Слой правил политики «Фильтр реходящего трафика»       74         6.23. Слой правил политики «Фильтр исходящего трафика»       74         6.24. Слой правил политики «Фильтр исходящего трафика»       74         6.25. Слой правил политики «Фильтр исходящего трафика»       74         6.26. Слой политики «Системы предотвращения вторжений»       83         6.28. Слой политики «Фильтра или исключения > Наборы сигнатур»       90         6.29. Слой правил политики «Фильтрация запросов»       84         6.30. Слой правил политики «Перенаправление по (САР»       98         6.31. Слой правил политики «Срертера зутентификации»       91			
6.12. Пракс по агрибутам правил и исключения       59         6.13. Поиск по агрибутам правил и исключения       60         6.14. Формирование правила и/или исключения       62         6.15. Включение/отялючение правила или исключения       62         6.16. Включение/отялючение правила или исключения       63         6.17. Кнопки для экспорта и импорта политики       67         6.19. Экспорт отдельного инструмента политики       68         6.19. Окспорт отдельного инструмента политики       69         6.10. Оклорт инструментов политики       67         6.19. Экспорт отдельного инструментов политики       67         6.19. Экспорт отдельного инструментов политики       67         6.21. Окно «Загрузить данные из файла»       71         6.22. Слой правил политики «Фильтр транзитного трафика»       74         6.23. Слой правил политики «Фильтр исходящего правила»       81         6.25. Слой правил политики «Фильтр исходящего правила»       81         6.26. Слой политики «Фильтрация адресов»       84         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой правил политики «Фильтрация запросов»       93         6.30. Слой правил политики «Скрытие НТРS»       97         6.32. Слой правил политики «Фильтрация запросов»       102         6.33. Слой правил политики	6.11.	Строка с правилом	58
6.13. Поиск по атрибутам правил и исключения       60         6.14. Формирование правила или исключения       62         6.14. Формирование правила или исключения       62         6.15. Включение/отключение правила или исключения       63         6.17. Кнопки для экспорта и импорта политики       63         6.19. Экспорт туплы инструментов политики       68         6.19. Экспорт туплы инструментов политики       68         6.19. Экспорт туплы инструментов политики       71         6.20. Импорт инструментов политики       71         6.21. Окно «Загрузить данные из файла»       71         6.22. Слой правил политики «Фильтр транзитного трафика»       74         6.23. Слой правил политики «Фильтр транзитного трафика»       77         6.24. Слой правил политики «Фильтр исходящего правила»       81         6.25. Слой политики «Предотвращение вторжений»       87         6.26. Слой политики «Предотвращение вторжений»       88         6.28. Слой политики «Предотвращение вторжений»       93         6.30. Слой правил политики «Декратврация апресов»       102         6.31. Слой правил политики «Перенаправление по ICAP»       93         6.32. Слой правил политики «Перенаправление по ICAP»       93         6.33. Слой правил политики «Перенаправление по ICAP»       94         6.34. Слой правил политики «Пере	6.12.	Раздел «Политика»: настройка отображения колонок таблицы	59
6.14. Формирование правила и/или исключения         62           6.15. Колиуование значений         62           6.16. Включение/отключение правила или исключения         63           6.17. Кнопки для экспорта и импорта политики         63           6.18. Экспорт трупы ниструментов политики         64           6.19. Экспорт трупы ниструментов политики         69           6.20. Импорт инструментов политики         69           6.21. Окно «Загрузить данные из файла»         71           6.22. Слой правил политики «Фильтр тразитного трафика»         74           6.23. Слой правил политики «Фильтр исходящего правила»         81           6.24. Слой правил политики «Фильтр исходящего правила»         81           6.26. Слой политики «Транспяция адресов»         84           6.26. Слой политики «Транспяция адресов»         84           6.29. Статистика о фаботе Окстемы предотвращения вторжений»         88           6.29. Слатистика предотвращения вторжений         93           6.30. Слой правил политики «Доступ без аутентификации»         94           6.31. Слой правил политики «Фильтрация ответов»         93           6.32. Слой правил политики «Доступ без аутентификации»         94           6.33. Слой правил политики «Достапа расинфорки»         116           6.32. Слой правил политики «Перенаправление по (САР»         98	6.13.	Поиск по атрибутам правил и исключений	60
b.1b. Копирование значении         62           c16. Включение/отключение правила или исключения         63           c17. Кнопки для экспорта и импорта политики         67           c18. Вхлюрот торального инструментов политики         68           c19. Экспорт отрального инструмента политики         68           c19. Экспорт отрального инструмента политики         69           c20. Импорт инструментов политики         71           c21. Окно «Загрузить данные из файла»         71           c22. Слой правил политики «Фильтр раходящего трафика»         74           c23. Слой правил политики «Фильтр исходящего правила»         81           c26. Слой политики «Предотвращение вторжений»         87           c27. Создание исключений «Системы предотвращения вторжений»         87           c28. Слой политики «Предотвращение вторжений > Наборы сигнатур»         90           c29. Статистика по работе Системы предотвращения вторжений         93           c30. Слой правил политики «Секрытие НТТРС»         97           c32. Слой правил политики «Секрытие НТРС»         97           c33. Слой правил политики «Правила расшифровки»         116           c34. Слой правил политики «Срернарадение вторжений > Наборы сигнатур»         90           c35. Слой правил политики «Секрытие НТТРС»         97           c36. Слой правил политики «Правила расшифровки	6.14.	Формирование правила и/или исключения	62
6.10. Включение слоключение правила или исключения         6.3           6.17. Кнопки для экспорта и импорта политики         67           6.18. Экспорт отдельного инструмента политики         68           6.19. Экспорт отдельного инструмента политики         68           6.20. Импорт инструментов политики         67           6.21. Оклоог инструментов политики         67           6.21. Оклоог инструментов политики         71           6.22. Слой правил политики «фильтр транзитного трафика»         71           6.23. Слой правил политики «фильтр еходящего трафика»         77           6.24. Слой правил политики «Трансляция адресов»         84           6.25. Слой правил политики «Тредотвращение вторжений»         87           6.26. Слой политики «Тредотвращение вторжений > Наборы сигнатур»         90           6.26. Слой политики «Тредотвращение вторжений > Наборы сигнатур»         90           6.29. Статистика по работе Системы предотвращения вторжений         93           6.30. Слой правил политики «Доступ без аутентификации»         94           6.31. Слой правил политики «Сперенаправление по ICAP»         97           6.32. Слой правил политики «Превила расшифровки»         115           6.34. Слой правил политики «Правила расшифровки»         115           6.35. Слой правил политики «Системы предотвращения вторжений         199	6.15.	Копирование значении	62
6.17. Кнопки для экспорта и импорта политики         6/           6.18. Экспорт группы инструментов политики         68           6.19. Экспорт отдельного инструмента политики         68           6.20. Импорт инструментов политики         71           6.21. Окно «Загрузить данные из файла»         71           6.22. Слой правил политики «Фильтр транзитного трафика»         74           6.23. Слой правил политики «Фильтр иходящего трафика»         74           6.24. Слой правил политики «Фильтр иходящего правила»         81           6.25. Слой правил политики «Трансляция адресов»         84           6.26. Слой политики «Предотвращение вторжений»         87           6.27. Создание исключений «Системы предотвращения вторжений»         88           6.28. Слой политики «Предотвращение вторжений > Наборы сигнатур»         90           6.29. Статистика по работе Системы предотвращения вторжений»         88           6.30. Слой правил политики «Скрытие НТТРS»         97           6.31. Слой правил политики «Скрытие прация ответов»         102           6.33. Слой правил политики «Предонарадиние поцключения > ICAP-серверы»         117           6.34. Слой правил политики «Предина расшифровки»         126           6.35. Слой правил политики «Предина расшифровки»         126           6.34. Слой правил политики «Предина одисмечения > ICAP-серверы»         117	6.16.	Включение/отключение правила или исключения	63
6.18. Экспорт гориль инструментов политики       68         6.19. Экспорт горального инструмента политики       69         6.20. Импорт инструментов политики       71         6.21. Окно «Загрузить данные из файла»       71         6.22. Слой правил политики «Фильтр транзитного трафика»       74         6.23. Слой правил политики «Фильтр реходящего трафика»       77         6.24. Слой правил политики «Фильтр исходящего трафика»       77         6.25. Слой правил политики «Трансляция адресов»       84         6.26. Слой политики «Тредотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой правил политики «Предотвращение вторжений > Наборы сигнатур»       90         6.30. Слой правил политики «Доступ без аутентификации»       93         6.30. Слой правил политики «Вскрытие НТТРS»       97         6.31. Слой правил политики «Вскрытие НТТРS»       97         6.33. Слой правил политики «Фильтрация ответов»       102         6.34. Слой правил политики «Фильтрация ответов»       102         6.35. Слой правил политики «Фильтрация ответов»       115         6.36. Слой правил политики «Фильтрация ответов»       112         6.37. Добавление ПСАР-сервера       118         6.38. Раздеп «Политика > Внешние подключения > Прокси-серверы»       117	6.17.	Кнопки для экспорта и импорта политики	67
6.19. Экспорт от дельного инструмента политики       69         6.20. Импорт инструмента политики «Фильтр транзитного трафика»       71         6.21. Окно «Загрузить данные из файла»       71         6.22. Слой правил политики «Фильтр транзитного трафика»       74         6.23. Слой правил политики «Фильтр исходящего трафика»       77         6.24. Слой правил политики «Фильтр исходящего трафика»       77         6.24. Слой правил политики «Трансляция адресов»       84         6.26. Слой политики «Предотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой политики «Предотвращение вторжений > Наборы сигнатур»       90         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Слой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Исренаправление по ICAP»       98         6.32. Слой правил политики «Ильтрация запросов»       102         6.34. Слой правил политики «Фильтрация ответов»       102         6.35. Слой правил политики «Иравила расшифровки»       115         6.36. Раздеп «Политика > Внешние подключения > ICAP-серверы»       117         6.35. Слой правил политики «Фильтрация ответов»       102         6.36. Раздеп «Политика > Внешние подключения > ICAP-серверы»       117         6	6.18.	Экспорт группы инструментов политики	68
6.20. Импорт инструментов политики       71         6.21. Окно «Загрузить данные из файла»       71         6.22. Слой правил политики «Фильтр транзитного трафика»       74         6.23. Слой правил политики «Фильтр входящего трафика»       74         6.24. Слой правил политики «Фильтр исходящего трафика»       74         6.25. Слой правил политики «Трансляция адресов»       84         6.26. Слой политики «Предотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой политики «Предотвращение вторжений»       88         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Слой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Вскрытие НТРS»       97         6.32. Слой правил политики «Истравила расшификации»       94         6.33. Слой правил политики «Истравила расшифровки»       115         6.34. Слой правил политики «Истравила расшифровки»       115         6.35. Слой правил политики «Предотвращение подключения > ІСАР-серверы»       117         74. Слой правил политики «Вскрытие Птрез»       109         6.35. Слой правил политики «Истравила расшифровки»       115         6.36. Слой правил политики «Фильтрация запросов»       109         6.37. Слой правил политики «Предотвращение подключени	6.19.	Экспорт отдельного инструмента политики	69
6.21. Окно «Загрузить данные из файла»       71         6.22. Слой правил политики «Фильтр транзитного трафика»       74         6.23. Слой правил политики «Фильтр еходящего трафика»       77         6.24. Слой правил политики «Фильтр исходящего правила»       81         6.25. Слой правил политики «Трансляция адресов»       84         6.26. Слой политики «Предотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой политики «Предотвращение вторжений»       86         6.29. Статистика о Воботе Системы предотвращения вторжений       93         6.30. Слой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Исрераправление по ICAP»       98         6.32. Слой правил политики «Ильтрация запросов»       102         6.33. Слой правил политики «Ильтрация ответов»       102         6.34. Слой правил политики «Ильтрация ответов»       102         6.35. Слой правил политики «Иравила расшифровки»       117         6.36. Раздеп «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление прокси-сервера       120         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздеп «Политика > Объекты политики > Списки IP-адресов»	6.20.	Импорт инструментов политики	71
6.22. Слой правил политики «Фильтр транзитного трафика»       74         6.23. Слой правил политики «Фильтр иходящего трафика»       77         6.24. Слой правил политики «Фильтр иходящего прафика»       81         6.25. Слой правил политики «Трансляция адресов»       84         6.26. Слой политики «Предотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой политики «Предотвращение вторжений > Наборы сигнатур»       90         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Слой правил политики «Системы предотвращения вторжений       94         6.31. Слой правил политики «Перенаправление по ICAP»       97         6.32. Слой правил политики «Прератвращения вторжений»       102         6.34. Слой правил политики «Ипьтрация запросов»       102         6.35. Слой правил политики «Иравила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление (CAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.34. Слой правил политики «Оравилочения > Прокси-серверы»       117         6.36. Раздел «Политика > Объекты политики > Списки IP-адресов»       120         6.40. Настройка параметров при работе с FTP-протоколами       121	6.21.	Окно «Загрузить данные из файла»	71
6.23. Слой правил политики «Фильтр входящего трафика»       77         6.24. Слой правил политики «Фильтр исходящего правила»       81         6.25. Слой правил политики «Трансляция адресов»       84         6.26. Слой политики «Предотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой политики «Предотвращение вторжений Наборы сигнатур»       90         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Слой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Церенаправление по ICAP»       97         6.32. Слой правил политики «Серенаправление по ICAP»       98         6.33. Слой правил политики «Перенаправление по ICAP»       98         6.34. Слой правил политики «Правила расшифровки»       115         6.35. Слой правил политики «Фильтрация запросов»       102         6.34. Слой правил политики «Правила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       120         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Лимиты трафика»       122         6.42. Поик пка > Объекты полит	6.22.	Слой правил политики «Фильтр транзитного трафика»	74
6.24. Слой правил политики «Фильтр исходящего правила»       81         6.25. Слой правил политики «Тредотвращение вторжений»       84         6.26. Слой политики «Предотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой политики «Предотвращение вторжений»       88         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Слой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Доступ без аутентификации»       94         6.32. Слой правил политики «Истренаправление по ICAP»       98         6.33. Слой правил политики «Истренаправление по ICAP»       98         6.34. Слой правил политики «Истрация этветов»       109         6.35. Слой правил политики «Иправила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       222         6.42. Поиск по параметрам       222         6.43. Саздание пруппы IP-адресов/диапазонов       124         6.44. Форматы спискокы IP-адресов/диапазонов       124	6.23.	Слой правил политики «Фильтр входящего трафика»	77
6.25. Слой правил политики «Транспяция адресов»       84         6.26. Слой политики «Предотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой политики «Предотвращение вторжений > Наборы сигнатур»       90         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Слой правил политики «Вскрытие НТТРS»       97         6.31. Слой правил политики «Вскрытие НТТРS»       97         6.32. Слой правил политики «Вскрытие НТТРS»       98         6.33. Слой правил политики «Вскрытие НТТРS»       98         6.34. Слой правил политики «Исренаправление по ICAP»       98         6.35. Слой правил политики «Иправила расшифровки»       102         6.34. Слой правил политики «Иправила расшифровки»       115         6.35. Слой правил политики «Правила расшифровки»       115         6.36. Раздеп «Политика > Внешние подключения > ПсАР-серверы»       119         6.39. Добавление ICAP-сервера       120         6.40. Настройка параметров при работе С FTP-протоколами       121         6.41. Раздеп «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.44. Форматы списков IP-адресов/диапазонов       124         6.44. Форматы списка IP-адресов       124	6.24.	Слой правил политики «Фильтр исходящего правила»	81
6.26. Спой политики «Предотвращение вторжений»       87         6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Спой политики «Предотвращение вторжений > Наборы сигнатур»       90         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Спой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Доступ без аутентификации»       94         6.32. Слой правил политики «Прераправление по ICAP»       98         6.33. Слой правил политики «Фильтрация запросов»       102         6.34. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Фильтрация ответов»       109         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление покси-сервера       120         6.40. Настройка параметров при работе с ГТР-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.47. Раздел «Политика > Объекты	6.25.	Слой правил политики «Трансляция адресов»	84
6.27. Создание исключений «Системы предотвращения вторжений»       88         6.28. Слой политики «Предотвращение вторжений > Наборы сигнатур»       90         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Слой правил политики «Доступ без аугентификации»       94         6.31. Слой правил политики «Вскрытие HTTPS»       97         6.32. Слой правил политики «Системы предотвращение по ICAP»       98         6.33. Слой правил политики «Инъграция запросов»       102         6.34. Слой правил политики «Фильтрация запросов»       109         6.35. Слой правил политики «Фильтрация запросов»       109         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поикс по параметра       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.44. Форматы списков IP-адресов       124         6.44. Форматы списка у Сбъекты политики > Расписания»       125	6.26.	Слой политики «Предотвращение вторжений»	87
6.28. Спой политики «Предотвращение вторжений > Наборы сигнатур»       90         6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Спой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Вскрытие HTTPS»       97         6.32. Спой правил политики «Сперенаправление по ICAP»       98         6.33. Слой правил политики «Фильтрация запросов»       102         6.34. Спой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Фильтрация запросов»       109         6.36. Слой правил политики «Фильтрация запросов»       109         6.35. Слой правил политики «Фильтрация запросов»       109         6.36. Слой правил политики «Правила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметра       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов/диапазонов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125	6.27.	Создание исключений «Системы предотвращения вторжений»	88
6.29. Статистика по работе Системы предотвращения вторжений       93         6.30. Слой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Вскрытие HTTPS»       97         6.32. Слой правил политики «Фильтрация запросов»       102         6.33. Слой правил политики «Фильтрация запросов»       102         6.34. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Фильтрация ответов»       102         6.36. Раздеп «Политика > Bнешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздеп «Политика > Bнешние подключения > Прокси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздеп «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы спискам IP-адресов/диапазонов       124         6.45. Раздеп «Политика > Объекты политики > Лимиты трафика»       125         6.47. Раздеп «Политика > Объекты политики > Ключевые словяи на заголовки       129         6.50. Добавление списка условий на заголовки	6.28.	Слой политики «Предотвращение вторжений > Наборы сигнатур»	90
6.30. Спой правил политики «Доступ без аутентификации»       94         6.31. Слой правил политики «Вскрытие НТТРЅ»       97         6.32. Слой правил политики «Сиренаправление по ICAP»       98         6.33. Слой правил политики «Фильтрация запросов»       102         6.34. Слой правил политики «Фильтрация запросов»       109         6.35. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Фильтрация ответов»       117         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметров       124         6.44. Форматы списков IP-адресов/диапазонов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.47. Раздеп «Политика > Объекты политики > Расписания»       126         6.49. Раздеп «Политика > Объекты политики > Условия на заголовки       129         6.50. Добавление списка условий на заголовки       129         6.50. Добавление списка условий на заголовки       130	6.29.	Статистика по работе Системы предотвращения вторжений	93
6.31. Слой правил политики «Вскрытие НТТРЅ»       97         6.32. Слой правил политики «Перенаправление по ICAP»       98         6.33. Слой правил политики «Фильтрация запросов»       102         6.34. Слой правил политики «Фильтрация запросов»       109         6.35. Слой правил политики «Фильтрация запросов»       109         6.36. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Правила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздеп «Политика > Объекты политики > Расписания»       127         6.48. Добавление списка условий на заголовки       129         6.50. Добавление списка условий на заголовки       130	6.30.	Слой правил политики «Доступ без аутентификации»	94
6.32. Слой правил политики «Перенаправление по ICAP»       98         6.33. Слой правил политики «Фильтрация запросов»       102         6.34. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Правила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление ICAP-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Римиты трафика»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Справочники > Ключевые слова»       133         6.53. Добавление	6.31.	Слой правил политики «Вскрытие HTTPS»	97
6.33. Слой правил политики «Фильтрация запросов»       102         6.34. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Правила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Справочники > Условия на заголовки»       129         6.52. Добавление списка условий на заголовки       133         6.54. Добавление списка адресов электронной почты       133         6.55. Раздел «Политика > Справочники > Ключевые слова»       133	6.32.	Слой правил политики «Перенаправление по ICAP»	98
6.34. Слой правил политики «Фильтрация ответов»       109         6.35. Слой правил политики «Правила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > IDoкси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов Диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.52. Добавление сипска адресов электронной почты       133         6.54. Добавление списка адресов электронной почты       134 <t< td=""><td>6.33.</td><td>Слой правил политики «Фильтрация запросов»</td><td>102</td></t<>	6.33.	Слой правил политики «Фильтрация запросов»	102
6.35. Слой правил политики «Правила расшифровки»       115         6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление ICAP-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.52. Добавление списка запоси пользователя       133         6.54. Добавление списка ключевых слов       137         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.55. Раздел «Политика > Справочники > Ключевые слова»       137	6.34.	Слой правил политики «Фильтрация ответов»	109
6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»       117         6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов/диапазонов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       126         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление списка адресов электронной почты       133         6.54. Добавление списка адресов электронной почты       133         6.55. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.56. Добавление списка ключевых слов       137	6.35.	Слой правил политики «Правила расшифровки»	115
6.37. Добавление ICAP-сервера       118         6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Лимиты трафика»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Иользователи (Basic Auth)»       132         6.52. Добавление списка адресов электронной почты       133         6.54. Добавление учетной записи пользователя       133         6.55. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.56. Добавление списка адресов электронной почты       134         6.57. Раздел «Политика > Справочники > Ключевые слова»       136	6.36.	Раздел «Политика > Внешние подключения > ICAP-серверы»	117
6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»       119         6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Лимиты трафика»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Расписания»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Иользователя       133         6.52. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ключевые слова»       136	6.37.	Добавление ІСАР-сервера	118
6.39. Добавление прокси-сервера       120         6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.47. Раздел «Политика > Объекты политики > Расписания»       126         6.49. Раздел «Политика > Объекты политики > Расписания»       129         6.50. Добавление расписания       129         6.51. Раздел «Политика > Объекты политики > Условия на заголовки»       130         6.52. Добавление списка условий на заголовки       130         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.54. Добавление списка ключевых слов       137         6.55. Раздел «Политика > Справочники > Ресурсы»       138         <	6.38.	Раздел «Политика > Внешние подключения > Прокси-серверы»	119
6.40. Настройка параметров при работе с FTP-протоколами       121         6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.47. Раздел «Политика > Объекты политики > Расписания»       126         6.49. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.54. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»      <	6.39.	Добавление прокси-сервера	120
6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»       122         6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.49. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Иользователи (Basic Auth)»       132         6.52. Добавление списка условий на заголовки       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ключевых слов       139         6.59. Раздел «Политика > Справочники > Ресурсы»      140	6.40.	Настройка параметров при работе с FTP-протоколами	121
6.42. Поиск по параметрам       122         6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Расписания»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ключевых слов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60.	6.41.	Раздел «Политика > Объекты политики > Списки IP-адресов»	122
6.43. Создание группы IP-адресов/диапазонов       124         6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Расписания»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Условия на заголовки»       132         6.52. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       137         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ключевых слов       137         6.59. Раздел «Политика > Справочники > Ресурсы»       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140	6.42.	Поиск по параметрам	122
6.44. Форматы списков IP-адресов       124         6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Расписания»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Условия на заголовки»       132         6.52. Добавление списка условий на заголовки       130         6.55. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.55. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140	6.43.	Создание группы IP-адресов/диапазонов	124
6.45. Раздел «Политика > Объекты политики > Лимиты трафика»       125         6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Условия на заголовки»       130         6.52. Добавление списка условий на заголовки       130         6.53. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.44.	Форматы списков IP-адресов	124
6.46. Настройка лимита трафика       125         6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Условия на заголовки»       130         6.52. Добавление списка условий на заголовки       130         6.53. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.45.	Раздел «Политика > Объекты политики > Лимиты трафика»	125
6.47. Раздел «Политика > Объекты политики > Расписания»       127         6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Иользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       133         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ключевых слов       137         6.59. Раздел «Политика > Справочники > Ресурсы»       138         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.46.	Настройка лимита трафика	125
6.48. Добавление расписания       128         6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.47.	Раздел «Политика > Объекты политики > Расписания»	127
6.49. Раздел «Политика > Объекты политики > Условия на заголовки»       129         6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ключевые слова»       138         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.48.	Добавление расписания	128
6.50. Добавление списка условий на заголовки       130         6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ключевые слова»       138         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.49.	Раздел «Политика > Объекты политики > Условия на заголовки»	129
6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»       132         6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ключевые слова»       138         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.50.	Добавление списка условий на заголовки	130
6.52. Добавление учетной записи пользователя       133         6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ключевые слова»       138         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.51.	Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»	132
6.53. Раздел «Политика > Справочники > Адреса электронной почты»       133         6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ключевых слов       137         6.59. Раздел «Политика > Справочники > Ресурсы»       138         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.52.	Добавление учетной записи пользователя	133
6.54. Добавление списка адресов электронной почты       134         6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.53.	Раздел «Политика > Справочники > Адреса электронной почты»	133
6.55. Раздел «Политика > Справочники > Ключевые слова»       136         6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.54.	Добавление списка адресов электронной почты	134
6.56. Добавление списка ключевых слов       137         6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141	6.55.	Раздел «Политика > Справочники > Ключевые слова»	136
6.57. Раздел «Политика > Справочники > Ресурсы»       138         6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141         6.62. Фильтрация по маркерам       142	6.56	Добавление списка ключевых слов	137
6.58. Добавление списка ресурсов       139         6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141         6.62. Фильтрация по маркерам       142	6.57	Раздел «Политика > Справочники > Ресурсы»	138
6.59. Раздел «Политика > Справочники > Ресурсы»       140         6.60. Правило для блокировки WhatsApp       140         6.61. Справочник «Маркеры правил КФ»       141         6.62. Фильтрация по маркерам       142	6.58	Добавление списка ресурсов	139
6.60. Правило для блокировки WhatsApp	6.59	Раздел «Политика > Справочники > Ресурсы»	140
6.61. Справочник «Маркеры правил КФ»	6.60	Правило для блокировки WhatsApp	140
6.62 Фильтрация по маркерам 142	6.61	Справочник «Маркеры правил КФ»	141
ייייייין איז ווי אמאגבאמא ייייייייייייייייייייייייייייייייייי	6.62.	Фильтрация по маркерам	143

6.63. Раздел «Политика > Справочники > Файлы»	14	44
6.64. Добавление списка фаилов	14	45
6.65. Раздел «Политика > Справочники > GeoIP»	14	46
6.66. Формирование шаблона для добавления заголовка	14	47
6.67. Формирование шаблона для изменения заголовка	14	48
6.68. Формирование шаблона для удаления заголовка	14	49
6.69. Формирование шаблона страницы	1	50
6.70. Формирование правила	1	51
6.71. Формирование правила	1	52
6.72. Формирование правила	1	53
6.73. Формирование правила	1	54
6.74. Формирование правила	1	55
6.75. Формирование правила	1	56
6.76. Формирование правила	1	57
6.77. Формирование правила	1	58
6.78. Формирование исключения по ID-сигнатуры	1	59
6.79. Формирование исключения по набору параметров: Источник, Назначение, Порт		
назначений	1	59
6.80. Формирование правила	10	60
6.81. Формирование правила	10	61
6.82. Формирование исключения	10	61
6.83. Добавление списка ресурсов	1	62
6.84. Создание исключения	1	63
6.85. Формирование правила	1	64
6.86. Формирование правила	1	64
6.87. Формирование правила	1	65
6.88. Добавление ІСАР-сервера	1	66
6.89. Формирование правила	1	67
6.90. Создание нового слоя	1	67
6.91. Формирование правила	1	68
6.92. Создание нового слоя	1	68
6.93. Формирование правила	1	69
6.94. Формирование правила	1	70
6.95. Формирование правила	1	71
6.96. Формирование правила	1	72
6.97. Формирование правила	1	73
6.98. Формирование правила	1	73
6.99. Формирование правила	1	74
6.100. Статус загрузки	1	75
6.101. Шаблон блокировки	1	75
6.102. Сохранение загруженного файла	1	76
6.103. Вкладка Политика > База категоризации	1	77
6.104. Проверка категории	1	78
7.1. Раздел «Статистика»	1	79
7.2. Меню действий с отчетом	18	80
7.3. Секция «Типы отчетов»	18	81
7.4. Копирование значения фильтра отчета	18	82
7.5. Копирование значения фильтра отчета	18	83
7.6. Отчет «По персонам/ТОП:25, Персоны: Валентина Иванова»	18	83
7.7. Календарь	18	84
7.8. Окно «Редактировать отчет» вкладка «Настройки отправки»	18	86
7.9. Сужение временного диапазона	1	88

7.10. Расширение временного диапазона	. 188
7.11. Формирование отчета «ТОП по объекту или группе объектов»	. 189
7.12. Фильтры Журнала запросов	. 190
7.13. Окно «Редактировать отчет» вкладка «Основное»	. 190
7.14. Окно «Поделиться отчетом»	. 191
7.15. Пример выгруженного отчета по персоне (в файле формата PDF)	. 193
7.16. Удаление отчета	. 194
7.17. Меню действий с папкой	. 195
7.18. Отправка копии папки с отчетами	. 196
7.19. Сбор статистики по сотрудникам, которые посещали социальные сети	. 197
7.20. Детализация запросов отдела «Управление информатизацией»	. 198
7.21. Детализация запросов конкретного сотрудника	. 199
7.22. ТОП 25 ресурсов, которые посетил конкретный сотрудник	. 200
7.23. Сбор статистики по приложению Skype	. 201
8.1. Раздел «Пользователи»: управление правами доступа пользователей	. 202
8.2. Раздел «Пользователи > Роли»	. 203
8.3. Раздел «Пользователи»: создание роли	. 205
8.4. Раздел «Пользователи > Роли»: редактирование роли, карточка роли	. 206
8.5. Раздел «Пользователи > Роли»: меню действий с ролью	. 207
8.6. Раздел «Пользователи > Роли»: удаление роли	. 207
8.7. Блок «Доступ к данным» карточки роли	. 208
8.8. Пример отображения раздела Досье с учетом прав доступа к данным	. 209
8.9. Блок «Доступ к записям журналов» карточки роли	. 209
8.10. Блок «Доступ к разделам интерфейса» карточки роли	. 210
8.11. Раздел «Пользователи > Пользователи»	. 212
8.12. Раздел «Пользователи»: создание локальной УЗ пользователя	. 214
8.13. Раздел «Пользователи»: создание доменной УЗ пользователя	. 215
8.14. Раздел «Пользователи > Пользователи»: редактирование локальной УЗ	
пользователя, карточка пользователя	. 216
8.15. Раздел «Пользователи > Пользователи»: смена пароля локальной УЗ	
пользователя	. 216
8.16. Раздел «Пользователи > Пользователи»: блокировка/разблокировка УЗ	
пользователя	. 217
8.17. Раздел «Пользователи > Пользователи»: удаление УЗ пользователя	. 218
8.18. Создание группы LDAP	. 219
8.19. Раздел «Пользователи > Пользователи»: выдача/отзыв нескольких наборов	
прав доступа пользователю	. 220
8.20. Раздел «Пользователи > Роли»: выдача/отзыв прав доступа нескольким	-
пользователям	221

# Список таблиц

6.1. Основные элементы политики ИБ	47
6.2. Значки для обозначения основных действий при формировании правил	
фильтрации запросов и ответов	48
6.3. Краткий обзор инструментов политики ИБ	48
6.4. Обзор действий, выполняемых со слоями	55
6.5. Примеры названий скопированных слоев	57
6.6. Обзор действий, выполняемых с правилами и исключениями	60
6.7. Примеры образования названий скопированных правил	62
6.8. Перечень инструментов политики	63
6.9. Обзор кнопок и действий, выполняемых с инструментами политики ИБ	64
6.10. Примеры образования названий скопированных инструментов политики	65
6.11. Обзор действий со слоями правил политики	71
6.12. Описание атрибутов слоя «Фильтр транзитного трафика»	74
6.13. Описание атрибутов слоя «Фильтр входящего трафика»	78
6.14. Описание атрибутов слоя «Фильтр исходящего трафика»	81
6.15. Описание атрибутов слоя «Трансляция адресов»	84
6.16. Описание столбцов слоя «Предотвращение вторжений > Правила и	
исключения»	87
6.17. Описание атрибутов слоя «Предотврашение вторжений»	88
6.18. Описание категорий сигнатур IPS	90
6.19. Описание атрибутов слоя «Доступ без аутентификации»	
6.20. Описание атрибутов правил и исключений слоя «Вскрытие HTTPS»	
6.21. Описание атрибутов правил и исключений слоя «Перенаправление по	
ICAP»	. 99
6.22. Описание атрибутов правил и исключений слоя «Фильтрация запросов»	102
6.23. Описание действий	106
6.24. Описание атрибутов правил и исключений слоя «Фильтрация ответов»	109
6.25. Описание действий	113
6.26. Описание атрибутов правил и исключений слоя «Правила расшифровки»	115
6.27. Перечень атрибутов для добавления ICAP-сервера	117
6.28. Перечень атрибутов для добавления прокси-сервера	119
6 29 Перечень атрибутов для добавления IP-адреса/диадазона IP-адресов	123
6.30. Перечень временных интервалов	126
6 31 Режимы проверки веб-ресурсов	139
6 32 Перечень атрибутов для проверки файлов	145
6.33. Перечень атрибутов для формирования шаблона	147
81 Права доступа к разделам интерфейса	210
В 1 Описание метасимвопов	224
С 1 Описание полстановочных симвопов	225
С 2 Перечень подстановочных символов для показа текущих значений расхода	220
трафика пользователя	225
D 1. Описание поллерживаемых методов HTTP-протокопа	227
Е 1. Перечень сетей	229
Е 2 Общая матрица доступов для explicit-прокси	229
Е. Сощал матрица доогулов для скрист прокой спорто статистики в Журнале	220
соелинений	232
F2 Описание параметров фильтрации запросов для сбора статистики в Журнале	202
запросов	233
	200

# Перечень терминов и сокращений

APM	Автоматизированное рабочее место
БД	База данных
OC	Операционная система
ПО	Программное обеспечение
ПК	Программный комплекс
ИБ	Информационная безопасность
КА	Контентный анализ
МЭ	Межсетевой экран
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЭЦП	Электронная цифровая подпись
CLI	Command Line Interface — интерфейс командной строки
CPS	Connection per Second — мера измерения, насколько быстро брандмауэр может создать и сохранить новый сеанс, принятый его политикой.
CSR	Certificate Signing Request — запрос на подпись сертификата
CRL	Certificate Revocation List — список отозванных сертификатов
DC	Domain controller — контроллер домена
DNAT	Destination Network Address Translation — скрытие IP-адреса назначения запроса пользователя путем перенаправления запроса пользователя преобразованием адреса назначения в IP-заголовке пакета
FAQ	Frequently asked questions — «часто задаваемые вопросы», справка с полезной информацией
GUI	Graphical User Interface — графический интерфейс пользователя
FQDN	Fully Qualified Domain Name — полное имя домена (имя домена, не имеющее неоднозначностей в определении)
IPS	Intrusion Prevention System — система предотвращения вторжений
MIME	Multipurpose Internet Mail Extension — спецификация для передачи по сети файлов различного типа: изображений, музыки, текстов, видео, архивов и др.
MITM	Man-In-The-Middle — атака «человек посередине», при которой злоумышленник тайно ретранслирует и при необходимости моди- фицирует данные между двумя сторонами
NAT	Network Address Translation — преобразование сетевых адресов
OWA	Outlook Web Access — веб-интерфейс почтового сервиса Microsoft Exchange
RFC	Request for Comments — спецификации и стандарты, применяемые в интернете
SMTP	Simple Mail Transfer Protocol — простой протокол передачи почты

SNAT	Source Network Address Translation — технология, позволяющая заменить исходный IP-адрес источника сетевого пакета на другой указанный IP-адрес
VLAN	Virtual Local Area Network — технология обмена данными, которая логически делит устройства локальной сети на сегменты для реализации виртуальных рабочих групп
VRRP	Virtual Router Redundancy Protocol — сетевой протокол, предназна- ченный для увеличения доступности маршрутизаторов, выполняю- щих роль шлюза по умолчанию
ZIP	Формат архивации файлов и сжатия данных без потерь

## 1. Введение

## 1.1. Область применения

В документе содержится подробная информация по использованию программного комплекса Solar NGFW.

Программный комплекс Solar NGFW – это платформа сетевой безопасности для защиты периметра сети организации от вредоносного трафика и вторжений. Для полноценного функционирования весь трафик должен проходить через Solar NGFW.

Документ предназначен для сотрудников служб безопасности и других IT-специалистов, которые заинтересованы в обеспечении безопасности корпоративных данных.

## 2. Назначение и условия применения

## 2.1. Назначение Solar NGFW

Программный комплекс Solar NGFW предназначен для комплексной защиты организации от сетевых и веб-угроз на сетевом периметре. Защита обеспечивается использованием различных модулей безопасности, инспектирующих трафик для выявления нарушений политики сетевой безопасности и вредоносной активности.

#### 2.2. Краткое описание возможностей

Solar NGFW представляет собой комплексную систему функциональных модулей информационной безопасности, таких как:

- фильтрация трафика (по IP-адресам, портам/протоколам),
- контроль приложений, поддерживаемых библиотекой nDPI,
- трансляция адресов (NAT),
- система предотвращения вторжений,
- анализ и фильтрация веб-трафика, передаваемого по протоколам HTTP, HTTPS и FTP over HTTP,
- категоризатор веб-ресурсов (на базе решения WebCat),
- потоковый антивирус (на базе решения Dr.Web),
- интеграция со смежными системами по ICAP,
- мониторинг состояния системы и действий пользователей,
- SSL-инспекция,
- кластеризация Solar NGFW с отказоустойчивостью.

#### 2.3. Условия применения

# 2.3.1. Требования к аппаратному обеспечению АРМ администратора безопасности

Для функционирования Solar NGFW APM пользователя должно быть оборудовано персональным компьютером с подключением к сети Интернет. К аппаратному обеспечению предъявляются следующие минимальные требования:

- процессор от Intel Pentium 4 с тактовой частотой 2 ГГц и выше;
- оперативная память не менее 4 ГБ после загрузки браузера;
- место на жестком диске 20 ГБ;
- сетевой интерфейс со скоростью передачи данных 1 Гбит/с и выше;
- разрешение экрана при работе с GUI от 1600 x 900.

# 2.3.2. Требования к программному обеспечению АРМ администратора безопасности

Данная версия Solar NGFW функционирует под управлением OC Astra Linux Special Edition версии 1.8.0 (версия ядра 6.1.50-1-generic) с максимальным уровнем защиты «Смоленск».

#### Примечание

Настоятельно не рекомендуется ставить пакет обновлений безопасности под управлением OC Astra Linux более новых версий (например, 1.8.1), т.к. это может нарушить штатную работу служб Solar NGFW и привести к нарушению работоспособности.

В состав программного обеспечения для APM администратора Solar NGFW должна входить программа-клиент, предоставляющая пользователю возможность навигации и просмотра веб-ресурсов (веб-браузер). Для корректной работы графического интерфейса (GUI):

- используйте браузеры Google Chrome или Mozilla Firefox актуальной версии (если версия браузера устарела или он не поддерживается, на экран будет выведено соответствующее сообщение);
- в настройках браузера разрешите выполнение JavaScript и сохранение файлов cookies;
- отключите сторонние расширения браузера;
- разрешите всплывающие окна.

Работа с управляющим интерфейсом Solar NGFW возможна в других браузерах, но в таком случае полноценная работоспособность Solar NGFW не гарантируется.

Для корректной работы Solar NGFW настройте браузер следующим образом:

- разрешите выполнение JavaScript и сохранение cookies (настройка по умолчанию);
- установите кодировку браузера UTF-8 (Юникод) для корректного отображения символов той или иной кодировки (если не настроена автоматически).

Оборудование с установленным Solar NGFW должно располагаться в охраняемом помещении с ограниченным доступом посторонних лиц.

#### 2.3.3. Уровень подготовки администратора безопасности

Квалификация администраторов безопасности Solar NGFW должна быть достаточной для формирования политики безопасности, на основании которой будет осуществляться управление доступом пользователей к внешним веб-ресурсам.

Задачей администратора безопасности Solar NGFW является создание и актуализация политик безопасности, а также анализ действий пользователей сети Интернет.

В своей работе администратор безопасности Solar NGFW должен опираться на поставляемую с продуктом эксплуатационную документацию (см. раздел <u>2.3.4</u>), обладать зна-

ниями по протоколам TCP/IP и понимать основы обеспечения безопасности операционной системы Linux.

#### 2.3.4. Перечень эксплуатационной документации для ознакомления

Пользователю Solar NGFW рекомендуется ознакомиться со следующими эксплуатационными документами:

- Руководство администратора безопасности (настоящий документ);
- Руководство по установке и настройке.

## 3. Общие сведения о Solar NGFW

## 3.1. Принцип работы Solar NGFW

Solar NGFW обеспечивает защиту периметра сети путем глубокого контроля информационных потоков, выявления и предотвращения сетевых атак, противодействия вебугрозам (зараженным, запрещенным, фишинговым сайтам) и вредоносному ПО, антивирусной защиты, интеграции с другими средствами защиты и т.д.

В связи с назначением и спецификой работы Solar NGFW программный комплекс устанавливается в разрыв сети в точках выхода в интернет. Ниже представлена концептуальная схема размещения Solar NGFW в сетевой инфраструктуре.



Рис. 3.1. Solar NGFW в архитектуре защиты сети

#### 3.1.1. Принцип работы прокси-сервера в Solar NGFW

Схема работы в прямом режиме:

- 1. При выполнении запроса пользователь авторизуется в подсистеме фильтрации и аутентификации.
- 2. По имени пользователя подсистемы фильтрации и аутентификации определяют набор групп (может быть пустым), в которые входит пользователь, и применяемую политику безопасности.
- 3. В соответствии с политикой безопасности выполняется проверка запроса.
- 4. Если запрос не соответствует политике безопасности, вместо него пользователь получает подготовленную страницу с описанием запрета.
- 5. Запрос, выполнение которого разрешено, обращается к серверу в сети Интернет.
- 6. Ответ, полученный кэшем от сервера, обрабатывается в соответствии с принятой политикой безопасности.

 Если передача данных разрешена, пользователю поступает ответ на запрос. Если ответ не соответствует политике безопасности, вместо него пользователь получает подготовленную страницу с описанием запрета.

Работа в обратном режиме позволяет публиковать внутренние ресурсы организации на внешние источники. Например, с помощью обратного прокси организация может предоставить своим сотрудникам доступ к корпоративной почте за пределами организации. При этом Solar NGFW проверяет и блокирует файлы с конфиденциальной информацией при попытке их выгрузить.

Схема работы в обратном режиме:

- 1. При выполнении запроса пользователь авторизуется в подсистеме фильтрации и аутентификации.
- По имени пользователя подсистемы фильтрации и аутентификации определяют набор групп (может быть пустым), в которые входит пользователь, и применяемую политику безопасности.

#### Примечание

Режим обратного прокси поддерживает только Basic и NTLM аутентификацию.

- 3. В соответствии с политикой безопасности выполняется проверка запроса. Если запрос:
  - не соответствует политике безопасности, вместо него пользователь получает подготовленную страницу с описанием причины запрета;
  - соответствует политике безопасности, пользователь получает доступ к внутреннему ресурсу (например, корпоративной почте).

Все данные о запросах и ответах можно получить в разделе Статистика (см. раздел 7).

#### Примечание

Политика контентной фильтрации для прямого и обратного режимов является общей и не требует дополнительных настроек.

При фильтрации данных в Solar NGFW применяются методики, которые позволяют выполнять подробный анализ передаваемой информации, определять форматы передаваемых данных, кодировку и язык для текстовых данных, не основываясь только на служебной информации, переданной сервером в сети Интернет, так как в зависимости от его настроек она может быть некорректной.

Например, веб-сервер может передавать аудиофайлы с расширением **txt** как файлы с типом данных **text/plain**, однако в политике с определением типов данных Solar NGFW будет самостоятельно определять тип данных для этого файла.

## 3.2. Политика безопасности доступа к веб-ресурсам

Политика безопасности доступа к веб-ресурсам представляет собой свод правил фильтрации веб-трафика, которые регулируют управление, защиту и распределение информации, передаваемой по сети Интернет.

Политика безопасности направлена на достижение таких целей, как:

- обеспечение гибкого контроля использования интернет-ресурсов;
- предотвращение утечки конфиденциальной и коммерческой информации;
- уменьшение неделового веб-трафика;
- снижение загрузки интернет-каналов;
- увеличение скорости доступа к веб-ресурсам за счет отказа от неделового трафика.

К каждой группе пользователей, определенной в Solar NGFW, можно применить одну из существующих политик безопасности. Элементами политики являются наборы правил фильтрации (слои правил политики). Правило включает в себя условия и набор действий, которые будут осуществляться при выполнении условий. Условия формируются из наборов фильтров, позволяющих проводить отбор веб-ресурсов по различным критериям, например, по ключевым словам, типам данных и т.д. (см. раздел <u>6</u>).

На <u>Рис.3.2</u> приведен пример проверки Solar NGFW данных информационного обмена на соответствие установленной политике безопасности.



Рис. 3.2. Пример проверки данных информационного обмена с помощью Solar NGFW

#### Примечание

Источником может быть персона, группа персон, неаутентифицированный пользователь, а также IP-адрес.

## 3.3. Принципы работы в интерфейсе Solar NGFW

#### 3.3.1. Начало работы. Вход в систему

Управление Solar NGFW выполняется с помощью графического веб-интерфейса, который по умолчанию доступен на порту 8443, по протоколу HTTPS.

#### Примечание

Если при первой загрузке веб-интерфейса в браузере возникает **Ошибка в сертификате безопасности этого веб-узла**, для доступа к интерфейсу Solar NGFW перейдите по ссылке **Продолжить открытие этого веб-узла** (не рекомендуется).

Если при первой загрузке веб-интерфейса в браузере Mozilla Firefox возникла **Ошибка при** установлении защищенного соединения, для доступа к Solar NGFW:

- 1. Перейдите по ссылке Или же вы можете добавить исключение....
- 2. На появившейся панели нажмите кнопку Добавить исключение.
- 3. В открывшемся окне **Добавить исключение безопасности** нажмите **Получить серти**фикат.
- 4. Нажмите Подтвердить исключение безопасности.

Для доступа к системе:

- 1. В адресной строке веб-браузера введите адрес сервера: https://<IP-адрес сервера Solar NGFW>:8443.
- 2. На отобразившейся странице в соответствующих полях укажите имя пользователя (логин) и пароль для входа в систему и нажмите **Войти** (<u>Рис.3.3</u>).

Solar NGFW
admin
Войти

Рис. 3.3. Авторизация

При первом входе в систему установите новый пароль требуемого уровня надежности и авторизуйтесь с ним.

После первоначальной смены пароля в верхней части экрана появится уведомление об отсутствии лицензии (<u>Рис.3.4</u>). Для загрузки лицензии нажмите **Лицензия > Загрузить лицензию**.

ЛИЦӨНЗИЯ отсутствует файл лицензии Идентификатор инсталляции: MNgb6ipYqF92g9m9oloYQA==	
Загрузить лицензию	

Рис. 3.4. Уведомление об отсутствии лицензии

В открывшемся окне проводника укажите путь к файлу с лицензией и нажмите **Открыть** (**Open**). Дождитесь загрузки лицензии — она автоматически сохранится в файле с именем **license.xml**.

Для просмотра сведений о лицензии Solar NGFW в главном меню выберите пункт **Лицензия**. При лицензировании Solar NGFW как отдельного продукта окно лицензии содержит текущее количество пользователей, использующих сеть Интернет.

		, .
33309 02.05.2023 (n.zhukova@rt-solar	.ru)	
Идентифика	атор инсталляции: T3FDPRHZIHkynakE4ZgvQQ==	
Наименование компании	000 "Солар Секьюрити"	
Договор	Внутреннее тестирование NGFW	
Примечание к лицензии	Тестовая лицензия	
Наименование продукта	Solar NGFW 1	
Максимальное количество персон	100	
Текущее количество персон	0	
Период действия	с 29.01.2024 00:00 по 28.04.2024 00:00	
Модули	<ul> <li>Техническая поддержка и получение обновлений Период действия с 29.01.2024 по 28.04.2024</li> <li>Категоризатор веб-ресурсов webCat Период действия с 29.01.2024 по 28.04.2024</li> <li>Система предотвращения вторжений Период действия с 29.01.2024 по 28.04.2024</li> <li>Контроль приложений период действия с 29.01.2024 по 28.04.2024</li> <li>Обратный прокси Период действия с 29.01.2024 по 28.04.2024</li> <li>Антивирусная защита Период действия с 29.01.2024 по 28.04.2024</li> </ul>	



Для просмотра сведений о лицензионном договоре Solar NGFW в главном меню выберите пункт **Лицензионный договор**. Чтобы распечатать лицензионный договор, нажмите

После успешной идентификации в системе администратор безопасности получает доступ к интерфейсу. На экране отобразится **Рабочий стол** (<u>Рис.3.6</u>) — единая информационная панель, предназначенная для оценки сетевой активности пользователей (сотрудников компании) на узлах фильтрации в режиме реального времени (подробнее см. в разделе <u>4</u>).

<i>?</i>	Solar NGFW			Поиск персоны Q 🗦
ώ	Мониторинг Статистика Узлы main ×			С 1 мин. У
×.	<ul> <li>Наличие проблем на узлах (средние и выше)</li> </ul>			
\$		ma	ain	
Ŗ		0	К	
R.	🗸 Подробные данные по узлу - main			
L.	Время работы	Средняя загрузка (LA)	Количество ядер ЦПУ	Доступно памяти
۲	2.0 ч	1.7	4	7.00 GB
Œ		ЦПУ и Память	на узле main	
~		IV Среди. Текущее — Пользовательские операции 8.08% 77.71% — Системные операции 10.16% 9.94% — Операции явода-выяюда 0.34% 0.23%	Tax 14 68 12 68 10 68 8 68 6 68 10 20 10 20 10 10 20 10 20 10 20 10 20 10 20 10 20 10	япь - Средок. Телущее - Доступная 7:175 68 6 6995 68 - Общая 12:561 68 12:561 68

Рис. 3.6. Рабочий стол

При вводе неверных данных:

- вход в систему не будет выполнен;
- на экране отобразится сообщение Неверный пароль или имя пользователя. В зависимости от настроек браузера может отображаться дополнительное окно браузера с запросом логина и пароля, что также означает ошибку входа в систему.

#### Примечание

Чтобы получить данные для входа в систему, обратитесь к системному администратору Solar NGFW.

Вы можете поменять параметры входа в систему в разделе Система > Расширенные настройки > Интерфейс > Сервер веб-интерфейса > Параметры входа в систему:

- Макс. количество неудачных попыток входа в систему до задержки значение параметра может быть от 3 до 100. По умолчаню 5.
- Задержка между попытками ввода пароля (с) значение параметра может быть от 1 до 20 секунд. По умолчанию 3.
- Блокировка входа при превышении числа попыток ввода пароля (м) значение параметра может быть от 5 до 180 минут. По умолчанию 15.

#### 3.3.2. Описание основных элементов интерфейса

Каждая страница веб-интерфейса Solar NGFW содержит необходимый для выполнения конкретных задач набор стандартных элементов управления и отображения: меню, панель навигации, кнопка, опция, поле ввода данных, переключатель, виджет, список объектов, таблица, вкладка и т.д.

#### Примечание

Приведенные в Руководстве изображения элементов интерфейса носят исключительно ознакомительный характер и могут отличаться от реальных.

При наведении курсора мыши на область меню отображается главное меню, пункты которого обеспечивают доступ к основным разделам GUI (<u>Рис.3.7</u>):

- Рабочий стол позволяет выполнять мониторинг активности сотрудников компании (см. раздел <u>4</u>).
- Досье обеспечивает доступ ко всей имеющейся личной, контактной и сетевой информации о персонах (сотрудниках компании). Вы можете отслеживать деятельность персон и групп персон на предмет подозрительного поведения (см. раздел <u>5</u>).
- Политика обеспечивает доступ к средствам настройки функций безопасности, а также к редактированию наборов групп пользователей и ПК (см. раздел <u>6</u>).
- Статистика обеспечивает доступ к отчетам системы, предоставляющим информацию о запросах пользователей в сети Интернет (см. раздел <u>7</u>).
- **Предотвращение вторжений** обеспечивает доступ к просмотру статистики по работе сигнатур для детектирования сетевых атак. Описание раздела приведено в документе *Руководство по установке и настройке*.
- Пользователи предназначен для управления правами доступа пользователей к различным объектам системы (см. раздел <u>8</u>).
- Сеть предназначен для управления статической и динамической маршрутизацией. Описание раздела приведено в документе *Руководство по установке и настройке*.
- Система обеспечивает доступ к настройкам конфигурации системы и служит для настройки различных параметров работы, их просмотра и редактирования. Описание раздела приведено в документе *Руководство по установке и настройке*.

#### Внимание!

В Solar NGFW вы можете разграничивать доступы к разделам интерфейса и системным функциям. Пользователь может просматривать только те разделы и выполнять только те функции, к которым у него есть доступ.



Рис. 3.7. Главное меню Solar NGFW

Чтобы зафиксировать меню, открывающееся при наведении на него курсора мыши, в

левом нижнем углу меню нажмите значок 🖄.

В правом верхнем углу расположено поле Поиск персоны, предназначенное для оперативного получения информации о персонах из Досье (подробнее см. раздел 5.6). Поиск персон могут выполнять пользователи, которым назначены роли:

- суперадминистратор; •
- администратор безопасности;
- аудитор.

#### Примечание

Для пользователя с ролью системного администратора поле поиска отображаться не будет.

При нажатии кнопки , расположенной в правом верхнем углу, отображается меню пользователя <Имя пользователя> (Рис.3.8), которое позволяет:

- сменить пароль на вход в систему (Сменить пароль) (при этом нужно ввести текущий и новый пароли);
- просмотреть информацию о лицензии (Лицензия) (при необходимости вы можете загрузить новый файл лицензии);
- завершить сеанс работы с системой (Выход).



Рис. 3.8. Меню пользователя

Рабочее пространство интерфейса, как правило, делится на две части.

Например, в разделах **Досье** и **Политика** в левой части экрана отображается специальная панель навигации, которая содержит существующие объекты (или наборы объектов) системы для управления ими:

- раздел Досье список персон и групп персон (сотрудников компании, <u>5</u>);
- раздел Политика перечень существующих элементов политики (или наборы элементов, <u>6</u>).

Например, после выбора раздела **Политика > Справочники > Ключевые слова** отобразятся группы используемых в политике ключевых слов, объединенных по определенному критерию.

#### Примечание

Выбранный раздел панели навигации выделяется цветом.

8	Solar NGFW			Поиск персоны	<b>t</b> ≓
۵	Настройки Импорт Экспорт	Политика / Справочники / Ключевые слова 💿			рименить политику
	межсетевой экран >				٩
\$	2 <sup>®</sup> предотвращение вторжений >	Hasaanne > Example	Создан admin	Изменен	១០
~	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ >		15.07.2024 13		
چ ۲	😫 внешние подключения 🛛 >				
۲	объекты политики >				
Œ	💿 справочники 🗸 🗸				
	Адреса электронной почты				
	Ключевые слова				
	Ресурсы				
	Маркеры правил КФ				
Ŕ	Файлы				

Рис. 3.9. Выбор раздела «Политика > Справочники > Ключевые слова»

Разделы навигационной панели подразделяются на системные и пользовательские:

- Системные разделы создаются при установке Solar NGFW и недоступны для редактирования.
- Пользовательские разделы создаются пользователями вручную. Например, системным разделом панели навигации является раздел **Досье > На особом контроле**.

Структура разделов панели навигации многоуровневый, т.е. раздел содержит подразделы.

Чтобы раскрыть или скрыть содержимое раздела, справа от его названия нажмите или .

На панели навигации с разделами или объектами системы можно выполнять такие действия, как создание, копирование, удаление, изменение названия и т.д. В меню действий с разделом или объектом системы выберите нужное (<u>Рис.3.10</u>). Размер списка действий в меню зависит от конкретного раздела или объекта системы.

Для вызова меню действий:

1. На панели навигации наведите курсор мыши на раздел или объект системы.

Нажмите отобразившуюся кнопку вызова меню действий <sup>1</sup>.

Для выполнения конкретных действий нажмите кнопку вызова меню действий и в отобразившемся меню выберите пункт меню с действием.

В основном окне, в правой части вкладки, отображается информация о выбранном объекте. С ним можно выполнять различные действия. Например, при выборе группы ключевых слов (Политика > Справочники > Ключевые слова), вы можете добавить конкретные ключевые слова в группу или удалить их из нее.



Рис. 3.10. Примеры меню действий

#### Внимание!

При одновременной работе двух и более администраторов с одной и той же вкладкой изменения, вносимые одним администратором, недоступны остальным администраторам до тех пор, пока они не обновят эту вкладку.

## 4. Рабочий стол: мониторинг работы системы

Раздел **Рабочий стол** (<u>Рис.4.1</u>) представляет собой Центр мониторинга нагрузки на узлы фильтрации Solar NGFW, который позволяет оценить в режиме реального времени состояние системы и сетевую активность пользователей (сотрудников компании) на узлах фильтрации. *Узел фильтрации* представляет собой межсетевой экран с ролью анализатора трафика.

<b>*</b> *	Solar NGFW			Поиск персоны 🔍 🔙
ଜ	Мониторинг Статистика Узлы main x			С 1 мин. 🗡
	<ul> <li>Наличие проблем на узлах (средние и выше)</li> </ul>			
\$		m	ain	
Ŗ		0	K	
R	🗸 Подробные данные по узлу - main			
£	Время работы	Средняя загрузка (LA)	Количество ядер ЦПУ	Доступно памяти
۲	2.0 ч	1.7	4	7.00 GB
Æ		ЦПУ и Памят	ь на узле main	
	20%	IV Среди. Текущее — Попьзоватольские операции 8.08% 7.71% — Октемные операции 10.16% 9.94% — Операции вкода-вывода 0.34% 0.23%	Tax 14 GB 12 GB 10 GB 5 GB 5 GB	мять - Среди. Тенущее — Доступная 7.175 GB 4.995 GB — Общая 12561 GB 12561 GB
Ŕ	10:20 10:30 10:40 10:50 11:00 11:	10	10:20 10:30 10:40 10:50 11:	00 11:10

Рис. 4.1. Раздел «Рабочий стол»

Статистику по параметрам состояния системы и активности сотрудников компании в сети Интернет за последние 15 минут можно просмотреть в виджетах и таблице на **Рабочем столе**. Регулярность обновления данных можно настроить на **Рабочем столе** в правом верхнем углу в раскрывающемся меню.



Рис. 4.2. Выбор периода обновления данных на рабочем столе

На графиках виджетов **ЦПУ**, **Память**, **Сетевой трафик** представлена сводная информация по соответствующим системным параметрам и проходящему трафику через один или несколько сетевых интерфейсов на определенном узле фильтрации Solar NGFW (по умолчанию main) за определенный период времени.

Статистику о среднем и текущем значении можно увидеть справа от графиков.

По умолчанию на графике отображаются сведения об основном узле фильтрации (main). Чтобы просмотреть данные статистики за определенный период времени, наведите курсор мыши на график.



Рис. 4.3. Раздел «Рабочий стол»: просмотр статистики системы

Также вы можете сузить или расширить временной диапазон, за который собрана статистика. При расширении или сужении диапазона данные в таблицах динамически меняются.

Для сужения временного диапазона курсором мыши на графике выделите отрезок времени, который необходимо детализировать (<u>Рис.4.4</u>).

Например, администратору безопасности необходимо просмотреть сетевой трафик за определенный период времени. Для этого на графике виджета Сетевой трафик выделите интересующий период времени. График будет перестроен согласно выбранному временному диапазону.



Рис. 4.4. Раздел «Рабочий стол»: сужение временного диапазона

Для расширения временного диапазона два раза нажмите левой кнопкой мыши на график (<u>Рис.4.5</u>).

Например, администратору безопасности необходимо просмотреть общую картину загрузки интерфейса сетевым трафиком. Для этого два раза нажмите на график виджета **Сетевой трафик**. График будет перестроен согласно выбранному временному диапазону.



Рис. 4.5. Раздел «Рабочий стол»: расширение временного диапазона

## 5. Досье: получение информации о пользователях

## 5.1. Общие сведения

В разделе **Досье** (<u>Рис.5.1</u>) можно просмотреть всю имеющуюся личную и контактную информацию о персонах (сотрудниках компании). Информация о сотрудниках компании группируется в соответствии с организационно-штатной структурой этой компании. Также можно вручную добавлять сотрудников в группы, относящихся к определенной категории.

Сотрудников, требующих особого внимания администратора безопасности (уволенных, увольняющихся, на испытательном сроке и т.п.), можно добавить в определенные группы категории **На особом контроле**. Внешних сотрудников можно объединить в группы категории **Внешние персоны**. Персоны, относящиеся к категории **Организационная структура**, создаются средствами Solar NGFW. Данные о персонах поступают из Active Directory или других LDAP-систем.

#### Примечание

В описании используются следующие понятия:

- **Персона** лицо, субъект коммуникации (например, сотрудник компании), объект внимания и контроля службы безопасности.
- **Адрес** электронный адрес лица, которое не удалось идентифицировать, являющийся объектом внимания и контроля службы безопасности.
- **Группа особого контроля** группа персон, деятельность которых требует особого внимания со стороны сотрудников службы безопасности.



Рис. 5.1. Раздел «Досье»

### 5.2. Управление источниками данных и синхронизация Досье

Вы можете управлять настройками конфигурации системы, актуальными для Досье, не покидая раздел. Вы можете настроить:

- обновление и автоматическую синхронизацию Досье Solar NGFW с Досье Solar Dozor или Solar NGFW, установленных на других серверах;
- доступ к источникам данных и т.д.

Параметры настройки идентичны параметрам в разделе Система > Основные настройки > Досье.

Для внесения изменений в параметры настройки:

- 1. В разделе Досье нажмите Настройки.
- 2. В открывшейся вкладке укажите/измените параметры настройки и нажмите Сохранить.
- 3. Поочередно нажмите кнопки Сохранить и Применить.

Настройки				х	
Сохранить Применить					
Сервис обновления Досье					
Автоматическая синхронизация источников Досье	•				
Периодичность синхронизации	4	ч.	0	м.	
	Не рекомендует	ся задавать перис	од меньше 20 м	ин	
Доступ к источникам данных		С Синхрон	изировать	Добавить	
> AD example					
> File example					
> 389 Directory Server Example					

Рис. 5.2. Раздел «Досье»: Вкладка «Настройки»

Автоматическая синхронизация позволяет использовать единое Досье с сохранением всех имеющихся в Solar Dozor и Solar NGFW данных персон.

Настройка синхронизации Досье описана в Руководстве по установке и настройке в разделе Синхронизация со сторонним Досье.

После синхронизации Досье Solar Dozor и Solar NGFW (Рис.5.3):

- в Solar NGFW будут импортированы новые персоны;
- информация о существующих персонах будет дополнена или заменена.

<b>*</b>	Solar NGFW		Поиск персоны Q 🗦	
ଜ	+ Раздел + Группу + Персону	Досье / Операционный отдел		
	операционны Найдено 1 📀 Q	Персоны		
\$	На особом контроле	Добавить персону		
Ŗ				
R	Организационная структура 🛛 💛			
£	Employees 🗸	Вавилов игорь Левович Заместитель начальника служ	бы	
Œ	pilot-groups 🗸 🗸		Solar NGFW	
۲	Операционны о	Золин Евгений Артемиевич Казначей	-Pasgen + Tpynny + Repcowy	Досье / Операционный отдел
			🗈 операционный Найдено 1 🛞 🔾	Персоны
			На особом контроле	Добанить персону
			Организационная структура 🗸	ФИО Т
			요하 Employees ~	Вавилов Игорь Левович Заместитель начальника службы
			pilot-groups V	
			(Е Операционный о	Золин Евгений Артемиевич Казначей
			۲	
				Операционист
				Талалина Дарья Фомевна Заместитель начальника отдела

Рис. 5.3. Синхронизация Досье

### 5.3. Структурирование персон/групп персон

#### 5.3.1. Общие сведения

В разделе **Досье** можно добавлять, переименовывать, перемещать или удалять персоны, группы персон или категории групп персон.

Добавить/переименовать/удалить персону или группу персон в организационно-штатной структуре (в разделе **Организационная структура**) средствами Solar NGFW невозможно, т.к. данные о персонах поступают из сторонней системы (например, Active Directory).

#### Примечание

Время кэширования данных раздела **Досье** составляет 5 минут. Поэтому обновленная информация может отображаться не сразу после синхронизации.

#### 5.3.2. Действия с группами персон

В структуре раздела **Досье** можно добавить новый раздел (категорию групп персон) или группу персон. Для этого нажмите **+ Раздел** или **+ Группу** (<u>Рис.5.4</u>). При добавлении раздела укажите его название, при добавлении группы — раздел и название группы.

Настройки + Раздел	+ Группу	+ Пер	сону
Начните вводить текст			Q
На особом контроле			$\sim$

Рис. 5.4. Кнопки для добавления раздела, группы или персоны

Для переименования группы персон:

- 1. В меню действий с соответствующим объектом выберите пункт Редактировать.
- 2. В открывшемся окне **Редактировать группу** в поле **Группа** отредактируйте наименование группы.
- 3. Нажмите Сохранить.

Для перемещения группы персон в другой раздел:

- 1. В меню действий с соответствующим объектом выберите пункт Редактировать.
- 2. В открывшемся окне Редактировать группу в списке Раздел выберите нужный раздел.
- 3. Нажмите Сохранить.

Для удаления выбранной группы персон:

- 1. В меню действий с соответствующим объектом выберите пункт Удалить.
- 2. В открывшемся диалоговом окне нажмите Да.



Рис. 5.5. Меню действий с группой персон

#### 5.3.3. Добавление и удаление персоны

Чтобы добавить персону в группу, нажмите **+ Персону** (таким образом можно ввести данные новой персоны). При добавлении персоны укажите ее группу, ФИО и один из ее сетевых адресов.

#### Примечание

В категорию (раздел верхнего уровня) можно добавлять только группы. Соответственно, для добавления персоны в конкретный раздел (например, **Внешние персоны**) необходимо сначала добавить группу в этот раздел.

Для удаления персоны из выбранной группы:

- 1. Наведите курсор мыши на строку с данными нужной персоны (Рис.5.6).
- 2. Нажмите значок
- 3. В открывшемся диалоговом окне подтвердите удаление.

#### Примечание

Удаляемая персона перемещается в системную группу **Неидентифицированные персоны** (**Необходимо распределение по группам > Неидентифицированные персоны**).

<i>?</i>	Solar NGFW				Поиск персоны Q	<b>₽</b> =
ର	+ Раздел + Группу + Персону	Досье / І				
E	Начните вводить текст Q	Персоны				
\$	На особом контроле 🗸 🗸	Добавит	ь персону			
Ŗ	Испытательный срок	ФИО 🕇				
R,	На увольнение		Семерикова Наталья Антониновна			Â
കൂ	Под подозрением					
Æ	Расходование материальных с		Снегирева Алина Потаповна Менелжер по работе с клиентами			
۲				Внимание	×	
	Организационная структура >			Удалить персону Семер из группы Под подозре	икова Наталья Антониновна нием?	
				Да	Нет	

Рис. 5.6. Удаление персоны из группы

#### 5.4. Получение информации о деятельности персон и групп персон

#### 5.4.1. Получение информации о деятельности группы персон

Для получения информации о конкретной группе персон в разделе **Досье** выберите соответствующий раздел навигационной панели, а затем — одну из вкладок (<u>Рис.5.7</u>):  Персоны — список сотрудников, которые входят в соответствующую группу (<u>Рис.5.7</u>). При этом есть возможность просмотра как основных сведений обо всех сотрудниках, так и подробных данных о каждом сотруднике (в карточке персоны, см. раздел <u>5.4.2</u>).



Рис. 5.7. Раздел «Досье». Получение информации о группе персон

Статистика запросов — статистика по посещаемым персонами, входящими в группу, ресурсам/категориям ресурсов и объему использованного интернет-трафика (<u>Pис.5.8</u>). В графиках отображаются сведения о разрешенных и заблокированных запросах, объеме входящего и исходящего интернет-трафика. В таблицах приводятся выборки по наиболее посещаемым ресурсам, категориям ресурсов, а также самых скачиваемым типам данных. Кроме того, данные можно отфильтровать, используя фильтры: Период, ТОП, Сортировать по, Запросы, Исключить ресурсы.

#### Примечание

Задать значения для фильтров можно с помощью раскрывающихся списков или счетчиков. Описание значений фильтров см. в разделе <u>Приложение F, Перечень фильтров для</u> формирования отчетов.


Рис. 5.8. Раздел «Досье». Получение информации о группе персон. Вкладка «Статистика запросов»

Для более детального анализа данные по каждому графику или таблице можно экспортировать в файл формата CSV (<u>Рис.5.9</u>).



Рис. 5.9. Получение информации о группе персон. Вкладка «Статистика запросов»: экспорт данных в CSV

## 5.4.2. Получение информации о деятельности конкретной персоны (карточка персоны)

Краткую информацию о сотруднике можно получить, открыв его карточку. Для этого в списке персон (в разделе **Досье**) выберите строку с данными нужного сотрудника, нажав в области его ФИО (<u>Рис.5.10</u>).



Рис. 5.10. Раздел «Досье», список персон. Краткая карточка персоны

Подробную информацию о сотруднике можно получить, открыв его полную карточку

(Рис.5.11). Для этого в краткой карточке нажмите значок 🌇.

В полной карточке персоны можно просмотреть всю имеющуюся личную и контактную информацию о персоне (вкладка **Основное**, <u>Рис.5.11</u>).

Для более удобного просмотра карточку персоны можно открыть в новой вкладке браузера, нажав значок **С**.

Кнопки перехода между карточками персон, относящихся к одной группе	Кнопка перехода к выбору карточек для юъединения данных двух и более персон в бу Содиенть картока	нопка для пирования ки на карточку уфер обмена Сколеровать ссаму Отера	ки для пления ом карточки карточки карточки вокодие Свернуть карточку Такрыть
Райзберг Василиса Лександровна Постанть на контроль Р. менеджер Пресс-служба Принят 10.08.16 Стаж 3 года	Роком редактирования Уданнъ персону Руководитель Золин Евгений Артемиевич № ПР.,иректор № Пресс. служба © «Нест данных» Адреса зат. почты	Группы Испытательный срок Под подозрением Пресс-лужба Персонализие дажные	Виспорт перелем Контактная информация В raizberg@companyru 6 67856 9 192.105.17 € 452 2 193 Примечания.
<ul> <li>Основное</li> <li>трафик</li> <li>Типы данных</li> <li>Мурнал</li> </ul>	SID         S-1-5-21-793904598-20           Login         vraizberg           Skype         Raiz           Почта         raizberg@company.ru           Рабочие станции	День рождения <b>15.01.1987</b> Дополнятельные свойства — — — — — — — — — — — — — — — — — — —	2 Соловина Соловить отчет для руководства
	Привилетии smb:\\\fc-8.2\revision\upravlenie\ - запись		

Рис. 5.11. Полная карточка персоны (вкладка «Основное»)

На вкладке **Трафик** (<u>Рис.5.12</u>) отображается статистика по посещаемым персоной ресурсам/категориям ресурсов и объему использованного интернет-трафика. В графиках отображаются сведения о разрешенных и заблокированных запросах, объеме входящего и исходящего интернет-трафика. В таблицах приводятся выборки по 25 наиболее посещаемым персоной ресурсам и категориям ресурсов.

На этой же вкладке администратор безопасности может просмотреть статистику по сработавшим разрешающим и запрещающим правилам политики и объему трафика для каждого из них.



Рис. 5.12. Полная карточка персоны (вкладка «Трафик»)

На вкладке **Типы данных** (<u>Рис.5.13</u>) отображается статистика по количеству запросов, объему интернет-трафика и типам данных, отправленным или полученным персоной. Графики отображают сведения о разрешенных и заблокированных запросах, объеме входящего и исходящего интернет-трафика для персоны. В таблицах приводятся выборки по 25 типам данных, наиболее часто получаемым и передаваемым персоной.

#### Примечание

Красным цветом в таблицах выделяется заблокированный тип данных.

8	Solar NGFW	Поиск персоны	Q 🖞 🛵
ଜ	Предыдущая персо Следующая персона	Соединить карточки Сколировать ссылку Открыть в новой вкладие Свернуть карточку	Закрыть
	Богачева Полина Семеновна	Период ТОП Запросы 180 дней — 25 Все (без технического трафика) ∨	
19 19	Заведущий секретариатом pilot-users	Количество запросов Объем трафика 150 200 МВ	
Ř.	Принят <b>10 Авг 2016</b> Стаж <b>4 года 5 мес</b>	100 150 MB 150 M	
£₀,		0 01.08 01.09 01.10 01.11 01.12 01.01 01.08 01.09 01.10 01.11 01.12 01.01	
۲	Основное	Мин. Макс. Средн. Всего Мин. Макс. Средн. В — Заблокированные запросы 6 51 42 338 — Входящий трафик 19 МВ 182 МВ 144 МВ	3cero 1 GB
۲	трафик	— Разоешенные запоски 7 69 55 440 — Исколяший тоафик 0 МВ 1 МВ 0 МВ V Типы данных	4 MB
	📩 Типы данных	Топ 25 типов скачанных данных танных Топ 25 типов переданных данных	
	🏥 журнал		
		Неизвестная категория / Неизвестный файл 150 21145 M8 Неизвестная категория / Неизвестный файл 150	0.73 MB
		Неизвестная категория / Неизвестный файл 123 <mark>И</mark> В Неизвестная категория / Неизвестный файл 123	0.60 MB
		Мультимедиа / Видео в формате МРЕG, МРЕG-4, 52.76 Мультимедиа / Видео в формате МРЕG, МРЕG-4, МРЕG- МРЕG-TS 15 MB TS 35	0.18 MB
		Инфолмационные технологии / Каскалкая таблица 42.15	013

Рис. 5.13. Полная карточка персоны (вкладка «Типы данных»)

На вкладке **Журнал** (<u>Рис.5.14</u>) отображается статистика по посещаемым персоной ресурсам/категориям ресурсов, разрешенным и заблокированным запросам. В зависимости от выбранных значений в таблице могут быть приведены сведения о протоколе HTTP, коде HTTP-ответа, заголовках запроса, IP-адресе источника, URL запросе, URL параметрах, URL пути, данных User agent, группах персон, правилах и слоях политики, результатах проверки, статусах фильтрации.

С помощью фильтра Колонки можно изменить набор отображаемых в таблице колонок. Для этого в раскрывающемся списке выберите названия нужных колонок.

	Соединить карточки		Скопировать ссылку	Открыть в новой вкладке Свернуть карточку	Закрыть
Коротаева Марта Тимуровна	Период	Колонки	Ресурсы	Запросы	НТТР-код
1 (U)	7 дней 📋	URL путь ×		Bce	
	Категории				Лимит
pilot-users	Мультимедиа × еще	e 2			/ 100
Принят 10 Авг 2016 Стаж 3 года 7 мес			Журнал (первые 100 строк)		
	11.03.2020 13:24:50	login.skype.com	/upload/iblock/759/759e118a88094aec5dc1	54fb4568df69.png	
🚺 Основное	11.03.2020 13:20:14	google.com	/Z29waGVy0i8vcm9zaW5mb25ld3MucnUvYXX S1ncnVkeXUtdS1iYXNzZXluYS1mb3RvLTE0NDM	DaWNsZXMvc2VtZW5vdmljaC1wb3RyeWFzbGEtcHlzaG5 130DI=/	ve
<b>е</b> Трафик	11.03.2020 13:06:49	instagram.com	/album/omsk/sculpt/index.htm		
	11.03.2020 13:06:40	web.skype.com	/togliatti/37.files/aist_provider.gif		
🗎 Типы данных	11.03.2020 12:42:03	www.cybersport.ru	/a/afanasxew_r_s/text_0230.shtml		
Журнал	11.03.2020 12:34:46	instagram.com	/togliatti/37.files/aist_provider.gif		
	11.03.2020 12:29:40	login.skype.com	/txt/1861.htm		
	11.03.2020 12:26:45	okru	/tvar.htm		
	11.03.2020 12:21:12	www.tns-counter.ru	/a/afanasxew_r_s/text_0230.shtml		
	11.03.2020 12:13:08	ok.ru	/a/afanasxew_r_s/text_0230.shtml		
	11.03.2020 12:12:34	yaplakal.com	/prel1/sociaLjpeg		
	11.03.2020 12:05:46	lenta.ru	/txt/1861.htm		

Рис. 5.14. Полная карточка персоны (вкладка «Журнал»)

Сведения на вкладках **Трафик**, **Типы данных** и **Журнал** отображены за последние 7 дней. Эти данные можно отсортировать по значениям, выбранным с помощью фильтров <u>Рис.5.15</u>.



Рис. 5.15. Полная карточка персоны (вкладки «Трафик», »Типы данных» и »Журнал»)

### 5.5. Операции с данными персон

#### 5.5.1. Перечень операций с данными персон

Пользователь может выполнить следующие операции с данными персон:

- Добавить примечания, комментарии и файлы (см. раздел 5.5.2).
- Отредактировать основные сведения о персоне (см. раздел 5.5.3).
- Объединить данные одной персоны, хранящиеся в разных карточках (объединить карточки персон, см. раздел <u>5.5.4</u>).
- Экспортировать сведения о персоне в формат vCard (электронная визитная карточка).
   Для этого в полной карточке персоны нажмите Экспорт персоны.
- Удалить персону, созданную средствами Solar NGFW (т.е. не входящую в группу Организационная структура). Для этого в полной карточке персоны нажмите Удалить персону и далее в отобразившемся диалоговом окне подтвердите удаление (см. раздел <u>5.3.3</u>).

#### 5.5.2. Добавление примечаний, комментариев и файлов

В полной карточке персоны администратор безопасности может добавлять текстовые примечания. Так можно указывать, например, рекомендации по дальнейшему наблюдению за персоной, напоминания, замечания и т.п.



Рис. 5.16. Полная карточка персоны: добавление, просмотр и удаление примечаний

#### Для добавления примечания:

- 1. В блоке для работы с примечаниями в соответствующее поле введите необходимый текст.
- 2. Нажмите 🗾

Для добавления файла:

- В блоке для работы с примечаниями прикрепите файл, нажав кнопку
- 2. При необходимости в соответствующее поле введите текст.
- 3. Нажмите

Для удаления примечания:

- <sup>1.</sup> Наведите курсор на область нужного примечания и нажмите 🔟.
- 2. В отобразившемся диалоговом окне Удалить примечание? нажмите Да.

#### 5.5.3. Редактирование данных персоны

Администратор безопасности может изменять основную информацию о персоне. К этой информации относятся сведения, отображающиеся в полной карточке персоны.

Для перехода в режим редактирования данных персоны в полной карточке персоны нажмите **Режим редактирования**. После этого блоки данных, которые можно отредактировать, станут подсвечены пунктирной линией (<u>Рис.5.17</u>). Для начала изменения данных нажмите в любом месте блока, содержащего данные персоны, которые нужно отредактировать.

<i>?</i> *	Solar NGFW					Поиск персоны	<b>}</b> ≡
۵	Предыдущая персона Следующая персона	Объединить карточки		Скопировать ссылку			
	Яковцов Игорь Платонович	Выйти из режима редактирования				Экспорт пе	ерсоны
\$\$ 	Начальник службы pilot-users Помият 10 авг 2016	Руководитель Горелова Анисья Данилевна А. Начальник отдепа ста⊥ & «Нет данных» А. pilot-users № «Нет данных» ⊠ ad.gorelova@akbprog. □ «Нет данных»	Группы досье Employees pilot-users	Служба персонала	Контактная информац ☑ ip.jakovcov@akbpro <i>З</i> <Нет данных> ፲ <Нет данных>	ия ggг [] <Нет данных> IP <Нет данных> Я <Нет данных>	
Te R	Стаж 7 лет 7 месяцев 3 дня	Адроса Windows-login ISIMO\ip.jakovcov Почта ip.jakovcov@akbprogress.ru					
۲	А основное	Логин ір.jakovcov SID S-1-5-21-3480291418-3434137707	Дополнительные свойства dn CN=ip.jakovcov,0U=pilot-users,0				
¢ <u>≣</u>	🌐 Трафик	Рабочие станции Атрибуты отсутствуют	Фамилия Яковцов orgunit OU=pilot	-users,OU=Employees,DC=i			
	🗋 типы данных						
	🖽 Журнал						
Ŷ							

Рис. 5.17. Полная карточка персоны. Режим редактирования данных

Для изменения данных персоны:

- 1. В полной карточке персоны перейдите в режим редактирования, нажав **Режим редактирования**.
- 2. Нажмите в любом месте блока с данными, которые хотите изменить.
- 3. В открывшемся окне Редактировать измените и/или добавьте данные (Рис.5.18).
- 4. Нажмите Сохранить.

Для выхода из режима редактирования данных в полной карточке персоны нажмите **Выйти из режима редактирования**.



Рис. 5.18. Режим редактирования данных: примеры окон для редактирования сведений о персоне

#### 5.5.4. Объединение карточек персон

Иногда данные одного и того же человека хранятся в разных карточках. Например, если одна карточка персоны была получена из внешней системы (например, из Active Directory), а другая — создана средствами Solar NGFW. Для таких случаев в системе есть возможность объединять несколько карточек в одну.

#### Внимание!

Можно объединять:

- Несколько карточек, созданных средствами Solar NGFW. При этом необходимо указать, в какую из карточек должны быть скопированы данные (основную карточку). Остальные карточки будут автоматически удалены.
- Карточки, созданные средствами Solar NGFW, с одной карточкой, в которой хранятся данные, полученные из внешней системы (например, из Active Directory). При этом в качестве основной может быть указана только карточка с данными из внешней системы.

Для объединения карточек:

- 1. В полной карточке персоны нажмите Объединить карточки.
- В отобразившемся окне Объединение карточек (<u>Рис.5.19</u>) в поисковом поле Выберите персону введите данные (ФИО или адрес) требуемой персоны и в отобразившемся списке выберите нужную персону.
- 3. При необходимости повторите п. 2, т.к. система позволяет соединять две и более карточек.
- 4. Сделайте основной карточку, в которой будут сохранены данные из других, включив соответствующую опцию.
- 5. Нажмите Сохранить.

Объединение карточек Выберите персону				Объ	единение карточек, созда	анных	
Выберите основную карту	<b>Удонта</b> Будет удалена С	стания Основной Картоная полученая из Домена контонии С	-	средст в оди пол (н: В эт может да	твами системы. при усло ной карточке хранятся да ученные из внешней сис: апример, из Active Directo ом случае основной карт г быть указана только кар анными из внешней систе	вии, что нные, темы лу). очкой точка с Мы	
ФИ0	Райзберг Василиса Александровна	Ивлева Ксения Брониславовна		Объединение карточек			
Должность	PR-менеджер	Заместитель начальника отдела	11	Выберите персону			
Подразделение	Пресс-служба	Пресс-служба			Valenta	Veneurs	
Принят	06.02.2019	10.08.2016			Основная	Будет удалена	
Почта	raizberg@company.ru			Выберите основную карту			
Skype	raiz						1
Сохранить					$\mathbf{i}$		
				ФИО	Райзберг Василиса Александровна	amadeus@gmaiLcom	\
				Должность	PR-менеджер		)
				Подразделение	Пресс-служба		
	Объединение	карточек, созданных 🌙 вами системы		Принят	06.02.2019		
	Можно указат	ь основную карточку,		Почта	raizberg@company.ru	amadeus@gmaiLcom	
	переключате	ель в положение on		Skype	raiz		1
				Сохранить			

Рис. 5.19. Объединение карточек персон

# 5.6. Поле «Поиск персоны»: оперативный доступ к данным о персоне/адресе

Для оперативного доступа к данным о персоне в каждом разделе интерфейса имеется поле **Поиск персоны**. С его помощью можно искать персону по следующим атрибутам:

- ФИО;
- должность;
- адрес электронной почты;
- Skype (имя учетной записи пользователя для авторизации в Skype);
- ICQ UIN (идентификатор учетной записи пользователя для авторизации в ICQ);
- Login (имя учетной записи, под которой пользователь вошел на локальную машину. Например, ivanov.ivan);
- SID (идентификатор безопасности учетной записи пользователя компьютера);
- Windows-login (имя учетной записи, под которой пользователь вошел на локальную машину, в виде <домен\имя пользователя>. Например, domain\ivanov.ivan);
- IP-адрес (IP-адрес локальной машины пользователя);
- имя хоста (имя локальной машины пользователя).

#### Внимание!

Поиск запускается при вводе первого символа и ведется **по всем вышеуказанным атрибутам**. При этом ищутся только те персоны, в данных которых имеется совпадение **начальных** символов с введенными (например, в фамилии, имени и/или должности, см. <u>Puc.5.20</u>).



Рис. 5.20. Особенности поиска персон: поиск ведется одновременно по нескольким атрибутам персоны

Таким образом, для оперативного получения сведений о персоне:

- Введите в поле Поиск персоны первый требуемый символ по мере ввода система будет отображать соответствующий список персон/адресов, в данных которых есть совпадение начальных символов с введенными (<u>Рис.5.21</u>).
- 2. В списке персон/адресов выберите строку с нужными данными. Отобразится карточка этой персоны/этого адреса.



Рис. 5.21. Оперативное получение данных о сотруднике

## 6. Политика: реализация политики ИБ

## 6.1. Описание элементов политики

Solar NGFW обеспечивает контроль проходящего сетевого трафика с помощью созданных офицером безопасности правил анализа, их обработки и исключений из них. Такие правила включают в себя условия проверки трафика и наборы действий, которые срабатывают при выполнении условий. Совокупность этих правил образует политику информационной безопасности.

Обработка трафика, поступающего в систему, выполняется с помощью фильтра — специальной программы, автоматически генерируемой по заданным условиям и правилам фильтрации. Для настройки правил фильтрации офицер безопасности использует определенный набор инструментов и элементов политики.

Основные элементы политики ИБ приведены в таблице далее.

Табл. 6.1. Основные элементы политики ИБ

Название	Описание
Слой правил политики	Набор правил и/или исключений политики, который предназначен для решения конкретной задачи политики (подробнее см. раздел <u>6.4</u> ).
Правило	Элемент политики, содержащий набор условий, которые проверяет система, и набор действий, которые выполняются в случае успешной проверки условий. Правила группируются в наборы правил политики (слои правил политики, см. раздел <u>6.5.1</u> ), что позволяет использовать сложные алгоритмы проверок.
Исключение	Объект политики, содержащий набор условий, которые проверяет система с целью исключения исследуемого объекта из проверки в текущем слое. При формировании исключения можно указать только условия.
Условие	Логическое выражение, применяемое к объекту системы и возвращающее либо значение "истина" (если объект удовлетворяет данному условию), либо "ложь" (в ином случае). Условия могут быть простыми и сложными.
Действие	Действие (операция), которое необходимо применить к объекту по результатам проверки условий. Например, передача запросов и ответов, перенаправление трафика. Действия являются системными элементами политики и задаются в правилах. Системные элементы политики пользователь не может создавать, ре- дактировать или удалять.

Действия могут быть основными и дополнительными, условными и безусловными. Основные действия будут применены к объекту при выполнения правила в первую очередь. После выбора основного действия можно выбрать одно или несколько дополнительных действий. Но это возможно только в процессе формировании правил и/или исключений для фильтрации запросов или ответов.

При выборе некоторых основных и дополнительных действий отобразится одно или несколько дополнительных полей, в котором необходимо указать соответствующее значение. Например, при выборе действия **Связать с персоной вручную**, отобразится поле, в котором необходимо указать персону. В одном правиле можно задавать несколько дополнительных действий, но при этом максимальное количество дополнительных действий не должно быть больше 7.

#### Примечание

Условные действия не приводят к выходу из цикла обработки политики, т.е. не нарушают естественной нисходящей проверки правил (сверху-вниз) и могут выполняться последовательно.

При выполнении безусловных действий обработка политики прекращается. К безусловным действиям относятся все основные действия, кроме: **Ничего не делать** и **Разрешить запрос** (доступно только в слое фильтрации запросов).

В таблице правил фильтрации запросов и ответов в колонке **Действия** будет отображен соответствующий значок вместо названия действия. Количество выбранных дополни-

тельных действий будет указано над значком (например, 2). Описание всех значков приведено в Табл.6.2.

Табл. 6.2. Значки для обозначения основных действий при формировании правил фильтрации запросов и ответов

Действие	Значок
Ничего не делать	0
Заблокировать	8
Запросить подтверждение	0
Перенаправить	0
Разрешить и не проверять дальше	3
Разрешить через ргоху-сервер	0
Разрешить запрос	0
Проверить сертификат	

Подробнее о работе с основными элементами политики см. в разделе 6.4.2.

В таблице далее приведены инструменты политики для формирования политики ИБ.

Табл. 6.3. Краткий обзор инструментов политики ИБ

Название	Описание
Внешние подключе- ния	Инструменты политики, в которых указаны параметры настройки для перенаправления пользовательского трафика (подробнее см. раздел <u>6.5.3</u> ).
Объекты политики	Инструменты политики, предназначенные для формирования правил и/или исключе- ний политики (подробнее см. раздел <u>6.5.4</u> ).
Справочники	Наборы (списки) элементов, сгруппированных по определенному признаку. Каждый из элементов содержит краткие сведения о конкретном объекте. Справочные данные могут использоваться в других объектах системы, что позволяет избежать многократного ввода одной и той же информации (подробнее см. раздел <u>6.5.5</u> ).
Шаблоны	Наборы правил проверки текстовой информации на наличие и/или отсутствие опре- деленных элементов текста. Также шаблоны могут представлять собой страницы для уведомления пользователей (подробнее см. раздел <u>6.5.6</u> ).

#### Примечание

Элементы и инструменты политики могут создаваться как самой системой, так и администратором безопасности.

Управление элементами и инструментами политики выполняется в разделе **Политика** (<u>Рис.6.1</u>), подробная информация приведена в разделе <u>6.5</u>.



Рис. 6.1. Раздел «Политика»

#### Примечание

Политика фильтрации считывается из файла **policy.xml**, который по умолчанию создается в процессе установки Solar NGFW.

Также вы можете приобрести лицензию с подпиской на распространяемую политику. В этом случае при загрузке лицензии выполняется загрузка и автоматическое применение распространяемой политики на узле. Проверка обновлений такой политики и их загрузка выполняется в автоматическом режиме.

Администратору безопасности распространяемая политика доступна только для просмотра (<u>Рис.6.2</u>). При этом он может формировать свои правила и/или исключения. Правила и исключения распространяемой политики выполнятся после применения всех пользовательских правил и исключений.

Настройки Импорт Экспорт	Политика / Запреще	нные ресурсы 🎯	)				Применит	ь политику
🛞 Перенаправление по ICAP						Поиск по названию, пе 🔍	Настрой	ка колонок
🗇 Фильтрация запросов 🛛 🕘 🗦	Количество Исключений	5 Количество Пр.	авил 9					
📣 Фильтрация ответов 🛛 🕣 🗸	Название	Действия Источн	ик Назначение	Протоколы	Форматы файлов	Размеры файлов	Доп.	Вкл.
Пользовательский слой фи_	a con	осмотр				×	± <b>1</b>	
Временный список до обновления	Включе	ено	💽 🛞 Правило	О Исключение				
Белый список	Назван	ние	Онлайн-тоговля					
В Запрещенные ресурсы	Rommer	нтарий	Заблокировать доступ пользовате	ля к страницам ресурсов, п	редоставляющих услуги он.	лайн-торго		
Запрешени е слова	Действ	вия						
	Основн	HOP	😣 Заблокировать	<ul> <li>Шаблон блокі</li> <li>Шаблон страницы</li> </ul>	провки блокировки	V		
Слой распростран	яемой	ия						
политики	Источн	ник	Любой			$\vee$		
			Персона, Группа персон, IP-диапазон, IP, ди	апазон вида IP - IP или маска под	cetur IP/xxx			
	Назнач	чение	🛛 Китайские товары_ресурсы)	Аукционы		$\checkmark$		
Значок			Список ресурсов, категория или полное им	я хоста (включая поддомены)				
распространяемой полит	Расшир	ренные настройки	[] Показать					
			Сохраниты	Отменить				

Рис. 6.2. Раздел «Политика»: распространяемая политика

## 6.2. Принципы работы

В процессе обработки политики каждый слой правил политики проверяется последовательно: **сверху-вниз**. Правила и/или исключения проверяются аналогичным образом сначала проверяются исключения, а потом уже правила:

- Если исключение сработает в слое Вскрытие HTTPS или Перенаправление по ICAP, начнется проверка следующего слоя.
- Если сработает исключение в слоях фильтрации запросов/ответов, проверка продолжится со следующего слоя этого же типа.
- Если сработает правило в слоях фильтрации запросов/ответов, обработка политики завершится. При выполнении правила в остальных слоях, обработка политики продолжится.

Чтобы упорядочить правила по приоритетам, при создании/редактировании соответствующего правила в поле установите его приоритет с помощью цифрового значения, начиная с 1.

Создать правило		×
Включено		
Название	Введите название	
	— Название правила обязательно	
Комментарий	Введите комментарий	
Приоритет	Укажите Всего правил в слое: 0	
Направление трафика	Входящий 🗸 Журналировать	
Действие	😢 Запретить 🗸	
Состояние соединения	Любое	$\sim$
Входящий интерфейс	Введите интерфейс	
	Сетевой интерфейс. Например: eth0	
Источник	Любой	
	IP, диапазон вида IP-IP, маска подсети IP/хх или MAC-адрес XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:	
Назначение	Любое	
	Сохранить Отменить	

Рис. 6.3. Приоритет правила

При понижении/повышении приоритета правило перемещается на соответствующую позицию. То правило, которое до этого занимало указанный приоритет, автоматически передвигается на строчку выше (например, в правиле с приоритетом 2 при изменении значения на 17, правило, находившееся до этого на 17 строке, поднимется на 16, а правило с приоритетом 3, на 2). Значения приоритета у смещенных правил в этом случае меняются автоматически.

При установлении значения 0, правило автоматически перемещается на верхнюю позицию. После сохранения правила, значение с 0 поменяется на 1.

При формировании политики необходимо учитывать следующее:

- В процессе настройки политики администратор безопасности работает с цепочками взаимосвязанных объектов (элементов политики ИБ). Для изменения или удаления определенного элемента (например, правила), необходимо удостовериться, что это не нарушит выполнения политики ИБ.
- При формировании некоторых правил и/или исключений необходимо заранее создать соответствующие элементы политики (внешние подключения, объекты политики и т.д.).

Например, при настройке набора правил и исключений политики для перенаправления трафика по ICAP следует задать соответствующие ICAP-серверы в разделе Политика > Внешние подключения > ICAP-серверы (см. раздел <u>6.5.3.1</u>).

Для просмотра настроек и перехода к редактированию какого-либо элемента политики ИБ (в том числе и набора условий) необходимо выбрать соответствующий раздел на панели навигации.

- Некоторые элементы политики достаточно ресурсоемки, что затрудняет работу политики и системы в целом. Например, ключевые слова являются самыми ресурсоемкими, что значительно снижает производительность системы. В данном случае на производительность влияет размер буфера для определения кодировки текста: чем он больше, тем медленнее работает система. Однако, если указать совсем малое значение размера буфера, кодировка определяться не будет.
- При возникновении внештатной ситуации, связанной с ошибками настройки Solar NGFW, применяются последние корректные настройки.

#### 6.3. Общий порядок настройки политики ИБ

Для формирования политики ИБ:

- 1. Создайте или отредактируйте элементы политики ИБ, необходимые для настройки правил и/или исключений политики (шаблоны, справочники и т.д., см. раздел <u>6.5</u>).
- Создайте или отредактируйте соответствующий набор правил и/или исключений для каждого слоя (см. раздел <u>6.5.1</u>). Для начала работы с определенным слоем выберите его на панели навигации.
- 3. Примените политику безопасности, нажав Применить политику.

#### Примечание

В Solar NGFW происходит автоматическое переприменение политик каждые 5 минут. Переприменение способствует противодействию ручному изменению конфигурации в CLI. Например, при изменении или добавлении и применении в CLI правил, которые не соответствуют политике безопасности, будет возвращена конфигурация, назначенная в веб-интерфейсе.

После нажатия кнопки **Применить политику** откроется окно (<u>Рис.6.4</u>), в котором будут отображены данные по последним внесенным в политику изменениям (время, дата и автор изменения). Также в окне будут приведены комментарии по настройкам политики.

Применить политику		×		
Последняя версия	22.01.2019 12:44   admin			
Комментарий	Настроил политику согласно договору.			
Комментарий к новой версии	Напишите комментарий	h,		
	Применить Отменить			

Рис. 6.4. Окно «Применить политику»

При формировании политики ИБ администратор безопасности может быстро перейти к настройке параметров конфигурации, используемых в работе:

- указать параметры фильтрации и анализа трафика пользователей (режим и метод аутентификации, блокировку рекламы и т.д.);
- настроить доступ администратора;
- указать лицензионный ключ для активации антивируса.

Перечень параметров настройки идентичен перечню в разделе Система > Основные настройки > Работа системы.

Система предотвращения вторжений	
Привязать очереди к ядрам CPU	•
Защищаемые сети (HOME_NET)	192.168.0.0/16,10.0.0.0/8,172.16.0.0/12 IP адреса которыми заполняем переменную \$HOME_NET для пр
Порт сервера для соединения	2270 По умолчанию сервис фильтрации skvt-wizor настроен на работ
Таймаут соединения	300 Если по почению указанного времени по полого хоста не пол
Сертифиты	Будет сгенерирован автомати Загрузны
Порт для защищенного соединения	8444
Порт для незащищенного соединения	8445
∨ Лицензия	<ul> <li>Ключевой</li> <li>Серийный</li> <li>файл</li> <li>номер</li> <li>лицензии</li> </ul>
Лицензионный ключевой файл	Необходимо загрузить agent Загрузить

Рис. 6.5. Окно «Настройка» в разделе «Политика»

Для внесения изменений в параметры фильтрации:

- 1. В разделе Политика нажмите Настройки.
- 2. В открывшейся вкладке укажите/измените параметры настройки и нажмите Сохранить.
- 3. Для применения изменений нажмите Применить и закройте вкладку.

Для облегчения настройки правил и исключений фильтрации воспользуйтесь справкой с полезной информацией (*Frequently asked questions – FAQ*), вызвав ее нажатием на значок 2. В справке можно просмотреть описание каждого слоя, детали и примеры формирования правил и исключений, а также перейти на внешние ресурсы по ссылке.

*	Solar NGFW			Справка Х
රු	Настройки Импорт Экспорт			
E.	межсетевой экран >			Основная задача слоя — дать возможность пройти запросам пользователя при невозможности их аутентификации настроенным методом, т.к. некоторые приложения и пользователи могут не
8	🖉 ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ 🔶			поддерживать NTLM и/или Kerberos-аутентификацию, настроенную в системе.
57	***		lioboe C	При создании правил чаще всего указываются следующие условия:
*	🔶 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🗸			• Источник — IP-адрес (один или диапазон)
\$a	😥 Доступ без аутентификации	всего 1 строка		• Назначение — ресурс назначения (домен)
				Inpunoxeenne konnenta — User-Agent (n i IP-saronobok)     Maourove
தி	🔐 Вскрытие HTTPS			
_				
	Перенаправление по юсе			• Связать автоматически
(≣)	👍 Фильтрация запросов 🛛 💿 🗸			<ul> <li>связать с персоной вручную</li> <li>Ничего не лелать</li> </ul>
	🗘 Фильтрация ответов 💮 🗸			Связать автоматически
				IP-адрес источника можно найти в:
	💾 внешние подключения 🔰 >			
				<ul> <li>Кэше НТТР фильтра успешных аутентификаций (<i>IP, привязанный к персоне</i>)</li> </ul>
	ОБЪЕКТЫ ПОЛИТИКИ >			<ul> <li>Если IP-адрес персоны не наиден, он приравнивается к неаутентифицированному пользователю</li> </ul>
				Связать с персоной вручную
	СПРАВОЧНИКИ 🗸 🗸			IP-адрес источника привязывается к выбранной в правиле персоне.
	Адреса электронной почты			
\$	Ключевые слова			Ничего не делать

Рис. 6.6. Справка в слое "Доступ без аутентификации"

## 6.4. Управление инструментами политики

#### 6.4.1. Принципы работы со слоями правил политики

Основные действия, которые можно выполнить с конкретным слоем, отображаются в меню действий с ним (<u>Рис.6.7</u>).



Рис. 6.7. Меню действий со слоем

В Табл.6.4 приведен обзор действий, которые можно выполнить со слоями правил политики, а также ограничения и комментарии к выполнению каждого действия.

#### Внимание!

После выполнения каждого действия нажмите **Применить политику** для сохранения и применения внесенных изменений.

Табл. 6.4. (	Обзор	действий,	выполняемых	со слоями
--------------	-------	-----------	-------------	-----------

N⁰	Наименование	Описание
1.	Создание	Можно создать новый слой только в разделах Фильтрация запросов и Фильтрация ответов. Название слоя должно быть уникальным.

N⁰	Наименование	Описание
		Для этого:
		1. В разделе Политика > Контентная фильтрация в строке слоев Филь-
		трация запросов/Фильтрация ответов нажмите 🖽
		<ol> <li>В открывшемся окне укажите название слоя, нажмите Сохранить и сформируйте список правил и исключений. При необходимости настройте состав колонок таблицы, в которой отображаются правила и исключения.</li> </ol>
2.	Переименование	Переименовать можно только слои фильтрации запросов или ответов. На- звание слоя должно быть уникально. Для изменения названия слоя в разделе Политика в меню действий с конкретным слоем выберите пункт Переиме- новать и в открывшемся окне измените название. Нажмите Сохранить.
3.	Перемещение	В разделе <b>Политика</b> на панели навигации можно изменять положение слоев одного типа относительно друг друга только <b>внутри</b> слоя. А именно, можно перемещать только слои фильтрации запросов и ответов (внутри раздела).
		Для перемещения слоя внутри группы в разделе <b>Политика</b> напротив нужного
		слоя нажмите 🔜 и переместите его выше или ниже, не отпуская курсор мыши. После применения политики проверка будет выполнена согласно новому расположению слоев.
4.	Копирование	Для копирования слоя в разделе <b>Политика</b> в меню действий с конкретным слоем выберите пункт <b>Скопировать</b> . Скопированный слой отобразится в конце списка слоев одного типа.
		ሱ Фильтрация запросов   ∨
		🗄 Категории (Categories) 🕴
		🗄 Общая политика (запросы) 📫
		🗄 Общая политика (запросы) 🚦
		Общая политика (запросы)-копия-1
		Рис. 6.8. Скопированный слой
		Копия отображается под исходным слоем. Все данные нового слоя, кроме названия, идентичны данным оригинала.
		Название скопированного объекта формируется следующим образом:
		<ul> <li>постоянная часть — &lt;название исходного слоя&gt; + &lt;копия&gt;;</li> </ul>
		<ul> <li>изменяемая часть — &lt;порядковый номер&gt;.</li> </ul>
		Порядковый номер — натуральное число, обозначающее номер копии, со- здаваемой в системе. Порядковый номер копии каждого слоя уникален.
		В <u>Табл.6.5</u> приведены примеры формирования названий скопированных слоев.
5.	Просмотр и редактирование содержимого (пра-	Для просмотра содержимого слоя (набора правил и/или исключений) в разделе Политика на панели навигации выберите нужный слой.

N⁰	Наименование	Описание					
	вил и исключений, содер- жащихся в слое)	Справа отобразится таблица с правилами и/или исключениями, которые при необходимости можно отредактировать.					
		Подробнее об управлении правилами и исключениями см. раздел <u>6.4.2</u> .					
6.	Включение/отключение	Включить или отключить можно только слои фильтрации запросов или отве- тов. После отключения слой меняет свой цвет. Если запустить применение политики после отключения слоя, проверка правил и исключений, содержа- щихся в этом слое, не будет выполнена, и будет применено действие «разрешить все». Для включения/отключения слоя в разделе Политика в меню действий с конкретным слоем выберите пункт Выключить слой/Включить слой. От- ключенный слой изменит свой цвет.					
		Фильтрация запросов 🕒 🗸					
		: Общая политика (запросы)					
		Categories					
		🗄 Запрет на скачивание ехе 🚦					
		🗘 Фильтрация ответов 🕒 >					
		Рис. 6.9. Включение/отключение слоя					
7.	Удаление	Удалить можно только слои фильтрации запросов или ответов. Если удалить все слои фильтрации запросов или ответов, по умолчанию будет применено действие «разрешить все».					
		Для удаления слоя в разделе <b>Политика</b> в меню действий с конкретным слоем выберите пункт <b>Удалить</b> и в открывшемся окне нажмите кнопку <b>Да</b> .					
		Слой невозможно удалить в момент его проверки. Отобразится соответству- ющее сообщение об ошибке.					

#### Табл. 6.5. Примеры названий скопированных слоев

Название правила	Название копии
Разрешаем Mail.ru	Разрешаем Mail.ru-копия-1
Разрешаем Mail.ru (повторное копирование объекта)	Разрешаем Mail.ru-копия-2
Разрешаем Mail.ru-копия-1	Разрешаем Mail.ru-копия-3
Разрешаем Mail.ru-копия-2	Разрешаем Mail.ru-копия-4

#### 6.4.2. Принципы работы с правилами и исключениями



Рис. 6.10. Раздел «Политика»: список правил и исключений

Наборы правил и исключений каждого слоя приведены в виде списков в таблице справа от панели навигации (<u>Рис.6.10</u>). Список исключений по умолчанию расположен выше списка правил.

Чтобы раскрыть или скрыть содержимое строки с конкретным правилом или исключением, нажмите ссылку **развернуть/свернуть** (<u>Рис.6.11</u>).

Правила								
∷	<b>6'</b> 4 4	чаза@maiLru123 vаза@maiLrub1 vаза@maiLrub1 Васимий Полшьзова васмий Литивна Незутепнофицирова VASKI Испытательный срок Неидентифицирова VaSki Vaski Vaski Vaski Vaski Valve Corporation (St	DNScrypt Dezer Pandora Twitter Backdoor Win32 Driv_ Backdoor Win32 Driv_ Trojan-Oswin32 Xtoo. Trojan-Oswin32 Xtoo. Trojan-Oswin32 Xtoo. Trojan-PSW Win32 Far. Trojan-PSW Win32 Far. Trojan-PSW Win32 Far. Winus Win32 Lamer Worm Win32 Fipp	Архивы и сжат Аудио Базм данных веб-страницы Видео Данвые докум Изображения Исполняемые Исполняемые Исполняемые Исполняемые Исполняемые Исполняемые фа Скраиты Справочники Текстовые фа Управление п Финансы Шрифты Электроиная п	admin 21.01.2019 17:32	4	•	00
			↓ развернуть	mart 5				

Рис. 6.11. Строка с правилом

Администратор безопасности может настроить состав *таблицы*, в которой отображаются правила и/или исключения. Для этого:

- 1. В выбранном слое раздела Политика нажмите кнопку Настройка колонок.
- В открывшемся окне рядом с названием колонки включите опцию, которую следует отобразить. Некоторые опции включены по умолчанию и недоступны для редактирования.
- 3. Нажмите Сохранить.

Политика / Фильтј	рация ответов	/ Общая политика ((	ответы) 🕐		Применить	политику
Создать правило				Поиск по названию, пе	Q Настройк	а колонок
Количество Исключен	ий 2 Количес	гво Правил 🙎				
Название Исключения	Действия	Источник	Назначение	Когда и кем изменено Доп.	Вкл.	
Разрешить youtu	ube	💄 Александров Па	🔋 block YouTube	admin 14.03.2022 15:47	•	0 Đ
Админам качать	бе	🕹 Большаков Влад	Любое	admin 14.03.2022 16:46	•	Q Ċ
Правила	Состав колон	ок таблицы			×	
🗄 Лимит трафика						0 Ĉ
🗄 Запретить всем	Можно добае	ить еще 10 параметр	OB			00
	🖌 Название	$\checkmark$	Действия	🕑 Источник		
	🕢 Назначені	1e 🗌	Протоколы	Методы		
	Порты		Заголовки Вазмори файлов	Форматы файлов	}	
	Расписани	ie 🗌	Лимиты трафика	<ul> <li>Когда и кем изме</li> </ul>	нено	
			Сохранить Отме	нить		

Рис. 6.12. Раздел «Политика»: настройка отображения колонок таблицы

Вы можете добавить или убрать колонки таблицы. Каждый слой имеет свой собственный набор колонок:

- колонки, которые отображаются в таблице по умолчанию;
- столбцы, отображение которых можно настроить.

Также со списком правил/исключений можно выполнить следующие действия:

- Скопировать атрибут правила/исключения (например, ресурсы, IP-адрес и т.д.). Для этого курсором мыши выделите значение и скопируйте его (с помощью сочетания клавиш или контекстного меню);
- Открыть карточку объекта или список объектов системы. Для этого перейдите по соответствующей ссылке. Ссылка представляет собой атрибут правила/исключения, выделенный синим цветом.

Для более оперативной работы с правилами и исключениями в разделе **Политика** предусмотрен поиск по атрибутам правил и исключений: по названию правила/исключения, значениям источника/назначения и комментариям. Поиск не является сквозным, а выполняется внутри выбранного слоя.

Политика / Фильтрация запро	Примениты	политику				
Создать правило			рабоч	8	Настройка	колонок
Количество Исключений 0 Колич	ество Правил	1				
Название Действия Правила	Источник	Назначение		Доп.	Вкл.	
III <mark>Рабоч</mark> ее время 😣	Любой	Любое		<b>*</b> ☆		Q C

Рис. 6.13. Поиск по атрибутам правил и исключений

Найти инструменты и объекты (справочники, внешние подключения и т.д.) в разделах политики можно только по их названию.

Для поиска следует ввести название в поисковую строку, расположенную над списком. По мере ввода текста ниже будет отображаться список результатов, удовлетворяющих условиям поиска. При этом совпадающие символы будут подсвечены желтым цветом.

В Табл.6.6 приведен обзор действий, которые можно выполнить с правилами и исключениями, а также ограничения и комментарии к выполнению каждого действия.

Nº	Наименование	Описание						
1.	Формирование	Для формирования правила и/или исключения:						
		<ol> <li>В разделе Политика выберите нужный слой на панели навигации и нажмите Создать правило.</li> </ol>						
		. Задайте параметры проверки и нажмите Сохранить.						
		. Нажмите <b>Применить политику</b> .						
		азвание нового правила и/или исключения должно быть уникально.						
		3 слое Предотвращение вторжения можно создать только исключение.						
		В слое <b>Доступ без аутентификации</b> можно создать только правила.						
		При создании нового правила и/или исключения должны быть заполнены обязательные поля. Иначе система не позволит сохранить правило и/или ис- ключение.						
2.	Редактирование	Для редактирования правила и/или исключения:						
		1. В разделе Политика в нужном слое нажмите на правило или исключение.						
		<ol> <li>Внесите необходимые изменения: отредактируйте название, измените условие или действие и т.д.</li> </ol>						
		3. Нажмите <b>Сохранить</b> и <b>Применить политику</b> .						
		Внести изменения в правило и/или исключение, проверяемое в текущий мо- мент, невозможно.						
		Выбранные в правилах действия по умолчанию сохраняются в системе — при преобразовании правила в исключение и обратно, заданное ранее действие отобразится автоматически.						

Табл. 6.6. Обзор действий, выполняемых с правилами и исключениями

Nº	Наименование	Описание
3. Копирование		Для копирования правила и/или исключения в строке с правилом/исключением нажмите кнопку Скопировать. Копия правила/исключения отобразится в конце списка. Затем нажмите Применить политику.
		Копия отображается в конце списка с правилами или исключениями. Все данные скопированного правила и/или исключения, кроме названия, идентичны данным оригинала.
		Название скопированного объекта формируется следующим образом:
		<ul> <li>постоянная часть — &lt;название копируемого правила и/или исключения&gt; + &lt;копия&gt;;</li> </ul>
		• <i>изменяемая часть</i> — <порядковый номер>.
		Порядковый номер — натуральное число, обозначающее номер копии, созда- ваемой в системе. Порядковый номер копии каждого правила и/или исключения уникален.
		Примеры формирования названий приведены в <u>Табл.6.7</u> .
4.	Включение/Отключе- ние	Чтобы отключить проверку правила и/или исключения на какое-то время, сделайте его неактивным с помощью переключателя, как в разделе, так и в окне с правилом и/или исключением.
		Отключить проверяемое правило и/или исключение невозможно.
5.	Перемещение	Можно перемещать правила только в пределах одного конкретного слоя. Ис- ключения перемещать невозможно.
		Для перемещения правила внутри слоя нажмите кнопку в строке конкретного правила и переместите его выше или ниже, не отпуская курсор мыши. Для применения внесенных изменений нажмите <b>Применить политику</b> . Проверка набора правил и исключений будет выполнена согласно новому расположению правил в таблице.
6.	Удаление	Для удаления правила и/или исключения в разделе Политика в строке с правилом или исключением нажмите Удалить. В открывшемся окне нажмите Да и Применить политику.
		Правило и/или исключение в момент его проверки удалить нельзя.

Создать правило		X
Включено		
Название	Персона на испытательном сроке	
Комментарий	Пользователь на испытательном сроке	
Приоритет	Укажите	
	Всего правил в слое: 0	
Не аутентифицировать и	Связать с персоной вручную	$\sim$
Персона	Иванов Иван Иванович	$\sim$
Источник	Любой	$\sim$
	Выбрать IP-диапазон или ввести: IP, диапазон вида IP - IP или маску подсети IP/xx	
Назначение	() www.rut.ru ×	$\sim$
	Список ресурсов или полное доменное имя, IP, диапазон вида IP - IP или маску подсети IP/xx	
Восшироши ю изстройии		
	Сохранить Отменить	

Рис. 6.14. Формирование правила и/или исключения

Вы можете скопировать значения атрибутов **Источник** и **Назначение**. Для этого нажмите специальный значок, который появится при наведении курсора мыши на значение. Скопированное значение будет сохранено в буфер обмена.

	Копировать в буфер обмена	1
Условия	1.1.1.1 🛱	
Источник	♥ 1.1.1.1×	
Условия		
Источник	♥ 1.1.1.1×	Копировать в буфер обмена
	Интернет-коммуникация / Соц	циальные сети 🕫 🔓 он вида IP - IP ил
Назначение	🛅 Социальные се	ети ×
	Список ресурсов, катего	рия или полное имя хоста

Рис. 6.15. Копирование значений

Табл. 6.7. Примеры образования названий скопированных правил

Название правила	Название копии
Правило-1	Правило-1-копия-1
Правило-1 (повторное копирование объекта)	Правило-1-копия-2

Название правила	Название копии
Правило-1-копия-1	Правило-1-копия-3
Правило-1-копия-2	Правило-1-копия-4

Политика / Фильтрац	ия запрос	юв / Categorie	25 🕜					Применить г	политику
Создать правило						Поиск по назв	анию, пе ۹	Настройка	колонок
Количество Исключений	0 Количе	ество Правил 🙎							
Название Правила	Действия	Источник	Назначение	Протоколы	Форматы файлов	Размеры файлов	Доп.	Вкл.	
🗄 Rule 1	8	Любой	GoogleDrive				☆	•	00
	8	Редактировать п	равило <b>Rule 1</b>			×		•	0 đ
Constraint States and States and		Включено		💿 Правило 🔷 И	1сключение		and the second second		
		Название	Rule 1						
		Комментарий	Введите комме	нтарий					
		Действия							
		Основное	😢 Заблокиров	ать 🗸	Block page	$\sim$			
					Шаблон страницы блокировки				
			Добавить допо	лнительное действие	~				
		Условия							
		Источник	Любой			~			
			Персона, Группа пер	хон, IP-диапазон или ввести: I	IP, диапазон вида IP - IP или маску подсети IP/xx				
		Назначение	GoogleDrive	×		~			
			Список ресурсов, ка	тегория или ввести полное им	ия хоста				
		Расширенные наст	тройки Показать						
				Сохранить	Отмена				

Рис. 6.16. Включение/отключение правила или исключения

#### 6.4.3. Принципы работы с инструментами политики

Элементы политики представляют собой инструменты для формирования политики фильтрации трафика.

Все инструменты политики расположены в виде списков (каждый в своем разделе) в соответствующем подразделе раздела **Политика**. Информация по каждому элементу списка представлена в виде таблицы с соответствующим набором колонок.

Некоторые инструменты могут быть объединены в группы (списки). Управление группами аналогично управлению их отдельными элементами.

Наименование	Описание
Внешние подключения	Инструменты, в которых указаны параметры настройки для перенаправ- ления пользовательского трафика, расположенные в разделе Политика > Внешние подключения.
Объекты политики	Инструменты фильтрации, предназначенные для формирования правил и/или исключений политики, расположенные в разделе Политика > Объекты Политики.
Справочники	Списки элементов, сгруппированных по определенному признаку. Каждый из элементов содержит краткие сведения о конкретном объекте. Работа со справочниками и их содержимым осуществляется в разделе Политика > Справочники и выполняется по общим принципам, описанным далее.
Шаблоны	<ul> <li>Инструменты для модификации заголовков НТТР-запросов, а также автоматической генерации веб-страниц для уведомления пользователей:</li> <li>шаблоны для модификации заголовков (добавление, изменение или удаление заголовков);</li> </ul>

Табл. 6.8. Перечень инструментов политики

Наименование	Описание
	• шаблоны для формирования веб-страниц.
	Шаблоны для модификации заголовков используют для создания правил политики фильтрации запросов и ответов. Их следует указать при выборе дополнительных действий, таких как добавление, изменение и удаление заголовков.
	Шаблоны страниц предназначены для автоматической генерации уве- домительных страниц с использованием предопределенного текста. В такие шаблоны можно вставить ту или иную информацию о переданных по сети данных, которые послужили причиной отображения уведомления.
	Управление шаблонами осуществляется в разделе Политика > Шабло- ны.

#### Для выполнения каких-либо действий с инструментами политики предназначены определенные кнопки/значки (см. <u>Табл.6.9</u>).

#### Табл. 6.9. Обзор кнопок и действий, выполняемых с инструментами политики ИБ

Кнопка/Значок	Описание
Значки 🚬 💙	Раскрыть/свернуть строки с информацией об инструменте.
	Сведения, представленные в таблице элемента справочника, можно отсортировать по любому из параметров (колонке таблицы).
	Для сортировки нажмите название выбранной колонки.
	Например, если в таблице одного из элементов справочника <b>Ресурсы</b> нажать на название колонки <b>Шаблон имени</b> , значения в этом столбце будут отсорти- рованы по возрастанию.
	При повторном нажатии на заголовок сортировка будет выполнена по убыванию.
Кнопка 🗍	Копировать список инструментов или инструмент.
	Копия отображается в конце списка. Все данные нового инструмента, кроме названия, идентичны данным оригинала.
	Название скопированного инструмента формируется следующим образом:
	<ul> <li>постоянная часть — &lt;название копируемого инструмента&gt; + &lt;копия&gt;;</li> </ul>
	<ul> <li>изменяемая часть — &lt;порядковый номер&gt;.</li> </ul>
	Порядковый номер — число, обозначающее номер копии, создаваемой в си- стеме. Порядковый номер копии каждого инструмента уникален.
	В <u>Табл.6.10</u> приведены примеры формирования названий.
Кнопка 🗇	Удалить инструмент.
	Для удаления инструмента (группы инструментов) политики необходимо:
	1. В зависимости от того, является ли это отдельным инструментом или группой:
	• Нажать кнопку 🛈 в строке соответствующей группы;
	<ul> <li>Раскрыть строку с данными конкретной группы и нажать кнопку строке соответствующего инструмента.</li> </ul>
	2. В открывшемся окне подтверждения нажать кнопку Да.

Кнопка/Значок	Описание
	<ol> <li>Если был удален элемент группы, нажать кнопку Сохранить для сохранения внесенных изменений.</li> </ol>
	Инструмент невозможно удалить при наличии у него связи с правилами и/или исключениями политики. Отобразится соответствующее сообщение об ошибке. Для удаления инструмента следует заменить его в правиле и/или исключении на другой
Кнопка «Добавить + назва-	Добавить новый инструмент.
ние инструмента»	Его название должно быть уникально в своем разделе.
	Добавление каждого типа инструментов подробно описано в соответствующих разделах
Кнопка Сохранить	Сохранить внесенные изменения
Кнопка Применить политику	Нажимать для сохранения и применения внесенных изменений в политику

Табл. 6.10. Примеры образования названий скопированных инструментов политики

Название инструмента	Название копии
Инструмент	Инструмент-копия-1
Инструмент (повторное копирование объекта)	Инструмент-копия-2
Инструмент-копия-1	Инструмент-копия-3

Для редактирования списка инструментов политики или его элемента необходимо:

- 1. Раскрыть строку с информацией о списке инструментов или его элементе и внести изменения.
- 2. Нажать кнопку **Сохранить**, которая станет доступной только после внесения какоголибо изменения.

#### Примечание

В работе со справочниками, следует учесть, что его будет невозможно открыть из-за большого объема. На экране отобразится текст, содержащий инструкции для решения проблемы:

«Список слишком большой. Для просмотра и редактирования, сохраните его в файл и откройте в любом редакторе.

Для редактирования этого справочника необходимо экспортировать его из системы, внести изменения и импортировать его обратно».

Основные изменения, внесенные в объект политики (дата создания/редактирования и инициатор этих действий), после сохранения автоматически запоминаются системой и отображаются в строке с данными этого объекта. Например:

>	icap-server 1	icap://tt48.solar.local:134	admin admin 26.11.2018 14:35 26.11.2018 14:35		00
		admin		admin	
>	linux	27.11.2018 17:09	)	29.11.2018 10:37	ŪŌ

Для более оперативной работы с инструментами политики в каждом разделе, в зависимости от типа инструмента, предусмотрен *поиск по тексту*. Для поиска следует ввести наименование инструмента (логин пользователя в разделе **Пользователи (Basic Auth)**) в поисковую строку, расположенную над списком.

По мере ввода текста будет отображаться список результатов, удовлетворяющих условиям поиска. При этом совпадающие символы будут подсвечены желтым цветом.

Аналогичный поиск предусмотрен и для содержимого справочников (поле Поиск по параметрам).

#### 6.4.4. Экспорт и импорт политики и ее отдельных инструментов

#### 6.4.4.1. Общие сведения

Solar NGFW позволяет экспортировать и импортировать как всю политику целиком, так и ее отдельные инструменты:

- слои правил политики со всеми элементами и инструментами, которые используются в них;
- группы инструментов политики одного типа;
- отдельный инструмент политики (например, списки IP-адресов, шаблон страницы и т.д.);
- базу сигнатур системы предотвращения вторжений.

При этом данные экспортируются в JSON- или CSV-файл, который сохраняется на диске. Место сохранения файла зависит от настроек браузера.

#### Примечание

Необходимо учесть следующее:

- Лимиты трафика и пользователей при Basic-аутентификации можно выгрузить/загрузить только при экспорте/импорте всей политики.
- Если файл имеет другой формат, при попытке его импорта отобразится уведомление об ошибке. Загрузка политики не будет выполнена.
- Если политика содержит какие-либо ошибки, она все равно будет импортирована в систему. Все существующие ошибки будут перечислены в сообщении об ошибке, которое отобразится в веб-браузере.
- Если в процессе экспорта политики или ее инструментов перейти в другой раздел, экспорт будет отменен.

#### 6.4.4.2. Экспорт и импорт политики

Для экспорта всех данных политики в разделе **Политика** нажмите кнопку **Экспорт** (<u>Рис.6.17</u>). Далее сформированный JSON-файл (например, **policy.json**), содержащий соответствующие данные о политике, будет сохранен в каталог, указанный в настройках

браузера. Имя файла с политикой имеет формат: <policy><дата экспорта><время экспорта>.json



Рис. 6.17. Кнопки для экспорта и импорта политики

При импорте политики данные из внешнего XML-файла загружаются в БД системы.

Для импорта политики:

- 1. В разделе Политика нажмите Импорт (<u>Рис.6.17</u>).
- 2. Выберите файл **<имя файла>.json** (например, **policy.json**), содержащий данные политики.
- 3. Нажмите Открыть.

#### Примечание

Необходимо учесть следующие особенности импорта политики:

- все элементы и инструменты старой политики удаляются;
- в правилах и/или исключениях импортируемой политики могут быть указаны персоны, которые отсутствуют в **Досье** Solar NGFW. В этом случае произойдет следующее:
  - если персона указана в правилах слоя Доступ без аутентификации, заданное действие Связать с персоной вручную изменится на Связать с персоной автоматически;
  - если персона указана в правилах других слоев, отобразится соответствующее уведомление. Уведомление будет содержать перечень ід всех отсутствующих персон. В этом случае перейдите в конкретное правило или исключение и внесите изменения.

Также в Solar NGFW вы можете импортировать пустую политику. Для этого:

- 1. В разделе Политика нажмите Импорт (Рис.6.17).
- 2. Убедитесь, что в разделе Политика отсутствуют правила в каждом из слоев.
- 3. Проверьте, что при создании правил в слоях фильтрации запросов и ответов присутствуют дефолтные шаблоны.
- 4. Выберите нужный файл и нажмите Открыть.
- 5. Нажмите Применить политику.

#### 6.4.4.3. Экспорт инструментов политики

Solar NGFW предоставляет возможность экспортировать группы инструментов политики одного типа. Это касается списка ICAP- и прокси-серверов.

Для экспорта группы инструментов политики в разделе **Политика > Внешние подклю**чения (<u>Рис.6.18</u>) выберите соответствующий раздел и нажмите **Экспорт**.

Ποι	итика / Внешние по	одключения / ІСАР-сервері		Применить политику	
Д	обавить ICAP-сервер	Импорт Экспорт		Поиск по имени сери	вера С
	Имя сервера	URL	Комментарий	Создан И	1зменен
e	Local reqmod	icap://localhost:	1344/reqmod	14.03.2022 14:56	
A	Local respmod	icap://localhost.	1344/respmod	14.03.2022 14:56	

Рис. 6.18. Экспорт группы инструментов политики

В указанном каталоге будет сохранен файл с расширением **CSV**, который содержит следующую информацию:

- названия столбцов в порядке их следования в веб-интерфейсе, слева-направо, разделенные символом табуляции;
- значения параметров, определенных названиями столбцов по порядку их следования, разделенные символом табуляции.

Примечание
Имя экспортируемого файла имеет формат: <b>&lt;название группы инструментов поли-</b> тики><дата экспорта><время экспорта>.csv

Также в Solar NGFW можно экспортировать отдельные инструменты политики. Данная функция доступна во всех инструментах, кроме:

- лимитов трафика;
- пользователей (Basic Auth);
- шаблонов страниц.

Для экспорта отдельного инструмента политики в разделе Политика:

- 1. Выберите соответствующий инструмент и раскройте строку с его данными, нажав значок ≥.
- 2. Нажмите кнопку Экспорт (Рис.6.19).

Название Без аутентификации Шаблон имени Тип шаблона Создан Изменен Комментарий	🗸 Сохранит	ь Отмена 🗾	обавить шаблон	Поиск по параметрам	Q	Импорт Экспорт 🗍
Шаблон имени Тип шаблона Создан Изменен Комментарий	Название	Без аутентификации				
	Шаблон имени		Тип шаблона	Создан	Изменен	Комментарий
mail         Имя хоста ∨         admin 16.03.2022 16:25         Введите комментарий	mail		Имя хоста 🗸	admin 16.03.2022 16:25		Введите комментарий

Рис. 6.19. Экспорт отдельного инструмента политики

В указанном каталоге будет сохранен файл с расширением **CSV**, который содержит следующую информацию:

- строку version 1;
- значения параметров, определенных названиями столбцов по порядку их следования, разделенные символом табуляции.

#### Примечание

Имя экспортируемого файла имеет формат: **<название инструмента политики><дата** экспорта><время экспорта>.csv

#### 6.4.4.4. Импорт инструментов политики

Solar NGFW предоставляет возможность импортировать из внешнего файла инструменты политики или группы инструментов.

Можно импортировать данные конкретного инструмента политики в момент его добавления в систему вручную.

Для того, чтобы импортировать список инструментов политики, сначала необходимо подготовить текстовый файл со списком. Файл должен иметь расширение **CSV**, а содержащийся в нем текст должен иметь кодировку **utf-8**. Файл должен иметь последовательно следующее содержимое:

- строку version 1;
- названия столбцов в порядке их следования в веб-интерфейсе, слева направо, разделенные точкой с запятой;

#### Внимание!

Названия столбцов должны быть в точности такими же, как и в экспортированном списке.

 значения параметров, определенных названиями столбцов по порядку их следования, разделенные точкой с запятой.

При этом следует учесть следующее:

- если параметр имеет логический тип (флажок в интерфейсе), то установленному флажку соответствует значение 1, а снятому – 0;
- если параметр не должен быть задан (например, пустой пароль), то значения предыдущего и следующего параметров должны быть разделены двумя символами табуляции.

Импорт отдельных инструментов политики доступен во всех инструментах, кроме:

- лимиты трафика;
- пользователи (Basic Auth);
- шаблоны страниц.

#### Примечание

Если название инструмента политики не задано, при импорте оно будет автоматически сформировано из имени файла и даты-времени.

Название инструмента имеет следующий формат: <filename><timestamp>.csv

Например:

имя файла: **NewList**, дата импорта: 2018.11.30, время импорта:18:27:57. В итоге, имя файла, сформированное автоматически, будет следующим: **NewList\_20181130\_18-27-57**.

Содержимым импортируемого файла можно либо дополнить имеющийся список, либо заменить его полностью с помощью кнопок **Добавить данные из файла** и **Заменить данные из файла**.

Для импорта инструментов политики или группы инструментов политики необходимо в разделе **Политика**:

- 1. Выбрать соответствующий инструмент или группу инструментов.
- 2. При необходимости раскрыть строку с данными этого инструмента (группы инструментов), нажав на значок ≥.
- 3. Нажать кнопку Импорт (<u>Рис.6.20</u>).
- 4. В открывшемся окне Загрузить данные из файла выбрать способ загрузки данных, нажав соответствующую кнопку (<u>Рис.6.21</u>).
- 5. В открывшемся стандартном окне выбрать файл и нажать кнопку Открыть.

Полит	ика / Внешние	подключени	я / ІСАР-серверы 🕜			Применить по	литику
Доба	вить ІСАР-сервер	Импорт	Экспорт		Поиск по имени	сервера	٩
	Имя сервера		URL	Комментарий	Создан	Изменен	
A	Local reqmod		icap://localhost:1344/reqmod		14.03.2022 14:5	56	
A	Local respmod		icap://localhost:1344/respmod		14.03.2022 14:5	56	

Рис. 6.20. Импорт инструментов политики

Загрузить данные из файла	×
Заменить данными из файла Файл: <i>Не выбран</i>	Добавить данные из файла
	Закрыть

Рис. 6.21. Окно «Загрузить данные из файла»

#### Примечание

Если при импорте списка ресурсов произошла ошибка, в окне браузера отобразится уведомление с детальным описанием причины сбоя.

## 6.5. Инструменты политики

#### 6.5.1. Слои правил политики

Каждый слой правил политики содержит в себе набор правил и исключений одного типа, которые предназначены для решения конкретной задачи политики (подробное описание каждого слоя приведено в <u>Табл.6.11</u>).

Табл. 6.11. Обзор действий со слоями правил политики

Наименование слоя	Примечание	Ссылка на подробное описание			
Межсетевой экран					
Фильтр транзитного трафика	Системный слой, его невозможно:	Раздел <u>6.5.1.1.1</u>			
Фильтр входящего трафика	• переименовать;	Раздел <u>6.5.1.1.2</u>			
Фильтр исходящего трафика		Раздел <u>6.5.1.1.3</u>			
Трансляция адресов	• переместить;	Раздел <u>6.5.1.1.4</u>			
	• копировать;				
	• удалить				
	Предотвращение вторжени	Й			

Наименование слоя	Примечание	Ссылка на подробное описание		
Правила и исключения	Системный слой, его невозможно:	Раздел <u>6.5.1.2.1</u>		
Наборы сигнатур	<ul><li>переименовать;</li><li>переместить;</li></ul>	Раздел <u>6.5.1.2.2</u>		
	<ul><li>копировать;</li><li>удалить</li></ul>			
Доступ без аутентификации	Системный слой, его невозможно:	Раздел <u>6.5.1.3.1</u>		
Вскрытие HTTPS	• переименовать;	Раздел <u>6.5.1.3.2</u>		
Перенаправление по ІСАР	• переместить;	Раздел <u>6.5.1.3.3</u>		
	• удалить			
Фильтрация запросов	Системный слой, его невозможно:	Раздел <u>6.5.1.3.4</u>		
Фильтрация ответов	• переименовать;	Раздел <u>6.5.1.3.5</u>		
	• удалить.			
	Однако Solar NGFW позволяет сформировать новые слои этого же типа и выполнить с ними дей- ствия, указанные выше			
SSL-инспекция				
Правила расшифровки	Системный слой, его невозможно: • переименовать;	Раздел <u>6.5.2.1</u>		
	<ul><li>переместить;</li><li>копировать;</li><li>удалить</li></ul>			

#### 6.5.1.1. Межсетевой экран

Межсетевое экранирование является базовой функциональностью Solar NGFW, позволяющей контролировать информационные потоки как на низких (L2, L3, L4), так и на высоких (L7) сетевых уровнях по следующим признакам: МАС-адресам, IP-адресам, сетевым интерфейсам, состояниям соединений, направлению трафика, портам, протоколам L3, L4, L7 и приложениям.

В качестве МЭ в Solar NGFW используется брандмауэр Netfilter. Для его настройки используются интерфейсы утилит nftables и iptables:

 Nftables используется для создания обработчика фрагментированных пакетов, который включается в работу практически в самом начале пути пакета через сетевой стек Astra Linux. Также, Nftables используется для настройки захвата трафика IPS (позволяет включить захват и передачу входящего и/или транзитного трафика на проверку в IPS прямо из ядра).
• Iptables используется для создания основной логики фильтрации сетевых пакетов (остальные функциональные возможности MЭ Solar NGFW).

С помощью настройки правил и исключений слоя **Межсетевой экран** можно решить следующие задачи:

- фильтрация трафика по описанным выше признакам,
- разграничение доступа к сетевым ресурсам,
- обнаружение и предотвращение сетевых вторжений,
- трансляция адресов пользователей (скрытие источника/назначения, экономия адресов),
- обнаружение событий и инцидентов нарушения политики сетевой безопасности.

В зависимости от выбранной задачи сформируйте правило политики в соответствующем подразделе слоя **Межсетевой экран**, заполнив необходимые параметры. Перечень параметров перечислен ниже в соответствующих разделах.

# Примечание

В Solar NGFW сервисы обмениваются данными между собой по сети (localhost), поэтому, чтобы не блокировать их работу, при настройке правил фильтрации необходимо учитывать данные, описанные в таблице <u>Приложение E. Mampuua MЭ Solar NGFW</u>.

Межсетевой экран и DPI имеют ограничения:

- При изменении действия в правилах фильтрации с Разрешить на Запретить новая политика распространяется только на новые соединения, устанавливаемые после применения изменений. Соединения, установленные до внесения изменений в политику фильтрации, продолжат фильтроваться по старым правилам, пока соединение не будет сброшено или переустановлено.
- Все RELATED-соединения, инициируемые разрешенными ESTABLISHED-соединениями, пропускаются, но не журналируются.
- Проверки трафика по правилам DPI начинаются с момента создания первого правила с классификатором DPI и не распространяются на соединения, установленные до создания первого правила.
- Для правил DPI создаются дополнительные правила, которые не видны в веб-интерфейсе. Такие правила служат для определения прикладного протокола или приложения DPI. В них могут попадать первые несколько пакетов других соединений, т.к. на данном этапе DPI проверяет, есть ли в трафике искомые протоколы.

При фильтрации некоторых прикладных протоколов с помощью DPI стоит учитывать:

• Чтобы заблокировать трафик Telegram, правило на его запрет необходимо поставить по приоритету выше всех остальных правил с классификатором DPI.

Telegram определяется в DPI по протоколу шифрования MTProto, а управление Telegramботами выполняется через API Telegram (стандартный HTTPS), поэтому трафик управления ботами не будет обнаружен через DPI. Чтобы заблокировать API Telegram, создайте блокирующее правило в разделе **Контентная фильтрация > Фильтрация запросов**.

 В связи с особенностями работы Тог не любой его трафик можно заблокировать. Тог можно блокировать только по адресам известных узлов, поэтому под блокировку будет попадать не весь трафик (перечень известных узлов Тог постоянно обновляется).

# 6.5.1.1.1. Фильтр транзитного трафика

Слой **Фильтр транзитного трафика** предназначен для управления фильтрацией трафика на основе транзитного направления (трафик, который проходит сквозь Solar NGFW, т.е. обрабатывается им как промежуточным узлом), протоколов L3, L4, приложений, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

Политика /	Межсетев	ой экран /	Фильтр транз	итного трафи	іка 🕜				l	Применить	политику
Создать пра	вило							Поиск по названию	о, пе Q	Настройк	а колонок
Название	Действие	Источник	Порт ист.	Назначение	Порт назн.	Протоколы	Приложения	Когда и кем изменено	Доп.	Вкл.	
∷ 1. Пр	8	Любой		Любое			Не использ	admin 04.09.2023 16:37		•	0 Đ
₿ 2.3a	8	Любой		Любое			YouTube	admin 04.09.2023 16:47		•	Q Đ
₿ 3. alL	>>>	Любой		Любое		UDP	Не использ	admin 04.09.2023 16:49			0 Đ
Всего 3 Строки								H <	1 >	▶  20	0 / стр. 🗸

Рис. 6.22. Слой правил политики «Фильтр транзитного трафика»

В таблице далее перечислены атрибуты для формирования правил политики этого слоя.

	Табл.	6.12. C	Описание	атрибутов	слоя	«Фильтр	транзитного	трафика»
--	-------	---------	----------	-----------	------	---------	-------------	----------

Название атрибута	Описание	Значение
	Основ	ные
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов. Максимальная длина текста не должна превы- шать 29 байт, где один латинский символ равен 1 байту, а один кириллический символ – 2 байтам.
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов.
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху- вниз. Правила и/или исключения проверяются ана- логичным образом — сначала проверяются исклю- чения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактиро- вании соответствующего правила в поле установите его приоритет с помощью цифрового значения, на- чиная с 1. Более подробно описано в разделе <u>6.2</u> .

Название атрибута	Описание	Значение
Журналировать	Опция позволяет отображать информацию о настроенном правиле в <b>Журнале соедине- ний</b> в разделе Статистика > Журнал соединений	Опция.
Действие	Действие, которое будет при- менено к объекту по результа- там проверки условий прави- ла	<ul> <li>Значение можно выбрать в раскрывающемся списке:</li> <li>Запретить;</li> <li>Разрешить;</li> <li>Ограничить скорость;</li> <li>Сброс ощибочных ТСР пакетов</li> </ul>
Фрагментированный трафик	Опция доступна только при выборе транзитного направле- ния трафика и позволяет раз- делить один сетевой пакет на два. Рекомендуется использо- вать при максимальном разме- ре полезного блока данных одного пакета более 1500	Флажок. <b>Примечание</b> Срабатывание правил МЭ с установленным флажком <b>Фрагментированный трафик</b> журналируется в файл <b>/var/log/kern.log</b> .
Протоколы	байт Протоколы передачи данных	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>TCP;</li> <li>UDP;</li> <li>ICMP;</li> <li>IGMP;</li> <li>GRE;</li> <li>AH;</li> <li>ESP.</li> <li>Если значение не выбрано, проверяться будет любой трафик, независимо от протокола.</li> </ul>
Входящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: <i>eth0</i> . Доступно только при выборе входящего или транзит- ного направления трафика.
Источник	Адрес отправителя пакетов	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>одиночный IP-адрес;</li> <li>диапазон IP-адресов;</li> <li>маска подсети IP-адресов;</li> <li>MAC-адрес;</li> <li>объекты GeoIP;</li> <li>«Любой» (<i>значение по умолчанию</i>).</li> </ul>
Порты источника	Номер (диапазон номеров) портов TCP и UDP	Число (меньше 65536), список или диапазон нату- ральных чисел. Можно выбрать не более 50. Первое

Название атрибута	Описание	Значение
		значение диапазона должно быть меньше, чем вто- рое.
Исходящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: <i>eth0</i> . Доступно только при выборе исходящего или тран- зитного направления трафика.
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>одиночный IP-адрес;</li> </ul>
		• диапазон IP-адресов;
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		• объекты GeoIP;
		• «Любое» ( <i>значение по умолчанию</i> )
Порты назначения	Номер (диапазон номеров) портов ТСР и UDP	Число (меньше 65536), список или диапазон нату- ральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем вто- рое.
Тип/код ІСМР	Фильтрация ICMP-трафика по отдельным типам/кодам сооб-	Поле доступно только после выбора протокола ICMP в поле <b>Протоколы</b> .
	щений	Значение можно выбрать в раскрывающемся списке:
		• [0] Эхо-ответ;
		• [3] Назначение недоступно;
		• [4] Сдерживание источника;
		• [5] Перенаправление;
		• [8] Эхо-запрос;
		• [9] Объявление маршрутизатора;
		• [10] Запрос маршрутизатора;
		• [11] Время жизни (ttl) истекло;
		• [12] Проблема с параметрами дейтаграммы;
		• [13] Запрос временной метки;
		• [14] Временная метка получена;
		<ul> <li>[17] Запрос адресной маски;</li> </ul>
		• [18] Адресная маска получена.
		Примечание
		В связи с особенностью реализации функции по фильтрации трафика по типам/кодам ICMP для блокирования определенного ти- па/кода ICMP нужно создать отдельное правило на блокировку этого типа/кода.
Приложения	Протоколы и приложения уровня L7	Значение можно ввести вручную или выбрать в раскрывающемся списке:

Название атрибута	Описание	Значение
		<ul> <li>все протоколы и приложения (категория верхнего уровня Все),</li> </ul>
		<ul> <li>одну или несколько категорий протоколов и приложений,</li> </ul>
		• определенные протоколы и приложения.

При включении опций <b>Журналировать</b> и/или <b>Фрагментированный трафик</b> в списке правил
в столбце <b>Дополнительные условия</b> отображается значок с количеством включенных опций.

Примеры решения задач с помощью правил и исключений слоя **Фильтр транзитного трафика** приведены в разделе <u>6.6</u>:

- блокировка ресурса по IP-адресу (см. раздел 6.6.1.1);
- блокировка пользователя с помощью его идентификации на сетевом уровне: по МАСадресу (см. раздел <u>6.6.1.2</u>);
- фильтрация трафика на основе принадлежности к тому или иному прикладному протоколу/приложению (см. раздел <u>6.6.1.5</u>).

## 6.5.1.1.2. Фильтр входящего трафика

Слой **Фильтр входящего трафика** предназначен для управления фильтрацией трафика на основе входящего направления (любой трафик, конечным получателем которого является Solar NGFW, т.е. в адресе назначения пакета указан один из его адресов), протоколов L3, L4, приложений, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

Политика /	Межсетев	ой экран /	Фильтр входя	ящего трафин	(a 🕐				Применит	ь политику
Создать пра	вило							Поиск по названию, пе Q	Настрой	ка колонок
Название	Действие	Источник	Порт ист.	Назначение	Порт назн.	Протоколы	Приложения	Когда и кем изменено Доп.	Вкл.	
₿ 1. <b>W</b>	8	🖗 1.1.1.1		Любое			WhatsApp	admin 04.09.2023 17:17	•	0 Đ
₿ 2. <b>Ya</b>	<b>&gt;&gt;&gt;</b>	Любой		Любое			YandexMail	admin 04.09.2023 17:18	•	0 Đ
Всего 2 Строки	1							H < 1 >	N Z	20 / стр. 🗸

Рис. 6.23. Слой правил политики «Фильтр входящего трафика»

## Примечание

Фильтрация трафика, проксируемого в явном режиме, осуществляется только правилами, действующими для входящего направления трафика (при использовании технологии проксирования в качестве значения адреса назначения пакета устанавливается адрес проксисервера, поэтому NGFW видит такой трафик входящим, а не транзитным).

# В таблице далее перечислены атрибуты для формирования правил политики этого слоя.

Табл. 6.13. Описание атрибутов слоя «Фильтр входящего трафика»	Þ
--	---

Название атрибута	Описание	Значение			
	Основ	ные			
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов. Максимальная длина текста не должна превы- шать 29 байт, где один латинский символ равен 1 байту, а один кириллический символ – 2 байтам.			
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов.			
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху- вниз. Правила и/или исключения проверяются ана- логичным образом — сначала проверяются исклю- чения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактиро- вании соответствующего правила в поле установите его приоритет с помощью цифрового значения, на- чиная с 1. Более подробно описано в разделе <u>6.2</u> .			
Журналировать	Опция позволяет отображать информацию о настроенном правиле в <b>Журнале соедине- ний</b> в разделе Статистика > Журнал соединений	Опция.			
Действие	Действие, которое будет при- менено к объекту по результа- там проверки условий прави- ла	<ul><li>Значение можно выбрать в раскрывающемся списке:</li><li>Запретить;</li><li>Разрешить.</li></ul>			
Протоколы	Протоколы передачи данных	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>TCP;</li> <li>UDP;</li> <li>ICMP;</li> <li>IGMP;</li> <li>GRE;</li> <li>AH;</li> <li>ESP.</li> <li>ECли значение не выбрано, проверяться будет любой трафик, независимо от протокола.</li> </ul>			
Входящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: <i>eth0</i> . Доступно только при выборе входящего или транзит- ного направления трафика.			

Название атрибута	Описание	Значение
Источник	Адрес отправителя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>одиночный IP-адрес;</li> </ul>
		• диапазон IP-адресов;
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		<ul> <li>МАС-адрес;</li> </ul>
		• объекты GeoIP;
		• «Любой» (значение по умолчанию).
Порты источника	Номер (диапазон номеров) портов ТСР и UDP	Число (меньше 65536), список или диапазон нату- ральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем вто- рое.
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>одиночный IP-адрес;</li> </ul>
		<ul> <li>диапазон IP-адресов;</li> </ul>
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		• объекты GeoIP;
		• «Любое» (значение по умолчанию)
Порты назначения	Номер (диапазон номеров) портов ТСР и UDP	Число (меньше 65536), список или диапазон нату- ральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем вто- рое.
Тип/код ІСМР	Фильтрация ICMP-трафика по отдельным типам/кодам сооб-	Поле доступно только после выбора протокола ICMP в поле <b>Протоколы</b> .
	щении	Значение можно выбрать в раскрывающемся списке:
		• [0] Эхо-ответ;
		• [3] Назначение недоступно;
		• [4] Сдерживание источника;
		• [5] Перенаправление;
		• [8] Эхо-запрос;
		• [9] Объявление маршрутизатора;
		• [10] Запрос маршрутизатора;
		• [11] Время жизни (ttl) истекло;
		• [12] Проблема с параметрами дейтаграммы;
		<ul> <li>[13] Запрос временной метки;</li> </ul>
		• [14] Временная метка получена;
		• [17] Запрос адресной маски;

Название атрибута	Описание	Значение
		<ul> <li>[18] Адресная маска получена.</li> <li>Примечание</li> <li>В связи с особенностью реализации функции по фильтрации трафика по типам/кодам ICMP для блокирования определенного ти- па/кода ICMP нужно создать отдельное правило на блокировку этого типа/кода.</li> </ul>
Приложения	Протоколы и приложения уровня L7	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>все протоколы и приложения (категория верхнего уровня Все),</li> <li>одну или несколько категорий протоколов и приложений,</li> <li>определенные протоколы и приложения.</li> </ul>

При включении опций Журналировать и/или Фрагментированный трафик в списке правил

в столбце **Дополнительные условия** отображается значок **с** количеством включенных опций.

Примеры решения задач с помощью правил и исключений слоя **Фильтр входящего трафика** приведены в разделе <u>6.6</u>:

- блокировка ресурса по IP-адресу (см. раздел 6.6.1.1);
- блокировка пользователя с помощью его идентификации на сетевом уровне: по МАСадресу (см. раздел <u>6.6.1.2</u>);
- фильтрация трафика на основе принадлежности к тому или иному прикладному протоколу/приложению (см. раздел <u>6.6.1.5</u>).

# 6.5.1.1.3. Фильтр исходящего трафика

Слой **Фильтр исходящего трафика** предназначен для управления фильтрацией трафика на основе исходящего направления (любой трафик, изначальным отправителем которого является Solar NGFW, т.е. в адресе источника пакета указан один из его адресов), протоколов L3, L4, приложений, используемых портов, адресов источника/назначения, сетевых интерфейсов и состояния соединений.

олитика /	Межсетев	ой экран / 🤉	Фильтр исход	ящего трафика 🕜				Применить политику
Создать пра	вило						Поиск по названию, пе Q	Настройка колонок
Название	Действие	Источник	Порт ист.	Назначение Порт назн.	Протоколы	Приложения	Когда и кем изменено Доп.	Вкл.
🗄 1. 3a	⊗	Любой		<b>9</b> 1.1.1.1		VPN	admin 04.09.2023 17:29	💽 🗍 Ū
🗄 2. Ya	<b>&gt;&gt;&gt;</b>	Любой		Ø 2222		YandexMusic	admin 04.09.2023 17:30	00
сего 2 Строки								ы 20 / стр. ∨

Рис. 6.24. Слой правил политики «Фильтр исходящего правила»

В таблице далее перечислены атрибуты для формирования правил политики этого слоя.

Табл. 6.14. Описание атрибутов слоя «Фильтр исходящего трафика»

Название атрибута	Описание	Значение
	Основ	ные
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов. Максимальная длина текста не должна превы- шать 29 байт, где один латинский символ равен 1 байту, а один кириллический символ – 2 байтам.
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов.
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху- вниз. Правила и/или исключения проверяются ана- логичным образом — сначала проверяются исклю- чения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактиро- вании соответствующего правила в поле установите его приоритет с помощью цифрового значения, на- чиная с 1. Более подробно описано в разделе <u>6.2</u> .
Журналировать	Опция позволяет отображать информацию о настроенном правиле в <b>Журнале соедине- ний</b> в разделе Статистика > Журнал соединений	Опция.
Действие	Действие, которое будет при- менено к объекту по результа- там проверки условий прави- ла	<ul><li>Значение можно выбрать в раскрывающемся списке:</li><li>Запретить;</li><li>Разрешить.</li></ul>
Протоколы	Протоколы передачи данных	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>TCP;</li> <li>UDP;</li> <li>ICMP;</li> <li>IGMP;</li> <li>GRE;</li> <li>AH;</li> <li>ESP</li> </ul>

Название атрибута	Описание	Значение
		Если значение не выбрано, проверяться будет лю- бой трафик, независимо от протокола.
Источник	Адрес отправителя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>одиночный IP-адрес;</li> </ul>
		<ul> <li>диапазон IP-адресов;</li> </ul>
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		• объекты GeoIP;
		• «Любой» (значение по умолчанию).
Порты источника	Номер (диапазон номеров) портов ТСР и UDP	Число (меньше 65536), список или диапазон нату- ральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем вто- рое.
Исходящий интерфейс	Сетевой интерфейс	Значение можно ввести вручную. Например: <i>eth0</i> . Доступно только при выборе исходящего или тран- зитного направления трафика.
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>одиночный IP-адрес;</li> </ul>
		<ul> <li>диапазон IP-адресов;</li> </ul>
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		• объекты GeoIP;
		• «Любое» (значение по умолчанию)
Порты назначения	Номер (диапазон номеров) портов ТСР и UDP	Число (меньше 65536), список или диапазон нату- ральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем вто- рое.
Тип/код ІСМР	Фильтрация ICMP-трафика по отдельным типам/кодам сооб-	Поле доступно только после выбора протокола ICMP в поле Протоколы.
	щений	Значение можно выбрать в раскрывающемся списке:
		• [0] Эхо-ответ;
		• [3] Назначение недоступно;
		• [4] Сдерживание источника;
		• [5] Перенаправление;
		• [8] Эхо-запрос;
		• [9] Объявление маршрутизатора;
		• [10] Запрос маршрутизатора;
		• [11] Время жизни (ttl) истекло;
		• [12] Проблема с параметрами дейтаграммы;
		• [13] Запрос временной метки;

Название атрибута	Описание	Значение
		• [14] Временная метка получена;
		• [17] Запрос адресной маски;
		• [18] Адресная маска получена.
		Примечание
		В связи с особенностью реализации функции по фильтрации трафика по типам/кодам ICMP для блокирования определенного ти- па/кода ICMP нужно создать отдельное правило на блокировку этого типа/кода.
Приложения	Протоколы и приложения уровня L7	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>все протоколы и приложения (категория верхнего уровня Все),</li> </ul>
		<ul> <li>одну или несколько категорий протоколов и приложений,</li> </ul>
		• определенные протоколы и приложения.

При включении опций Журналировать и/или Фрагментированный трафик в списке правил

в столбце **Дополнительные условия** отображается значок с количеством включенных опций.

Примеры решения задач с помощью правил и исключений слоя **Фильтр исходящего трафика** приведены в разделе <u>6.6</u>:

- блокировка ресурса по IP-адресу (см. раздел 6.6.1.1);
- фильтрация трафика на основе принадлежности к тому или иному прикладному протоколу/приложению (см. раздел <u>6.6.1.5</u>).

## 6.5.1.1.4. Трансляция адресов

*Network Adress Translation* технология трансляции сетевых адресов, которая заключается в объединение компьютеров в мелкие локальные сети, каждой из которых присвоен единый IP-адрес.

Слой Трансляция адресов предоставляет возможность скрыть:

- источник запроса по технологии Source NAT (SNAT),
- назначение запроса по технологии **Destination NAT** (DNAT).

Политика / М	Лежсетево	й экран / Тр	ансляция адр	есов 🕜			(	Применить политику
Создать прави	ило						Поиск по названию, пе Q	Настройка колонок
Название	Действие	Источник	Назначение	Интерфейс	Параметр	Порты	Фрагмент Когда и кем изменено	Вкл.
🗄 1. web	DNAT	Любой	Любое		To-destination 1.1.1.1:443 UDP	123	admin 04.09.2023 20:31	💽 Ū Ū
Всего 1 Строка							I4 < 1 >	ы 20 / стр. ∨

Рис. 6.25. Слой правил политики «Трансляция адресов»

Технологии **SNAT** позволяет заменить исходный IP-адрес источника сетевого пакета на другой указанный вручную (действие **SNAT**) или автоматически (действие **MASQUERADE**) IP-адрес.

**DNAT** позволяет преобразовать адрес назначения в IP-заголовке пакета. Если пакет попадает под критерий правила, выполняющего **DNAT**, то этот пакет и все последующие из этого же потока, будут подвергнуты преобразованию адреса назначения и переданы на требуемое устройство, узел или сеть. Данное действие может, к примеру, успешно использоваться для предоставления доступа к веб-серверу, находящемуся в локальной сети, и не имеющему публичного IP-адреса.

Для этого сформируйте правило, которое перехватывает пакеты, идущие на HTTP-порт брандмауэра, и передайте их на локальный адрес web-сервера, выполняя DNAT. Для этого действия также можно указать диапазон адресов назначения, тогда для всех пакетов, подходящих под это условие, адрес и порт назначения будут изменены на целевые.

В таблице далее перечислены атрибуты для формирования правил политики этого слоя.

## Примечание

Набор атрибутов правила зависит от выбранного действия.

Название атрибута	Описание	Значение				
	Основ	ные				
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов.				
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов.				
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху- вниз. Правила и/или исключения проверяются ана- логичным образом — сначала проверяются исклю- чения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактиро- вании соответствующего правила в поле установите его приоритет с помощью цифрового значения, на- чиная с 1. Более подробно описано в разделе <u>6.2</u> .				
Действие	Действие, которое будет при- менено к объекту по результа- там проверки условий прави- ла	Значение можно выбрать в раскрывающемся списке: • PAT (Masquerading),				

Табл. 6.15. Описание атрибутов слоя «Трансляция адресов»

Название атрибута	Описание	Значение
		Source NAT,
		Destination NAT.
Журналировать	Опция позволяет отображать информацию о настроенном правиле в <b>Журнале соедине- ний</b> в разделе Система > Журналы	Опция.
Интерфейс	Сетевой интерфейс для скрытия	Значение можно ввести вручную. Например: <i>eth0</i>
Источник	Адрес отправителя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>одиночный IP-адрес;</li> </ul>
		<ul> <li>диапазон IP-адресов;</li> </ul>
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		• объекты GeoIP;
		• «Любой» ( <i>значение по умолчанию</i> )
Назначение	Адрес получателя пакетов	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>одиночный IP-адрес;</li> </ul>
		<ul> <li>диапазон IP-адресов;</li> </ul>
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		• объекты GeoIP;
		<ul> <li>«Любое» (значение по умолчанию)</li> </ul>
Протокол	Протоколы передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		• TCP;
		• UDP;
		• GRE;
		• ICMP;
		• AH.
		Если значение не выбрано, проверяться будет лю- бой трафик, независимо от протокола.

Примеры настройки правил слоя Фильтр приведены в разделе 6.6:

- SNAT:
  - объединение источников запроса под одним IP-интерфейсом вручную Source NAT (см. раздел <u>6.6.1.3</u>);
  - автоматическое объединение источников запроса под одним IP-интерфейсом PAT (Masquerading) (см. раздел <u>6.6.1.5</u>).

• DNAT — скрытие IP-адреса назначения запроса пользователя (см. раздел <u>6.6.1.6</u>).

# 6.5.1.2. Предотвращение вторжений (IPS)

Система предотвращения вторжений (IPS) Solar NGFW позволяет контролировать сетевой трафик в части его анализа на предмет вредоносной или подозрительной активности с возможностью последующей блокировки.

Система предотвращения вторжений применяется для фильтрации входящего и транзитного трафика.

# Примечание

По умолчанию настроена фильтрация транзитного трафика. Изменить настройки можно в разделе Система > Расширенные настройки > Фильтрация и кэширование трафика > Система предотвращения вторжений.

# 6.5.1.2.1. Правила и исключения

Слой **Предотвращение вторжений > Правила и исключения** представляет собой набор правил (сигнатур), сгруппированных по классам угроз. Применение правил фильтрации происходит по степени критичности анализируемой угрозы.

Каждый класс содержит в себе правила, которые анализируют определенный тип сигнатур с определенным уровнем угроз:

- Критично 💷,
- Опасно 💷,
- Предупреждение 💷,
- Не распознано 💷,

<b>*</b> *	Solar NGFW							Поиск персоны	<b>L</b> =
ଜ	Настройки Импорт Экспорт			чения 🕜					
E.	межсетевой экран >	Травила (177) И	сключения (0) Создать исключение						
\$	🖉 ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ 🗸 🗸	Фильтр			٩				
Ŗ	🔢 Правила и исключения								
Rø	🕞 Наборы сигнатур	ID							
L.		19900196	[4RAYS] TOOLS Chisel C&C connect v2		http	Ботнет		any	any
۲	Y KONTENTION WINDINGUN	19900195	[4RAYS] TOOLS Chisel C&C connect v1		http	Ботнет	alert 🗸	any	any
Æ	🕞 SSL-ИНСПЕКЦИЯ >	19900194	[4RAYS] MALWARE Ducktail Payload Download		http	Сетевой троян	alert 🗸	\$HOME_NET	\$EXTERNAL_
	🗄 внешние подключения 🗦	19900193	[4RAYS] MALWARE Ducktail Stealer C&C connect		http	Сетевой троян	alert v	\$HOME_NET	\$EXTERNAL_
	ОБЪЕКТЫ ПОЛИТИКИ >	19900192	[4RAYS] MALWARE Kryplod C&C connect		tcp	Ботнет	alert 🗸	\$HOME_NET	\$EXTERNAL_
	💿 справочники >	19900191	[4RAYS] MALWARE Kryplod C&C connect silent		tcp	Ботнет	alert 🗸	\$EXTERNAL_NET	\$HOME_NET
		19900190	[4RAYS] MALWARE Emotet payload retrieve		http	Сетевой троян	alert 🗸	\$HOME_NET	\$EXTERNAL_
Ŕ	вій шаблоны >				< 1	2 3 4	5 6 7	7 8 9 >	20 / c 🗸

Рис. 6.26. Слой политики «Предотвращение вторжений»

Администратору безопасности доступно включение и отключение применяемых сигнатур с возможностью редактирования самих правил. Для включения/отключения правил используйте переключатель (столбец **Состояние**).

В таблице Табл.6.16 представлено описание столбцов для каждой сигнатуры.

Табл. 6.16. Описание столбцов слоя «Предотвращение вторжений > Правила и исключения»

Название стобца	Описание						
ID	Идентификатор сигнатуры						
Наименование	Название сигнатуры						
Критичность	Уровень угрозы						
Протокол	Протокол, по которому была получена сигнатура						
Категория	Категория сигнатуры						
Действие	<ul> <li>Действие, которое будет выполняться IPS по обнаруженному трафику:</li> <li>alert – соединение с призывом обратить внимание администратора безопасности;</li> <li>drop – сброс соединения.</li> </ul>						
Источник	IP-адрес источника, например: any, \$HOME_NET, \$HTTP_SERVERS и др						
Порт источника	Порт источника запроса						
Назначение	IP-адрес назначения запроса, например: any, \$EXTERNAL_NET, \$SMTP_SERVERS и др						
Порт назначения	Порт назначения запроса						
Референс	Образец сигнатуры для распознавания IPS						
Тело сигнатуры	Текстовое значение, в котором содержится полное тело сигнатуры						

Для удобного просмотра сигнатур используйте поле **Фильтр**, с помощью него можно найти нужные сигнатуры по необходимым значениям параметров. Чтобы убрать фильтрацию и отобразить все имеющиеся сигнатуры, нажмите **Сбросить фильтр**.

Чтобы изменить состояние (Включить/Выключить) или действие (Изменить на alert/Изменить на drop) для определенных сигнатур, воспользуйтесь флажками слева

от столбца **ID**. При выборе сигнатуры автоматически выделяются остальные сигнатуры с идентичным идентификатором.

Также предусмотрена возможность создавать исключения из правил. Например, исключить сигнатуру для всех пользователей или исключить из фильтрации трафик пользователя. Это позволяет минимизировать число ложных срабатываний системы. Для таких случаев предусмотрено два способа настроить исключения:

- по ID-сигнатуры для отключения правила всем пользователям,
- по параметрам (Источнику, Назначению, Порту назначения) для отключения правила по IP-адресу источника запроса, IP-адресу назначения запроса и порту назначения.

Создать исключение		×
Включено		
Название	Исключить трафик для пользователя	
Комментарий	Заявка 1514	
Исключение на основе	Сетевых параметров	$\sim$
Источник	♥ 2.2.2.2 ×	
	IP-адрес или маска подсети IP/xx. Обязательно если не указаны остальные поля	
Назначение	♥ 8.8.8.×	
	IP-адрес или маска подсети IP/xx	
Порты назначения	Не задано	$\vee$
	Сохранить Отменить	

Рис. 6.27. Создание исключений «Системы предотвращения вторжений»

# В таблице Табл.6.17 перечислены атрибуты для формирования правил политики.

Табл. 6.17. Описание атрибутов слоя «Предотвращение вторжений»

Название атрибута	Описание
Название	Название сигнатуры
Комментарий	Дополнительные сведения о правиле
Исключение на основе	Выбор основы для создания исключения: сетевые параметры или ID сигнатуры (правила)
ID сигнатуры	Один или несколько идентификаторов сигнатур (правил)
	Примечание
	Доступно, если в поле <b>Исключение</b> на основе выбрано <b>ID сигнатур</b> (правил)

Название атрибута	Описание
Источник	IP-адрес источника. Запись в формате IP-адрес или маска подсети IP/хх
Назначение	IP-адрес назначения запроса. Запись в формате IP-адрес или маска подсети IP/xx
Порты назначения	Номер (диапазон номеров) портов ТСР и UDP

Созданные исключения будут отображаться на вкладке Исключения.

Пример решения задачи с помощью правил и исключений слоя **Предотвращение вторжений** приведен в разделе <u>6.6.3</u>.

Общие принципы работы с исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе <u>6.4.2</u>.

## 6.5.1.2.2. Наборы сигнатур

В разделе **Предотвращение вторжений > Наборы сигнатур** можно управлять сигнатурными наборами, чтобы своевременно получать обновления на новые угрозы безопасности.

Чтобы добавить новый набор сигнатур, нажмите одну из кнопок:

#### Примечание

В загружаемом файле не должно быть свыше 50000 сигнатур.

- Импорт сигнатур замена сигнатур (включая исключения, наборы и категории) из файла в формате JSON.
- Добавить набор добавление новых сигнатур из файла в формате JSON поверх уже существующих.

## Примечание

При добавлении новых наборов сигнатур необходимо импортировать файл **nips.rules**.

Перед добавлением сигнатур в систему убедитесь, что их синтаксис является корректным, а SID каждой сигнатуры уникален.

Если в файле с набором сигнатур есть закомментированные сигнатуры (строка начинается с символа #), они не будут добавлены в БД.

Нажмите кнопку Обновить категории, чтобы с помощью загрузки обновленного файла:

- Обновить информацию для тех категорий, для которых есть изменения в файле.
- Добавить новые категории из файла.

Категория сигнатур, у которых не указан параметр **classtype**, в системе будет определена как **unknown**. Чтобы такие сигнатуры работали корректно, добавьте новую категорию **unknown** с помощью кнопки **Обновить категории**.

Для корректной работы сигнатур их категории должны быть добавлены в Solar NGFW. В противном случае сигнатура работать не будет.

С помощью кнопки 🔲 можно настроить столбцы таблицы.

Чтобы загрузить файл со всеми наборами и категориями сигнатур, а также с информацией по ним, нажмите кнопку Экспорт сигнатур.

Чтобы удалить набор сигнатур, в строке с ним нажмите кнопку

<i>?</i>	Solar NGFW						Поиск перс	соны 🗦
۵	Настройки Импорт Экспорт	Политика / Предо	твоашение вторже	ний / Наборы сигна				Поименить политику
E	🔛 МЕЖСЕТЕВОЙ ЭКРАН 🗸 🗸	Экспорт сигнарто	Инпорт сигнатир	Обновить изтегории	Побренть набор			
\$		Skilopi chilaryp			Accentration			
₩.	🕼 Фильтр входящего трафика							
R <sub>w</sub>	🕼 Фильтр исходящего трафика	nips	35276	39		26.02.2024 14:23	admin	
La ba	Трансляция адресов	nips-rules-1				05.03.2024 15:26	admin	
۲	🖉 ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ 🗸 🗸							> 10 / стр. ∨
Æ	Правила и исключения							
	🕞 Наборы сигнатур							
	👻 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🗸 🗸							
	🙇 Доступ без аутентификации							
	<b>Вскрытие HTTPS</b>							
\$	🛞 Перенаправление по ІСАР							

Рис. 6.28. Слой политики «Предотвращение вторжений > Наборы сигнатур»

## 6.5.1.2.3. Описание категорий сигнатур IPS

#### Описание категорий сигнатур IPS представлено в таблице.

Табл.	6.18.	Описание	категорий	сигнатур	IPS
-------	-------	----------	-----------	----------	-----

Classtype сиг- натуры	Категория	Критичность	Описание
attempted-user	Получение при- вилегий пользо- вателя (попыт- ка)	Критично	Обнаружение активности, связанной с попыткой полу- чения привилегий пользователя (попытка атаки на по- вышение привилегий)
command-and- control	Ботнет		Обнаружение активности, связанной с управлением и контролем вредоносного ПО, организующего ботнет
credential-theft	Кража учетных данных		Обнаружение активности, связанной с возможной кра- жей учетных данных

Classtype сиг- натуры	Категория	Критичность	Описание
domain-c2	Домен ботнета		Обнаружение активности, связанной с доменами, ис- пользуемыми для обеспечения функционирования и распространения ботнета
exploit-kit	Эксплойт		Обнаружение активности, связанной с использованием ПО, эксплуатирующего уязвимости, их инфраструктурой (включая домены TDS) и доставкой
shellcode-detect	Исполняемый код		Обнаружение активности, связанной с использованием исполняемого кода
successful-admin	Получение при- вилегий адми- нистратора (успех)		Обнаружение активности, связанной с несанкциониро- ванным получением привилегий администратора (атака на повышение привилегий)
successful-recon- largescale	Масштабная утечка инфор- мации		Обнаружение активности, связанной с утечкой защища- емой информации, масштаб которой можно оценить как значительный или существенный
successful-user	Получение при- вилегий пользо- вателя (успех)		Обнаружение активности, связанной с несанкциониро- ванным получением привилегий пользователя (атака на повышение привилегий)
targeted-activity	Таргетирован- ная активность		Обнаружение активности, связанной с потенциальным проведением таргетированной (целенаправленной) атаки на защищаемые ресурсы
trojan-activity	Сетевой троян		Обнаружение активности, связанной с использованием сетевого трояна
unsuccessful- user	Получение при- вилегий пользо- вателя (неуда- ча)		Обнаружение активности, связанной с неуспешной по- пыткой получения привилегий пользователя (попытка атаки на повышение привилегий)
web-application- attack	Атака на веб- приложение		Обнаружение активности, связанной с проведением атак на защищаемые веб-приложения и веб-серверы
attempted-admin	Получение при- вилегий адми- нистратора (по- пытка)	Опасно	Обнаружение активности, связанной с попыткой полу- чения привилегий администратора (попытка атаки на повышение привилегий)
attempted-recon	Утечка инфор- мации (попыт- ка)		Обнаружение активности, связанной с попыткой дове- дения системы до состояния, при котором возможна утечка информации
coin-mining	Майнинг крипто- валюты		Обнаружение активности, связанной с добычей крипто- валюты (майнингом)
denial-of-service	DoS-атака		Обнаружение активности, связанной с проведением DoS-атаки (атака "Отказ в обслуживании") на защища- емые ресурсы
external-ip-check	Нелегитимный внешний IP-ад- рес		Обнаружение активности, связанной с несанкциониро- ванными попытками или успешным получением внеш- него IP-адреса устройством, не имеющим прав на него
misc-attack	Прочие атаки		Обнаружение активности, связанной с потенциальным проведением атаки на защищаемые ресурсы (проводи- мая атака не относится ни к одной другой категории)
network-scan	Сетевое скани- рование		Обнаружение активности, связанной с несанкциониро- ванным сканированием сети (может являться признаком разведывательного этапа готовящейся атаки)
non-standard- protocol	Нестандартный протокол		Обнаружение активности, связанной с использованием нестандартных протоколов или возникновением вне- штатных сетевых ситуаций (событий)

Classtype сиг- натуры	Категория	Критичность	Описание
policy-violation	Нарушение корпоративной конфиденциаль- ности		Обнаружение активности, связанной с любыми потен- циальными нарушениями корпоративной конфиденци- альности
rpc-portmap- decode	Декодирование RPC		Обнаружение активности, связанной с декодированием запроса RPC
social- engineering	Социальная инженерия		Обнаружение активности, связанной с потенциальным использованием методов и средств социальной инже- нерии (включая фишинг)
successful-recon- limited	Утечка инфор- мации (успех)		Обнаружение активности, связанной с утечкой защища- емой информации
s u s p i c i o u s - filename-detect	Подозритель- ное имя файла		Обнаружение активности, связанной с передачей фай- лов с подозрительным именем
suspicious-login	Обход аутенти- фикации		Обнаружение активности, связанной с попыткой входа с использованием подозрительного имени пользователя (логина)
s y s t e m - c a l l - detect	Системный вы- зов		Обнаружение активности, связанной с потенциальным использованием системных вызовов
unusual-client- port-connection	Нестандартный порт		Обнаружение активности, связанной с использованием нестандартного порта клиентом сети (узлом/приложе- нием/процессом)
web-application- activity	Уязвимое веб- приложение		Обнаружение активности, связанной с попыткой полу- чения доступа к защищаемому и потенциально уязви- мому веб-приложению
attempted-dos	DoS-атака (по- пытка)	Предупреждение	Обнаружение активности, связанной с попыткой осуще- ствить DoS-атаку (атака "Отказ в обслуживании"), кото- рая может привести к недоступности тех или иных сервисов
bad-unknown	Потенциально плохой трафик		Обнаружение активности, связанной с использованием потенциально плохого и нежелательного трафика
default-login- attempt	Взлом стан- дартного поль- зователя (по- пытка)		Обнаружение активности, связанной с попыткой входа с помощью стандартного имени пользователя (логина) и/или пароля
misc-activity	Прочая актив- ность		Обнаружение активности, не связанной ни с одной другой категорией и предположительно не являющейся атакой на защищаемые ресурсы (требует контроля)
not-suspicious	Неподозритель- ный трафик		Обнаружение активности, связанной с использованием нормального, но требующего контроля, трафика
protocol- command-decode	Декодирование команд общих протоколов		Обнаружение активности, связанной с попыткой деко- дирования команд общих протоколов
pup-activity	Нежелатель- ное ПО		Обнаружение активности, связанной с использованием потенциально нежелательного программного обеспече- ния
string-detect	Подозритель- ная строка		Обнаружение сетевой активности, связанной с наличи- ем подозрительных строк в передаваемом трафике
unknown	Неизвестный трафик		Обнаружение активности, связанной с неизвестным подозрительным трафиком, требующим аудита

#### 6.5.1.2.4. Просмотр статистики по предотвращению вторжений

Просмотреть информацию по работе сервиса можно в главном меню **Предотвращение вторжений**.

В таблице представлены:

- дата и время произошедшего события;
- предпринятое действие над ним;
- степень критичности сигнатуры;
- наименование сигнатуры;
- категория (класс угроз) сигнатуры;
- ID сигнатуры;
- используемый протокол;
- IP-адрес источника;
- ІР-адрес назначения запроса.

<b>*</b>	Solar NGFW							Поиск персоны	<b>J</b> ≓
ଜ	Предотвращени	е вторжени	й						
	Узел main			Действие Все 🗸 Критичность Лю	бая 🗸 Категория Любая,	Назначение ІР-адрес	: Порт Протс	кол Любой 🗸 Еще	v C
\$	Время	Действие К	(ритичность	ь Сигнатура	Категория	ID сигнатуры Протокол	Источник	Назначение	
Ŗ	04.03.2024 16:44	>>>		[4RAYS] Cobaltstrike beacon connect HTTP	solar-test	19900090 TCP	192.168.100.93:49169	193.161.193.99:33579	
$\mathbb{R}_{w}$	04.03.2024 16:44	<b>&gt;&gt;&gt;</b>		ET MALWARE Cobalt Strike Beacon Observed	#suricata.class.targeted-activity.help	2033713 TCP	192.168.100.93:49169	193.161.193.99:33579	
L.	04.03.2024 16:44	<b>&gt;&gt;&gt;</b>		ET POLICY DNS Query to a Reverse Proxy Service Observed	#suricata.class.policy-violation.help	2027941 UDP	192.168.100.93:64040	192.168.100.2:53	
۲	04.03.2024 16:44	200		[4RAYS] Cobaltstrike beacon connect HTTP	solar-test	19900090 TCP	192.168.100.93:49170	193.161.193.99:33579	
۲	04.03.2024 16:44	222		ET MALWARE Cobalt Strike Beacon Observed	#suricata.class.targeted-activity.help	2033713 TCP	192.168.100.93:49170	193.161.193.99:33579	
	04.03.2024 16:44	200		[4RAYS] Cobaltstrike beacon connect HTTP	solar-test	19900090 TCP	192.168.100.93:49169	193.161.193.99:33579	
	04.03.2024 16:44	200		ET MALWARE Cobalt Strike Beacon Observed	#suricata.class.targeted-activity.help	2033713 TCP	192.168.100.93:49169	193.161.193.99:33579	
	04.03.2024 16:44	222		ET POLICY DNS Query to a Reverse Proxy Service Observed	#suricata.class.policy-violation.help	2027941 UDP	192.168.100.93:64040	192.168.100.2:53	

Рис. 6.29. Статистика по работе Системы предотвращения вторжений

Для быстрого поиска информации по записям журнала воспользуйтесь фильтрами над таблицей. Для этого выберите из раскрывающегося списка или введите вручную значения

фильтров и нажмите **Обновить** . Часть фильтров доступна в раскрывающемся меню **Еще**: Источник, ID сигнатуры.

Если в разделе появляются непросмотренные уведомления о срабатывании сигнатуры, рядом со значком раздела **Предотвращение вторжений** будет отображена красная

точка –

# 6.5.1.3. Контентная фильтрация

Контентная фильтрация предназначена для контроля доступа пользователей к Интернетресурсам и защиты утечки конфиденциальной информации.

С помощью настройки правил и исключений слоя Контентная фильтрация можно решить следующие задачи:

- разрешать доступ без аутентификации к определенным ресурсам;
- вскрывать HTTPS-трафик для дальнейшего анализа;
- перенаправлять трафик по протоколу ІСАР для проверки антивирусом;
- настраивать фильтрацию запросов/ответов по содержимому запросов;
- блокировать загрузку файлов в режиме обратного прокси.

# 6.5.1.3.1. Доступ без аутентификации

Слой **Доступ без аутентификации** представляет собой набор правил исключения аутентификации, которые задаются для приложений и пользователей, не поддерживающих NTLM и/или Kerberos-аутентификацию, настроенную в системе. Этот слой необходим, чтобы разрешать доступ в интернет для неаутентифицированных пользователей и/или приложений.

Настройки Импорт Экспорт	Политика / Ко	нтентная фильт	рация / Доступ	без аутентификации 📀		Применить	политику
🔛 межсетевой экран >	Создать правило			Поиск по н	азванию, пе 🔍	Настройка	а колонок
💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🗸 🗸	Название	Источник	Назначение	Не аутентифицировать и П	ерсона Доп.	Вкл.	
🙇 Доступ без аутентификации	: Обновлен	10.2.20.28 10.3.20.26 10.3.20.33	Любое	Связать автоматически			0 t
🔐 Ескрытие HTTPS	ii Bce	Любой	Любое	Ничего не делать		•	Q Đ
🛞 Перенаправление по ІСАР							

Рис. 6.30. Слой правил политики «Доступ без аутентификации»

# В Табл.6.19 перечислены атрибуты для формирования правил политики.

Табл. 6.19. Описание атрибутов слоя «Доступ без аутентификации»

Название атрибута	Описание	Значение
	Осно	вные
Название	Название правила	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов
Комментарий	Дополнительные сведения о правиле	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов
Не аутентифицировать и	Действие, которое будет применено к объекту по ре- зультатам проверки условий правила	<ul> <li>Значение можно выбрать в раскрывающемся списке:</li> <li>Ничего не делать – Solar NGFW позволит настроить доступ к веб-ресурсу без аутентификации для источника запроса или ответа. Система сохранит источник как неавторизованного пользователя (веб-ресурс);</li> </ul>

Название атрибута	Описание	Значение
		<ul> <li>Связать с персоной автоматически – Solar NGFW выполнит следующие действия:</li> </ul>
		<ul> <li>определит IP-адрес источника запроса;</li> </ul>
		<ul> <li>выполнит поиск данного IP-адреса, сравнивая с данными персон из <b>Досье</b>. Если источник не будет найден, система сохранит его как неав- торизованного пользователя, а также предоста- вит доступ без аутентификации;</li> </ul>
		<ul> <li>Связать с персоной вручную (значение по умолчанию) – Solar NGFW сопоставит данные источника с данными персоны, указанной в правиле вручную администратором безопасности. При запросе доступа от источника система свяжет данные с персоной из Досье, а также предоставит ему доступ без аутентификации</li> </ul>
Персона	Персона из <b>Досье</b> , с кото- рой будет связана аутенти- фикация. Атрибут становит- ся видимым, если в правиле указано, что необходимо вручную связать данные о пользователе с персоной, существующей в системе. При выборе персоны автома- тически отобразится группа персон, в которой она состо- ит	Персона, выбираемая из <b>Досье</b> . В процессе ввода текста отображается список персон, совпадающих по введенном набору символов
Источник	Приложение, веб-браузер	Значение можно ввести вручную или выбрать в рас-
	инициировал соединение	<ul> <li>одиночный IP-адрес;</li> </ul>
		<ul> <li>диапазон IP-адресов;</li> </ul>
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		• «Любой» ( <i>значение по умолчанию</i> )
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в рас- крывающемся списке:
		<ul> <li>одиночный IP-адрес;</li> </ul>
		<ul> <li>диапазон IP-адресов;</li> </ul>
		<ul> <li>маска подсети IP-адресов;</li> </ul>
		• домен;
		• списки веб-ресурсов;
		• «Любое» ( <i>значение по умолчанию</i> )
	Дополни	тельные
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в рас- крывающемся списке:
		• HTTP;

Название атрибута	Описание	Значение
		• HTTPS;
		• FTP.
		Если значение не выбрано, при применении политики будут проверены все протоколы
Методы	Методы протоколов HTTP и FTP OVER HTTP	Значение можно ввести вручную или выбрать в рас- крывающемся списке:
		• CONNECT;
		• COPY;
		• DELETE;
		• GET;
		• HEAD;
		• LOCK;
		• MKCOL;
		• MOVE;
		• OPTIONS;
		• PATCH;
		• PROPPATCH;
		• POST;
		• PROPFIND;
		• PUT;
		• TRACE;
		• UNLOCK.
		Если значение не выбрано, при применении политики будут проверены все методы. Подробнее о методах см. в разделе Приложение D, Методы НТТР-прото- кола
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (меньше 65536), список или диапазон натураль- ных чисел. Можно выбрать не более 50 штук. Первое значение диапазона должно быть меньше, чем второе
Заголовки	Служебные заголовки паке- та данных	Значение можно выбрать в раскрывающемся списке. В этом списке отображены все условия на заголовки, сформированные в системе. Можно выбрать не более 50.
		Подробнее о заголовках см. в разделе 6.5.4.4

Пример решения задачи с помощью слоя **Доступ без аутентификации** приведены в разделе <u>6.6.4</u>.

Общие принципы работы с правилами этого слоя (копирование, редактирование и т.д.) описаны в разделе <u>6.4.2</u>.

# 6.5.1.3.2. Вскрытие HTTPS

Слой **Вскрытие HTTPS** представляет собой набор правил и исключений для расшифровки HTTPS-трафика с целью дальнейшей проверки. Если этот слой не сформирован, политику можно будет настраивать далее, и она будет работать. Но будут срабатывать только те правила и заданные в них условия, для которых не требуется вскрытие HTTPS.

Настройки Импорт Экспорт	Политика / Контентная фильт	грация / Вскрытие HTTPS 🕜	I	Применить политику
😫 межсетевой экран	Создать правило		Поиск по названию, пе Q	Настройка колонок
💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🕚	Количество Исключений 1 Колич	чество Правил (1)		Antes
🛕 Доступ без аутентификации	Название Источник Исключения - Трафик не вскрываетс	Назначение Заголовки ся	Когда и кем изменено	Вкл.
Вскрытие HTTPS	Не вскрывать Любой	🔁 Экономика, фин	admin 15.03.2022 16:00	<b>O</b> Ū Ū
🛞 Перенаправление по ICAP	Правила - Трафик вскрывается			
🕎 Фильтрация запросов 💮 🔅	🗄 Вскрытие HTTPS Любой	Любое	admin 09.03.2022 15:39	💿 Q Ö
🗘 Фильтрация ответов 🕘 🔅				

Рис. 6.31. Слой правил политики «Вскрытие HTTPS»

Для всех источников, указанных в правилах этого слоя, будет применено действие **Вскрыть HTTPS-трафик**. Это означает, что при использовании пользователем HTTPSпротокола Solar NGFW расшифрует весь передаваемый трафик для дальнейшей проверки и анализа. Для источников, указанных в исключениях этого слоя, расшифровка трафика выполняться не будет.

Для более подробного анализа контента перед формированием этого слоя необходимо использовать соответствующий сертификат, используемый для входящих соединений (подробнее см. в документе *Руководство по установке и настройке*).

## Примечание

При формировании правил и/или исключений этого слоя расширенные настройки не предусмотрены.

# В Табл.6.20 перечислены атрибуты для формирования правил и исключений.

Название атрибута	Описание	Значение
Название	Название правила и/или ис- ключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов
Источник	Пользователь, приложение, веб-браузер или иной источ- ник, который инициировал со- единение. Для источника, указанного в исключении, трафик расшифровываться не будет	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>Персона из Досье;</li> <li>Группа персон из Досье;</li> <li>Неаутентифицированный пользователь;</li> </ul>

Табл. 6.20. Описание атрибутов правил и исключений слоя «Вскрытие HTTPS»

Название атрибута	Описание	Значение
		<ul> <li>Одиночный IP-адрес или диапазон IP-адресов;</li> </ul>
		<ul> <li>Маска подсети IP-адресов;</li> </ul>
		• «Любой» ( <i>значение по умолчанию</i> )
Назначение	Адрес назначения запроса, отправленного источником	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		• Домен;
		• Списки веб-ресурсов;
		• Категория веб-ресурсов;
		• Одиночный IP-адрес или диапазон IP-адресов;
		<ul> <li>Маска подсети IP-адресов;</li> </ul>
		• «Любое» ( <i>значение по умолчанию</i> )
Заголовки	Служебные заголовки пакета	Значение можно выбрать в раскрывающемся списке.
	данных	В этом списке отображены все условия на заголовки, сформированные в системе. Можно выбрать не бо- лее 50.
		Подробнее о заголовках см. в разделе 6.5.4.4

Примеры решения задач с помощью правил и исключений слоя **Вскрытие HTTPS** приведены в разделе <u>6.6</u>:

- исключение вскрытия HTTPS-трафика пользователей <u>6.6.5;</u>
- блокировка загрузки ZIP-файлов по протоколу HTTPS 6.6.6.

Общие принципы работы с правилами этого слоя (копирование, редактирование и т.д.) описаны в разделе <u>6.4.2</u>.

# 6.5.1.3.3. Перенаправление по ІСАР

Слой **Перенаправление по ICAP** представляет собой набор правил и исключений, который предназначен для перенаправления трафика (запросов и ответов) внешнему источнику. Внешний источник может быть антивирусом, сторонней системой перехвата вебтрафика и т.д. Для перенаправления трафика в другие системы следует учитывать их специфику и выбирать соответствующее действие: **Передавать запросы**, **Передавать ответы**, **Передавать запросы и ответы**.

Настройки Импорт Экспорт	Политика / Контентная фильтрация / Перенаправление по ІСАР 📀	Применить политику
🗳 межсетевой экран >	Создать правило	Q Настройка колонок
😚 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🗸 🗸	Количество Исключений 0 Количество Правил 1	
🙇 Доступ без аутентификации	Название Действия ICAP-сервер Источник Назначение Доп Правила	Вкл.
🔓 Вскрытие HTTPS	🗄 ICAP 🥠 Local respinod Любой Любое	00
🛞 Перенаправление по ІСАР		

Рис. 6.32. Слой правил политики «Перенаправление по ICAP»

Перенаправление трафика необходимо в случае, если веб-страница или ее содержимое вызывают подозрение. Другими словами, если страница может содержать в себе вредоносные скрипты, файлы и т.д. Перенаправление трафика выполняется строго по протоколу ICAP (Internet Content Adaptation Protocol).

Например, веб-браузер передает адрес веб-страницы и запрашивает разрешение на доступ. Solar NGFW с помощью протокола ICAP перенаправляет запрос антивирусу для проверки, не является ли этот веб-адрес вредоносным. Если веб-адрес опасен, на экране пользователя отобразится страница блокировки (подробнее см. раздел <u>6.5.6</u>).

Для уведомления администратора о срабатывании проверки антивируса следует установить флажок **Уведомить**, указать адрес электронной почты или список адресов пользователей, которые будут оповещены, и соответствующий шаблон страницы. Внешний вид шаблона можно сформировать аналогично другим шаблонам в разделе **Политика > Шаблоны > Шаблоны страниц**.

При срабатывании правила система отправляет пользователю на электронную почту письмо с уведомлением.

В Табл.6.21 перечислены атрибуты для формирования правил и исключений.

Название атрибута	Описание	Значение
	Основ	ные
Название	Название правила и/или ис- ключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов
Действие	Действие, которое определя- ет, какой именно трафик систе- ма должна передавать	<ul> <li>Значение можно выбрать в раскрывающемся списке:</li> <li>Передавать запросы – Solar NGFW перенаправит поступающий запрос на указанный в правиле ICAP-сервер для проверки и анализа. ICAP-сервер необходимо выбрать из существующего списка;</li> <li>Передавать ответы – Solar NGFW перенаправит поступающий ответ на указанный в правиле ICAP-сервер для проверки и анализа. ICAP-сервер необходимо выбрать из существующего списка;</li> <li>Передавать запросы и ответы (<i>значение по умолчанию</i>) – Solar NGFW перенаправит поступающие запросы и ответы на указанный в правиле ICAP-сервер для проверки и анализа. ICAP-сервер необходимо выбрать из существующего списка;</li> <li>Передавать запросы и ответы (<i>значение по умолчанию</i>) – Solar NGFW перенаправит поступающие запросы и ответы на указанный в правиле ICAP-сервер для проверки и анализа. ICAP-сервер необходимо выбрать из существующего списка. Действие следует использовать только для перенаправления трафика Solar Dozor</li> </ul>
Имя сервера	Сервер, на который будет перенаправлен трафик (запросы и/или ответы) для проверки и анализа	Значение можно выбрать в раскрывающемся списке ( <i>по умолчанию не задано</i> ). Но если в раздел <b>Внешние подключения</b> был до- бавлен только один сервер, он будет значением по умолчанию

Табл. 6.21. Описание атрибутов правил и исключений слоя «Перенаправление по ICAP»

Название атрибута	Описание	Значение	
Шаблон блокировки	Шаблон страницы уведомле- ния или блокировки	Значение можно выбрать в раскрывающемся списке	
Уведомить	Действие, которое позволяет настроить отправку уведомле- ния пользователю о срабаты- вании правила слоя Перена- правление по ICAP	Флажок	
Источник	Пользователь, приложение, веб-браузер или иной источ- ник, который инициировал со- единение. Для источника, указанного в исключении, пе- ренаправление трафика (за- просов и/или ответов) выпол- няться не будет	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>Персона из Досье;</li> <li>Группа персон из Досье;</li> <li>Неаутентифицированный пользователь;</li> <li>Одиночный IP-адрес;</li> <li>Диапазон IP-адресов;</li> <li>Маска подсети IP-адресов;</li> <li>«Любой» (<i>значение по умолчанию</i>)</li> </ul>	
Назначение	Адрес назначения запроса	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>Домен;</li> <li>Списки веб-ресурсов;</li> <li>Категория веб-ресурсов;</li> <li>Одиночный IP-адрес;</li> <li>Диапазон IP-адресов;</li> <li>«Любое» (значение по умолчанию)</li> </ul> Примечание При указании нескольких диапазонов IP-адресов будет использоваться логическая операция «И», т.е. результатом операции будет пересечение этих диапазонов. При указании нескольких одиночных IP-адресов или масок подсетей IP-адресов будет использоваться операция «ИЛИ», т.е. результатом операции будет любое из указанных значений. При указании нескольких одиночных IP-адресов/масок подсетей IP-адресов вместе с диапазонами IP-адресов результатом операции будут любые IP-адреса/маски подсетей IP-адресов, входящие в пересечение указанных диапазонов.	
Дополнительные			

Название атрибута	Описание	Значение
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		• HTTP;
		• HTTPS;
		• FTP.
		Если значение не выбрано, при применении полити- ки будут проверены все протоколы
Методы	Методы протоколов HTTP и FTP OVER HTTP	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		• CONNECT;
		• COPY;
		• DELETE;
		• GET;
		• HEAD;
		• LOCK;
		• MKCOL;
		• MOVE;
		OPTIONS;
		• PATCH;
		• POST;
		• PROPFIND;
		• PROPPATCH;
		• PUT;
		• TRACE;
		• UNLOCK.
		Если значение не выбрано, при применении полити- ки будут проверены все методы. Подробнее о мето- дах см. в разделе <u>Приложение D, <i>Методы HTTP-</i> протокола</u>
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (менее 65536), список или диапазон натураль- ных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем вто- рое
Тип файлов	Поддерживаемые форматы файлов	Значение можно выбрать в раскрывающемся списке с помощью флажков (по умолчанию не задано). Можно выбрать несколько форматов файлов (не более 50)
Размеры файлов	Диапазон допустимых размеров файлов «от» и «до» (включительно)	Значение можно выбрать в раскрывающемся списке с помощью флажков
Единица измерения	Единица измерения файлов	Значение можно выбрать в раскрывающемся списке:
		<ul> <li>Б (байты);</li> </ul>

Название атрибута	Описание	Значение
		• КБ (килобайты);
		• МБ (мегабайты);
		• ГБ (гигабайты);
		• ТБ (терабайты).
		Единица измерения по умолчанию задается в мега- байтах

Пример решения задачи с помощью правил и исключений слоя **Перенаправление по ICAP** приведены в разделе <u>6.6.7</u>.

Общие принципы работы с правилами и/или исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе <u>6.4.2</u>.

6.5.1.3.4. Фильтрация запросов

## 6.5.1.3.4.1. Общие сведения

Слой **Фильтрация запросов** представляет собой набор правил и исключений для разрешения или запрета определенных типов запросов. Фильтрация может выполняться по содержимому запросов (например, источнику, HTTP-заголовкам, расширению файлов и т.д.).

Настройки Импорт Экспорт	Политика / Фильтрация запре	осов / Categories 🕐			Применить политику
😭 Ескрытие HTTPS	Создать правило		Поиск по названи	ю, пе Q	Настройка колонок
🛞 Перенаправление по ІСАР	Количество Исключений 🔍 Коли	ичество Правил 2			
🥎 Фильтрация запросов 💮 🗸	Название Действи Правила	ия Источник	Назначение	Доп.	Вкл.
Определение категорий	🗄 Запрет разработ_ 🛛 ጸ		Алкоголь, курение Веб-рошта	☆ <sup>1</sup>	0 0
: Categories			Вредоносное ПО, вирусы Запрещенные сайты		
🗄 Без авторизации 🕴			Криминал, мошенничество Поиск работы, карьера Половое воспитание		
Разрешено всем :			Порнография Сайты знакомств, брачные аг Социальные сети		
# Teams :			Шпионское ПО, спам Эротика, нудизм, интимная од		
🗘 Фильтрация ответов 🕀 🗦	Назработчики		Любое		I 💽 💿 🗊

Рис. 6.33. Слой правил политики «Фильтрация запросов»

## В Табл.6.22 перечислены атрибуты для формирования правил и исключений.

Табл. 6.22. Описание атрибутов правил и исключений слоя «Фильтрация запросов»

Название атрибута	Описание	Значение		
	Основные атрибуты			
Название	Название правила и/или ис- ключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов		
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов		
Действия				

Название атрибута	Описание	Значение
Основные	Основные Основные действия, которые будут применены к объекту после срабатывания правила	Значение можно выбрать в раскрывающемся списке:
		• «Ничего не делать» (значение по умолчанию);
		• Заблокировать;
		• Перенаправить;
		• Разрешить и не проверять дальше;
		• Разрешить через прокси-сервер;
		• Разрешить запрос;
		• Запросить подтверждение;
		• Проверить сертификат
Дополнительные	Дополнительные действия, которые будут применены к	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано):
	объекту после срабатывания правила	• Архивировать;
		• Добавить заголовки запроса;
		• Изменить заголовки запроса;
		• Не журналировать;
		• Определять категорию ресурса;
		• Определять тип данных;
		• Уведомить;
		• Добавить маркер в журнал;
		<ul> <li>Добавить уведомление для WS/WSS</li> </ul>
	Услов	вия
Источник	Пользователь, приложение, веб-браузер или иной источ-	Значение можно ввести вручную или выбрать в раскрывающемся списке:
	ник, которыи инициировал со- единение. Для источника,	• Персона из <b>Досье</b> ;
	указанного в исключении, фильтрация запросов выпол-	• Группа персон из <b>Досье</b> ;
	няться не будет	• Неаутентифицированный пользователь;
		<ul> <li>Одиночный IP-адрес;</li> </ul>
		<ul> <li>Диапазон IP-адресов;</li> </ul>
		<ul> <li>Маска подсети IP-адресов;</li> </ul>
		• «Любой» ( <i>значение по умолчанию</i> )
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		• Домен;
		• Списки веб-ресурсов;
		• Категория веб-ресурсов;

Название атрибута	Описание	Значение
		<ul> <li>Одиночный IP-адрес;</li> </ul>
		<ul> <li>Диапазон IP-адресов;</li> </ul>
		<ul> <li>Маска подсети IP-адресов;</li> </ul>
		• «Любое» ( <i>значение по умолчанию</i> )
	Дополнительн	ые атрибуты
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		• HTTP;
		• HTTPS;
		• FTP.
		Если значение не выбрано, при применении полити- ки будут проверены все протоколы
Методы	Методы протоколов HTTP и FTP OVER HTTP	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		• CONNECT;
		• COPY;
		• DELETE;
		• GET;
		• HEAD;
		• LOCK;
		• MKCOL;
		• MOVE;
		OPTIONS;
		• PATCH;
		• POST;
		PROPFIND;
		• PROPPATCH;
		• PUT;
		• TRACE;
		• UNLOCK.
		Если значение не выбрано, при применении полити- ки будут проверены все методы. Подробнее о мето- дах см. в разделе <u>Приложение D, <i>Методы НТТР-</i> протокола</u>
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (меньше 65536), список или диапазон нату- ральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем вто- рое

Название атрибута	Описание	Значение	
Заголовки	Служебные заголовки пакета данных	Значение можно выбрать в раскрывающемся списке В этом списке отображены все условия на заголовки сформированные в системе. Можно выбрать не бо- лее 50.	
		Подробнее о заголовках см. в разделе <u>6.5.4.4</u>	
Тип файлов	Поддерживаемые форматы файлов	Значение можно выбрать в раскрывающемся списке с помощью флажков (по умолчанию не задано). Можно выбрать несколько форматов файлов (не более 50)	
Размеры файлов	Диапазон допустимых разме- ров файлов «от» и «до» (включительно)	Значение можно выбрать в раскрывающемся списке с помощью флажков	
Единица измерения	Единица измерения файлов	Значение можно выбрать в раскрывающемся списке:	
		• Б (байты);	
		• КБ (килобайты);	
		• МБ (мегабайты);	
		• ГБ (гигабайты);	
		• ТБ (терабайты).	
		Единица измерения по умолчанию задается в мега- байтах	
Ключевые слова	Условия проверки ключевых слов	Значение можно выбрать в раскрывающемся списке, который содержит перечень значений из справочни- ка Ключевые слова.	
		Подробнее о ключевых словах см. в разделе <u>6.5.5.2</u>	
Спорогом	Суммарный вес всех найден- ных ключевых слов (или одно- го, если установлен флажок Игнорировать повторы фраз), по достижению которо- го к объекту будет применено действие, указанное в прави- ле. Атрибут становится види- мым только после указания значения атрибута Ключевое слово	Значение можно ввести вручную: целое число	
Игнорировать повторы фраз	Определяет необходимость учета каждого слова только один раз (независимо от часто- ты его появления в тексте). Атрибут становится видимым только после указания значе- ния атрибута Ключевое сло- во	Опция (включена/выключена)	
Использовать внешние распаковщики	Определяет необходимость использования Tika-сервера для распаковки данных. Атрибут становится видимым только после указания значе- ния атрибута Ключевое сло- во	Опция (включена/выключена)	
тами HTML-разметки	поиска ключевых слов вместе	Опция (включена/выключена)	

Название атрибута	Описание	Значение
	с элементами HTML-разметки. Атрибут становится видимым только после указания значе- ния атрибута Ключевое сло- во	
Расписания	Расписание выполнения пра- вила	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе объектов политики <b>Расписания</b> . Можно выбрать не более 20. Подробнее о расписаниях см. в разделе <u>6.5.4.3</u>
Лимиты трафика	Разрешаемый объем переда- ваемого трафика	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе объектов политики <b>Лимиты трафика</b> . Можно вы- брать не более 4. Подробнее о лимитах трафика см. в разделе <u>6.5.4.2</u>

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в <u>Табл.6.23</u>.

# Табл. 6.23. Описание действий

Название действия	Описание
	Основные
Ничего не делать	Solar NGFW не предпринимает никаких действий.
Заблокировать	Solar NGFW заблокирует доступ к запрашиваемому ресурсу, файлу и т. д. Для этого действия выберите шаблон блокировки из существующего списка.
	Примечание
	Из-за особенностей сервиса шаблон блокировки в некоторых случаях может не отображаться.
	Возможны следующие случаи блокировки:
	<ul> <li>при переходе пользователя по вредоносной ссылке в браузер будет отобра- жена страница блокировки;</li> </ul>
	• при попытке скачать вредоносный файл загрузка будет приостановлена;
	<ul> <li>при обращении приложения за доступом к ресурсам Solar NGFW заблокирует ему доступ.</li> </ul>
	При передаче данных по шифрованному каналу, например, при использовании протокола HTTPS, шаблон блокировки страниц не используется.
Запросить подтверждение	В браузере пользователя отобразится веб-страница или окно с запросом на подтверждение доступа:
	• для согласия пользователь нажимает кнопку Да и переходит на веб-ресурс;
	<ul> <li>для отказа пользователь нажимает кнопку Нет. Веб-браузер возвращается к предыдущей странице. Если это была первая открытая страница или вкладка, следует ее закрыть.</li> </ul>
	Для этого действия выберите шаблон для подтверждения доступа из существу- ющего списка.

Название действия	Описание	
Перенаправить	Solar NGFW перенаправит запрос на указанный в правиле URL страницы веб- ресурса, который необходимо ввести вручную. Для передачи параметров запроса установите флажок <b>Сохранить параметры запроса</b> .	
Разрешить и не проверять дальше	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом. Проверка трафика политикой будет остановлена. Для этого действия укажите URL страницы веб-ресурса.	
Разрешить через прокси- сервер	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом через вышестоящий прокси-сервер, указанный в правиле. Выберите прокси- сервер из существующего списка. Действие применяется, если Solar NGFW взаимодействует с другими системами контроля веб-трафика.	
Разрешить запрос	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом. Для этого действия укажите URL страницы веб-ресурса.	
Проверить сертификат	Solar NGFW проверит наличие установленного сертификата для вскрытия HTTPS-трафика (подробнее см. в разделе <u>6.5.1.3.4.2</u> )	
Дополнительные		
Архивировать	Solar NGFW сформирует email (сообщение электронной почты) и поместит в него запрос. Далее система отправляет это сообщение в Solar Dozor для хранения.	
Добавить заголовки запро- са	При обработке HTTP-трафика Solar NGFW добавит заголовки запросов. Для этого действия выберите шаблон для добавления заголовка из списка шаблонов, настроенных ранее.	
Изменить заголовки запро- са	При обработке HTTP-трафика Solar NGFW изменит заголовки запросов. Для этого действия выберите шаблон для изменения заголовка из списка шаблонов, настроенных ранее.	
Не журналировать	Данные о действиях пользователей в системе не будут зарегистрированы в Журнале запросов Solar NGFW.	
Определять категорию ре- сурса	Solar NGFW определит категорию ресурса с помощью встроенного категориза- тора. Эта категория будет записана в <b>Журнал запросов</b> . Просмотреть, экспор- тировать и импортировать базы категоризации можно в разделе Политика > База категоризации.	
Определять тип данных	Solar NGFW определит MIME-тип данных запроса. Тип данных будет записан в Журнал запросов. Это действие не будет поддерживаться при использовании протокола HTTPS.	
Уведомить	Solar NGFW отправит email (сообщение электронной почты) о каком-либо дей- ствии, произошедшем в системе. Это уведомление получат администраторы безопасности, чьи адреса электронной почты указаны в правиле. Для этого действия выберите шаблон страницы уведомления из существующего списка или создайте свой.	
Удалить заголовки запроса	При обработке HTTP-трафика Solar NGFW изменит заголовки запросов. Для этого действия выберите шаблон для удаления заголовка из списка шаблонов, настроенных ранее.	
Добавить маркер в журнал	При срабатывании правила действие добавляет указанный маркер в <b>Журнал</b> запросов.	
Добавить уведомление для WS/WSS	При срабатывании правила в браузере будет показано уведомление о неудачной попытке подключения по протоколам WebSocket или WebSocket Secure.	
	Если совместно с дополнительным действием были выбраны основные действия Ничего не делать, Разрешить и не проверять дальше, Разрешить запрос, Запросить подтверждение или Проверить сертификат, при WS/WSS-соеди- нении уведомление будет показано, только если есть неисправности в работе протоколов WebSocket или WebSocket Secure со стороны ресурса.	

Название действия	Описание
	Примечание
	Работа основных действий Заблокировать и Перенаправить совместно с дополнительным действием Добавить уведомление для WS/WSS невозможна.

Примеры решения задач с помощью правил и исключений слоя **Фильтрация** запросов приведены в разделе <u>6.6</u>:

- управление фильтрацией запросов пользователей (см. раздел 6.6.8);
- блокировка загрузки содержимого черновиков в ОWA в режиме обратного прокси (см. раздел <u>6.6.10</u>);
- блокировка загрузки писем с запрещенными файлами в OWA в режиме обратного прокси (см. раздел <u>6.6.11</u>).

Общие принципы работы с правилами и/или исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе <u>6.4.2</u>.

# 6.5.1.3.4.2. Проверка наличия сертификата

Проверка на наличие сертификата для вскрытия HTTPS-трафика происходит при активном действии **Проверить сертификат** правил слоя **Фильтрация запросов**.

Для доступа к веб-ресурсу при отсутствии установленного сертификата пользователю будет предложена инструкция по его установке.

Страницу с инструкцией можно выбрать из двух вариантов:

• по умолчанию;

Страница по умолчанию содержит инструкции по установке сертификата для различных операционных систем. При нажатии на значок нужной операционной системы отобразится соответствующая инструкция.

• внешний ресурс (необходимо указать URL страницы).

## Примечание

Для корректной работы страницу внешнего ресурса необходимо добавить в исключения слоя **Вскрытие** 

При обращении к веб-ресурсу с префиксом HTTPS в URL в браузере отобразится сообщение о небезопасном соединении. В этом случае, чтобы перейти на страницу с инструкцией по установке сертификата необходимо согласиться с угрозой безопасности.
# Внимание!

Для более надежной работы механизма перенаправления пользователя на страницу с инструкцией по установке сертификата, настоятельно рекомендуется добавить в поле **На**значение правила проверки сертификата список ресурсов, содержащий следующее регулярное выражение:

(.\*/\$|.\*html\??|.\*/[^\.]\*\$|.\*search.\*)

#### 6.5.1.3.5. Фильтрация ответов

Слой **Фильтрация ответов** представляет собой набор правил и исключений для разрешения или запрета определенных типов ответов. Фильтрация может выполняться по содержимому ответов (например, назначению, ключевым словам, лимитами трафика и т.д.).

Настройки Импорт Экспорт	Политика / Фильтрация ответов / Лимиты YouTube 🔞		Применить политику
🔛 МЕЖСЕТЕВОЙ ЭКРАН 🔶	Создать правило	Поиск по названию, пе ۹	Настройка колонок
💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🗸 🗸	Количество Исключений 0 Количество Правил 1		
Доступ без аутентификации	Название Действия Источник Назначение Правила	Когда и кем изменено Доп.	Вкл.
🔐 Вскрытие HTTPS	🗄 Лимиты YouTube 😵 Любой 🃮 block YouTube	admin 5.03.2022 16:29	💽 🗍 Ū
🛞 Перенаправление по ІСАР			
Фильтрация запросов			
🗘 Фильтрация ответов 🕘 🗸			
: Общая политика (ответы) 🕴 🚦			
🗄 Лимиты YouTube 🔅			

Рис. 6.34. Слой правил политики «Фильтрация ответов»

# В Табл.6.24 перечислены атрибуты для формирования правил и исключений.

Табл. 6.24. Описание атрибутов правил и исключений слоя «Фильтрация ответов»

Название атрибута	Описание	Значение
	Основные а	атрибуты
Название	Название правила и/или ис- ключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 500 симво- лов
	Дейст	вия
Основные	Основные действия, которые будут применены к объекту	Значение можно выбрать в раскрывающемся списке:
	после срабатывания правила	<ul> <li>«Ничего не делать» (значение по умолчанию);</li> </ul>
		• Заблокировать;
		• Перенаправить;
		• Разрешить и не проверять дальше;

Название атрибута	Описание	Значение
		• Разрешить через прокси-сервер
Дополнительные	Дополнительные действия, которые будут применены к	Значение можно выбрать в раскрывающемся списке (по умолчанию не задано):
	объекту после срабатывания правила	• Добавить заголовки ответа;
		• Изменить заголовки ответа;
		• Не журналировать;
		• Определять категорию ресурса;
		• Определять тип данных;
		• Уведомить;
		• Удалить заголовки ответа;
		• Добавить маркер в журнал;
		<ul> <li>Добавить уведомление для WS/WSS</li> </ul>
	<u> </u> Услов	<u> </u>
Источник	Пользователь, приложение, веб-браузер или иной источ-	Значение можно ввести вручную или выбрать в раскрывающемся списке:
	ник, который инициировал со- единение. Для источника, указанного в исключении, фильтрация запросов выпол- няться не будет	<ul> <li>Персона из Досье;</li> </ul>
		• Группа персон из <b>Досье</b> ;
		• Неаутентифицированный пользователь;
		<ul> <li>Одиночный IP-адрес;</li> </ul>
		<ul> <li>Диапазон IP-адресов;</li> </ul>
		<ul> <li>Маска подсети IP-адресов;</li> </ul>
		• «Любой» ( <i>значение по умолчанию</i> )
Назначение	Адрес назначения ответа	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>Одиночный IP-адрес;</li> </ul>
		<ul> <li>Диапазон IP-адресов;</li> </ul>
		<ul> <li>Маска подсети IP-адресов;</li> </ul>
		• Домен;
		<ul> <li>Списки веб-ресурсов;</li> </ul>
		<ul> <li>Категория веб-ресурсов;</li> </ul>
		• «Любое» ( <i>значение по умолчанию</i> )
	Дополнительн	ые атрибуты
Протокол	Протокол передачи данных	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>HTTP;</li> </ul>

Название атрибута	Описание	Значение	
		HTTPS;	
		• FTP.	
		Если значение не выбрано, при применении полити- ки будут проверены все протоколы	
Методы	Методы протоколов HTTP и FTP OVER HTTP	Значение можно ввести вручную или выбрать в раскрывающемся списке:	
		• CONNECT;	
		• COPY;	
		• DELETE;	
		• GET;	
		• HEAD;	
		• LOCK;	
		• MKCOL;	
		• MOVE;	
		• OPTIONS;	
		• PATCH;	
		• PROPPATCH;	
		• POST;	
		• PROPFIND;	
		• PUT;	
		• TRACE;	
		• UNLOCK.	
		Если значение не выбрано, при применении полити- ки будут проверены все методы. Подробнее о мето- дах см. в разделе <u>Приложение D, <i>Методы HTTP-</i> протокола</u>	
Порты	Номер (диапазон номеров) портов TCP, включенных в URL-адреса запросов	Число (меньше 65536), список или диапазон натуральных чисел. Можно выбрать не более 50. Первое значение диапазона должно быть меньше, чем второе	
Заголовки	Служебные заголовки пакета данных	Значение можно выбрать в раскрывающемся списке. В этом списке отображены все условия на заголовки, сформированные в системе. Можно выбрать не бо- лее 50.	
		Подробнее о заголовках см. в разделе <u>6.5.4.4</u>	
Тип файлов	Поддерживаемые форматы файлов	Значение можно выбрать в раскрывающемся списке с помощью флажков (по умолчанию не задано). Можно выбрать несколько форматов файлов (не более 50)	
Файлы	Условие проверки файлов	Значение можно выбрать в раскрывающемся списке, который содержит перечень значений из справочни- ка <b>Файлы</b> .	

Название атрибута	Описание	Значение	
		Подробнее о атрибутах файлов х см. в разделе <u>6.5.5.5</u>	
Размеры файлов	Диапазон допустимых разме- ров файлов «от» и «до» (включительно)	Значение можно выбрать в раскрывающемся списке с помощью флажков	
Единица измерения	Единица измерения файлов	Значение можно выбрать в раскрывающемся списке:	
		<ul> <li>Б (байты);</li> </ul>	
		• КБ (килобайты);	
		<ul> <li>МБ (мегабайты);</li> </ul>	
		• ГБ (гигабайты);	
		• ТБ (терабайты).	
		Единица измерения по умолчанию задается в мега- байтах	
Ключевые слова	Условия проверки ключевых слов	Значение можно выбрать в раскрывающемся списке, который содержит перечень значений из справочни- ка Ключевые слова.	
		Подробнее о ключевых словах см. в разделе <u>6.5.5.2</u>	
Спорогом	Суммарный вес всех найден- ных ключевых слов (или одно- го, если установлен флажок Игнорировать повторы фраз), по достижению которо- го к объекту будет применено действие, указанное в прави- ле. Атрибут становится види- мым только после указания значения атрибута Ключевое слово	Значение вводится вручную: целое число	
Игнорировать повторы фраз	Определяет необходимость учета каждого слова только один раз (независимо от часто- ты его появления в тексте). Атрибут становится видимым только после указания значе- ния атрибута Ключевое сло- во	Опция (включена/выключена)	
Использовать внешние распаковщики	Определяет необходимость использования Тіка-сервера для распаковки данных. Атрибут становится видимым только после указания значе- ния атрибута Ключевое сло- во	Опция (включена/выключена)	
Искать вместе с элемен- тами HTML-разметки Расписания	Определяет необходимость поиска ключевых слов вместе с элементами HTML-разметки. Атрибут становится видимым только после указания значе- ния атрибута Ключевое сло- во Расписание выполнения пра-	Опция (включена/выключена) Значение можно выбрать в раскрывающемся списке	
	вила	который содержит перечень созданных в системе	

Название атрибута	Описание	Значение
		объектов политики <b>Расписания</b> . Можно выбрать не более 20.
		Подробнее о расписаниях см. в разделе 6.5.4.3
Лимиты трафика	Разрешаемый объем переда- ваемого трафика	Значение можно выбрать в раскрывающемся списке, который содержит перечень созданных в системе объектов политики <b>Лимиты трафика</b> . Можно выбрать не более 4.
		Подробнее о лимитах трафика см. в разделе <u>6.5.4.2</u>

Перечень действий, которые можно использовать при формировании правила или исключения, приведены в <u>Табл.6.25</u>.

Табл.	6.25.	Описание	действи	Й
100711	0.201	onnounno	Housiph	

Название действия	я Описание					
	Основные					
Ничего не делать	Solar NGFW не предпринимает никаких действий					
Заблокировать	Solar NGFW заблокирует доступ к запрашиваемому веб-ресурсу, файлу и т.д. Для этого действия необходимо выбрать шаблон блокировки из существующего списка. Возможны следующие случаи блокировки:					
	<ul> <li>при переходе пользователя по вредоносной ссылке в браузер будет отобра- жена страница блокировки;</li> </ul>					
	• при попытке скачать вредоносный файл загрузка будет приостановлена;					
	<ul> <li>при обращении приложения за доступом к ресурсам Solar NGFW заблокирует ему доступ.</li> </ul>					
	При передаче данных по шифрованному каналу, например, при использовании протокола HTTPS, шаблон блокировки страниц не используется					
Перенаправить	Solar NGFW перенаправит ответ на указанный в правиле URL страницы веб- ресурса, который следует ввести вручную. Для передачи параметров запроса следует установить флажок <b>Сохранить параметры запроса</b>					
Разрешить и не проверять дальше	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом. Проверка трафика политикой будет остановлена. Для этого действия необходимо указать URL страницы веб-ресурса					
Разрешить через прокси- сервер	Solar NGFW разрешит соединение источника с запрашиваемым веб-ресурсом через вышестоящий прокси-сервер, указанный в правиле. Прокси-сервер необ- ходимо выбрать из существующего списка. Действие применяется в случае, если Solar NGFW взаимодействует с другими системами контроля веб-трафика					
	Дополнительные					
Добавить заголовки ответа	При обработке HTTP-трафика Solar NGFW добавит заголовки ответов. Для этого действия необходимо выбрать шаблон для добавления заголовка из списка шаблонов, настроенных ранее					
Изменить заголовки ответа	При обработке HTTP-трафика Solar NGFW изменит заголовки ответов. Для этого действия необходимо выбрать шаблон для изменения заголовка из списка шаблонов, настроенных ранее					
Не журналировать	Данные о действиях пользователей в системе не будут зарегистрированы в <b>Журнале запросов</b> Solar NGFW					
Определять категорию ре- сурса	Solar NGFW определит категорию ресурса с помощью встроенного категориза- тора. Эта категория будет записана в <b>Журнал запросов</b> . Для просмотра, экс- порта и импорта базы категоризации следует в разделе Политика > База кате- горизации					

Название действия	Описание
Определять тип данных	Solar NGFW определит MIME-тип данных ответа. Тип данных будет записан в Журнал запросов. Это действие не будет поддерживаться при использовании протокола HTTPS
Уведомить	Solar NGFW отправит email (сообщение электронной почты) о каком-либо дей- ствии, произошедшем в системе. Это уведомление получат администраторы безопасности, чьи адреса электронной почты указаны в правиле. Для этого действия необходимо выбрать шаблон страницы уведомления из существующего списка или создать свой
Удалить заголовки ответа	При обработке HTTP-трафика Solar NGFW изменит заголовки ответов. Для этого действия необходимо выбрать шаблон для удаления заголовка из списка шаблонов, настроенных ранее
Добавить маркер в журнал	При срабатывании правила действие добавляет указанный маркер в <b>Журнал</b> запросов

Примеры решения задач с помощью правил и исключений слоя **Фильтрация ответов** приведены в разделе <u>6.6</u>:

- управление фильтрацией ответов пользователей (см. раздел <u>6.6.9</u>);
- блокировка загрузки содержимого черновиков в ОWA в режиме обратного прокси (см. раздел <u>6.6.10</u>);
- блокировка загрузки писем с запрещенными файлами в OWA в режиме обратного прокси (см. раздел <u>6.6.11</u>).

Общие принципы работы с правилами и/или исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе <u>6.4.2</u>.

# 6.5.2. SSL-инспекция

Раздел позволяет просматривать и управлять политикой инспекции зашифрованного трафика, чтобы анализировать, расшифровывать и проверять трафик.

#### 6.5.2.1. Правила расшифровки

Слой **Правила расшифровки** представляет собой набор правил и исключений для расшифровки и инспекции SSL/TLS-трафика для гибкого управления политикой инспекции зашифрованного трафика и своевременного выявления скрытых угроз.

1	Solar NGFW					Поиск	персоны
ଜ	Настройки Импорт Экспорт		ция / Правила расшифрог	вки 🕜			Применить политику
E	🔛 межсетевой экран >	Правила Исключен	ия				
8	2 <sup>®</sup> предотвращение вторжений >	Создать правило Название					Действия
~	💝 контентная фильтрация >	: 1.example	admin 25 12 2024 4 34 35	V 1.1.1.1	<b>?</b> 1.1.1.2	Автоматически	<u>c</u> 2 8
0 22	🔓 SSL-ИНСПЕКЦИЯ 🗸 🗸	1 Строка					< 1 > 10 / стр. у
*	🚱 Правила расшифровки						
Æ	😫 внешние подключения 🗸 🗸						
	ІСАР-серверы						
	Прокси-серверы						
	ОБЪЕКТЫ ПОЛИТИКИ						
	Списки IP-адресов						
\$	Лимиты трафика						

Рис. 6.35. Слой правил политики «Правила расшифровки»

С помощью кнопки 🔲 можно настроить столбцы таблицы:

- Название (обязательный столбец),
- Комментарий,
- Кто и когда изменил,
- Источник (обязательный столбец),
- Назначение,
- Входящий интерфейс,
- Способ определения SSL/TLS.
- В Табл.6.26 перечислены атрибуты для формирования правил и исключений.

Табл. 6.26. Описание атрибутов правил и исключений слоя «Правила расшифровки»

Название атрибута	Описание	Значение
Название	Название правила и/или ис- ключения	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 50 симво- лов
Приоритет	Порядок обработки правила	В процессе обработки политики каждый слой правил политики проверяется последовательно: сверху- вниз. Правила и/или исключения проверяются ана- логичным образом — сначала проверяются исклю- чения, а потом уже правила. Чтобы упорядочить правила по приоритетам, при создании/редактиро- вании соответствующего правила в поле установите его приоритет с помощью цифрового значения, на- чиная с 1. Более подробно описано в разделе <u>6.2</u> .
Источник	Источник, который иницииро- вал соединение	<ul> <li>Значение можно ввести вручную или выбрать в раскрывающемся списке:</li> <li>Одиночный IP-адрес;</li> <li>Диапазон IP-адресов;</li> </ul>

Название атрибута	Описание	Значение
		<ul> <li>Маска подсети IP-адресов;</li> </ul>
		• «Любой» ( <i>значение по умолчанию</i> )
Назначение	Адрес назначения запроса	Значение можно ввести вручную или выбрать в раскрывающемся списке:
		<ul> <li>Одиночный IP-адрес;</li> </ul>
		<ul> <li>Диапазон IP-адресов;</li> </ul>
		<ul> <li>Маска подсети IP-адресов;</li> </ul>
		• Домен;
		• Списки веб-ресурсов;
		• «Любой» (значение по умолчанию)
Входящий интерфейс	Сетевой интерфейс	Значение можно выбрать в раскрывающемся списке с созданными ранее сетевыми интерфейсами. На-пример: <i>eth0</i> .
Способ определения	Способ определения	Значение можно выбрать в раскрывающемся списке:
SSL/ILS	SSL/TLS-трафика	• По портам;
		• Автоматическое определение
HTTPS	Порт для определения	Целое числовое значение от 0 до 65535. Поле до-
SMTPS	ISSL/TLS-трафика	ступно, только если для параметра Способ опреде-
POPS		
IMAPS		
DoT		
Комментарий	Дополнительные сведения о правиле и/или исключении	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 симво- лов

Общие принципы работы с правилами и/или исключениями этого слоя (копирование, редактирование и т.д.) описаны в разделе <u>6.4.2</u>.

# 6.5.3. Внешние подключения

# 6.5.3.1. ІСАР-серверы

При фильтрации информации может проводиться проверка на наличие вирусов в передаваемых файлах. Для выполнения такой проверки Solar NGFW перенаправляет трафик внешнему источнику (например, серверу с установленным антивирусным ПО или внешней системе перехвата веб-трафика, такой как, например, Dozor Traffic Analyzer). При этом взаимодействие с внешним источником происходит только по протоколу ICAP.

Данная версия Solar NGFW имеет свой собственный модуль антивируса, который обеспечивает защиту интернет-трафика по протоколам HTTP/FTP/HTTPS, поиск и обезвреживание угроз. Настройки ICAP-серверов антивируса в разделе **Политика** доступны только для чтения. Подробная информация о настройках антивируса приведена в документе *Руководство по установке и настройке*. Также поддерживается антивирусное ПО Symantec Scan Engine 5.1 и выше, DrWeb версии 4.44 и выше, Kaspersky Antivirus версии 5.5 и выше и ClamAv версии 0.93 и выше.

Управление ICAP-серверами выполняется в разделе **Политика > Внешние подключения > ICAP-серверы** (<u>Рис.6.36</u>). Все внешние подключения расположены в виде списков (каждый в своем разделе). Информация по каждому элементу списка представлена в виде таблицы с соответствующим набором столбцов.

<i>*</i> *	Solar NGFW		Настро дост	ики ICAP-серверс гупны только для	в антивируса просмотра	Поиск случае г	по разделу (в данном ю имени ICAP-сервер	a)
ራ	Настройки Импорт	Экспорт		ика / Внешние подключ	ения / ІСАР-сереры 🕜		Примен	ить политику
	🔛 МЕЖСЕТЕВОЙ ЭКРАН		Доба	вить ІСАР-сервер Импорт	Экспорт		Поиск по имени сервера	۹
\$	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ		-	Имя сервера	URL	Комментарий	Создан Изменен	
¥	🖶 внешние подключения		Ĥ	Local reqmod	icap://localhost:1344/reqmod		14.03.2022 14:56	
R.	ІСАР-серверы		-	Local respmod	icap://localhost:1344/respmod		14.03.2022 14:56	
-	Происи-серверы			ІСАР в Дозоре	icap://10.201.28.111.1344	test	admin 15.03.2022 16:44	00
26	пролен серверы			ICAP1	icap://10.200.28.10:1344		admin 15.03.2022 16:44	00
(H	🛞 объекты политики			ICAP2	icap://10.201.28.185:1344		admin 15.03.2022 16:45	00
	СПРАВОЧНИКИ			ICAP сторонний	icap://10.201.29.133		admin 15.03.2022 16:45	00
	🗳 шаблоны							
	🆄 БАЗА КАТЕГОРИЗАЦИИ							

Общие принципы работы с ІСАР-серверами приведены в разделе 6.4.3.

Рис. 6.36. Раздел «Политика > Внешние подключения > ICAP-серверы»

Для добавления ICAP-сервера необходимо:

- 1. Нажать кнопку Добавить ІСАР-сервер.
- 2. Указать необходимые значения (см. Табл.6.27).

Табл.	6.27.	Перечень	атрибутов	для добавления	ІСАР-сервера
raor.	0.27.	перечены	alphoylob	для дооавления	юлі -сервера

Название	Описание	Значение
Имя сервера	Название ІСАР-сервера	Вводиммый вручную текст. Максимальный размер введенного текста не должен превышать 200 символов
ICAP URL	URL-адрес ICAP-сервера	<ul> <li>URL указывается в формате</li> <li>ICAP://<host>:<port>/ или ICAP://<host>/, где:</host></port></host></li> <li><host> – адрес сервера, на котором установлено антивирусное ПО;</host></li> <li><port> – порт соединения.</port></li> </ul>
Комментарий	Дополнительные сведения об ICAP- сервере	Вводимый вручную текст. Максимальный раз- мер введенного текста не должен превышать 200 символов

Нажать кнопку Сохранить и Применить политику.

Цоба	авить ІСАР-сервер Импорт	Экспорт		Поиск по имен	и сервера	م
	Имя сервера	URL	Комментарий	Создан	Изменен	
)	Local reqmod	icap://localhost:1344/reqmod		14.03.2022.1	1:56	
1	Сохранить Отмена					
	Имя сервера	New ICAP				
	ICAP URL	icap://tt13.solar.local:1344				

Рис. 6.37. Добавление ІСАР-сервера

# Примечание

ІСАР-серверы антивируса недоступны для редактирования.

При проверке данных с использованием Symantec Scan Engine:

- в запросе используется формат URL антивируса: ICAP://<host>:<port>/avscanreq.
- в ответе используется формат URL антивируса: ICAP://<host>:<port>/avscanresp.

При проверке данных с использованием Kaspersky Antivirus:

- в запросе используется формат URL антивируса: ICAP://<host>:<port>/av/reqmod.
- в ответе используется формат URL антивируса: ICAP://<host>:<port>/av/respmod.

# 6.5.3.2. Прокси-серверы

#### 6.5.3.2.1. Управление прокси-серверами

Прокси-серверы используются в настройке набора правил политики для фильтрации трафика (запросов и/или ответов). При необходимости через прокси-серверы можно предоставить пользователю, приложению и т.д. доступ к запрашиваемому веб-ресурсу.

Управление прокси-серверами выполняется в разделе **Политика > Внешние подклю**чения > **Прокси-серверы** (<u>Рис.6.38</u>). Общие принципы работы с прокси-серверами приведены в разделе <u>6.4.3</u>.

*	Solar NGFW			Поиск по разделу (в данном случае по имени прокси-сервера)	Поиск персоны Q 🔙
ିଲ କ	настроики импорт экспорт	политика / внешние подключения / прокси-серверы			применить политику
43	Доступ без аутентификации	Добавить прокси-сервер Импорт Экспорт			Гоиск по имени сервера Q
8	🔓 вскрытие HTTPS	Имя сервера IP-адрес	Логин	Комментарий Создан	Изменен
Ŗ	🛞 Перенаправление по ІСАР	Прямое соединение			
Ξw	🗇 Фильтрация запросов 🛛 🕣 🗸				
£	Режим белого списка				
<b>(</b> II)	🗘 Фильтрация ответов  💮 🗸				
۲	🔁 внешние подключения 🗸 🗸				
	ІСАР-серверы				
	Прокси-серверы				

Рис. 6.38. Раздел «Политика > Внешние подключения > Прокси-серверы»

#### Примечание

При установке Solar NGFW по умолчанию формируется прокси-сервер, который настроен для прямого соединения. Его невозможно отредактировать или удалить. Этот сервер отображается в разделе **Политика > Внешние подключения > Прокси-серверы** под названием **Прямое соединение**.

Для добавления прокси-сервера необходимо:

- 1. Нажать кнопку Добавить прокси-сервер.
- 2. Указать необходимые значения (см. Табл.6.28).

#### Примечание

Если поля будут заполнены неправильно, под ними отобразятся уведомления об ошибках:

- при указании некорректного IP-адреса прокси-сервера «Неверный формат IP»;
- при несовпадении указанных паролей «Пароли не совпадают».

#### Нажать кнопку Сохранить и Применить политику.

Название	Описание	Значение
Имя сервера	Название прокси-сервера	Вводимый вручную текст. Максимальный размер введенного текста не должен превы- шать 200 символов
IP-адрес сервера	IP-адрес прокси-сервера, на который будет перенаправлен трафик	Значение можно ввести вручную. Одиночный IP-адрес
Порт	Номер порта, на котором прокси-сервер ожидает соединение	Число (меньше 65536) можно ввести вручную
Логин и пароль	Имя и пароль учетной записи пользова- теля, которому будет доступно соедине- ние с прокси-сервером	Вводимый вручную текст. Максимальный размер введенного текста не должен превы-

Табл. 6.28. Перечень атрибутов для добавления прокси-сервера

Название	Описание	Значение
		шать 200 символов. Пароль следует ввести дважды
Комментарий	Дополнительные сведения о сервере	Вводимый вручную текст. Максимальный размер введенного текста не должен превы- шать 200 символов

Лобавил								именить политику	
Hoodan	ть прокси-сервер	Импорт	Экспорт			Поиск по име	ени сервера	م	
	Имя сервера	ІР-адрес	Логин	Коммент	арий	Создан	Изменен		
a	Прямое соеди								
>	∨ Сохранить	Отмена							
	Имя сервера		Рабочий						
	ІР-адрес сервера		10.10.10.10						
	Порт		3128						
	Логин и пароль		admin		•••••	••	•••	•••••	
	Комментарий		Использовать	ь в рабочих целях					

Рис. 6.39. Добавление прокси-сервера

#### 6.5.3.2.2. Варианты задания вышестоящего прокси-сервера

В Solar NGFW указать вышестоящий прокси-сервер (parent-proxy) можно как с помощью правила политики, так и в настройках конфигурации.

# В политике

При создания правила необходимо указать следующие условия:

- Действие Разрешить через прокси-сервер;
- Прокси-сервер Выбрать прокси-сервер из списка, который предварительно следует создать в разделе <u>6.5.3.2</u>.

#### В конфигурации

В секции Вышестоящий прокси-сервер (parent-proxy) в разделе Система > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей расширенных настроек конфигурации указать параметры: IP-адрес прокси-сервера и номер порта. Также можно ввести логин и пароль для базовой аутентификации.

### Внимание!

Если были заданы разные parent-proxy одновременно и в политике, и в конфигурации, то учитывается следующий приоритет: вышестоящим прокси-сервером считается тот, который указан в политике, то есть перекрываются параметры конфигурации.

#### 6.5.3.2.3. Устранение проблем с кодировкой (кириллица) при работе с FTP-узлами

При формировании политики рекомендуется исключить использование вышестоящих прокси-серверов для доступа к FTP-узлам, поскольку FTP-клиент, встроенный в различные прокси-серверы (включая **skvt-cache**), может некорректно работать с кириллицей.

Для корректного отображения кириллицы для некоторых FTP-серверов требуется настроить параметры Сетевой адрес FTP-сервера и Кодировка FTP-сервера секции Кодировка FTP-серверов раздела Система > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей (<u>Рис.6.40</u>).

V Кодировки FTP-серверов ftp-charsets	Параметры настройки шаблонов FTP-серверов с применяемой на них кодировкой
∽ 1	
Сетевой адрес FTP-сервера pattern	zebrajob.*
	Регулярное выражение, задающее сетевой адрес FTP- сервера. Если регулярное выражение для имени FTP- сервера не удалось определить, то конфигурация не применяется
Кодировка FTP-сервера charset	koi8-r
	Название кодировки, применяемой на указанном FTP- сервере. По умолчанию применяется кодировка UTF-8. Если название кодировки не удалось определить или заданная кодировка не поддерживается Java Virtual Machine (JVM), то конфигурация не применяется

Рис. 6.40. Настройка параметров при работе с FTP-протоколами

Чтобы указать параметры нового шаблона для FTP-узла необходимо нажать кнопку **Добавить**, которая отобразится справа от имени секции **Кодировки FTP-серверов** при наведении курсора (<u>Рис.6.40</u>) и нажать кнопку **Сохранить**.

Во всех случаях, когда администратор безопасности принимает решение о разрешении доступа к FTP-узлам, при создании правила следует указать следующие условия:

- Действие Разрешить через прокси-сервер;
- Прокси-сервер Прямое соединение.

#### Примечание

Действие **Разрешить через прокси-сервер** следует применить для всех соединений по протоколу **FTP**.

# 6.5.4. Объекты политики

# 6.5.4.1. Списки ІР-адресов

Solar NGFW позволяет задавать списки IP-адресов для их дальнейшего использования при создании политики.

<i>.</i>	Solar NGFW			Поиск по разделу (в данном	Поиск перс	соны 🗦
ଜ	Настройки Импорт Экспорт		иски IP-адресов 🕐	случае по имени IP-диапазона)		
	🔛 межсетевой экран >				Поиск	٩
\$	2 <sup>®</sup> предотвращение вторжений >	Название списка	IP-диапазон	Создан	Изменен	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ >	Apple Inc.	1.1.1.1	admin 15.01.2025 19:11		00
ΪÅ <sub>ø</sub>	🕞 ssl-инспекция >	Netflix Streaming	23.246.0.0 - 23.246.63.255	admin 15.01.2025 19:12		0 0
26 -		Office 365	13.107.1.0	admin 15.01.2025 19:13		0 0
۲		OpenDNS	146.112.0.0 - 146.112.225.225	admin 15.01.2025 19:15		00
Æ	🛞 ОБЪЕКТЫ ПОЛИТИКИ 🗸 🗸					
	Списки IP-адресов					
	Лимиты трафика					
	Расписания					
	Условия на заголовки					
\$	Пользователи (Basic Auth)					

Рис. 6.41. Раздел «Политика > Объекты политики > Списки IP-адресов»

Управление списками IP-адресов выполняется в разделе **Политика > Объекты политики > Списки IP-адресов** (<u>Рис.6.41</u>). Общие принципы работы с инструментами политики описаны в разделе <u>6.4.3</u>. Для удобной работы с IP-адресами они объединены в группы (списки), и предусмотрен поиск по списку IP-адресов (<u>Рис.6.42</u>).

Политика / Объекты полити	ки / ІР-диапазоны 🕜					Применить пол	итику
Добавить список IP-диапазонов			Поиск по параме	етрам			٩
Название списка		IP диапазон		Создан	Изменен		
Сохранить Отмена	Добавить IP-адрес/диап	азон Поиск по г	параметрам	٩	Импорт	Экспорт	Ū
Название списка	Netflix Inc Netflix Stream	ning Services Inc					
IP-адрес/диапазон		Создан	Изменен	Комментарий			
37.77.184.0 - 37.77.191.255		admin 15.03.2022 17:39		Введите комме	ентарий		Ū
23.246.0.0 - 23.246.63.255		admin 15.03.2022 13:32	admin 15.03.2022 17:39	Введите комме	ентарий		Û

Рис. 6.42. Поиск по параметрам

При использовании фильтра по IP-адресам следует учесть, что:

- в запросе проверяется IP-адрес источника;
- в ответе проверяется IP-адрес назначения.

# Примечание

Фильтрация по IP-адресу назначения не выполняется при использовании вышестоящего прокси-сервера.

Для добавления IP-адреса/диапазона IP-адресов необходимо в разделе Политика > Объекты политики > Списки IP-адресов:

- 1. Нажать кнопку Добавить список IP-адресов.
- 2. Указать необходимые данные (см. Табл.6.29).

Табл.	6.29.	Перечень	атрибутов	для до	бавления	ІР-адреса/	диапазона	IP-адресов

Название	Описание	Значение
Название списка	Название списка IP-адресов	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 сим- волов
IP-адрес/диапазон	IP-адреса/диапазоны IP-адре- сов, которые будут использо- ваться при настройке правил фильтрации	<ul> <li>Значение можно ввести вручную:</li> <li>Одиночный IP-адрес;</li> <li>Диапазон IP-адресов IP-диапазоны можно указывать в следующих форматах:</li> <li>через «-». Пример: 192.168.205.0-192.168.205.24;</li> <li>через «/» – в формате бесклассовой междоменной маршрутизации (<i>Classless Inter-DomainRouting , CIDR</i>). А именно, 0.0.0.0/16. Пример: 192.168.205.0/24</li> </ul>
Комментарий	Дополнительные сведения об IP-адресе/диапазоне	Вводимый вручную текст. Максимальный размер введенного текста не должен превышать 200 сим- волов

- 3. Для добавления в текущий список нового адреса или диапазона нажать кнопку **Добавить IP-адрес/диапазон**.
- 4. Нажать кнопку Сохранить и Применить Политику.

Полит	ика / Объекты по	олитики / IP-диапаз	оны 🕐					оименить	политику			
Доба	зить список IP-диапаз	онов				Поиск по н	названию		٩			
	Название списка		IP диапаз	он	Создан		Изменен					
	Apple Inc		1.1.1.11		admin 15.03.202	22 13:32	admin 15.03.2022 17:4	46	00			
	Netflix Inc Netfli	x Streaming Services	23.246.0.0	- 23.246.63.255	admin 15.03.202	22 17:29	admin 15.03.2022 17::	39	00			
	OFFICE 365	🗸 Сохранить	Отмена	Добавить IP-адрес/диапаз	он Поис	к по параме	трам	٩	Для поиска и сохраните и	и сортировки зменения	Импорт	Экспорт
	OpenDNS, LLC	Название списка		Soundcloud								
	Twitter Inc	IP-адрес/диапазон		Созд	цан	Изме		Комме	нтарий			
		35.160.100.86						Введі	ите коммент	арий		
		Всего 1 Строка					11					4

Рис. 6.43. Создание группы ІР-адресов/диапазонов

Название списка	IP диапа	130Н	Создан	Изменен	
🗸 Сохранить Отмена	Добавить IP-адрес/диапазон	Поиск по параметрам	٩	Импорт Эксг	юрт
Название списка	Список ІР-диапазонов				
IP-адрес/диапазон	Создан	Изменен	Комментарий		
10.0.0.0 - 10.0.1.2	admin 21.01.202	2 15:13	Введите комментарий		Ū
192.168.12.1	admin 21.01.202	2 15:13	Введите комментарий		Ð
10.0.0.0 - 10.0.0.255	10.0.0.0/24 admin 21.01.202	2 15:12	Введите комментарий		Ū
Всего 3 Строки					

Рис. 6.44. Форматы списков ІР-адресов

# 6.5.4.2. Лимиты трафика

#### 6.5.4.2.1. Управление лимитами трафика

Solar NGFW позволяет устанавливать лимиты на трафик, используемый пользователем, по объему в единицу времени (час, сутки, неделя, месяц). Объем трафика измеряется в байтах, а также в кило/мега/гига/терабайтах.

Ограничение используемого трафика задается в разделе **Политика > Объекты политики > Лимиты трафика** (<u>Рис.6.45</u>). Общие принципы работы с инструментами политики описаны в разделе <u>6.4.3</u>.

<u>م</u>	Solar NGFW		a grant a	Поиси по	< по разде названию	елу (в данном случ о лимита трафика)	Поис	к персоны	۹ 🗜
ណ៍	Настройки Импорт Экспор	Полити	ика / Объекты по	литики / Лимиты т	рафика 🕐			Применит	ь политику
£	🔛 межсетевой экран	Добае	вить лимит трафика				Поиск по назе	анию	۹
\$	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ		Название	Объем трафика	Период	Комментарий	Создан	Изменен	
Ŗ			Отдел продаж	1 M5	Час		15.03.2022 13:33	15.03.2022 17:53	00
~	с впешние подключения		Отдел кадров	216	Час		admin 15.03.2022 17:53		ឲ្
75	🍥 ОБЪЕКТЫ ПОЛИТИКИ								
A	IP-диапазоны								
(III)	Лимиты трафика								
۲	Расписания								
	Условия на заголовки								
	Пользователи (Basic Auth)								

Рис. 6.45. Раздел «Политика > Объекты политики > Лимиты трафика»

Для добавления нового лимита трафика необходимо:

- 1. В разделе Политика > Объекты политики > Лимиты трафика нажать кнопку Добавить лимит трафика.
- 2. Указать необходимые данные. Нажать кнопку Сохранить и Применить политику.

Полит	гика / Объекты по	литики / Лимиты	трафика 🕜			Примени	ть политику
Доба	авить лимит трафика				Поиск по на	званию	٩
	Название	Объем трафика	Период	Комментарий	Создан	Изменен	
>	Отдел продаж	1 M5	Час		admin 15.03.2022 13:33	admin 15.03.2022 17:53	0 Đ
>	Отдел 🗸 🖸 Сс	охранить Отмена					
	Название		Бухгалтерия				
	Объем и п	ериод	1000	мб ∨	Неделя 🗸		
	Коммента	рий	Введите коммен	ітарий			

Рис. 6.46. Настройка лимита трафика

# Внимание!

Единица измерения лимита по умолчанию указывается в мегабайтах (МБ).

```
В системе предусмотрено ограничение на максимальное значение объема трафика: 9223372036854775807 (=2^63 - 1) байт.
```

При этом используются абсолютные значения времени. То есть, если указать ограничение трафика 50 МБ в час, это значит, что будет разрешена передача 50 МБ не за фактический час работы, а за период времени, например, с 13:00 до 13:59:59, после чего пойдет новый отсчет трафика. Соответственно, другие значения в списке временных интервалов означают следующее:

Табл. 6.30	Перечень	временных	интервалов
------------	----------	-----------	------------

Период времени	Пояснение	Рекомендации
Сутки	Период времени с 00:00:00 до 23:59:59	
Неделя	Период времени с каждого по- недельника 00:00:00 до каждого воскресенья 23:59:59	Временные рамки для недели зависят от системной локализации – для русской локализации неделя начи- нается с понедельника, для американской – с воскре- сенья
Месяц	Период времени с 00:00:00 ча- сов первого числа месяца до 23:59:59 последнего числа ме- сяца (в зависимости от месяца)	Если сформированная политика предоставляет опре- деленный одинаковый лимит каждому из группы пользователей, то в случае израсходования каким- либо пользователем этого лимита трафика, доступ к интернету будет ограничен только у него. У остальных членов группы доступ в интернет будет ограничен только тогда, когда каждый из них израсходует свой лимит. При превышении лимита будет выполнено действие, заданное в правиле политики

При необходимости можно не учитывать трафик при обращении к конкретным веб-ресурсам. Для этого необходимо указать доменные суффиксы всех таких веб-ресурсов в секции whitelist конфигурационного файла config.json (раздел Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей в секции Нетарифицируемые ресурсы).

# 6.5.4.2.2. Информация о текущем расходе трафика

В Solar NGFW есть возможность показывать пользователю информацию о его текущем расходе трафика. Для этого настраивается специальный шаблон с информацией о трафике пользователя, шаблон размещается по специальному уникальному URL. Этот URL указывается в настройках skvt-wizor (раздел Система > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей параметры URL страницы лимитов трафика (traffic-summary-url) и Путь к файлу шаблона страницы (traffic-summary-template) в секции Отладка), по нему пользователю будет отображен шаблон.

Определены специальные подстановочные символы, которые используются для шаблона показа пользователю его трафика (см. <u>Приложение С, Использование подстановочных</u> <u>символов</u>).

Для настройки шаблона необходимо выполнить следующие действия:

- 1. В разделе Политика > Шаблоны > Шаблоны страниц создать шаблон traffic, заполнить его подстановочными символами и сохранить.
- 2. В каталоге policy-final/templates найти сохраненный шаблон, скопировать относительный путь к нему (относительно каталога policy-final).
- Скопированный путь указать в параметре debug/traffic-summary-template в настройках skvt-wizor. Например, путь к шаблону может выглядеть следующим образом: templates/5137BF69-DAEC-436C-8417-E601E3AD74AB

4. Нажмите последовательно кнопки Сохранить и Применить.

Запрос пользователя к этому шаблону через прокси будет отображаться в отчетах и журнале с действием Запретить.

# 6.5.4.3. Расписания

Solar NGFW позволяет фильтровать трафик по времени доступа пользователей к вебресурсам. Для этого создаются расписания.

Расписание представляет собой установленный для определенных дней недели порядок доступа к веб-ресурсам, который задается начальным и конечным интервалами времени в формате **чч:мм**. Таким образом можно, например, запретить доступ к веб-ресурсам в будние дни с 9:30 до 17:30.

Управление расписаниями выполняется в разделе **Политика > Объекты политики > Расписания** (<u>Рис.6.47</u>). Общие принципы работы с инструментами политики описаны в разделе <u>6.4.3</u>.

<i>.</i>	Solar NGFW			Поиск по разделу (в да случае по названию расг	анном писания)	Тоиск персоны	२ 🛵
ធ	Настройки Импорт	Экспорт	Политика / Объекты политики / Распи	сания		Примени	ть политику
	🔛 МЕЖСЕТЕВОЙ ЭКРАН		Добавить расписание		Поиск по н	названию	٩
<b>3</b> ()	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ		Название	Комментарий	Создан	Изменен	
Ref.			> Отдел продаж		admin 15.03.2022 13:34	admin 15.03.2022 18:07	00
	е впешние подключения		> Отдел маркетинга		admin		00
0" Ř.	🛞 объекты политики		> Группа по подбору персонала		admin 15.03.2022 18:07		00
8 1	IР-диапазоны		> Отдел снабжения		admin 15.03.2022 18:07		00
	Лимиты трафика						
۲	Расписания						
	Условия на заголовки						
	Пользователи (Basic Auth)						

Рис. 6.47. Раздел «Политика > Объекты политики > Расписания»

При создании нового расписания необходимо задать временной интервал доступа. Для этого следует указать начало и конец интервала в полях **Начало интервала** и **Конец интервала** с помощью клавиатуры или кнопок (<u>Рис.6.48</u>). Затем установить флажки для требуемых дней недели.

Для добавления нового интервала расписания в разделе **Политика > Объекты политики > Расписания**:

1. Нажать кнопку Добавить список расписаний.

# Примечание

Время окончания интервала должно быть больше его начала.

2. Указать необходимые данные . Нажать кнопку Сохранить и Применить политику.

Для добавления нового расписания в группу следует нажать кнопку **Добавить расписание**. Максимальное количество интервалов в расписании не должно быть более 20.

Политі	ика / Объекты пол	итики / Расписания					Применит	политику	
Добав	вить расписание				Поиск по на	званию		٩	
	Название	Комментарий		Создан		Изменен			
>	Группа по подбору г	персонала		admin 15.03.202	2 13:34	admin 15.03.202	2 18:26	Q D	
>	Отдел маркетинга	Сохранить Отмена	Добавить						Импорт Экспорт
>	Отдел продаж	Название	Отдел снабжения						
>	Бухгалтерия	Комментарий	Введите коммента	рий					
		Дни недели			Время о		Создан	Изменен	Комментарий
		🕑 Пн 🔜 Вт 🕓 Ср 🗌	Чт 🔽 Пт 📃 Сб	6 🔲 Bc	10:00	18:30			Введите

Рис. 6.48. Добавление расписания

# 6.5.4.4. Условия на заголовки

При фильтрации трафика могут использоваться значения служебных заголовков протокола HTTP. Запросы и ответы в протоколе HTTP содержат некоторое количество заголовков. Формат заголовков соответствует общему формату заголовков текстовых сетевых сообщений. Каждый заголовок представляет собой строку формата **<название>:<значение>**.

Часто используемые заголовки:

- User-Agent описание клиентского ПО;
- Referer URL исходной страницы, с которой был осуществлен данный запрос.

Для обработки этих заголовков и их значений могут применяться регулярные выражения (см. <u>Приложение В, *Язык описания регулярных выражений*).</u>

Для удобства использования заголовки протокола НТТР объединяются в группы (списки). Формирование условий на заголовки выполняется в разделе **Политика > Объекты политики > Условия на заголовки**(<u>Рис.6.49</u>). Общие принципы работы с инструментами политики описаны в разделе <u>6.4.3</u>.

<b>*</b> *	Solar NGFW			Поиск по разделу (в данном с	пучае по	Поиск персо	оны С	. 2≓
ଜ	Настройки Импорт Экспор		ика / Объекты политики / Условия на заголовки 🛛 🕐	названию списка услови	ій́)			
E	🔛 МЕЖСЕТЕВОЙ ЭКРАН	Доба	вить список условий на заголовки			Поиск по названию		٩
\$	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ		Название		Создан	Изменен		
			YouTube разрешенные видео		admin 05.05.2023	3 19:00		0 C
~~	🖶 внешние подключения		Режим белого списка		admin 05.05.2023	3 19:00		00
8	🍥 ОБЪЕКТЫ ПОЛИТИКИ		Pafarar moil		admin			
<u></u>	ID визрозоции				05.05.2023	3 19:00		
(E)	г-дианазоны		Онлайн уроки		admin 05.05.2023	3 19:01		J D
-	Лимиты трафика		Discord		admin			a <del>n</del>
۲	Расписания				05.05.2023	3 19:01		6 6
	Условия на заголовки							
	Пользователи (Basic Auth)							
	СПРАВОЧНИКИ							
	Адреса электронной почты							
Ŕ	Ключевые слова							

Рис. 6.49. Раздел «Политика > Объекты политики > Условия на заголовки»

#### Примечание

При фильтрации по НТТР-заголовкам не учитывается регистр букв имени заголовков.

Для добавления нового списка условий на заголовки в разделе Политика > Объекты политики > Условия на заголовки:

- 1. Нажмите кнопку Добавить список условий на заголовки (Рис.6.52).
- 2. Укажите название списка условий (не более 200 символов).
- 3. Введите необходимые значения для формирования условия:
  - Шаблон для названия HTTP-заголовка наименование HTTP-заголовка (не более 250 символов). Чтобы найти все заголовки с похожими названиями, укажите часть, которая повторяется.
  - Шаблон для значения НТТР-заголовка значение НТТР-заголовка (не более 500 символов).

#### Примечание

Установите флажок **Рег. выр.** в соответствующем столбце таблицы для названий и значений HTTP-заголовков, которые будут использоваться как регулярные выражения (<u>Puc.6.50</u>).

 Комментарий – дополнительные сведения об условии (указывать необязательно; не более 500 символов).

Объект	ы политики / Условия на заго	оловки			Пр	именить политику		
Добав	ить список условий на заголовки			Поис	к по названию	۹		
	Название			Создан	Изменен			
>	Youtube разрешенные видео			unknown 08.05.2019 16:17	admin 17.04.2020 20:4	, <b>0</b> 0	A	
>	Режим Белого списка	<ul> <li>Сохранить</li> <li>Отмена</li> </ul>	Добавить условие				Импорт	Экспорт
>	Referer mail	Название Ус	ловие на получение	е и отправлени				
		Шаблон для названия НТТР-загол	к Шаблон для знач	ения HTTP-заго	олс Создан	Изменен	Комментарий	
		X-receive-from	dozor/k.petrov				Введите комментарий	
		Регулярное выражение	🗹 Регулярное в	ыражение				Ŭ
		X-forwarder-for	dozor/v.karp				Введите комментарий	
		Регулярное выражение	🕑 Регулярное в	ыражение				đ

Рис. 6.50. Добавление списка условий на заголовки

 Установите флажок Регулярное выражение, если необходимо, чтобы Шаблон для названия НТТР-заголовка и/или Шаблон для значения НТТР-заголовка использовались как регулярные выражения.

После включения вы можете проверить регулярное выражение. Для этого:

- а. Нажмите 🕜.
- b. В поле **Текст для проверки** введите значения, которые необходимо проверить.

Примечание

Каждое новое значение необходимо указывать с новой строки.

Максимальная длина значения в каждой строке составляет 2083 символа.

Не допускается использование посторонних символов, не относящихся к значению или синтаксису регулярных выражений.

с. Нажмите Проверить. В столбце Совпадение будет отражен результат проверки.

Проверить регулярное выражение	×
Шаблон для названия HTTP-заголовка	
s{1,3}	
Текст для проверки	Совпадение
s ss	$\bigcirc$
SSS SSSS	⊘ ⊗
Новая проверка Сохранить Отм	ленить

# Примечание

Если результат отсутствует, регулярное выражение введено некорректно. В этом случае в столбце **Совпадение** результата не будет, поле **Шаблон для названия HTTP**заголовка или **Шаблон для значения HTTP-заголовка** будет выделено красным, и под ним будет отображен комментарий.

Проверить регулярное выражение	Х
Шаблон для значения HTTP-заголовка	
s{}	8
Некорректное регулярное выражение: Illegal repetition near index 0 s{} ^	
Текст для проверки	
1 2	h
Проверить Сохранить Отменить	

Чтобы добавить значения, нажмите Новая проверка.

d. Нажмите Сохранить.

Для добавления нового условия нажмите кнопку Добавить условие.

# 6.5.4.5. Пользователи при Basic-аутентификации

Solar NGFW позволяет задать список пользователей, которые будут авторизованы с помощью Solar NGFW, если для них выбрана Basic-аутентификация в конфигурации.

Добавление новых учетных записей пользователей и управление ими выполняются в разделе Политика > Объекты политики > Пользователи (Basic Auth) (<u>Рис.6.51</u>). Общие принципы работы с инструментами политики описаны в разделе <u>6.4.3</u>.

*	Solar NGFW			Поиск по разделу (в данног		Іоиск персоны	۹ 🛃
ଜ	Настройки Импорт Экспорт	Политика / Объекты политики / Пользовате	ели (Basic Auth) 🛛 🕐	случае по пользователям)			
E	🔛 МЕЖСЕТЕВОЙ ЭКРАН >				Поиск по	логину	٩
8	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ >	Логин IP	диапазон Активен	н Комментарий	Создан	Изменен	
		> user1 10	.199.20.63 Да		admin 05.05.2023 19:11		Q Đ
~	ВНЕШНИЕ ПОДКЛЮЧЕНИЯ >	> user2 10	.199.1.1 Нет		admin 05.05.2023 19:11	admin 05.05.2023 19:14	ΟĊ
8	🍥 ОБЪЕКТЫ ПОЛИТИКИ 🗸 🗸	> user3 10	.199.1.2 Да		admin 05 05 2023 19 <sup>-</sup> 13		00
46	IP-диапазоны	> user4 1.	1 2222 Да		admin		ឲ្
\$ <b>E</b>	Лимиты трафика		$\prec$		05.05.2023 19.18		
۲	Расписания	Учетная запись пользователя заблокирована		Учетная запись			
	Условия на заголовки			пользователя активна			
	Пользователи (Basic Auth)						
	💿 справочники 🗸 🗸						
	Адреса электронной почты						
\$	Ключевые слова						

Рис. 6.51. Раздел «Политика > Объекты политики > Пользователи (Basic Auth)»

Для добавления новой учетной записи пользователя в разделе Политика > Объекты политики > Пользователи (Basic Auth):

- 1. Нажмите кнопку Добавить пользователя (Рис.6.52).
- 2. Заполните следующие поля:
  - Логин и пароль имя пользователя (например, ФИО; не более 200 символов) и пароль этой учетной записи. Пароль необходимо ввести дважды (не более 200 символов).
  - ІР-диапазоны ІР-адрес или диапазон ІР-адресов рабочих станций, с которых указанный пользователь будет выходить в интернет. Можно указать несколько ІРдиапазонов.

#### Примечание

Последний IP-адрес в диапазоне должен быть больше первого значения диапазона или равен ему.

• Комментарий – дополнительные сведения о пользователе (указывать необязательно; не более 500 символов).

#### Примечание

Чтобы заблокировать ту или иную учетную запись, используйте переключатель **Пользо**ватель активен: **СО**, а затем поочередно нажмите кнопки **Сохранить** и **Применить** политику.

екты политики / Пользов	атели (Basic Auth)					Примения	ть политику
обавить пользователя				Πα	риск по логину		٩
Логин	IP диапазон	Активен	Комментарий	Создан	Изме	нен	
user1	2222, 0.0.0255_	Да		unknown 08.05.2019 16	admi 17 17.04	n 2020 21:44	O D
user2	Сохранить Отмена	Добави	ить IP				100
user3	Логин и пароль user			•••••			
	IP или IP-диапазон		Создан		Изменен	Комме	нтарий
	1.1.1.1					Введи	те комментари
	Пользователь активен						
	Комментарий	Введите к	омментарий				

Рис. 6.52. Добавление учетной записи пользователя

# 6.5.5. Справочники

#### 6.5.5.1. Адреса электронной почты

Solar NGFW позволяет управлять списками адресов электронной почты, на которые будут приходить соответствующие уведомления. Например, могут приходить уведомления о нарушении политики безопасности.

Для удобства использования адреса электронной почты объединены в группы (списки). Добавление и управление списками адресов выполняется в разделе **Политика > Справочники > Адреса электронной почты** (<u>Рис.6.53</u>). Общие принципы работы со справочниками описаны в разделе <u>6.4.3</u>.

*	Solar NGFW			Поиск по разделу (в данном случае по наз списка с адресами электронной почте	ванию ы)	Поиск персоны	م _₌
ය	Настрояки Импорт	Экспорт		bl 🕜		Приме	
E	🔛 межсетевой экран		Добавить список адресов электронной почты			Поиск по названию	٩
\$	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ		Логин		Создан	Изменен	
₩.	B1		> Важные		admin 31.03.2023	admin 15:32 20.04.2023 20:33	00
	та внешние подключения		> Администраторы		admin 31.03.2023	admin 15:32 20.04.2023 20:33	ឲ្
22	🍥 объекты политики						
246 SE	СПРАВОЧНИКИ						
<u></u>	Адреса электронной почты						
	Ключевые слова						

Рис. 6.53. Раздел «Политика > Справочники > Адреса электронной почты»

Для добавления списка с адресами электронной почты необходимо в разделе **Политика > Справочники > Адреса электронной почты**:

- 1. Нажать кнопку **Добавить список адресов электронной почты** и указать следующие параметры:
  - название списка адресов электронной почты (не более 200 символов, Рис.6.54);
  - адрес электронной почты в поле Адрес электронной почты (не более 200 символов);

### Примечание

При вводе некорректного электронного адреса (без символа «@») поле будет выделено красным, и под ним отобразится соответствующее уведомление.

• адрес SMTP-сервера, используемого для рассылки уведомлений по электронной почте, в поле **SMTP хост** (не более 200 символов), например: **www.host.com**;

#### Примечание

При задании адресов SMTP-серверов допускается указание корректных hostname или IPv4 адресов.

- TCP-порт SMTP-сервера, используемого для рассылки уведомлений по электронной почте, в поле SMTP-порт. Значение поля SMTP-порт должно соответствовать диапазону от 1 до 65535.
- 2. Нажать кнопку Сохранить и применить политику.

Полити	ка / Справочники / Адреса э	лектронной почты	2		Применить по	литику			
Добав	ить список адресов электронной почт	1		Поиск по названию		Q			
	Логин		Создан	Измене	н				
>	Важные		admin 16.03.2022 1	15:24		0 C			
>	Сохранить Отмена	Добавить адрес	Поиск по	параметрам	٩		Импорт		Ū
>	Название	Администраторы							
	Адрес электронной почты	SMTP хост		SMTP NODT	Создан	Изменен	Комментарий		
	karp@gmaiLcom	1		25	admin 16.03.2022 15:3	13	Введите комме	нтарий	

Рис. 6.54. Добавление списка адресов электронной почты

Чтобы указать новый адрес электронной почты, необходимо нажать кнопку **Добавить** адрес в строке уже существующего адреса.

#### 6.5.5.2. Ключевые слова

При анализе передаваемых данных может выполняться поиск тех или иных ключевых слов и фраз и подсчет их весов. Если суммарный вес всех ключевых слов будет больше или равен пороговому значению, заданному в политике, то будет выполнено соответствующее действие.

Для удобства использования ключевые слова объединены в группы (списки). Формирование списков ключевых слов выполняется в разделе **Политика > Справочники > Ключевые слова** (<u>Рис.6.55</u>). Общие принципы работы со справочниками описаны в разделе <u>6.4.3</u>.

При добавлении нового списка ключевых слов необходимо учитывать следующее:

- Если требуется, в поле Вес можно задать весовой коэффициент, значение которого должно соответствовать диапазону от 1 до 65535 (<u>Рис.6.56</u>). Если значение этого поля не задано, то по умолчанию ключевому слову назначается вес, равный 1.
- Для тех ключевых слов, в описании которых должно использоваться регулярное выражение, установите флажок **RegExp**.

После включения появляется возможность проверки регулярного выражения. Для этого:

- <sup>1.</sup> Нажмите 🕜.
- 2. В поле Текст для проверки введите значения, которые необходимо проверить.

#### Примечание

Каждое новое значение необходимо указывать с новой строки.

Максимальная длина значения в каждой строке составляет 2083 символа.

Не допускается использование посторонних символов, не относящихся к значению или синтаксису регулярных выражений.

Проверить регулярное выражение	X
Ключевое слово	
(? class="Checkbox-Label" )[И и][Г Г][Р р][Ы ы]	
Текст для проверки	Совпадение
игра игры почта	⊗ ⊘ ⊗

3. Нажмите Проверить. В столбце Совпадение будет отражен результат проверки.



Если результат отсутствует, регулярное выражение введено некорректно. В этом случае в столбце **Совпадение** результата не будет, поле **Ключевое слово** будет выделено красным, и под ним будет отображен комментарий.

роверить регулярное выражение	
(? class="Checkbox-Label" )[И И][Г Г][Р р][Ы ы	8
екорректное регулярное выражение: Unclosed character class near index 46 (? class="Checkbox-<br abel">)[И и][Г г][Р р][Ы ы ^ екст для проверки	
игры	le.
Проверить Сохранить Отменить	

Чтобы добавить значения, нажмите Новая проверка.

# 4. Нажмите Сохранить.

<u>م</u>	Solar NGFW			Поиск по разделу (в данном случае	۹ 🛵
ଜ	Настройки Импорт Эксг	порт	Политика / Справочники / Ключевые слова 📀	по названию списка ключевых слов)	
	🔛 МЕЖСЕТЕВОЙ ЭКРАН		Добавить список ключевых слов	Поиск по названию	۹
\$	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ		Название	Создан Изменен	
₩.			> Платежные системы и валюта	aunin 05.05.2023 21:11	00
ŝ	с внешние подключения		> Отложенное скачивание	admin 05.05.2023 21:11	0 C
يد م	🛞 ОБЪЕКТЫ ПОЛИТИКИ		> Финансовый аудит	admin 05.05.2023 21.12	00
<i>~</i> ∞	СПРАВОЧНИКИ				
@	Адреса электронной почты				
	Ключевые слова				
	Ресурсы				
	Маркеры правил КФ				
	Файлы				
\$	шаблоны	~			

Рис. 6.55. Раздел «Политика > Справочники > Ключевые слова»

Спран	1. На вочники , авить списо	жать кнопку / К очевые слова к ключевых слов	в. Нажать кнопк Сохранить	у	риск по названию	Применить политику	2. Указать необходимые данные и нажать кнопку <b>Добавить</b>
	Названи	ие	Создан		Изменен		
>	Контра	агенты и поставщии	admin 18 12 2018 11·30			លិបិ	
>	Страхо	<ul> <li>Сохранить</li> <li>Отмена</li> </ul>					Импорт Кспорт 🗋
		Название:	Поиск работы				
		Добавление ключевого слова	: работа	рег. выражение:	Bec: 1	Введите комментарий	Добавить
		Ключевое слово	Рег выраж	Вес Создан	Изменен	Комментарий	
		вакансия				Введите комм	ентарий
			Зада отобр	анное ключее азится в конц	вое слово це таблицы		

Рис. 6.56. Добавление списка ключевых слов

При создании фильтра по ключевым словам следует учитывать некоторые особенности:

- поиск ключевых слов (фраз) выполняется в текстовых данных: в теле запроса и в поле Query URL-запроса;
- регулярные выражения можно использовать только для поиска по ключевым словам, но не по ключевым фразам;
- длина ключевой фразы не должна превышать 16000 букв;
- т.к. при задании ключевой фразы не допускается использование знаков-разделителей ("\.,;:!?'`=+()<>\$%^&\*/@|#~[]{}), то необходимо их удалить или заменить на пробел. Например, вместо фразы «путь-дорогу» следует писать «путь дорогу».

#### Примечание

При вводе ключевого слова пробелы не учитываются.

#### 6.5.5.2.1. Пример использования проверки по ключевым словам

В политике фильтрации заданы ключевые слова: **яблоко** с весом 1 и **апельсин** с весом 2, пороговое значение равно 3.

#### Примечание

Пороговое значение задается при формировании политики в разделе Политика.

В тексте: «Российская Объединенная Демократическая Партия «ЯБЛОКО» от имени десятков тысяч членов партии и миллионов избирателей поздравляет тех, кто смог сделать реальностью в условиях советской системы «Хронику текущих событий» и бла-

годарит всех, кто заплатил за это своей свободой. Председатель Партии «ЯБЛОКО» Г.А.Явлинский» ключевое слово **яблоко** с весом 1 встречается 2 раза, то есть суммарный вес равен 2. Так как суммарный вес меньше порогового значения (2\*1 < 3), фраза считается допустимой.

В тексте: «4. Держите фрукты на видном мыесте. Ваза с фруктами должна составлять неотъемлемую часть вашей кухни. Это, к тому же, не только полезно, но и очень красиво. Если у вас под рукой всегда есть яблоко или апельсин, то, возможно, вам не захочется перекусывать чипсами или сухариками.» ключевое слово **яблоко** с весом 1 встречается 1 раз, ключевое слово **апельсин** с весом 2 встречается 1 раз, суммарный вес равен 1\*1 + 1\*2 = 3. Так как суммарный вес равен пороговому значению (1\*1 + 1\*2 = 3), фраза считается недопустимой.

# 6.5.5.3. Ресурсы

# 6.5.5.3.1. Общие сведения

Solar NGFW позволяет фильтровать трафик по URL-адресам ресурсов, указанным в запросах пользователей. Данный метод фильтрации позволяет ограничить доступ на уровне запроса сетевых ресурсов. С помощью регулярных выражений можно запретить доступ как к целым сайтам, так и к отдельным веб-страницам.

Для удобства использования ресурсы объединяются в группы (списки). Управление ресурсами (группами ресурсов) выполняется в разделе **Политика > Справочники > Ресурсы**(<u>Рис.6.57</u>). Общие принципы работы со справочниками описаны в разделе <u>6.4.3</u>.

<i>.</i>	Solar NGFW			Поиск по разделу (в данном случае	персоны Q 🛵
ଜ	Настройки Импорт Экспој	рт	Политика / Справочники / Ресурсы 📀	по названию списка ресурсов)	
<b>K</b>	🔛 МЕЖСЕТЕВОЙ ЭКРАН			Поиск по назва	нию Q
\$	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ		Название	Создан Из аdmin	менен
Ŗ	Внешние подключения		> Musically	055,2023,21:19	
R <sub>ø</sub>			> Yahoo	admin 05.05.2023 21:19	00
£	ОБЪЕКТЫ ПОЛИТИКИ		> OpenDNS	admin 05.05.2023 21:20	<b>0</b> 0
4E)	🙆 СПРАВОЧНИКИ				
) (j	Адреса электронной почты				
	Ключевые слова				
	Ресурсы				
	Маркеры правил КФ				
	Файлы				
	<b>Б</b> атарияны				
Ŕ	0-6				

Рис. 6.57. Раздел «Политика > Справочники > Ресурсы»

# Внимание!

При вводе имени ресурса протокол (НТТР или FTP) не задается.

Один и тот же ресурс, заданный с **www** и без, воспринимается системой как два разных ресурса. Для добавления нового списка ресурсов необходимо в разделе **Политика > Справочники > Ресурсы**:

- 1. Нажать кнопку Добавить список ресурсов (не более 3000 строк) (Рис.6.58).
- 2. Заполнить следующие поля и нажать кнопку Сохранить:
  - Название название списка ресурсов (не более 200 символов);
  - Шаблон имени URL-адрес ресурса, указанного пользователем в запросах (не более 200 символов);
  - Тип шаблона тип шаблона ресурса (см. Табл.6.31);
  - Комментарий дополнительные сведения о ресурсе (указывать необязательно; не более 500 символов).

Для добавления ресурса, необходимо нажать кнопку **Добавить шаблон** в строке соответствующего ресурса.

Политика / Справочники / Ресу	рсы 🕐			Применить политику	
Добавить список ресурсов		Πο	иск по названию	Q	
Название		Создан	Изменен		
> Linkedln		admin 22.12.2020 22:	admin 58 16.03.2022 1	16:14 ŪŪ	
Сохранить Отмена Добави	ить шаблон Поиск по пар	аметрам	Для поиска и сортир сохраните изменени	ювки ИІ	ипорт Экспорт
Название Без аутентификации					
Шаблон имени	Тип шаблона	Создан	Изменен	Комментарий	
mail	Домен и все по 🗸			Введите комментарий	
Bcero 1 Строка					

#### Рис. 6.58. Добавление списка ресурсов

Табл. 6.31. Режимы проверки веб-ресурсов

Название	Описание
Домен и все поддомены	Поиск веб-ресурсов по их доменам и поддоменам
Регулярное выражение	Поиск веб-ресурсов с использованием регулярных выражений
Начинается с	Поиск веб-ресурсов, URL-адрес которых начинается с заданной строки символов
Содержит	Поиск веб-ресурсов, URL-адрес которых содержит заданную строку символов
Доменное имя содержит	Поиск веб-ресурсов, имя узла которых содержит заданную строку символов
Доменное имя равно	Поиск веб-ресурсов, имя узла которых полностью совпадает с заданной строкой символов
Доменное имя оканчивается на	Поиск веб-ресурсов, имя узла которых оканчивается на заданную строку символов

#### 6.5.5.3.1.1. Пример использования списка ресурсов в политике фильтрации

Задача:

Заблокировать ресурс **whatsapp.com** и его верхние поддомены так, чтобы пользователь не мог перейти на этот ресурс даже через поисковые запросы. Например, через **google.com**.

### Порядок действий для решения задачи:

Для блокировки whatsapp.com необходимо:

1. В разделе Политика > Ресурсы сформировать список ресурсов (см. Рис.6.59).

🗸 Сохрани	пъ Отмена	Добавить шаблон По	оиск по параметрам	م طبع مر د م م م م	риска и сортировки ните изменения	Импорт	Экспорт
Название	Whatsapp						
Шаблон имен	и	Тип шаблона	Создан	Изменен	Комментарий		
whatsapp.co	m	Домен и все… 🗸			Введите комм	ентарий	
Всего 1 Строка							

Рис. 6.59. Раздел «Политика > Справочники > Ресурсы»

2. В разделе **Политика** сформировать правило политики как показано на рисунке далее, добавив созданный список ресурсов (см.).

Создать правило		×			
Включено	Правило     Исключение				
Название	Block WhatsApp				
Комментарий Введите комментарий					
Действия					
Основное	😢 Заблокировать 🗸 Блокировка: Нарушение политики безопасности	$\vee$			
	Шаблон страницы блокировки				
Добавить дополнительное действие 🗸 🗸					
Условия					
Источник	Любой	$\vee$			
	Персона, Группа персон, IP-диапазон, IP, диапазон вида IP - IP или маска подсети IP/xx				
Назначение	Whatsapp ×	$\vee$			
	Список ресурсов, категория или полное имя хоста (включая поддомены)				
Расширенные настройки	Показать				
	Сохранить Отменить				

Рис. 6.60. Правило для блокировки WhatsApp

3. Применить политику. В результате, после применения политики пользователь не сможет посетить этот ресурс и страницы ресурсов с любым из его верхних поддоменов. Вместо этого в окне браузера отобразится страница блокировки.

# 6.5.5.4. Маркеры правил контентной фильтрации

Маркеры правил контентной фильтрации облегчают процесс поиска и фильтрации событий в разделе **Статистика > Журнал запросов** и делают его более гибким. Дополнительная маркировка позволяет группировать события контентной фильтрации по общему признаку вне зависимости от других условий в правилах.

# Примечание

При создании маркера правил контентной фильтрации название маркера должно быть уникальным.

Маркеры правил контентной фильтрации можно создать:

• В разделе Политика > Справочники > Маркеры правил КФ с помощью кнопки Добавить маркер.

Поли	гика / Справочники / Маркеры прави	л КФ 🕜			Применить политику
Доб	вить маркер			Поиск по названию	Q
	Название	Комментарий	Создан	Изменен	
	req_mark1		admin 22.03.202	23 19:35	00
	resp_mark2		admin 22.03.20	23 19:36	Q O

Рис. 6.61. Справочник «Маркеры правил КФ»

- При создании правил в разделах Фильтрация запросов или Фильтрация ответов.
   Для этого:
  - 1. Нажмите Создать правило.
  - 2. В поле Добавить дополнительное действие выберите Добавить маркер в журнал. В выпадающем списке отображаются уже существующие в справочнике маркеры. Чтобы задать новое значение маркера, укажите его в поле внизу списка. После сохранения правила новый маркер автоматически будет добавлен в справочник Маркеры правил КФ.

×		Создать правило
	• Правило Исключение	Включено
	Укажите Всего правил в слое: 2	Приоритет
		Действия
	• Разрешить запрос	Основное
v đ	Добавить маркер в журнал 🗸 🗸	Дополнительно
- 1	Шаблон	
	Добавить дополнительное действие 🗸	
_		Условия
$\sim$	Любой	Источник
	Персона, Группа персон, IP-диапазон, IP, диапазон вида IP - IP или маска подсети IP/xx	
$\sim$	Любое	Назначение
	Назначение	

Для каждого правила контентной фильтрации можно назначить несколько маркеров.

# Примечание

При создании через конструктор правил маркер создается с пустым полем **Комментарий**, которое можно заполнить позднее в справочнике **Маркеры правил КФ**. Это поле необязательно, но оно помогает раскрыть смысл или назначение маркера.

После срабатывания правила маркеры будут отображаться в записях Журнала запросов.

# Примечание

Допускается повторное использование одного маркера в рамках одного правила. При этом действия **Добавить маркер в журнал** с одинаковыми названиями маркеров после перезагрузки списка правил будут объединены в одно, а в **Журнал запросов** будет добавлено только одно значение.

При обработке запроса несколькими правилами с маркировкой в одном или нескольких слоях контентной фильтрации все маркеры правил будут последовательно добавлены в записи **Журнала запросов**.

#### Примечание

Маркеры, используемые в каком-либо существующем правиле, не могут быть удалены.

Имя маркера используется при пометке события в **Журнале запросов**. Изменение имени маркера приведет к появлению записей в **Журнале запросов** с новым указанным именем, но

не позволит выполнять фильтрацию по старым записям. При необходимости рекомендуется создавать новый маркер, а не изменять существующий.

Если маркер больше не используется ни в одном правиле политики, он может быть удален. Однако это сделает невозможным фильтрацию ранее зарегистрированных событий, помеченных этим маркером в **Журнале запросов**.

В столбце **Комментарий ресурса** можно просмотреть дополнительную информацию о ресурсах, к которым пользователь получал или пытался получить доступ (если информация была добавлена ранее в разделе **Политика > Справочники > Ресурсы** для конкретных шаблонов имени ресурсов в поле **Комментарий**).

Также маркеры правил помогают более гибко выполнять фильтрацию в **Журнале запросов** для отбора помеченных событий при формировании отчетов. Для этого в разделе Статистика > Журнал запросов > По узлам фильтрации нажмите кнопку Еще и выберите Фильтр по маркерам.

#### Примечание

В текущей реализации фильтрация в **Журнале запросов** доступна только для отчета **По узлам фильтрации**.

*	Solar NGFW				Поиск персоны
ŵ	Журнал зап <0тчет не со	росов /По узлам фильтрации з охранен>			Сохранить 💙 С 10 сек. 💙
	Период	Узлы фильтрации	Ресурсы	Колонки	Запросы
\$	Эта неделя	🗎 🛛 main 🗴		IP-адрес источника × еще 3	V Bce V Eue V
5.01	> Графики запро	OCOB			Фильтр по маркерам
~	🗸 Журнал запро	осов			IP-адрес сервера назначения
R,			Журнал (і	ервые 500 строк)	Тип проверки
0.					Результат НТТР-код
-10					проверки ІР-адреса источников
۲	17.01.2025	test1 tes2 play.google.com	10.214.216.57	55, Allow CONNECT for	Лимит METHOD(CONNECT)
तन्त्र		tes3			Режим прокси
82				55, Переход к слою Ісар	Тип фильтрации
				Request,	
				переход к слою	
	17 01 2025	test1		white_list, Dependent	
	09:15:35	tes2 play.google.com	10.214.216.57 /log	слою Ісар	
		0.32		Response, Deperon k	
				Слою	
~				Завершение обработки	
\$2				политики	

Рис. 6.62. Фильтрация по маркерам

Использование маркеров при фильтрации позволяет игнорировать различия в значениях других признаков события, ранее являвшихся группирующими элементами. При создании правил контентной фильтрации с помощью маркеров можно логически сгруппировать события, не имеющие других общих признаков.

В раскрывающемся списке при нажатии кнопки **Еще** в **Журнале запросов** доступно также включение условия фильтрации **Тип фильтрации**. Поле содержит раскрывающийся список с типами фильтрации и применяется только вместе с полем **Фильтр по маркерам**.

По умолчанию значение в поле Тип фильтрации установлено в значение Гибкий фильтр. Это значит, что запись Журнала запросов будет присутствовать в отчете, если

в ней присутсвует хотя бы один из введенных маркеров. Такой фильтр полезен, если достоверно неизвестно, какие правила могли сработать в ходе обработки запросов/ответов и какие маркеры были записаны в **Журнал запросов**.

Значение в поле **Тип фильтрации** может быть изменено на **Строгое совпадение**. В этом случае запись **Журнала запросов** будет присутствовать в отчете, только если в ней присутствуют указанные маркеры и отсутсвуют те, которые не указаны в поле **Фильтр по маркерам**. Это позволяет выполнить отбор событий, соответствующих срабатыванию строго определенного правила или набора правил вне зависимости от других условий.

При включении условия **Фильтр по маркерам** в строке фильтрации появляется поле со значением по умолчанию **Все**. Такой фильтр не накладывает никаких ограничений на выборку событий. Поле недоступно для редактирования, однако позволяет выбрать интересующие значения маркеров из существующих в справочнике **Маркеры правил КФ**.

# 6.5.5.5. Файлы

Solar NGFW позволяет фильтровать трафик по файлам, запрошенным пользователями. Данная фильтрация основана на проверке по хеш-функциям, размерам файлов и другим атрибутам, которые помогают определить относится ли файл к вредоносному программному обеспечению. С помощью списка запрещённых файлов можно ограничить загрузку файлов, которые не соответствуют требованиям контекстной фильтрации данных в сети Интернет.

Для удобства использования файлы объединены в группы (списки). Формирование списков файлов выполняется в разделе **Политика > Справочники > Файлы** (<u>Рис.6.63</u>). Общие принципы работы со справочниками описаны в разделе <u>6.4.3</u>.

ج	Solar NGFW		Поиск персоны Q 🛵
ធ	Настройки Импорт Экспорт	Поиск по Политика / Справочники / Файлы 🕜 На	о разделу (в данном случае по званию списка файлов) Применить политику
E	🔛 межсетевой экран >	Добавить список файлов	Поиск по названию Q
\$	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🔶	Название	Создан Изменен
₩.		> Тестовые файлы	05.05.2023 23:00
Can a	впешние подключении /	> Вредоносные программы	admin 🗍 🗍
л О	объекты политики >	> Хеш-функции	admin 05.05.2023 23:18
-240) (	🖸 справочники 🗸 🗸	> Файлы	admin 05.05 2023 23:49
<u>ب</u>	Адреса электронной почты		
	Ключевые слова		
	Ресурсы		
	Маркеры правил КФ		
	Файлы		
\$	в шаблоны ∨		

Рис. 6.63. Раздел «Политика > Справочники > Файлы»

Для добавления нового списка файлов необходимо в разделе **Политика > Справочники > Файлы**:

- 1. Нажать кнопку Добавить список файлов (Рис.6.64).
- 2. Заполнить следующие поля и нажать кнопку Сохранить:
- Название название списка файлов (не более 200 символов);
- Значение значение атрибута файла (не более 200 символов).
- Тип идентификации файла выбор атрибута, который однозначно определяет файл (см. <u>Табл.6.32</u>);
- Комментарий дополнительные сведения о файле (указывать необязательно; не более 500 символов).

## Примечание

В зависимости от выбранного типа идентификации файла, формат ввода данных для поля **Значение** будет отличаться. Например, если в качестве атрибута файла выбрать его размер, то при вводе символов латинского алфавита в поле **Значение** отобразится соответствующее предупреждение.

Справ	очники / Файлы								При	менить политику	
Доба	вить список файлов							Поиск по н	азванию	٩	
	Название						Создан		Изменен		
>	Текстовые файлы						admin 17.04.20	20 18:29	admin 23.04.2020 10:31	00	
>	Важные файлы	Сохранить	Отмена	Добавить данные о	о файле	Пои	кк по парам	етрам		Импорт	Экспорт 🗍
>	Файлы для тестировани:	Название		Файлы для тестов							
9.2		Значение	Тип идентиф	икации файла		Создан	и	зменен	Комментарий		
		311111111	MD5			admin 17.04.202	ad 2019:01 20	fmin ).04.2020 22:23			Û
			Размер фа	йла (Байт)		admin 17.04.202	ad 20 19:00 20	lmin ).04.2020 22:26			Û
		Bcero 2 строки									

Рис. 6.64. Добавление списка файлов

Табл. 6.32	Перечень	атрибутов	для	проверки	файлов
------------	----------	-----------	-----	----------	--------

Название	Описание
MD5	Поиск файла, хеш-функция (уникальный идентификатор файла, полученный при помощи алгоритма MD5) которо- го полностью совпадает с заданной строкой символов
SHA1	Поиск файла, хеш-функция (уникальный идентификатор файла, полученный при помощи алгоритма SHA1) кото- рого полностью совпадает с заданной строкой символов
SHA256	Поиск файла, хеш-функция (уникальный идентификатор файла, полученный при помощи алгоритма SHA256) ко- торого полностью совпадает с заданной строкой симво- лов
Имя файла (Регулярное выражение)	Поиск файла, в названии которого содержится регуляр- ное выражение
Имя файла (Равно)	Поиск файла, название которого полностью совпадает с заданной строкой символов (не более 200 символов)
Размер файла	Поиск файла, размер которого совпадает с заданной величиной (размер файла определяется в байтах)

## 6.5.5.6. GeoIP

В политиках фильтрации Solar NGFW можно использовать наборы IP-адресов/подсетей, принадлежащих к конкретному географическому региону.

В разделе **Политика > Справочники > GeoIP** представлена актуальная база объектов GeoIP в виде таблицы. Объекты в таблице отсортированны по типу (**Страна**, **Сою**з, **Континент**). В базе присутствуют 250 стран, 7 континентов, СНГ и Евросоюз.

*	Solar NGFW				Поиск персоны	<b>₽</b> =
ଜ	Настройки Импорт	Экспорт				^
	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ				поиск по IP-адресу	۹
•	🖶 внешние подключения					
~	🛞 ОБЪЕКТЫ ПОЛИТИКИ		Европа	Континент		
R.			Токелау	Страна		
<u></u>	🖸 СПРАВОЧНИКИ		Ямайка	Страна		
۲	Адреса электронной почты		Мексика	Страна		
Œ	Ключевые слова		Кюрасао	Страна		
	Ресурсы		Израиль	Страна		
	Маркеры правил КФ			Союз		
	Файлы		Сент-Люсия	Страна		
	GeolP		Новая Каледония	Страна		
Ŕ	🗳 шаблоны	~	Латкия	Страна		-



Чтобы проверить, к какому географическому объекту принадлежит IP-адрес, укажите его в строке поиска в правом верхнем углу.

## 6.5.6. Шаблоны заголовков и страниц

## 6.5.6.1. Добавление заголовка

Для добавления заголовков при обработке HTTP-запросов создайте один или несколько шаблонов в разделе **Политика > Шаблоны > Добавление заголовка**. Общие принципы работы с шаблонами описаны в разделе <u>6.4.3</u>.

Для создания шаблона:

- 1. Перейдите в соответствующий раздел и нажмите кнопку **Добавить шаблон добавления заголовка** (<u>Рис.6.66</u>).
- 2. Укажите имя шаблона (не более 200 символов), а также укажите необходимые значения для его создания:
  - Шаблон для названия НТТР-заголовка наименование НТТР-заголовка или шаблон наименования (не более 200 символов);
  - Шаблон для значения HTTP-заголовка значение HTTP-заголовка или шаблон значения (не более 500 символов);
  - Комментарий дополнительные сведения о шаблоне (указывать необязательно; не более 500 символов).

## 3. Нажмите кнопку Сохранить.

ш	абло	ны / Добавление	заго	ловка			Применить политику	
	Добав	ить шаблон добавлени	я заго	повка		Поиск по назван	ию Q	
		Название		Создан		Изменен		
:	>	Заголовки		admin 18.12.201	8 11:30		J 8	
	~	Сохранить О	гмена				Импорт	Экспорт 🗖
	Наз	вание:		User-Agent				
	Ша	аблон для названия HTTF	р. Шаб	ілон для значения HTTP	- Создан	Изменен	Комментарий	
		User-Agent	Y	ОУО	supaadmin 09.12.2018 19:27		комментарий	₫ ⊕
		User-Agent2	Y	0Y02	supaadmin 09.12.2018 19:27		Введите коммент.	₫ ⊕

Рис. 6.66. Формирование шаблона для добавления заголовка

Для добавления нового условия на добавление заголовка, нажмите кнопку **Добавить шаблон** в строке сформированного условия.

## 6.5.6.2. Изменение заголовка

Для изменения заголовков при обработке HTTP-запросов следует создать один или несколько шаблонов в разделе **Политика > Шаблоны > Изменение заголовка**. Общие принципы работы с шаблонами описаны в разделе <u>6.4.3</u>.

Для создания шаблона необходимо:

- 1. Перейти в соответствующий раздел и нажать кнопку **Добавить шаблон изменения** заголовка (<u>Рис.6.67</u>).
- 2. Указать имя шаблона (не более 200 символов), а также указать необходимые значения для его создания (см. <u>Табл.6.33</u>).

## 3. Нажать кнопку Сохранить и применить политику.

Табл. 6.33. Перечень атрибутов для формирования шаблона

Название	Описание
Шаблон для названия НТТР-заголовка	Наименование HTTP-заголовка или шаблон наиме- нования (не более 200 символов)
Шаблон для значения НТТР-заголовка	Значение НТТР-заголовка или шаблон значения (не более 500 символов)
Шаблон для заменяемой части значения	Значение изменяемой части заголовка либо шаблон значения (не более 500 символов)
На что заменить	Значение, на которое будет изменена часть, задан- ная в предыдущем поле (не более 500 символов)
Комментарий	Дополнительные сведения о шаблоне (указывать необязательно; не более 500 символов)

Полит	ика / Шаблоны / Изм	енение заголовка 🕜				Пр	именить политику
Доба	зить список шаблонов измен	нения заголовков				Поиск по названию	٩
	Название				Создан	Изменен	
	Изменение контента				admin 17.07.2024 22:2	admin 17.07.2024 22:42	Q <del>C</del>
	Название				Создан	Изменен	
$\sim$		Добавить шаблон				Импорт	Экспорт 🗍
Назва	ние	Изменение контента					
Комме	ентарий	Введите комментарий					
			Создан	Изменен	Комментарий		
con	itent_type	text/html; charset=ut	admin 17.07.2024 22:28	admin 17.07.2024 22:42	Введите коммент	арий	
utf	-8	koi8-r					

Рис. 6.67. Формирование шаблона для изменения заголовка

Для добавления нового шаблона на изменение заголовка необходимо нажать кнопку **Добавить шаблон** в строке сформированного условия.

## 6.5.6.3. Удаление заголовка

Для удаления заголовков при обработке HTTP-запросов создайте один или несколько шаблонов в разделе **Политика > Шаблоны > Удаление заголовка**. Общие принципы работы с шаблонами описаны в разделе <u>6.4.3</u>.

Для создания шаблона:

- 1. Перейдите в соответствующий раздел и нажмите кнопку **Добавить шаблон удаления** заголовка (<u>Рис.6.68</u>).
- 2. Укажите имя шаблона (не более 200 символов) и необходимые значения для его создания:
  - Шаблон для названия НТТР-заголовка наименование НТТР-заголовка или шаблон наименования (не более 250 символов);
  - Шаблон для значения HTTP-заголовка значение HTTP-заголовка или шаблон значения (не более 500 символов);
  - Комментарий дополнительные сведения о шаблоне (указывать необязательно; не более 500 символов).
- 3. Нажмите кнопку Сохранить и примените политику.

Ша	блоны / Удаление заголовка		Применить	толитику
Д	обавить шаблон удаления заголовка		Поиск по названию	٩
	Название С	оздан	Изменен	
>	del1 a	dmin 8.12.2018 11:30		00
>	Сохранить Отмена			Импорт Экспорт 🗍
	Название:	any		
	Шаблон для названия Н Шаблон для	я значения F Создан	Изменен	Комментарий
	User-agent .*			Введите комм 🕀

Рис. 6.68. Формирование шаблона для удаления заголовка

Для добавления нового условия на удаление заголовка в строке сформированного условия нажмите кнопку **Добавить шаблон**.

## 6.5.6.4. Шаблоны страниц

Шаблоны страниц служат для автоматической генерации уведомительных страниц. Возможно использовать предопределенный текст и подстановку той или иной информации о переданных по сети данных, которые послужили причиной отображения уведомления. Примером использования шаблонов может быть отображение сообщений об ошибках, текст которых определяется в шаблоне.

Для управления шаблонами страниц следует в разделе **Политика > Шаблоны > Шаблоны страниц** и выбрать необходимый шаблон или создать новый. Для отображения содержимого шаблона необходимо нажать в любой области строки с соответствующим шаблоном.

Общие принципы работы с шаблонами описаны в разделе 6.4.3.

Шаблон можно создавать в виде HTML-документа, в том числе с изображением. Для этого в Solar NGFW встроен редактор TinyMCE v4, который позволяет:

- формировать таблицы;
- писать и редактировать исходный код;
- работать с текстом, используя различные инструменты форматирования;
- вставлять изображения и ссылки на веб-ресурсы;
- выполнять предпросмотр страницы.

Для формирования или редактирования шаблона страницы необходимо:

 Нажать кнопку Добавить шаблон страницы и сформировать шаблон с помощью объектов для работы с HTML-документом, которые находятся на панели инструментов (<u>Рис.6.69</u>).





Рис. 6.69. Формирование шаблона страницы

В тексте HTML-документа могут использоваться подстановочные символы, определенные в системе (см. <u>Приложение С, Использование подстановочных символов</u>). Они будут автоматически заменяться конкретными значениями в процессе генерации уведомительного сообщения. Подстановочные символы возможно выбрать в раскрывающемся списке **Параметры подстановки** на панели инструментов.

## 6.6. Примеры настройки политики фильтрации

Далее приведены примеры настройки правил и исключений для решения реальных задач.

В каждом разделе описано формирование правила и/или исключения конкретного слоя политики фильтрации в зависимости от поставленной задачи.

Для получения подробных сведений об инструментах политики и управлении ими перейдите в раздел <u>6.5</u>.

## 6.6.1. Использование межсетевого экрана в политике фильтрации

## 6.6.1.1. Блокировка ресурса по IP-адресу

Задача: запретить доступ к ресурсу vk.com по его IP-адресам

## Порядок действий для решения задачи:

- 1. Узнайте IP-адреса, присвоенные vk.com на сайте <u>https://whois.ru/</u>.
- 2. В разделе Политика в слое Межсетевой экран > Фильтр транзитного трафика создайте правило и укажите параметры настройки (см. <u>Рис.6.70</u>).
- 3. Сохраните правило и примените политику.

## Примечание

При данной настройке политики страница с шаблоном блокировки не отображается, т.к. запрет идет на сетевом уровне L3.

Фильтр транзитного тра	афика: созда	ть правило	×						
Включено									
Название	Заблокиро	Заблокировать VK							
Комментарий	Введите ко	мментарий							
Приоритет	Укажите пр	риоритет Всего прав	зил в слое: 4						
Журналировать									
Действие	🙁 Запрети	ИТЬ	v						
Фрагментированный трафик		Фильтр транзитного тра	афика: создать правило	×					
Состояние соединения	Любое	Включено							
Входящий интерфейс	Введите и	Фрагментированный трафик							
Исходящий интерфейс	Сетевой инте Введите и	Состояние соединения	Любое	$\vee$					
		Входящий интерфейс	Введите интерфейс						
		Исхоляциий интерфейс	Сетевой интерфейс. Например: eth0						
		пекодладининтерфене	Сетевой интерфейс. Например: eth0	-1					
		Источник	Любой						
			IP, диапазон вида IP-IP, маска подсети IP/xx или один MAC-адрес XX:XX:XX:XX:XX:XX						
		Назначение	♥ 84.240.190.0/22 × ♥ 87.240.139.0/22 × ♥ 93.186.255.0/22 ×						
		Протоколы	л с домпазан онде и не ним насели надеение у ка Любой	~					
		Порты	Назначения 🗸 Не задано	$\mathbf{v}$					
		Приложения	Допустимо только для протоколов ICP и UUP Не используется	V					
			Сохознить Отменить						

Рис. 6.70. Формирование правила

# 6.6.1.2. Блокировка пользователя путем его идентификации на сетевом уровне: по МАС-адресу

Задача: заблокировать пользователей по МАС-адресу устройств, с которых они выходят в сеть Интернет

## Порядок действий для решения задачи:

## Примечание

Блокировка по МАС-адресу работает только при выборе входящих или транзитных пакетов.

 В зависимости от направления трафика выберите нужный слой в разделе Политика > Межсетевой экран: Фильтр транзитного трафика или Фильтр входящего трафика (см. <u>Рис.6.71</u>).

#### Примечание

В одном правиле задайте условие и на МАС-адрес, и на приложения. Если в поле **Источник** (для входящего и транзитного направления) будет введено значение **МАС-адрес**, поле **Приложения** станет неактивным для установки значений.

#### 2. Сохраните правило и примените политику.

Фильтр входящего траф	ика: создать правило			
Включено				
Тазвание	Блок			
(омментарий	Введите комментарий			
Іриоритет	Укажите приоритет Всо	Фильтр входящего трас	рика: создать правило	
Журналировать		Включено		
ействие	😢 Запретить	Действие	😢 Запретить	
остояние соединения	Любое	Состояние соединения	Любое	
Входящий интерфейс	Введите интерфейс Сетевой интерфейс. Например: eth0	Входящий интерфейс	Введите интерфейс	
1сточник	▶ <b>f8:0d:ac:0c:56:80</b> × IP, диапазон вида IP-IP, маска подсети	Источник	Сетевои интерфеис. Например: etr	
значение	Любое	Назначение	IP, диапазон вида IP-IP, маска подсе Любое	ти IP/хх или один
	Сохра	Протоколы	IP, диапазон вида IP-IP или маска п ТСР ×	одсети IP/xx
		Порты	Назначения 🗸 Не	2 задано
		Приложения	Доп Не используется	устимо только для
			Не может использоваться совмест	но с условием на

Рис. 6.71. Формирование правила

## Примечание

Чтобы отображать журнальные записи о срабатывании этого правила в разделе **Статистика > Журнал соединений**, установите флажок **Журналировать**.

## 6.6.1.3. Объединение источников запроса под одним IP-интерфейсом (SNAT)

**Задача:** скрыть вручную диапазон IP-адресов локальной сети под одним IP-интерфейсом (IP-адресом)

## Порядок действий для решения задачи:

- 1. В разделе Политика в слое Межсетевой экран > Трансляция адресов создайте правило и укажите параметры настройки (см. <u>Рис.6.72</u>):
  - Действие тип скрытия источников запроса;
  - Источник локальный IP-адрес или диапазон IP-адресов;
  - Интерфейс сетевой интерфейс для скрытия;
  - **SNAT IP (Внешний адрес)** IP-адрес, на который будет заменен IP-адрес источника для трафика NAT.

#### Примечание

Чтобы отображать журнальные записи о срабатывании этого правила в разделе **Система > Журналы**, установите флажок **Журналировать**.

2. Сохраните правило и примените политику.

Создать правило			X
Включено			
Название	SNAT		
Комментарий	Введите комментарий		
Приоритет	Укажите приоритет Всего прави	Создать правило	
Действие	PAT (Masquerading)	Включено	
Журналировать		Действие	Destination NAT
Интерфейс	ens192	Журналировать	
	Сетевой интерфейс. Например: eth0	Интерфейс	Введите интерфейс
Источник	♥ 192.168.205.200-192.168.205.209 ×		Сетевой интерфейс. Например: eth0
	IP, диапазон вида IP-IP или маска подсети IP/xx	Источник	Любой
азначение	Любое		IP, диапазон вида IP-IP или маска подсети I
	IP, диапазон вида IP-IP или маска подсети IP/xx	Назначение	♥ 10.201.31.10×
Іротокол	Любой		IP, диапазон вида IP-IP или маска подсети I
	Сохранить	Протокол	TCP
		Порты назначения	440-450 ×
			Число (меньше 65536) или диапазон
		Целевой адрес	10.202.32.10:8443
			Целевой адрес в формате IP:PORT

Рис. 6.72. Формирование правила

## 6.6.1.4. Фильтрация трафика на основе приложений

Задача: запретить прохождение трафика приложения YouTube для всех пользователей

## Порядок действий для решения задачи:

1. В разделе Политика в слое Межсетевой экран > Фильтр транзитного трафика создайте правило и укажите параметры настройки (см. <u>Рис.6.73</u>). 2. Сохраните правило и примените политику.

Фильтр транзитного тра	афика: создать правило		×			
Включено						
Название	Запрет YouTube					
Комментарий	Введите комментарий					
Приоритет	Укажите приоритет	Фильтр транзитного тра	афика: создать правило	x		
Журналировать		Включено				
		Фрагментированный трафик				
Действие	😢 Запретить	Состояние соединения	Любое	~		
Фрагментированный трафик		Входящий интерфейс	Введите интерфейс			
Состояние соединения	Любое		Сетевой интерфейс. Например: eth0			
		Исходящий интерфейс	Введите интерфейс			
Входящий интерфейс	Введите интерфейс	Источник	сетевои интерфеис. например: етло Любой			
	Сетевой интерфейс. Наприм		IP, диапазон вида IP-IP, маска подсети IP/хх или один MAC-адрес XX:XX:XX:XX:XX:XX:XX			
исходящии интерфеис	введите интерфеис	Назначение	Любое			
			IP, диапазон вида IP-IP или маска подсети IP/xx			
		Протоколы	Любой	$\sim$		
		-				
		Порты	ИСТОЧНИКА V НЕ ЗАДАНО			
		Приложения	YouTube × YouTubeUpload ×	$\sim$		
		•				
				-		
			Сохранить Отменить			

Рис. 6.73. Формирование правила

## Примечание

Чтобы в разделе **Журнал соединений** отображалось срабатывание данного правила, в меню создания правила установите флажок Журналировать.

## 6.6.1.5. Объединение источников запроса под одним IP-интерфейсом (MASQUERADE)

Задача: автоматически скрыть диапазон IP-адресов локальной сети (источники запроса) под одним IP-интерфейсом (IP-адресом)

#### Порядок действий для решения задачи:

- 1. В разделе Политика в слое Межсетевой экран > Трансляция адресов создайте правило и укажите параметры настройки (см. <u>Рис.6.74</u>):
  - Действие тип скрытия IP-адресов;
  - Источник локальный IP-адрес или диапазон IP-адресов;
  - Интерфейс сетевой интерфейс для скрытия IP-адресов.

## Примечание

Чтобы отображать журнальные записи о срабатывании этого правила в разделе **Система > Журналы**, установите флажок **Журналировать**.

2. Сохраните правило и примените политику.

Редактировать правил	o AUTO NAT	х
Включено		
Название	AUTO NAT	
Комментарий	Введите комментарий	
Действие	Автоматический NAT (MASQUERADE)	$\vee$
Журналировать		
Источник	♥ 192.168.205.0/24×	
	IP, диапазон вида IP-IP или маска подсети IP/xx	
Интерфейс	ens192	
	Сетевой интерфейс. Например: eth0	
	Сохранить Отменить	

Рис. 6.74. Формирование правила

## 6.6.1.6. Скрытие IP-адреса назначения запроса пользователя (DNAT)

Задача: перенаправить запрос пользователя путем преобразования адреса назначения в IP-заголовке пакета

#### Порядок действий для решения задачи:

1. В разделе Политика в слое Межсетевой экран > Трансляция адресов создайте правило и укажите параметры настройки (см. <u>Рис.6.75</u>).

#### Примечание

В поле **Целевой адрес** укажите внешний адрес, на который необходимо перенаправить IP-адрес назначения.

2. Сохраните правило и примените политику.

Создать правило			×	
Включено	C			
Название	Скрытие			
Комментарий	Введите комментарий	Создать правило		×
Приоритет	Укажите приоритет Всего пра	Включено		
Действие	Destination NAT	Действие	Destination NAT	$\sim$
Журналировать		Журналировать		
Интерфейс	Введите интерфейс	Интерфейс	Введите интерфейс	
Источник	Сетевой интерфейс. Например: eth0 Любой	Источник	Cereboli wrepdelic. Hanpiwep: eth0 Любой	
Назначение	IP, диапазон вида IP-IP или маска подсети IP/x: Ф 10.201.31.10 ×	Назначение	P: днапазен вида IP-IP или маска подсети IP/xx     ♥ 10.201.31.10 ×	
Протокол	IP, диапазон вида IP-IP или маска подсети IP/x: ТСР	Протокол	IP, днапазон вида IP-IP или маска подсети IP/xx ТСР	$\vee$
	Сохранить	Порты назначения	440-450 ×	~
		Целевой адрес	10.202.32.10:8443	
			Целевой адрес в формате IP-PORT	

Рис. 6.75. Формирование правила

## Примечание

Чтобы отображать журнальные записи о срабатывании этого правила в разделе **Система** > **Журналы**, установите флажок **Журналировать**.

## 6.6.1.7. Блокирование HTTPS-трафика

Задача: заблокировать HTTP-трафик с помощью МЭ и nDPI.

Порядок действий для решения задачи:

- 1. В разделе Политика в слое Межсетевой экран > Фильтр транзитного/входящего/исходящего трафика создайте правило и укажите параметры настройки:
  - Приложения Safe > TLS;
  - Протоколы ТСР;
  - Порты назначения 443, 8443.

Фильтр транзитного тр	афика: создать правило	Х
Включено		
Фрагментированный трафик		
Состояние соединения	Любое	×
Входящий интерфейс	Выберите интерфейс	V
Исходящий интерфейс	Сетевой интерфейс. Например. есло Выберите интерфейс	V
Источник	Сетевой интерфейс. Например: eth0 Любой	
Назначение	IP, диапазон вида IP-IP, маска подсети IP/xx или один MAC-адрес XX:XX:XX:XX:XX:XX Любое	
_	IP, диапазон вида IP-IP или маска подсети IP/xx	
Протоколы	TCP ×	~
Порты	Назначения v 443 × 8443 ×	V
Приложения	TLS x	~
	Сохранить Отменить	

Рис. 6.76. Формирование правила

2. Сохраните правило и примените политику.

## 6.6.2. Управление веб-сервисами и приложениями (nDPI)

Задача: для диапазона IP-адресов заблокировать доступ к приложению WhatsApp.

## Порядок действий для решения задачи:

- 1. В разделе Политика > Межсетевой экран > Фильтр транзитного трафика создайте правило и укажите приложение WhatsApp.
- 2. Сохраните правило и примените политику.

Включено				
Название	Блок WhatsApp			
Комментарий	Введите комментарий	Редактировать правил	о Блок WhatsApp	×
Приоритет	5	Включено		
Журналировать		Фрагментированный трафик		
		Состояние соединения	Любое	
Действие	😢 Запретить			
		Входящий интерфейс	Введите интерфейс	
Фрагментированный трафик			Сетевой интерфейс. Например: eth0	
ipaquit		Исходящий интерфейс	Введите интерфейс	
Состояние соединения	Любое		Сетевой интерфейс. Например: eth0	
		Источник	♥ 192.168.100.0·192.168.100.255 ×	
Входящий интерфейс	Введите интерфейс		IP, диапазон вида IP-IP, маска подсети IP/хх или один MAC-адрес XX:XX:XX:XX:XX:XX	
	Сетевой интерфейс. Например: е	Назначение	Любое	
Исходящий интерфейс	Введите интерфейс		IP, диапазон вида IP-IP или маска подсети IP/xx	
		Протоколы	Любой	
	Ca	Порты	Назначения у Не залано	
		hopital	Допустимо только для протоколов ТСР и UDP	
		Придожоция	WhatsApp	

Рис. 6.77. Формирование правила

## Примечание

При включенном шифровании в торрент-клиентах нельзя распознать протокол BitTorrent внутри TCP-соединения (передача данных через протокол UDP распознается). При отключении шифрования детектирование выполняется в полной мере, как при TCP-, так и UDP-соединении.

# 6.6.3. Исключение сигнатуры для правил Системы предотвращения вторжений

Задача: исключить ложное срабатывание выбранной сигнатуры при работе с PKGфайлами. Например, 2017294 на используемом APM.

## Порядок действий для решения задачи:

1. В разделе Политика в слое Межсетевой экран > Предотвращение вторжений создайте исключение и укажите параметры настройки.

## Примечание

Можно сформировать несколько типов исключений:

- по ID-сигнатуры (см. <u>Рис.6.78</u>),
- по набору параметров: Источник, Назначение, Порт назначения (см. <u>Рис.6.79</u>).

Сохраните и примените политику.

Создать исключение		х
Включено		
Название	Исключение сигнатуры	
Комментарий	Заявка №1502	
Исключение на основе	ID сигнатур (правил)	$\vee$
ID-Сигнатуры	2017294 ×	$\vee$
	Сохранить Отменить	



Создать исключение		x
Включено		
Название	Исключить трафик для пользователя	
Комментарий	Заявка №1512	
Исключение на основе	Сетевых параметров	$\sim$
Источник	♥ 10.195.163.155 ×	
	IP-адрес или маска подсети IP/xx. Обязательно если не указаны остальные поля	
Назначение	♥ 8.8.8.8 ×	
	IP-адрес или маска подсети IP/хх	
Порты назначения	Не задано	$\sim$
	Сохранить Отменить	

Рис. 6.79. Формирование исключения по набору параметров: Источник, Назначение, Порт назначений

## 6.6.4. Настройка доступа без аутентификации

Задача: выдать всем пользователям компании доступ к ресурсу drive.google.com без ввода логина и пароля.

## Порядок действий для решения задачи:

- 1. В разделе Политика > Справочники > Ресурсы создать список, который содержит в себе следующие ресурсы:
  - www.googleapis.com;
  - Ih3.googleusercontent.com;
  - play.google.com;

- accounts.google.com;
- ssl.gstatic.com;
- crl.pki.goog;
- ocsp.pki.goog.
- 2. В слое Контентная фильтрация > Доступ без аутентификации раздела Политика создать правило и задать параметры проверки (см. <u>Рис.6.80</u>).
- 3. Сохранить правило и применить политику.

1	Solar NGFW			Поиск персон	ы ۹ 🗜
۵	Настройки Импорт Экспор	Romanuko / Kouros	алион финалогиин ( Востоя 600 оказанандинонии - Ф		Применить политику
	o <del>y</del> → NAI	создать правило	^	юиск по названию, пе 🔍	Настройка колонок
\$	Карание вторжений	Включено		а и кем изменено Доп.	Вкл.
<b></b>	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ	название	Google Drive		
c <sub>e</sub>	🙇 Доступ без аутентификации	Комментарий	Введите комментарий		
0.	👫 Вскрытие HTTPS	Приоритет	Укажите Всего правил в слое: 0		
යාකු යැක	🛞 Перенаправление по ICAP	Не аутентифицировать и	Свазать автоматицасим		
	ሱ Фильтрация запросов 💮	пе аутентифицировать и	Consult diatronic information		
۲	Режим белого списка	Источник	Любой 🗸		
	🗘 Фильтрация ответов 🕑	Назначение	Вибрать (Р-диклазон или ввести: (Р.диклазон вида (Р - (Р или маску подсети (Р/хх Сооде Drive x	)	
	🖶 внешние подключения	Расшилециые настлойии	Список ресурсов или полное доменное имя		
	ІСАР-серверы	госалранные настронки			
	Прокси-серверы		Сохранить Отланить		
	🛞 объекты политики	>		I4 < 1 >	ы 207 стр. ∨
Ŕ	СПРАВОЧНИКИ				

Рис. 6.80. Формирование правила

## 6.6.5. Исключение вскрытия HTTPS-трафика пользователей

**Задача:** исключить расшифровку HTTPS-трафика для отдельных сотрудников, чтобы получить доступ к веб-почте.

## Порядок действий для решения задачи:

1. В слое Контентная фильтрация > Вскрытие HTTPS раздела Политика создать правило вскрытия HTTPS-трафика (<u>Рис.6.81</u>).

## Примечание

В полях Источник/Назначение/Заголовки по умолчанию указаны значения Любой/Любое/Не задано. Изменять значения для решения данной задачи не требуется.

<b>*</b> *	Solar NGFW			Поиск персон	ы Q 🗶=
ଜ		Создать правило	x		
	🔛 МЕЖСЕТЕВОЙ ЭКРАН	Включено	• • Правило Исключение	по названию, пе 🔍	
<del>©</del>	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ	Название	Вскрытие (все)		
Ŗ	🧟 Доступ без аутентификац	Комментарий	Вскрыть весь трафим	гда и кем изменено	Вкл.
$\mathfrak{R}_{p}$		Приоритет	Укажите		
L	🛞 Перенаправление по ICAP		Всего правил в слое: 0		
<b>(</b>	🕢 Фильтрация запросов	Источник	Любой 🗸		
۲	🗘 Фильтрация ответов	Назначение	Персона, Группа персон, IP-дикапазон, IP, дикапазон вида IP - IP или маска подсети IP/xx Любое V		
	🗄 внешние подключения	7970 900 99	Список ресурсов, категория или полное имя хоста (включая поддомены)		
	🛞 ОБЪЕКТЫ ПОЛИТИКИ	291 010888	ne salamu 🗸 🗸		
	СПРАВОЧНИКИ		Сохранить Отменить		
\$7	🛱 шаблоны				ы 20 / стр. ∨

Рис. 6.81. Формирование правила

2. Создать **исключение**, которое запретит вскрывать HTTPS для определенных персон при использовании веб-почты (см. <u>Рис.6.82</u>).

## Примечание

В поле **Источник** указать персоны, для которых расшифровка HTTPS-трафика не будет выполняться.

3. Сохранить и применить политику.

<b>*</b> *	Solar NGFW			Поиск персон	ы Q 🛵
ଜ		Создать правило	x		
æ	🔛 МЕЖСЕТЕВОЙ ЭКРАН	Protocologica	Правило Исключение	по названию, пе Q	
\$	ျံး Фильтр	Название	Не вскрывать веб-почты		
Ŗ	→ nat	Комментарий	Введите комментарий	гда и кем изменено	
Ry	<u>к</u> » Предотвращение вторжен	Приоритет	Vkawure_		
So	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ		Всего правил в слое: О		
(E	🛕 Доступ без аутентификаци	Источник	↓ Иванов Иван Иванович × ∨		
۲		Назначение	Персона, Группа персон, IP-диапазон, IP-диапазон вида IP- IP или маска подсети IP/xx  Т Ингеонет-коммуникация / Веб-ПОЧТА Х У		
	🛞 Перенаправление по ICAP		Список ресурсов, категория или полное имя хоста (включая поддомены)		
	👍 Фильтрация запросов	Заголовки	Не задано 🗸		
	🗘 Фильтрация ответов				
			Сохранить Отменить		
	са внешние подключения				
Ŕ	ІСАР-серверы	Всего О Строк			207 crp. V

Рис. 6.82. Формирование исключения

## 6.6.5.1. Исключение ресурсов, которые обнаруживают подмену сертификата

В Solar NGFW с помощью контентной фильтрации можно вскрывать HTTPS-трафик, проверять его по заданным политикам и шифровать его обратно, подменяя сертификат на свой.

Ресурсы, использующие систему фильтрации веб-приложений, могут заблокировать такое соединение. В этом случае в режиме отладки веб-браузера (для вызова нажмите F12) будет ответ на заблокированный запрос от системы фильтрации, например:

- < HTTP/1.1 200 OK
- < Server: QRATOR
- < Date: Wed, 05 Oct 2022 15:01:28 GMT
- < Content-Type: text/html; charset=utf-8
- < Content-Length: 1323594
- < Connection: **keep-alive**
- < Keep-Alive: timeout=15

Также некоторые приложения (например, Citrix, десктопные версии веб-сервисов и файлообменных ресурсов (Dropbox, Яндекс Диск и т.д.), приложения банк-клиент) содержат встроенный клиентский сертификат. Когда Solar NGFW вскрывает HTTPS-трафик такого приложения и подменяет его сертификат на свой, трафик пользователя блокируется.

Чтобы решить эту проблему:

1. В слое Справочники > Ресурсы раздела Политика добавьте список ресурсов для исключения вскрытия HTTPS-трафика (<u>Рис.6.83</u>).

Настройки Импорт Экспорт	Политика / Справочники / Ресурсы 🕜		Применить политику
IP-диапазоны	Добавить список ресурсов	Поиск по названию	٩
Лимиты трафика	Название	Создан Изменен	
Расписания	> mail domains	isa 24.08.2022 18:43	00
Условия на заголовки	> drophox	isa 04.10.2022 13:25	00
Пользователи (Basic Auth)			
💿 справочники 🗸 🗸			
Адреса электронной почты			
Ключевые слова			
Ресурсы			
Файлы		A CONSTRUCTION	

Рис. 6.83. Добавление списка ресурсов

2. В слое Контентная фильтрация > Вскрытие HTTPS создайте исключение вскрытия HTTPS-трафика.

## Примечание

Трафик, добавленный в исключение, не будет инспектироваться по другим политикам. Добавляйте трафик только доверенных приложений.

3. Создайте исключение, которое при использовании созданного ресурса запретит вскрывать HTTPS для всех (<u>Рис.6.84</u>).

â	Настройки Импорт Экспорт	Полит	ика / Контентная фильт	рация / Воррагие НТТР5 💿	
	🔛 межсетевой экран 🗸 🗸				Поис
	б(]‡ Фильтр	Количе	ство Исключений 🔍 Коли	чество Правил 💿	
	→ nat		Создать правило	x	
ಕ್ಕ	🖳 Контроль приложений		Включено	Правило     О Исключение	
<b>£</b>	Карание вторжений		Название	except dropbox	
<b>a</b>	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🗸 🗸		Комментарий	Введите комментарий	
	🙇 Доступ без аутентификации		Метонник	Refea	
	BCKPЫTИE HTTPS		источник	Лиосии • Персона, Группа персон, IP-диапазон, IP, диапазон вида IP - IP или маска подсети IP/xx	
	🤫 Перенаправление по ICAP		Назначение	dropbox ×	
	🚓 Фильтрация запросов 💮 🗸		Заголовки	Списки ресурсов П mail domains	
	🗄 редирект			C dropbox	
	🖒 Фильтрация ответов 💮 🗸			патегории ресурсов показать дерево Сохранить Отменить	
	ii test				
	😫 внешние подключения 🗸 🗸				

Рис. 6.84. Создание исключения

4. Сохраните и примените политику.

## 6.6.6. Блокировка загрузки ZIP-файлов по протоколу HTTPS

Задача: запретить всем пользователям компании загружать файлы с расширением ZIP по протоколу HTTPS.

## Порядок действий для решения задачи:

 В слое Контентная фильтрация > Вскрытие НТТРЅ раздела Политика создать правило вскрытия HTTPS-трафика (Рис.6.85). Сохранить правило и применить политику.

## Примечание

В полях Источник/Назначение/Заголовки по умолчанию указаны значения Любой/Любое/Не задано. Изменять значения для решения данной задачи не требуется.

Создать правило		х
Включено	<ul> <li>Правило</li> <li>Исключение</li> </ul>	
Название	Вскрытие HTTPS трафика	
Комментарий	Введите комментарий	
Источник	Любой Пелона Гоупра персон IP-пиалазон IP-пиалазон вида IP- IP или маска полсети IP/их	$\vee$
Назначение	Любое	$\sim$
	Список ресурсов, категория или полное имя хоста (включая поддомены)	
Заголовки	Не задано	$\sim$
	Сохранить Отменить	

Рис. 6.85. Формирование правила

- 2. В слое Фильтрация запросов создать новый слой Certificate.
- 3. В слое Фильтрация запросов > Certificate создать правило и установить для параметра Основное действие значение Проверить сертификат (см. <u>Рис.6.86</u>).

Сохранить правило и применить политику.

Создать правило		×
Включено	• Правило Исключение	
Название	Проверка сертификата	
Комментарий	Введите комментарий	
Действия		
Основное	Ороверить сертификат У Инструкция по установке По умолчанию	$\sim$
	Добавить дополнительное действие 🗸	
Условия		
Источник	Любой	$\sim$
	Персона, Группа персон, IP-диапазон, IP, диапазон вида IP - IP или маска подсети IP/xx	
Назначение	Любое	$\sim$
	Список ресурсов, категория или полное имя хоста (включая поддомены)	
Расширенные настройки	Показать	
	Сохранить Отменить	

Рис. 6.86. Формирование правила

- 4. В слое Фильтрация ответов создать новый слой Блокировка ответов с ZIP-файлами.
- 5. В слое Фильтрация ответов > Блокировка ответов с ZIP-файлами создать правило и задать параметры (см. <u>Рис.6.95</u>):
  - Основное действие Заблокировать;
  - Типы файлов Архивы и сжатые файлы.

Сохранить правило и применить политику.

Создать правило			x
Включено	• Правило	Исключение	
Название	Блокировка ответов с ZIP-файлами	Создать правило	x
Комментарий	Введите комментарий	Включено	• Правило Исключение
Действия		Протокол	Не задано 🗸
Основное	😣 Заблокировать	Методы	Не задано
		Порты	Не залано У
	Добавить дополнительное действие	Заголовки	Не запано У
Условия			
Источник	Любой	типы фаилов	архивы и сжатые фаилы ×
	Персона, Группа персон, IP-диапазон, IP, диаг	Файлы	Не задано 🗸
Назначение	Любое	Размер файлов	От Не ограничен МБ 🗸
Расширенные настройки	Показать		
		Ключевые слова	Выберите из списка 🗸
		Расписания	Выберите из списка
		Лимиты трафика	Без ограничений 🗸
			Сохранить Отменить

Рис. 6.87. Формирование правила

## 6.6.7. Перенаправление трафика пользователей антивирусу

Задача: необходимо заблокировать загрузку тестового вируса *eicar* путем перенаправления трафика антивирусу для проверки.

## Порядок действий для решения задачи:

1. В разделе Политика > Внешние подключения > ICAP-серверы создать ICAP-сервер (<u>Рис.6.88</u>), через который будет передаваться трафик.

*	Solar NGFW		Поиск персоны Q 🛵
ណ	Настройки Импорт Экспорт	Политика / Внешние подключения / КАР-серверы 🕜	Применить политику
E	🛞 Перенаправление по ІСАР	Добавить КАР-сервер Импорт Экспорт Пои	
\$	👍 Фильтрация запросов 🕒 🗸	Имя сервера URL Комментарий Создан	Изменен
₩.	🗘 Фильтрация ответов 🛛 🕣 🗸	Local regmod icap://localhost:1344/regmod 05.05.2023 13:4	9
Ry	🗄 внешние подключения 🗸 🗸	Local respmod icap://localhost:1344/respmod 05.05.202313:4	0
£,	ІСАР-серверы	🗸 Сохранить Отмена	
Œ	Прокси-серверы	Имя сервера Антивирус	
		ICAP URL icap://rtulocal:1344	
Ē	🍥 ОБЪЕКТЫ ПОЛИТИКИ 🗸 🗸	Комментарий Проверка вирусов	
	IP-диапазоны		
	Лимиты трафика		
	Расписания		
	Условия на заголовки		
\$	Пользователи (Basic Auth)		

Рис. 6.88. Добавление ІСАР-сервера

2. В слое **Перенаправление по ICAP** раздела **Политика** создать правило и задать параметры проверки (<u>Рис.6.89</u>).

## Примечание

Поле **Имя сервера** – название сервера, на который будет перенаправлен трафик: Local **respmod** (создается автоматически после настройки антивируса);

Поле **Шаблон блокировки** – необходимый шаблон, который необходимо создать заранее (<u>6.5.6</u>).

В полях **Источник/Назначение** по умолчанию указаны значения **Любой/Любое**. Изменять значения не следует.

Создать правило		x
Включено	О Правило Исключение	
Название	Проверка на вирусы	
Комментарий	Запрет скачивания тестового вируса	
Действие	🚸 Передавать ответы	$\vee$
Имя сервера	Local respmod	$\vee$
Шаблон блокировки	Блокировка: Запрет скачивания файла по решению антивируса	V
Уведомлять		
Источник	Любой	V
	Персона, Группа персон, IP-диапазон, IP, диапазон вида IP - IP или маска подсети IP/xx	
Назначение	Любое	$\sim$
	Список ресурсов, категория, полное имя хоста (включая поддомены), IP или диапазон вида IP - IP	
Расширенные настройки	Показать	
	Сохранить Отменить	

Рис. 6.89. Формирование правила

3. Сохранить и применить политику.

## 6.6.8. Управление фильтрацией запросов пользователей

Задача: запретить всем пользователям компании использовать веб-ресурс mail.ru.

Порядок действий для решения задачи:

1. В разделе Политика > Фильтрация запросов создать новый слой (Рис.6.90).





2. В добавленном слое создать новое правило и задать параметры проверки (Рис.6.91):

## Примечание

Шаблон блокировки необходимо создать заранее.

\$**	Solar NGFW	Создать правило		×	Поиск персон	ы ۹ 🛃
	Настройки Импорт	Включено	• Правило Исключение		(	
	99 mai	Название	Banper mail.ru		по названию, пе 🔍	
	Детистика и предотвращение вторжен	Комментарий	Введите комментарий			
	👾 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ	Приоритет	Укажите		м изменено Доп.	
	🙇 Доступ без аутентификаци		Всего правил в слое: 0			
	Вскрытие HTTPS	Действия				
540	😧 Перенаправление по ІСАР	Основное	8 Заблокировать У Блокировка: Нарушение политики безопасности	~		
	💮 Фильтрация запросов		Шэблон страницы блокировки Добавить дополнительное действие V			
	Режим белого списка	Условия		_		
	🗄 3anper maiLru	Источник	Любой	~		
	🗘 Фильтрация ответов		Персона, Группа персон, IP-диапазон, IP, диапазон вида IP - IP или маска подсети IP/xx			
	🔒 внешние подключения	Назначение				
	ІСАР-серверы		Сохранить Отменить			

Рис. 6.91. Формирование правила

3. Сохранить и применить политику.

## 6.6.9. Управление фильтрацией ответов пользователей

Задача: запретить определенным подразделениям компании скачивать файлы мультимедиа в рабочее время.

#### Порядок действий для решения задачи:

1. В разделе Политика > Фильтрация ответов создать новый слой (Рис.6.92).

<u>م</u>	Solar NGFW
	🔛 межсетевой экран >
\$	💝 КОНТЕНТНАЯ ФИЛЬТРАЦИЯ 🗸 🗸
ş	🚊 Доступ без аутентификации
ħ,	🔐 Вскрытие HTTPS
ஆ	🛞 Перенаправление по ІСАР
(H	🦙 Фильтрация запросов 💮 🗸
۲	🗄 Режим белого списка 🕴
	🗄 3anper malLru 🚦
	🗘 Фильтрация ответов 💮 🗸
	🖶 внешние подключения 🗸 🗸
	ICAP-серверы
\$	Прокси-серверы



2. В добавленном слое создать новое правило и задать параметры проверки (Рис.6.93).

## Примечание

Шаблоны необходимо создать заранее.

Зключено	<ul> <li>Правило</li> <li>Исключение</li> </ul>	
Название	Запрет скачивания мультимедиа	
(омментарий	Введите комментарий	
1ействия		
Основное	😢 Заблокировать 🗸 Block page	
	Шаблон страницы блокировки	
	Добавить дополнительное действие 🗸	
словия		
Істочник	В Бухгалтерия х В Секретариат х	~
аголовки	He sagaite	
ипы файлов	Мультимедиа х	V
	Не задано	· · · ·
Райлы		
Райлы Размер файлов	От Не ограничен МБ	~
айлы азмер файлов (лючевые слова	От Не ограничен МБ Выберите	~
айлы азмер файлов (лючевые слова асписания	От Не ограничен МБ Выберите Рабочие часы х	~
айлы аэмер файлов (лючевые слова асписания Іимиты трафика	От Не ограничен МБ Выберите Рабочие часы х Без ограничений	

Рис. 6.93. Формирование правила

## 3. Сохранить и применить политику.

# 6.6.10. Блокировка загрузки содержимого черновиков в OWA в режиме обратного прокси

**Задача:** запретить всем пользователям компании загружать содержимое черновиков с веб-ресурса **Outlook Web Access (OWA)** в режиме обратного прокси. Блокировать письма по ключевому слову **Договор**.

## Порядок действий для решения задачи:

- 1. В разделе **Политика > Справочники > Ключевые слова** создать список, который содержит в себе следующие регулярные выражения:
  - .\*договор.\*;
  - .\*Договор.\*.

2. В слое Контентная фильтрация > Вскрытие HTTPS создать правило вскрытия HTTPS-трафика (<u>Рис.6.94</u>). Сохранить правило и применить политику.

## Примечание

В полях Источник/Назначение/Заголовки по умолчанию указаны значения Любой/Любое/Не задано. Изменять значения для решения задачи не требуется.

Создать правило		х
Включено	<ul> <li>Правило</li> <li>Исключение</li> </ul>	
Название	Вскрытие HTTPS трафика	
Комментарий	Введите комментарий	
Источник	Любой	~
	Персона, Группа персон, IP-диапазон, IP, диапазон вида IP - IP или маска подсети IP/xx	
Назначение	Любое	$\vee$
	Список ресурсов, категория или полное имя хоста (включая поддомены)	
Заголовки	Не задано	$\sim$
	Сохранить Отменить	

Рис. 6.94. Формирование правила

- 3. В слое Фильтрация запросов создать новый слой Connect.
- В слое Фильтрация запросов > Connect создать правило и задать параметры (см. <u>Рис.6.95</u>):
  - Основное действие Разрешить запрос;
  - Метод Connect.

Сохранить правило и применить политику.

Создать правило			×
Включено	💽 💿 Правил	ю Исключение	
Название	Разрешить доступ к OWA	Расширенные настройки	🔽 Показать
Комментарий	Введите комментарий	Протокол	Не задано 🗸
Действия		Методы	CONNECT × V
Основное	• Разрешить запрос	Порты	Не задано 🗸
	Добавить дополнительное	Заголовки	Не задано 🗸
Условия	·	Типы файлов	Не задано 🗸
Источник	Любой	Размер файлов	От Не ограничен МБ 🗸
	Персона, Группа персон, IP-диапаз		
Назначение	Любое	Ключевые слова	Выберите из списка 🗸
	Список ресурсов, категория или п	Расписания	Выберите из списка 🗸
		Лимиты трафика	Без ограничений У
			Сохранить Отменить

Рис. 6.95. Формирование правила

- 5. В слое Фильтрация ответов создать новый слой Блокировка ответов по ключевым словам.
- 6. В слое Фильтрация ответов > Блокировка ответов по ключевым словам создать правило и задать параметры (см. <u>Рис.6.96</u>):
  - Основное действие Заблокировать и шаблон страницы блокировки;
  - Созданный список ключевых слов;
  - Установить порог, равный 1;
  - Установить флажок **Использовать внешние распаковщики**. Сохранить правило и применить политику.

Создать правило			×	<
Включено	• Пр	авило ОКсключ	ение	
Название	Блокировка запросов			
Комментарий	Введите комментарий			
Действия				
)сновное	😢 Заблокировать	~	Блокировка: Нарушение политики безопасности 🛛 🗸	
			Шаблон страницы блокировки	
	Ключевые слова	Выражения для сл	ова "Договор"	
словия	Спор	оогом 1	Игнорировать повторы фраз	
точник		Целое число	<ul> <li>Искать вместе с элементами HTML-разм</li> </ul>	етки
значение				
	Расписания	Выберите из списк	3	
	Лимиты трафика	Без ограничений		
			Сохранить Отменить	

Рис. 6.96. Формирование правила

# 6.6.11. Блокировка загрузки писем с запрещенными файлами в ОША в режиме обратного прокси

Задача: запретить всем пользователям компании загружать письма с веб-ресурса OWA в режиме обратного прокси. Блокировать по хеш-функции файлов c6acbdb157e04fba48f4809d9b7e05c0.

## Порядок действий для решения задачи:

- 1. В разделе Политика > Справочники > Файлы создать список файлов. Тип идентификации файла указать MD5, значение – c6acbdb157e04fba48f4809d9b7e05c0.
- 2. В слое Контентная фильтрация > Вскрытие HTTPS раздела Политика создать правило вскрытия HTTPS-трафика (см. <u>Рис.6.94</u>). Сохранить правило и применить политику.

## Примечание

В полях Источник/Назначение/Заголовки по умолчанию указаны значения Любой/Любое/Не задано. Изменять значения для решения задачи не требуется.

Создать правило		х
Включено	Правило Исключение	
Название	Вскрытие HTTPS трафика	
Комментарий	Введите комментарий	
Источник	Любой	$\sim$
Назначение	Любое	$\sim$
	Список ресурсов, категория или полное имя хоста (включая поддомены)	
Заголовки	Не задано	$\sim$
	Сохранить Отменить	

Рис. 6.97. Формирование правила

- 3. В слое Фильтрация запросов создать новый слой Connect.
- В слое Фильтрация запросов > Connect создать правило и задать параметры (см. <u>Рис.6.98</u>):
  - Основное действие Разрешить запрос;
  - Метод **Connect**.

Сохранить правило и применить политику.

Создать правило			x	
Включено	• Правил	ю Исключение		
Название	Разрешить доступ к OWA	Расширенные настройки	🕑 Показать	
Комментарий	Введите комментарий	Протокол	Не задано	~
Действия		Методы	CONNECT ×	~
Основное	• Разрешить запрос	Порты	Не задано	
	Добавить дополнительное	Заголовки	Не задано	
Условия		Типы файлов	Не задано	
Источник	Любой	Размер файлов	От Не ограничен МБ	
	Персона, Группа персон, IP-диапаз			_
Назначение	Любое	Ключевые слова	Выберите из списка	
	Список ресурсов, категория или по	Расписания	Выберите из списка	
		Лимиты трафика	Без ограничений	
				-
			Сохранить Отменить	

Рис. 6.98. Формирование правила

5. В слое Фильтрация ответов создать новый слой Блокировка ответов по атрибутам файлов.

- 6. В слое Фильтрация ответов > Блокировка ответов по атрибутам файлов создать правило и задать параметры (см. <u>Рис.6.96</u>):
  - Основное действие Заблокировать;
  - Шаблон страницы блокировки;
  - Созданный список файлов.

Сохранить правило и применить политику.

Создать правил	0		>	×		
Включено		Правило Исклю	чение			
Название	Блокировать о	Блокировать файлы по хэшу				
Комментарий	Введите комментарий					
Действия						
Основное	😢 Заблокировать 🗸 🗸		Блокировка: Нарушение политики безопасности 🛛 🗸			
			Шаблон страницы блокировки			
	Файлы	Файлы договоров $\times$				
Условия	Размер файлов	От Не ограничен	МБ			
сточник						
	Ключевые слова	Выберите из списка				
Іазначение	Расписания	Выберите из списка				
	Лимиты трафика	Без ограничений				
			Сохранить Отменить			

Рис. 6.99. Формирование правила

## 6.7. Отложенное скачивание

В системе реализована возможность использования отложенного скачивания. После проверки антивирусом или обработки политикой фильтрации объекта по типам файлов или списку файлов ссылка на обрабатываемый объект будет передана пользователю.

Для включения режима отложенного скачивания выполните следующие действия:

- В разделе Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей включите параметр Поддержка отложенного скачивания (enabled) в секции Отложенное скачивание.
- 2. Установите требуемый предел, начиная с которого будет использоваться отложенное скачивание, в поле Макс. объем данных для перехода в режим отложенного скачивания (Б) (threshold).

Режим отложенного скачивания включается только в том случае, если размер загружаемого файла превышает значение параметра **threshold**. Для поддержки данного режима в Solar NGFW запускается специальный веб-сервер, который используется для показа статуса загрузки и для передачи загруженного файла. При переходе в режим отложенного скачивания открывается новая вкладка веб-браузера **Статус загрузки** (<u>Рис.6.100</u>) с автоматическим обновлением, в которой отображается статус загрузки.



Рис. 6.100. Статус загрузки

По окончании загрузки возможны два варианта действий:

- Появляется окно для открытия загруженного файла или для указания пути его сохранения (<u>Рис.6.102</u>).
- Отображается шаблон блокировки открытия загруженного файла. Этот шаблон генерируется политикой фильтрации. Если открытие файла запрещено используемой политикой фильтрации, информация об этом сохраняется в **Журнал запросов**.



# БЛОКИРОВКА. НАРУШЕНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ

Доступ к ресурсу \${URL} запрещен политикой безопасности.

## СВЕДЕНИЯ О СРАБАТЫВАНИИ ПОЛИТИКИ:

Сработавшее правило: \${POLICY}/\${CONDITION} Категория ресурса: \${CATEGORY} Логин пользователя: \${LOGIN}

Если Вы считаете запрет необоснованным, свяжитесь с Вашим системным администратором.

Рис. 6.101. Шаблон блокировки



Рис. 6.102. Сохранение загруженного файла

Полностью загруженный файл хранится на сервере в течение 30 минут, по истечении этого времени он автоматически удаляется. При попытке открыть файл по истечении 30 минут появится уведомление, что файл не найден или удален из хранилища.

Факт загрузки или удаления файла сохраняется в Журнал запросов.

Пользователь может открывать только те файлы, которые загружал сам. К объектам, которые загружал другой пользователь, доступа у него нет.

## 6.8. Управление базами категоризации

Управление базой категоризации выполняется в разделе **Политика > База категоризации** (<u>Рис.6.103</u>). Для работы с базой убедитесь, что в разделе **Система > Узлы и роли** в списке серверов указан **Анализатор трафика**.

В Solar NGFW для фильтрации веб-трафика используются пользовательский категоризатор customist и категоризатор webCat, разработанный **Ростелеком-Солар**. Возможно подключение внешних категоризаторов (например, **SkyDNS**).

## Примечание

По умолчанию к разделу имеют полный доступ пользователи с ролями суперадминистратор и администратор безопасности. Для пользователя с ролью аудитор доступна только проверка категорий ресурсов.

Администратор безопасности может выгрузить все категории для просмотра в отдельный файл текстового формата, нажав кнопку **Экспорт категорий**.

Также можно загрузить свою базу категоризации. Она будет записана поверх существующей.



Рис. 6.103. Вкладка Политика > База категоризации

Для импорта базы категоризации:

- 1. Нажмите кнопку Импорт категорий.
- 2. В отобразившемся уведомлении нажмите кнопку Ок.
- 3. В открывшемся окне выберите файл текстового формата и нажмите кнопку Открыть.

Загружаемый файл должен быть текстового формата (**TXT**) в кодировке utf-8. Файл должен иметь следующую структуру: идентификатор категории <пробел> название категории. Затем должны быть прописаны домены в виде: <пробел>Домен<новая строка>.

Например:

711 Сервисы распространения данных 712 Поисковые системы/порталы google.com google.ru yandex.ru ya.ru rambler.ru 713 Пиринговые сети

Если категория не определена в системе, она игнорируется. Если формат загружаемой базы не удовлетворяет требованиям, появляется сообщение «Файл не соответствует формату для импорта категорий». Если импорт был выполнен успешно, отобразится

уведомление: «Импорт категорий ресурсов прошел успешно». При возникновении проблем при загрузке отобразится уведомление об ошибке.

Для определения категории ресурса (URL) введите название одного или нескольких ресурсов в секции **Управление категориями** и нажмите кнопку **Проверить** (<u>Рис.6.104</u>). В таблице ниже отобразится информация о категориях, к которым они относятся. Если какая-то категория определена неверно, можно ее изменить.

Управление категориями		Импорт категорий	Экспорт категорий	Применить политику
vk.com				
Проверить				
Результат проверки				
Ресурс	Категория	Источники		
vk.com	Алкоголь, Здоровье Негосуда Социальн	customlists customlists customlists blacklists		2

Рис. 6.104. Проверка категории

Описание процедуры изменения категории ресурса см. в документе «Руководство по установке и настройке».

Для удаления ресурса из какой-либо категории в этом же окне нажмите крестик рядом с названием категории. Можно добавить или удалить несколько категорий.

## Внимание!

После выполнения какой-либо операции с категориями нажмите кнопку Применить политику.

# 7. Статистика: получение сводных статистических отчетов

# 7.1. Общие сведения

Solar NGFW позволяет проводить мониторинг деятельности пользователей в Интернете и получать сводные данные об их работе в виде отчетов.

Все действия с отчетами выполняются в разделе **Статистика** (<u>Рис.7.1</u>). Раздел доступен для редактирования данных только пользователям, которым назначены роли *суперадминистратор* или *администратор безопасности*. Пользователи с ролями *системный администратор* и *аудитор* могут только просматривать раздел.



Рис. 7.1. Раздел «Статистика»

Раздел состоит из нескольких секций: Типы отчетов, Сохраненные отчеты, Рекомендуемые отчеты.

Секция **Типы отчетов** содержит шаблоны для создания отчетов, которые сгруппированы по определенным типам и категориям (подробнее см. раздел <u>7.2.2</u>).

В секции **Сохраненные отчеты** отображаются сформированные и сохраненные пользователем отчеты. Сохраненные отчеты можно группировать и помещать в папки для более удобного хранения (см. раздел <u>7.3</u>).

В секции **Рекомендуемые отчеты** представлены системные отчеты, которые содержат уже заданные настройки фильтрации. В отличие от сохраненных отчетов, рекомендуемые отчеты можно только просматривать или на их основе создавать новые.

## 7.2. Работа с отчетами

## 7.2.1. Общие сведения

Для работы с конкретным отчетом предназначено меню действий в разделе **Статистика** или в самом отчете (<u>Рис.7.2</u>). Для выполнения какой-либо операции выберите в меню действий пункт с одноименным названием.



Рис. 7.2. Меню действий с отчетом

Администратор безопасности может выполнять следующие операции с отчетами:

- формирование отчета (см. раздел 7.2.2);
- просмотр отчета (см. раздел 7.2.3);
- просмотр из отчета подробных сведений (детализации) по количеству запросов (см. раздел <u>7.2.3</u>);
- редактирование отчета (см. раздел 7.2.4);
- отправка копии отчета пользователю системы (см. раздел 7.2.5);
- настройка отправки отчета по расписанию (см. раздел 7.2.2.4);
- экспорт отчета в файл формата PDF (см. раздел 7.2.6);
- удаление отчета (см. раздел 7.2.7).

## 7.2.2. Формирование отчета

## 7.2.2.1. Общие сведения

Формирование отчета подразумевает построение отчета с его последующим сохранением (см. раздел <u>7.2.2.5</u>). Все сохраненные отчеты отображаются в блоке **Сохраненные отчеты**.

Если администратор безопасности не сохранит сформированный отчет перед формированием другого отчета или переходом в другой раздел, отчет не будет сохранен в системе.
Построить отчет можно как с помощью шаблона (см. раздел <u>7.2.2.2</u>), так и используя уже существующие отчеты (ранее сохраненные или рекомендуемые, подробнее см. раздел <u>7.2.2.3</u>).

Все типы отчетов сгруппированы по четырем категориям:

- Топ источников статистика посещения конкретными пользователями популярных ресурсов и категорий ресурсов в Интернете. Например, можно просмотреть сведения о десяти пользователях, которые посещали соцсети чаще других.
- Топ назначений статистика по пользователям, которые чаще всего посещали определенные ресурсы и категории ресурсов. Например, можно просмотреть ресурсы, наиболее посещаемые сотрудниками бухгалтерии.
- **Передаваемые данные** статистика по конкретным пользователям, которые скачивали или отправляли в Интернете определенные типы данных. Например, можно просмотреть данные по десяти пользователям, которые чаще других отправляли текстовые файлы в облачные хранилища.
- Журнал соединений статистика пакетов через узлы фильтрации. Например, количество пакетов через главный узел фильтрации за последние сутки.
- Журнал запросов статистика по запросам через узлы фильтрации. А именно, по работе узлов фильтрации, правилам политики и неавторизованным пользователям. Например, можно узнать количество запросов через главный узел фильтрации за последние сутки. Также можно просмотреть статистику по приложениям и используемым ими протоколам.

# Примечание

Администратор безопасности может собрать статистику как по персонам, у которых есть карточки Досье, так и по неаутентифицированным пользователям или группам пользователей.

Чтобы просмотреть информацию о сетевой активности неаутентифицированных пользователей, выберите в фильтре **Персоны** значение **Неаутентифицированный пользователь** (отчет **Топ назначений по персонам** и **Журнал запросов**). Чтобы просмотреть информацию о сетевой активности группы неаутентифицированных пользователей, выберите в фильтре **Группы** значение **Нет группы** (отчет **Топ назначений по группам персон)**.

# 7.2.2.2. Построение отчета с помощью шаблона

Для построения отчета с помощью шаблона:

 В секции Типы отчетов нажмите кнопку с названием соответствующего шаблона отчета (<u>Рис.7.3</u>).

இ Топ источников 🕕	🛃 Топ назначений 🛈	Передаваемые данные 🕦	🕂 Журнал соединений 🕚	Журнал запросов 🛈		
По ресурсам По категориям	По персонам По группам п_ По IP источни_	По типам дан_	По IP По порту По узлу филь_ По приложен_	По персонам По IP источни_ По узлам фил_ По приложен_		

Рис. 7.3. Секция «Типы отчетов»

2. В открывшемся шаблоне задайте значения для фильтров с помощью раскрывающихся списков или счетчиков.

При указании значений для фильтров следует учесть следующие моменты:

 Можно просмотреть «полный путь» расположения группы персон в фильтре Группы в отчете Топ назначений по группам.



Рис. 7.4. Копирование значения фильтра отчета

Это позволяет исключить неправильный выбор группы, если в системе зарегистрировано несколько групп с одинаковым названием, которые принадлежат разным доменам или разным департаментам.

 Значения фильтров можно вводить вручную или копировать, нажав специальный значок, который появится при наведении курсора мыши на значение. Скопированное значение сохранится в буфер обмена.

Описание значений фильтров см. <u>Приложение F, Перечень фильтров для</u> формирования отчетов.



Рис. 7.5. Копирование значения фильтра отчета



Рис. 7.6. Отчет «По персонам/ТОП:25, Персоны: Валентина Иванова»

- 3. При необходимости измените период времени, за который отображается информация в отчете:
  - откройте календарь, нажав в области поля Период (Рис.7.7);
  - укажите даты начала и окончания периода для сбора статистики вручную или выберите период, настроенный автоматически;
  - нажмите кнопку **Оk**.

#### Примечание

Автоматическая проверка и корректировка даты начала и конца исключает возможность ошибки.

#### 4. Сохраните отчет (см. раздел <u>7.2.2.5</u>).

Перед сохранением отчета также можно просмотреть детализацию отчета, экспортировать его в файл формата PDF (см. раздел <u>7.2.6</u>) и т.д.

18.03.2	2021 1	6:17					_	30.04	.2021	16:17				
« < 2021 мар.										20	)21 a	пр.		> >>
пн	вт	ср	ЧТ	пт	сб	BC		пн	BT	ср	ЧТ	пт	сб	BC
1	2	3	4	5	6	7		29	30	31	1	2	3	4
8	9	10	11	12	13	14		5	6	7	8	9	10	11
15	16	17	18	19	20	21		12	13	14	15	16	17	18
22	23	24	25	26	27	28		19	20	21	22	23	24	25
29	30	31	1	2	3	4		26	27	28	29	30	1	2
5	6	7	8	9	10	11		3	4	5	6	7	8	9
Сегод	цня	Вчер	ba	Эта не	еделя	Эт	от ме	сяц	Этот	г год	1 ча	ac		
3 часа 12 часов 24 часа 7 дней 30 дней 90 дней 180 дней								Ok						

Рис. 7.7. Календарь

#### 7.2.2.3. Построение отчета на основе сохраненного или рекомендуемого

Для построения нового отчета на основе сохраненного:

- 1. В секции Сохраненные отчеты откройте конкретный отчет.
- 2. Отредактируйте значения фильтров, измените период времени, за который отображается информация в отчете, или настройте отправку отчета по расписанию (см. раздел <u>7.2.2.4</u>).
- 3. Сохраните отчет под новым названием.

Для создания нового отчета на основе рекомендуемого выберите отчет в секции **Реко**мендуемые отчеты и выполните действия, описанные выше.

#### 7.2.2.4. Настройка отправки отчета по расписанию

Администратор безопасности может настроить отправку отчета по расписанию в процессе его формирования или редактирования. Отчет передается по электронной почте в файле формата PDF, поэтому получателями отчета могут быть не только пользователи Solar NGFW. Настройку можно выполнить с помощью меню действий в разделе Статистика и в самом отчете.

Для настройки отправки отчета с помощью меню действий в разделе Статистика:

- 1. В секции Сохраненные отчеты в строке соответствующего отчета нажмите кнопку
- 2. В отобразившемся меню действий выберите пункт Редактировать.
- 3. В открывшемся окне перейдите на вкладку **Настройки отправки** и задайте необходимые настройки:
  - период времени, с учетом которого будет выполнена отправка (по дням, по неделям, по месяцам);
  - дату отправки отчета и точное время;
  - список адресов электронной почты получателей отчета (не более 5);

#### Примечание

Данные о получателях содержатся в разделе **Политика > Справочники > Адреса электронной почты**. Для добавления нового адреса электронной почты перейдите в указанный раздел и выполните соответствующие действия.

• тему и текст письма (при необходимости).

Если все действия были выполнены правильно, отчет будет отправлен на указанные адреса электронной почты согласно установленному расписанию. Определить настроено ли у отчета расписание отправки можно в секции **Сохраненные отчеты** по значку будильника рядом с названием отчета.

Для настройки расписания из отчета вызовите меню действий и продолжите процедуру согласно описанию выше. Для вызова меню нажмите кнопку Справа от кнопки **Сохранить**.

Основное	Настройки отправки	
Отправлять	по месяцам \vee начиная с 27-07-2019 02:36 📋	
Каждый ∨	1 месяц	
Дни месяца	✓ 1 2 3 4 5 6 7 8	
	9 10 11 12 13 14 15 16	
	17 18	
	25 26 27 28 29 30 31	
	Последний день месяца	
Получатели	III df ×	$\sim$
	Список объектов политики из справочника "Адреса электронной почты". Не более 5-ти	
Тема письма	Отчет	
	Тема обязательна. Длина не более 250 символов	
Текст письма	Отчет необходимо просмотреть.	



#### 7.2.2.5. Сохранение отчета

Для сохранения отчета:

- 1. В отчете нажмите кнопку Сохранить.
- 2. В открывшемся окне Сохранить отчет:
  - в поле Название измените автоматически сформированное название отчета;

#### Примечание

Название отчета должно быть уникальным среди всех отчетов одного конкретного пользователя.

- в раскрывающемся списке Папка выберите папку или введите название новой;
- в поле Комментарий укажите комментарий.

#### Примечание

Изменять название отчета, указывать папку или комментарий необязательно.

3. Нажмите кнопку Сохранить.

После сохранения в левом верхнем углу отчета отображается его название в формате: **<Тип отчета>|<Название первого фильтра:первое указанное значение фильтра>,<Название второго фильтра:первое указанное значение фильтра>.pdf**. Например, По группам персон | ТОП: 25, Группы персон: Отдел кадров.

Для сохранения отчета из формы отчета вызовите меню действий с помощью кнопки и выберите пункт **Сохранить как ..**.. Продолжите процедуру сохранения согласно описанию выше.

# 7.2.3. Просмотр отчета

Для просмотра сохраненного или рекомендуемого отчета в секции **Сохраненные отчеты**/ **Рекомендуемые отчеты** нажмите название интересующего отчета.

Чтобы после просмотра отчета вернуться обратно, в браузере нажмите кнопку Назад.

#### Примечание

Каждый раз при открытии отчет будет перестроен согласно установленному в нем периоду времени, начиная с текущей даты просмотра.

Также в процессе просмотра отчета можно:

- Сузить или расширить временной диапазон, за который отображаются сведения на графике.
- Отсортировать сведения по определенному параметру (столбцу таблицы).
- Перейти на конкретный ресурс.
- Перейти в краткую карточку персоны (при условии, что у пользователя есть карточка персоны).
- Сформировать ТОП по объекту или группе объектов:
  - ТОП по персоне;
  - ТОП по группе персон;
  - ТОП по ресурсу;
  - ТОП по категории ресурсов;
  - ТОП по типам данных;
  - ТОП по IP-адресу источника.
- Просмотреть подробную информацию (детализацию) по запросам.
- Изменить состав столбцов таблицы с данными и скрыть неиспользуемые фильтры (доступно только для Журнала запросов и Журнала соединений).

Для сужения временного диапазона курсором мыши выделите на графике отрезок времени, за который необходимо посмотреть подробную информацию. Например, администратору безопасности необходимо просмотреть почасовое количество запросов конкретной персоны за сутки. Для этого на графике выделите интересующий период времени. В итоге, график будет перестроен согласно выбранному временному диапазону. Сведения, приведенные в таблицах, динамически изменятся.



Рис. 7.9. Сужение временного диапазона

Для расширения временного диапазона левой кнопкой мыши дважды нажмите по графику.

Например, администратору безопасности необходимо просмотреть общую картину посещения пользователем ресурсов. Для этого дважды нажмите график. В итоге, график будет перестроен согласно выбранному временному диапазону. Сведения, приведенные в таблицах, динамически изменятся.



Рис. 7.10. Расширение временного диапазона

Также можно отображать на графике только заблокированные или разрешенные запросы, нажимая на линию необходимого цвета под графиком.

*Для перехода на ресурс к краткой карточке персоны* нажмите соответствующую ссылку в таблице виджета. Доступная для перехода ссылка выделена подчеркиванием. В итоге

в браузере откроется новая страница с выбранным ресурсом/краткая карточка выбранной персоны.

Для сортировки сведений нажмите название столбца таблицы, по которому будет выполнена сортировка. Изначально данные отсортированы по убыванию.

Для формирования отчета **ТОП по объекту или группе объектов** в таблице нажмите значок в строке интересующего объекта (ресурса, персоны и т.д.). В результате откроется сформированный отчет по выбранному объекту.

Топ 25 доменов 2го уровня для персоны Валентина Иванова										
	Домен 2го уровня	Кол-во	Объем вх.	Объем исх.						
	<u>maiLru</u>	<u>81</u>	117.54 MB	0.38 MB						
	Просмотреть ТОП по ре	сурсу	85.99 MB	0.29 MB						
	google.com	<u>49</u>	72.78 MB	0.26 MB						
	<u>okko.tv</u>	<u>44</u>	62.38 MB	0.20 MB						
	wikipedia.org	<u>43</u>	60.92 MB	0.19 MB						
	<u>cybersport.ru</u>	<u>42</u>	61.88 MB	0.21 MB						
	<u>ok.ru</u>	<u>41</u>	61.19 MB	0.20 MB						

Рис. 7.11. Формирование отчета «ТОП по объекту или группе объектов»

Для просмотра детализации по запросам:

- 1. В конкретной таблице отчета нажмите ссылку (число в столбце Кол-во таблицы).
- 2. При необходимости в открывшемся отчете с подробной информацией о запросах:
  - отсортируйте в таблицах сведения о запросах;
  - выгрузите детализацию по запросам в файл формата PDF (аналогично экспорту отчетов, см. раздел 7.2.6).

Чтобы после перехода к детализации по запросам вернуться обратно к отчету, в браузере нажмите кнопку **Назад**.

Из детализации по запросам можно перейти в **Журнал запросов** конкретного ресурса. Для этого нажмите число запросов в строке определенного ресурса (столбец **Кол-во** в таблице).

В отчетах категории **Журнал запросов** можно изменить состав таблицы. По умолчанию таблица имеет набор столбцов: **URL путь**, **Результат проверки**. Для изменения состава таблицы откройте раскрывающийся список фильтра **Колонки** и нажмите названия колонок, которые следует отобразить в таблице. Можно отобразить все колонки из списка.

Чтобы изменить состава фильтров в отчете категории **Журнал запросов**, добавьте или скройте неиспользуемые фильтры с помощью раскрывающегося меню **Еще**.

K	Журнал запросов <Отчет не сохран	/По узлам фильтрации ∨ ?Н>							Сохранить 🔍 С 1	10 cex. 🗸
Перио	<b>1</b>	Узлы фильтрации	Колонки		Ресурсы		Запросы	Лимит	Режим прокси	
	24 часа 📋		∨ URL путь × еще 2				Bce	v 500	Bce 🗸	Eue 🗸
> Гр	фики запросов								IP-адреса источников	
~ ж	/рнал запросов								НТТР-код	
									Тип проверки	
				журнал (пер	вые 500 строк)				IP-адрес сервера назн	начения
						проверки			🗸 Лимит	
	19.03.2021 16:57:56	10.199.167.19	content-signature-2.cdn.mozilla.net			METHOD(CONNEC	T) HTTPS mitm, HTTPS m	itm, Переход к	<ul> <li>Режим прокси</li> </ul>	
	19.03.2021 16:57:50	10.199.167.19	classify-client.services.mozilla.com			METHOD(CONNEC	T) HTTPS mitm, HTTPS m	itm, Переход к сл	oio connect, conn	
	19.03.2021 16:57:49	10.199.167.19	normandy.cdn.mozilia.net			METHOD(CONNEC	T) HTTPS mitm, HTTPS m	itm, Переход к сл	юю connect, conn	
	40.02 2024						ITTOC mitter LITTOC m	the Bosovos v ca	ous connect. Renewas a case	

Рис. 7.12. Фильтры Журнала запросов

# 7.2.4. Редактирование отчета

Администратор безопасности может отредактировать только сохраненные отчеты с помощью меню действий в разделе **Статистика** и в самом отчете.

Для редактирования отчета в разделе Статистика:

- 1. В секции Сохраненные отчеты в строке соответствующего отчета нажмите кнопку
- 2. В отобразившемся меню действий выберите пункт Редактировать.
- 3. В открывшемся окне **Редактировать отчет** (<u>Рис.7.13</u>) внесите соответствующие изменения (измените название отчета, место хранения (папку) и комментарий).
- 4. Нажмите кнопку Сохранить.

Редактироват	ь отчет	×
Основное	Настройки отправки	
Название	ТОП: 25, Категории ресурсов: Веб-почта	
Папка	Отчеты для руководства	$\sim$
	Выберите папку или введите название новой	
Комментарий	Внимательно просмотреть	le
	Сохранить Отмена	

Рис. 7.13. Окно «Редактировать отчет» вкладка «Основное»

Для изменения основных параметров из формы отчета вызовите меню действий и продолжите процедуру согласно описанию выше (начиная с шага 3). Для вызова меню действий нажмите кнопку Справа от кнопки Сохранить.

# 7.2.5. Отправка копии отчета

Администратор безопасности может поделиться отчетом с одним, несколькими или всеми пользователями, которые обладают соответствующими правами доступа. При этом он отправляет только копию отчета, а не оригинал. Это позволяет отправителю и получателю вносить независимые друг от друга изменения в отчеты. Поделиться можно как собственным отчетом, так и полученным от другого пользователя.

#### Примечание

Копия отчета отправляется без установленного расписания отправки, если оно было настроено.

Система позволяет поделиться копией сохраненного отчета в разделе Статистика и в самом отчете.

Для отправки отчета в разделе Статистика:

- 1. В секции Сохраненные отчеты в строке соответствующего отчета нажмите кнопку
- 2. В отобразившемся меню действий выберите пункт Поделиться.
- В открывшемся окне Поделиться отчетом установите флажок напротив ФИО одного или нескольких пользователей (<u>Рис.7.14</u>).

Примечание
Для отправки копии отчета всем пользователям системы установите флажок <b>Все</b> .

4. Нажмите кнопку Отправить. Отобразится уведомление об успешной отправке.

Поделиться отчетом	x
Bce	
Van Koshelev Pavel	
Zubrova	
Поделиться Отмена	

Рис. 7.14. Окно «Поделиться отчетом»

В итоге, у получателя в секции Сохраненные отчеты будет создана папка, содержащая отправленную копию отчета.

Название папки будет следующего формата: **<Отчеты>-<логин отправителя>**. Все отчеты, поступающие от одного и того же пользователя сохраняются в одной папке. Если в папке дублируются названия нового или уже существующего отчетов, к названию нового отчета добавляется слово «копия» и порядковый номер копии.

Для отправки отчета с помощью меню действий из формы отчета воспользуйтесь кнопкой для вызова этого меню (справа от кнопки **Сохранить**) и продолжите процедуру согласно описанию выше (начиная с шага 2).

# 7.2.6. Экспорт отчета в PDF

Администратор безопасности может экспортировать как сохраненные, так и несохраненные отчеты с помощью меню действий в разделе Статистика и в самом отчете.

Для экспорта отчета в разделе Статистика:

- 1. В секции Сохраненные отчеты в строке соответствующего отчета нажмите кнопку
- 2. В отобразившемся меню действий выберите пункт Экспорт в PDF.

#### Примечание

Дождитесь окончания экспорта. Состояние выгрузки можно отследить по линии загрузки в верхней части экрана. В противном случае, если перейти в процессе экспорта в другой раздел системы, экспорт отчета будет отменен.

Название файла формируется в следующем формате:

- для сохраненного отчета: <Название отчета>|с <ДД.ММ.ГГГГ> по <ДД.ММ.ГГГГ>.pdf. Например: По типам данных | ТОП: 25, Типы данных: Служебные файлы с 14.06.2019 по 15.06.2019;
- для несохраненного отчета: <Тип отчета> с <ДД.ММ.ГГГГ> по <ДД.ММ.ГГГГ>|<Название первого фильтра: первое указанное значение фильтра>,<Название второго фильтра: первое указанное значение фильтра>.pdf. Например: По персонам с 13.05.2019 по 19.05.2019| ТОП: 25, Персоны: Доброва Прасковья Вениминовна mrs.Toster 31.

Для экспорта отчета с помощью меню действий из формы отчета нажмите кнопку справа от кнопки **Сохранить** и в отобразившемся меню действий выберите пункт **Экспорт в PDF**.

При экспорте отчета формируется файл в формате PDF, который содержит в себе графики и таблицы с соответствующими данными.

				Дата формирования отчёта: 05.07.2019 15:05:38			
	Отчёт П	о персонам   Т(	DT: 25	Сформирован: admin 5. Персоны: Ханипов Фома Еремеевич			
Фильтры							
Период: с 28.06.201	9 00:00 no 05.07.20	19 23:59					
ТОП: 25 Персоны: Ханилов	Фома Еремеевич						
Сортировать по: Ко	личеству запросо	в					
Направление: Уоыв Запросы: Разреше	ание		Ton 2	25 доменов 2го уровня по персоне Ханипов Фома Еремеевич			
Ханилов Фона							
	Домен	2го уровня		Kon. Bx. Vicx.			-
	igroman			Ton 25 категории по персоне Ханипов Фома Еремеевич			
12	vk.com						
8	redd.it	Катег	ория	pecypca Kon. Bx.		Mcx.	
6	microso	Соци		Тол 25 типла сизиациану принану по полоща Уацилов Фона Б	DeMoepu		
4	gazeta	Меди		тон 20 текля сказаления далная на нерсопе лалиние чожа с	ремесьи	•	
2	pornhub	Pacn					
28.06	lenta.ru	Банк		Тип данных	Кол.	Bx.	Исх.
	cybersp	Спис		Неизвестный файл	80	130.59 MB	0.42 MB
- Заблокированна	google.	Sanp		Неизвестный файл	46	71.24 MB	0.26 MB
- Разрешенные з	livejourr	Лека		Видео в формате MPEG, MPEG-4, MPEG-TS	17	28.99 MB	0.07 MB
	megogo	Служ		Звукозапись, используемая в ОС Unix, Mac OS, Akai MPC, Amiga и пр.	12	18.02 MB	0.06 MB
	101.ru	3anp		Видео в формате MPEG, MPEG-4, MPEG-TS	12	21.10 MB	0.07 MB
25 MB	youtube	Проч		Растровое изображение в формате PNG без сжатия	11	18.37 MB	0.04 MB
20 MB	mail.ru	Хаки		Анимация в формате Adobe Flash	9	10.24 MB	0.05 MB
15 MB	google.	X066		Файл данных, разделенных запятыми	9	16.96 MB	0.04 MB
10 MB	ok.ru	Дома		Документ MS Publisher	7	12.53 MB	0.03 MB
5 мв —	gmail.co	Зако		Растровое изображение в формате TIFF без сжатия	7	14.46 MB	0.03 MB
0 MB	wikiped	Лоте		Веб-страница	7	13.05 MB	0.04 MB
20.00	whatsa	Myas		Видео в формате AVI	6	8.70 MB	0.03 MB
- Объем вх.	mail.ru	Рекл		Растровое изображение в формате TIFF без сжатия	6	9.59 MB	0.02 MB
<ul> <li>Объем исх.</li> </ul>	gmail.co	Afon		Документ PDF	6	11.63 MB	0.03 MB
	rbc.ru	000		Растровое изображение в формате GIF	6	6.62 MB	0.03 MB
	mirtese	Solf		Видео в формате AVI	5	6.34 MB	0.02 MB
	trinixy.n	- Faur		Растровое изображение в формате JPEG	5	4.81 MB	0.02 MB
	megoga	Kum	1	Каскадная таблица стилей	5	6.22 MB	0.03 MB
		Orea		Документ MS Publisher	5	7.63 MB	0.02 MB
		Onch	ī	Каскадная таблица стилей	5	8.44 MB	0.04 MB
		Дома	1	Документ MS Visio	5	7.56 MB	0.02 MB
		ringo		Документ MS Visio	5	6.03 MB	0.02 MB
				Текстовый файл	4	3.00 MB	0.01 MB
				Документ MS Word	4	5.51 MB	0.02 MB
				Анимация в формате Adobe Flash	4	8.23 MB	0.02 MB
		·					
				4			

Рис. 7.15. Пример выгруженного отчета по персоне (в файле формата PDF)

Информацию в таблицах можно редактировать и скопировать в другой документ. Файл сохраняется на диске (место сохранения файла зависит от настроек браузера).

Далее этот файл можно открыть (Рис.7.15), распечатать, переслать по почте и т.д.

Экспорт детализации по запросам выполняется аналогичным образом.

# 7.2.7. Удаление отчета

Администратор безопасности может удалить только сохраненные отчеты с помощью меню действий в разделе Статистика и в самом отчете.

Для удаления отчета с помощью меню в разделе Статистика:

1. В секции Сохраненные отчеты в строке соответствующего отчета нажмите кнопку

2. В отобразившемся меню действий выберите пункт Удалить и нажмите кнопку Да.



Рис. 7.16. Удаление отчета

# Примечание

Можно удалить сохраненные отчеты, полученные от других пользователей или отправленные им. У других пользователей не произойдет никаких изменений.

Для удаления отчета с помощью меню действий из формы отчета вызовите это меню и продолжите операцию согласно описанию выше. Для вызова меню нажмите кнопку справа от кнопки **Сохранить** 

# 7.3. Работа с папками сохраненных отчетов

Чтобы выполнить какое-либо действие с папкой, воспользуйтесь соответствующим меню действий (<u>Рис.7.17</u>), с помощью которого можно создавать, редактировать, делиться и удалять папку. Для выполнения действия с папкой выберите в меню пункт с одноименным названием.



Рис. 7.17. Меню действий с папкой

Создать папку возможно как с помощью кнопки **н** в разделе **Статистика > Сохраненные отчеты**, так и при формировании отчета (см. раздел <u>7.2.2.2</u>). При этом название папки должно быть уникальным среди папок одного конкретного пользователя.

Следует учесть, что при удалении созданной вручную или полученной папки, у других пользователей не произойдет никаких изменений.

При необходимости отчет можно переместить в требуемую папку. Для этого нажмите конкретный отчет и переместите его в нужную папку, не отпуская курсор мыши.

Администратор безопасности также может *поделиться копией папки*, содержащей отчеты с одним, несколькими или всеми пользователями, которые обладают соответствующими правами доступа. При этом он отправляет только копию папки со всем ее содержимым, а не оригинал. Это позволяет отправителю и получателю вносить независимые друг от друга изменения. Поделиться можно как собственной папкой с отчетами, так и полученной от другого пользователя. Отправка копии папки пользователю, содержащей отчеты, аналогична отправке копии отчета (подробнее см. раздел <u>7.2.5</u>). В итоге, у получателя в секции **Сохраненные отчеты** отобразится копия отправленной папки со всеми содержащимися в ней отчетами.

Название папки будет формата: **<название оригинальной папки>-<логин отправителя>**. Если дублируются названия новой или уже существующей папки, к названию новой папки добавляется слово «копия» и порядковый номер копии.

Поделиться папкой с отчетами	×
Bce	
🛃 Ivan	
Koshelev	
Pavel	
Zubrova	
Поделиться Отмена	

Рис. 7.18. Отправка копии папки с отчетами

# 7.4. Примеры формирования отчетов

# Задача:

Собрать статистику по сотрудникам, которые посещают социальные сети в течение 7 дней.

# Порядок действий для решения задачи:

Администратору безопасности необходимо сформировать отчет Топ источников/ по категориям ресурсов. Для этого:

- 1. В разделе Статистика в виджете категории отчетов Топ источников нажмите кнопку По категориям.
- 2. В открывшемся шаблоне отчета в фильтре **Категории ресурсов** выберите значение **Интернет-коммуникация**/ Социальные сети.

В построенном отчете отображается информация по всем запросам, не учитывая технический трафик (<u>Рис.7.19</u>).



Рис. 7.19. Сбор статистики по сотрудникам, которые посещали социальные сети

Просмотреть подробную информацию по запросам сотрудников конкретного отдела. Например, отдела «Управление информатизацией».

# Порядок действий для решения задачи:

Для этого в таблице **Топ 25 групп по категории - Социальные сети** нажмите в колонке **Кол-во** цифру напротив названия отдела. В построенном отчете можно просмотреть имена сотрудников и название ресурсов, которые они посещали (<u>Рис.7.20</u>).

Детализация:	Запросы на категории	и ресурсов /По группам персон 🗸						Сохранить 🗸			
Периол	Francis										
c 28-06-2019 00:00	труппы персон		Показыв	атькатегор	ии		запросы				
no 05-07-2019 23:59	В Управление	информатизации Х		циальные се	ети ×		~ все	~			
<ul> <li>Графики количе</li> </ul>	ества запросов и об	щего трафика по группам пер	сон								
Количе	ство запросов по группе	е Управление информатизации		Объем	общего трафик	а по группе	Управление информатизации				
1,25			3.0 MB								
1			23 MB								
0,75	Подробные график	и объема входящего и исход	ящего трафика по	группам	персон					1	
	Объем входящ	его трафика по группе Управление	информатизации		06	ьем исходя	щего трафика по группе Упр	вление информати	зации	1	
0,25 3.0	омв				0.010 MB					1	
0 28.06 29.0	5 МВ				0.008 MB					1	
2.0	омв				0.006 MB					1	
<ul> <li>Социальные</li> <li>Заблокиров</li> </ul>	5 MB				0.004 MB					1	
1.0	омв				0.004 Mill					1	
0.5	<sup>5 мв</sup> – Подро	обные данные в табличном в	иде по группе Упр	авление и	нформатиза	ции					
	0 MB 28.06	Данные за 28-06-2019 по групп	е Управление информ	атизации			Данные за 02-07-2019 n	о группе Управлени	е информатизации		
	— Социальн Черн Нико	ниченко Олеся Социалы олаевна	ные сети gazeta.ru	<sup>во</sup> 1 2.57 1 мв	0.01 MB	Xar Epe	нипов Фома Социа емеевич	пьные сети www.ig	gromania.ru <u>1</u> N	.11 0.00 MB MB	
	Снег	ирева Алина Потаповна Социалы	ные сети 101.ги	<u>1.66</u> <u>М</u> В	0.00 MB						
	Элли	Данные за 03-07-2	019 по группе Управле	ние информ	иатизации		Данные за	14-07-2019 no rpynn	е Управление инфо	орматизации	
	Сщ	Персона									Исх.
		Печеников Алексей Кириллович	Социальные сети	gazeta.ru	<sup>во</sup> 0.85 1 мв	0.01 MB	Ветрова Татьяна Глебовна	Социальные сети	www.cybersp	ort.ru <u>1</u> 0.8	36 0.01 3 MB
		Кристина Коваленко	Социальные сети	youtube.co	m <u>1</u> 0.95 MB	0.01 MB					
					Да	нные за О	5-07-2019 по группе Управ	ление информат	изации		
									Кол:Вх. Ис	ĸ	
					Розенбах И Данилевна	несса	Социальные сети	trinixy.ru	1 2.56 0.0 MB MB	1	
					Пичушкин I Эрнестович	Кузьма	Социальные сети	instagram.com	1.41 0.0 1 MB ME	1	

Рис. 7.20. Детализация запросов отдела «Управление информатизацией»

Просмотреть статистику посещения социальных сетей за неделю конкретным сотрудником. Например, Ханиповым Фомой Еремеевичем.

# Порядок действий для решения задачи:

Вернитесь в первый построенный отчет (<u>Рис.7.19</u>) и в таблице отчета **Топ 25 персон по** категориям - Социальные сети в колонке Кол-во нажмите цифру напротив ФИО сотрудника. В отобразившемся отчете можно просмотреть ресурсы и время их посещения, входящий и исходящий трафик (<u>Рис.7.21</u>).



Рис. 7.21. Детализация запросов конкретного сотрудника

Просмотреть статистику по Топ 25 ресурсов, которые посетил этот сотрудник.

# Порядок действий для решения задачи:

Для этого вернитесь в отчет по посещению социальных сетей (<u>Рис.7.19</u>) и в таблице отчета **Топ 25 персон по категориям - Социальные сети** нажмите значок напротив ФИО сотрудника.

В построенном отчете можно отобразить информацию по всем запросам этого сотрудника, выбрав в фильтре **Запросы** значение **Все** (<u>Рис.7.22</u>).



Рис. 7.22. ТОП 25 ресурсов, которые посетил конкретный сотрудник

Просмотреть статистику по использованию приложения Skype.

# Порядок действий для решения задачи:

Для этого откройте раздел Статистика > Журнал соединений > По приложениям (<u>Pис.7.19</u>) и укажите значения *Skype\_TeamsCall* и *Skype\_Teams* в фильтре Приложения. В результате отобразится вся необходимая информация по приложению Skype, перехватываемая Сервисом контроля приложений: даты, IP-адреса источников и назначений и используемые протоколы.

Для корректировки отображаемой статистики используйте фильтры, расположенные в верхней части страницы.



Рис. 7.23. Сбор статистики по приложению Skype

# 8. Пользователи: управление правами доступа пользователей

Раздел Пользователи предназначен для управления правами доступа пользователей к различным объектам системы. В разделе можно:

- настраивать для пользователей права доступа к данным персон, группам персон и разделам интерфейса системы;
- управлять учетными записями пользователей системы: создавать, редактировать, блокировать, удалять.



Рис. 8.1. Раздел «Пользователи»: управление правами доступа пользователей

# 8.1. Роли: назначение прав доступа к функциям и разделам системы

Управление доступом на основе ролей – это политика избирательного управления доступом, при которой права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли. Роль представляет собой набор прав доступа, который назначается пользователю, в результате чего он получает полномочия на выполнение конкретных действий, заданных в параметрах роли. Ролевая модель позволяет реализовать гибкие правила разграничения доступа.

При установке Solar NGFW создаются следующие системные роли:

- Суперадминистратор предоставляет максимальные права доступа ко всем разделам и данным системы. По умолчанию роль назначена пользователю admin.
- Системный администратор предоставляет доступ к разделам Система (полный доступ), Сеть (полный доступ) и Пользователи (просмотр, создание и редактирование учетных записей пользователей, создание и редактирование групп LDAP).

- Администратор безопасности предоставляет полный доступ ко всем разделам, кроме разделов Система и Сеть. Раздел Пользователи доступен для просмотра, создания и редактирования и назначения ролей.
- Аудитор предоставляет права только на просмотр всех разделов и объектов системы.
- Central management agent (Агент ЦУ) предоставляет права на работу с Централизованным управлением.

#### Примечание

Системные роли удалить или отредактировать невозможно.

Solar NGFW позволяет настраивать ролевую модель с помощью различных операций с ролями: можно создавать/редактировать роли, задавая права доступа к данным или разделам интерфейса системы, и назначать эти роли пользователям. Также роли можно удалить или скопировать.

Для управления ролями предназначен раздел **Пользователи > Роли**.

<i>.</i>	Solar NGFW							۹ 🛃	
ଜ	🔊 РОЛИ								
E	🐴 Администратор безопасности	и :	Сохранить Удалить	Сохранить Удалить					
÷	🐴 Аудитор		Название роли	Испытательный о	рок				
Ŗ	<ul> <li>Системный администратор</li> <li>Суперадминистратор</li> <li>Испытательный срок</li> </ul>		Комментарий	Введите коммент	арий				
R			Пользователи						
4			Группы LDAP						
ی ا	👌 ПОЛЬЗОВАТЕЛИ								
백르	🔓 admin			Brev					
	👸 ГРУППЫ LDAP		Газрешить доступ	Для поиска персон вви					
			Кроме	Иванов Иван І	Иванович × 🕹 Сидоров Петр Сергеевич ×				
				для поиска персон вы	дите ФИО, логин, адрес электронной почты или должность				
			Доступ к записям журналов						
			Разрешить просмотр записей	🔲 Системных	Ӯ Фильтрации 📄 Безопасности				
			Доступ к разделам интерфейса						
				🔳 Выбрать все	🔳 Выбрать все				
			Рабочий стол	🗹 Просмотр					
			Досье	🛃 Просмотр	🗹 Полный				
			Политика	📄 Просмотр	📄 Полный				
			Статистика	📄 Просмотр	Полный				
			Сеть	🔲 Просмотр	Полный				
			Предотвращение вторжений	🔲 Просмотр					

Рис. 8.2. Раздел «Пользователи > Роли»

# 8.1.1. Задание ролевой модели доступа

# 8.1.1.1. Создание, редактирование и удаление ролей

При наличии соответствующих прав доступа можно создавать, редактировать, копировать или удалять роли.

Для создания роли:

<sup>1.</sup> В разделе Пользователи в блоке Роли нажмите 🕥 (<u>Рис.8.3</u>).

- 2. Укажите название новой роли (не более 100 символов).
- 3. Нажмите кнопку Создать.
- 4. В строке Пользователи укажите пользователей, которым хотите назначить роль.
- 5. В строке **Группы Ldap** укажите группу пользователей AD, которой хотите назначить роль.
- 6. В блоках **Доступ к данным** и **Доступ к разделам интерфейса** задайте необходимые права доступа к данным персон и разделам системы (подробнее см. раздел <u>8.1.1.2</u>).

#### Примечание

Если в блоках **Доступ к данным** и **Доступ к разделам интерфейса** не заданы значения, по умолчанию доступ ко всем данным персон и разделам системы запрещен.

7. Нажмите кнопку Сохранить.

Создать роль Создать пользователя	Права доступа / Новая роль		
Роли 🗸	Создать Отменить		
Администратор безопасности :			
🔒 Аудитор 🗧 🗄	Название роли	Новая роль	
Системный администратор	комментарии	введите комментарии	
🔒 Суперадминистратор 🔹 🗄	Тюльзователи	<u>user</u> × <u>user1</u> ×	V
new :			
Администратор безопасности-копи	Разрешить доступ	Bce ×	
Испытательный период		Для поиска персон введите ФИО,	логин, эл. адрес или должность
Новый сотрудник :	Кроме	Митрохов Алексей Титови Для поиска персон введите ФИО,	ч × 🕹 Ветров Тихон Платонович × 🔹 🗸
	Доступ к разделам интерфейса	Выбрать все	Bufforth BCP
	Рабочий стол	Иросмотр	
	Досье	🛃 Просмотр	🕑 Полный
	Политики	🔲 Просмотр	Полный
	Статистика	🔲 Просмотр	Полный
	Права доступа	Просмотр	Создание и редактирование пользователей
			Создание, редактирование и назначение ролей
	Система	Просмотр	Полный

Рис. 8.3. Раздел «Пользователи»: создание роли

Для редактирования выбранной роли:

- 1. В разделе Пользователи > Роли выберите необходимую роль.
- Отредактируйте требуемые параметры. В карточке роли можно переименовать роль, изменить список пользователей, которым назначена роль, и/или набор прав доступа к данным системы и разделам интерфейса.

Для поиска персоны можно ввести ФИО, логин, адрес электронный почты или название должности. Для поиска группы пользователей введите ее название.

#### Примечание

Чтобы перейти к карточке пользователя (зависит от наличия прав доступа), нажмите на логин пользователя).

#### 3. Нажмите кнопку Сохранить.

#### Примечание

Пользователь не может назначать роли себе или редактировать роли, которые ему назначены.

Создать роль Создать пользователя	Права доступа / роль "Нов	зый сотрудник*	
Системный администратор	Сохранить Удалить		
🔒 Суперадминистратор 🔒 🗄			
new :	Название роли	Новый сотрудник	
Администратор безопасности-копи	Комментарий	Введите комментарий	
Испытательный период	Пользователи	mike_vazovsky × olga_antonova ×	~
Новый сотрудник		admin antonova_sofia	
	Разрешить доступ	mike_vazovsky	~
Пользователи 🗸		olga_antonova user	~
admin 🔒	Кроме	user1	
Доступ к данным			
Despensive source			
газрешить доступ		хо всем объкетам	
Кроме	Персоны В Балина <mark>Пол</mark> ина Ели Рре.balina ♥ s-1-5	сеевна Начальник отдела 21-3480291418-3434137707-263	
Доступ к разделам интерфейса Магээр Торгонориина Семеновна <i>Заведущий секретариатом</i> ♪ psbogachjova 🐨 s-1-5-21-3480291418-3434137707-263			
	Pman1 ♥ s-1-5-21	-3480291418-3434137707-263	
Рабочий стол	Специальные значени	идены (я	
Лосье	Неаутентифициров	анный <mark>пол</mark> ьзователь	

Рис. 8.4. Раздел «Пользователи > Роли»: редактирование роли, карточка роли

#### Примечание

Если у пользователя нет доступа к конкретной персоне, но при этом есть права доступа управления ролями, такой пользователь может создавать роли с правами доступа к объектам системы, к которым он сам не имеет доступа.

Роль можно скопировать и отредактировать. Это удобно, если нужно выдать одинаковые права доступа к разделам интерфейса нескольким пользователям с разными правами доступа к данным. Для копирования роли в меню действий с ролью выберите пункт **Скопировать** — скопированная роль отобразится в разделе **Пользователи > Роли**.

#### Примечание

Пользователь может скопировать присвоенную ему роль. Скопированная роль не будет ему назначена.



Рис. 8.5. Раздел «Пользователи > Роли»: меню действий с ролью

Для удаления выбранной роли:

- 1. В разделе Пользователи > Роли выберите необходимую роль.
- 2. В карточке роли нажмите кнопку Удалить (Рис.8.6).
- 3. В открывшемся диалоговом окне подтвердите удаление.



Рис. 8.6. Раздел «Пользователи > Роли»: удаление роли

# 8.1.1.2. Настройка ролей: назначение прав доступа

В процессе создания/редактирования роли задается набор прав доступа к данным персон и разделам интерфейса системы (см. <u>Рис.8.7</u>). Этими правами доступа обладают все пользователи, которым назначена роль.

Можно задавать права доступа к:

- данным персон и группам персон системы;
- разделам интерфейса системы (например, доступ к разделу Политика).

Управление доступом на основе ролей в Solar NGFW предполагает, что каждому пользователю необходимо настраивать доступ к данным персон, журналам событий и к разделам интерфейса системы. По умолчанию доступ к этим сведениям ограничен.

Для разрешения доступа *к данным* в карточке роли укажите список разрешенных персон или групп.

Ограничение доступа к данным персон или группам означает, что в системе пользователю доступна информация только по тем персонам или группам, которые указаны для него в качестве разрешенных. При этом учитываются права доступа к разделам интерфейса, которые имеются у пользователя в соответствии с его ролью. То есть во всех разделах интерфейса, к которым у пользователя есть доступ, будет доступна информация, которая касается только разрешенных персон или групп. Разрешенные персоны или группы можно найти при помощи главного поиска.

#### Примечание

Доступ к данным персон и группам персон следует учитывать при работе с отчетами. Сформировать отчеты можно по данным разрешенных персон или групп. В сформированном отчете для просмотра доступны данные разрешенных персон или групп.

Пользователь с соответствующими правами доступа к разделу **Статистика** может поделиться отчетом с другим пользователем. Если у получателя нет доступа ни к одной из указанных в отчете персон или групп, он получит отчет, но не сможет просмотреть данные запрещенных персон или групп.

Доступ к данным		
Разрешить доступ	Bce ×	~
	Для поиска персон введите ФИО, логин, эл. адрес или должность	
Кроме	👃 👃 Иван Сергеевич Иванов 🛛 🕹 Оксана Симка 🗙 😫 Грабарь Софья Семеновна 🗵	
	Богачева Полина Семеновна × Абабков Ярослав Наумович ×	
	Для поиска персон введите ФИО, логин, эл. адрес или должность	

Рис. 8.7. Блок «Доступ к данным» карточки роли

Например, если у пользователя полный доступ к разделу **Досье**, но доступ к данным ограничен одной персоной, в разделе **Досье** он сможет просматривать данные только

этой разрешенной персоны (см. <u>Рис.8.8</u>). Если разрешенная персона принадлежит к группе, можно узнать название группы, но перейти к данной группе нельзя.

Доступ к данным					
Разрешить доступ	Давыдов Мирослав Ерофеев	вич х	Пользователю разрешен доступ к данным одной персоны		
	Для поиска персон введите ФИО, ло	огин, эл. адрес или			
Кроме	Не выбрано Для поиска персон введите ФИО, ло			V	
Доступ к разделам интерфейса				and the second	
	🕑 Выбрать все	🔳 Выбрать все	Пользователь имеет полный доступ к разделу интерфейся <b>Досье</b>		
Рабочий стол	🕑 Просмотр				
Досье	<table-cell> Просмотр</table-cell>	🗹 Полный			
Политики + Раздел Начните в	+ Группу + Персону водить текст Q	Досье / Перс Персоны	коны В разделе Досье пользователю дост данные разрешенной персо	упны только ны	
Предост	авлен доступ	Добавить пер ФИО †	сону		
		Дав Зам	ыдов Мироспав Ерофеевич сститель начальника отдела		

Рис. 8.8. Пример отображения раздела Досье с учетом прав доступа к данным

#### Примечание

Если пользователю назначено две роли, в одной из которых персона разрешена, а в другой доступ к данным этой персоны ограничен, доступ к данным персоны запрещен.

Для назначения прав на просмотр *журналов событий* в карточке роли выберите одну или несколько категорий журналов, установив в секции **Доступ к записям журнала** флажок рядом с названием категории.

Доступ к записям журналов.			
Разрешить просмотр записей 🛛 🛩	Системных	Фильтрации	Безопасности

Рис. 8.9. Блок «Доступ к записям журналов» карточки роли

Пользователь может просмотреть записи только тех категорий журналов, права на которые ему выданы. Все доступные для просмотра журналы отображаются в списке фильтров поля **Сервис**.

Для системных ролей с предустановленными настройками предусмотрено следующее разделение прав:

- Суперадминистратор все журналы событий;
- Системный администратор системные журналы событий;

- Администратор безопасности системные журналы, журналы фильтрации и безопасности, статистики (отчеты раздела Статистика);
- Аудитор системные журналы, журналы фильтрации и безопасности.
- Central management agent (Агент ЦУ) журналы событий работы с Централизованным управлением.

Описание содержимого каждой категории журналов событий приведено в документе Руководство по установке и настройке.

Для предоставления доступа к *разделам интерфейса* в карточке роли выберите разделы интерфейса, с которыми можно выполнять действия (Полный доступ) или доступные только для просмотра (Доступ на просмотр).

Доступ к разделам интерфейса		
	🔳 Выбрать все	📄 Выбрать все
Рабочий стол	🛃 Просмотр	
Досье	🔲 Просмотр	🗍 Полный
Политика	🖌 Просмотр	🗍 Полный
Статистика	🖌 Просмотр	🗍 Полный
Права доступа	Просмотр	Создание и редактирование пользователей
State State		Создание, редактирование и назначение ролей
Настройки, узлы и роли, мониторинг	Просмотр	Полный

Рис. 8.10. Блок «Доступ к разделам интерфейса» карточки роли

В <u>Табл.8.1</u> приведены сведения обо всех настраиваемых правах доступа к разделам интерфейса системы.

Табл. 8	3.1.	Права	доступа	К	разделам	интерфейса
---------	------	-------	---------	---	----------	------------

Права доступа	Значения	Пояснения
РАБОЧИЙ СТОЛ	·	
Доступ к рабочему столу	Просмотр	Если значение не выбрано, доступ к рабочему столу запрещен. При запрещенном доступе на просмотр пользователь не сможет видеть раз- дел интерфейса в системе.
ДОСЬЕ	·	
Доступ к разделу	Просмотр/Полный	Если не выбрано ни одного значения, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр. При выборе до- ступа только на просмотр раздела <b>Досье</b> пользователь будет видеть данные кратких и полных карточек персон, но не сможет выпол- нять действия с ними.

Права доступа	Значения	Пояснения
		Примечание:
		Если у пользователя есть полный доступ к разделу <b>Досье</b> и есть доступ только на про- смотр раздела <b>Политика</b> , он не сможет редак- тировать инструменты политики, но сможет пе- рейти к разрешенным группам или карточкам персон из правила/исключения политики.
	L	
Доступ к разделу	Просмотр/Полный	Если не выбрано ни одного значения, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр.
		Примечание:
		Если у пользователя есть полный доступ к разделу <b>Политика</b> , но нет доступа к разделу <b>Досье</b> , пользователь сможет редактировать инструменты политики, но не сможет перейти к разрешенным группам или к карточкам персон из правила/исключения политики.
СТАТИСТИКА		
Доступ к разделу	Просмотр/Полный	Если значение не выбрано, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр.
СЕТЬ		
Доступ к разделу	Просмотр/Полный	Если значение не выбрано, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр.
ПРЕДОТВРАЩЕНИЕ ВТОРЖ	КЕНИЙ	
Доступ к разделу	Просмотр	Если значение не выбрано, доступ к рабочему столу запрещен. При запрещенном доступе на просмотр пользователь не сможет видеть раз- дел интерфейса в системе.
ПРАВА ДОСТУПА		
Доступ к разделу	Просмотр	Если значение не выбрано, доступ к разделу запрещен.
Создание и редактировани	е пользователей	
Действия над учетными запи- сями пользователей	Создание, редактирование пользователей	Если значение не выбрано, доступ к действиям над учетными записями пользователей (созда- ние, редактирование, удаление) запрещен.
Создание, редактирование	и назначение ролей	
Доступ к управлению права- ми	Создание, редактирование и назначение ролей	Если значение не выбрано, доступ к управле- нию правами (создание, редактирование, предоставление и отзыв прав доступа) запре- щен.
Создание и редактировани	е групп LDAP	
Доступ к управлению группа- ми LDAP	Создание и редактирование групп LDAP	Если значение не выбрано, доступ к управле- нию группами LDAP (создание, редактирование, удаление) запрещен.
СИСТЕМА		
Доступ к разделу	Просмотр/Полный	Если значение не выбрано, доступ к разделу запрещен. Выбор полного доступа включает доступ на просмотр.

Права доступа	Значения	Пояснения
		Если в настройках карточки роли разрешен до- ступ к какой-либо категории журнала событий, но запрещен к разделу Система. Журналы до- ступа будут тоже недоступны для просмотра
Редактирование настроек		
Доступ к редактированию конфигураций системы	Редактирование настроек	Если значение не выбрано, доступ к редактиро- ванию настроек запрещен.
Управление узлами и серв	исами	
Доступ к управлению узлами и сервисами	Управление узлами и сервиса- ми	Если значение не выбрано, доступ к управле- нию узлами и сервисами запрещен.
Управление сетевыми сое,	динениями	
Доступ к управлению сетевы- ми соединениями	Управление сетевыми соеди- нениями	Если значение не выбрано, доступ к управле- нию сетевыми соединениями запрещен.

# 8.2. Пользователи: операции с учетными записями пользователей системы

# 8.2.1. Общие сведения

В Solar NGFW предусмотрено управление учетными записями (УЗ) пользователей системы.

При установке Solar NGFW создается учетная запись **admin** — УЗ пользователя с максимальными правами доступа ко всем разделам и данным системы (по умолчанию ему назначена роль **Суперадминистратор**)

При наличии соответствующих прав можно:

- создавать, редактировать и удалять учетные записи пользователей системы;
- блокировать/разблокировать учетные записи.

Все операции с УЗ выполняются в разделе Пользователи > Пользователи.



Рис. 8.11. Раздел «Пользователи > Пользователи»

# 8.2.2. Создание учетной записи пользователя

В Solar NGFW можно организовать разные способы входа в систему. Для пользователей можно создавать два типа учетных записей:

- Локальная с использованием логина и пароля пользователя, учетная запись которого существует в системе.
- Доменная с использованием данных учетной записи пользователя, полученных из Active Directory (AD).

#### Примечание

Логин для доменной учетной записи, указанный в системе вручную, должен совпадать с соответствующим доменным логином в AD.

Для организации доменного доступа задайте соответствующие параметры в настройках системы (более подробно см. в документе «Руководство по установке и настройке»).

Для создания локальной учетной записи (УЗ) пользователя:

- 1. В разделе Пользователи нажмите кнопку Создать пользователя.
- 2. Снимите флажок Пользователь домена.
- 3. Укажите имя (Логин) и пароль (Пароль) пользователя для входа в систему (Рис.8.12).

#### Примечание

Логин может содержать только символы латинского алфавита в нижнем регистре, арабские цифры и служебные символы: «\_», «-», «.». Допустимая длина логина пользователя – от трех до ста символов. Логин должен начинаться и заканчиваться буквой латиницы или цифрой.

Пароль может содержать символы латинского алфавита в верхнем или нижнем регистре, арабские цифры и служебные символы: «~», «!», «@», «#», «\$», «%», «^», «&». «\*», «(», «)», «+», «-», «=», «`», «'», «\_», «/», «|», «"». Допустимая длина пароля – от шести до двенадцати символов.

- 4. Нажмите кнопку Создать.
- 5. При необходимости назначьте пользователю одну или несколько ролей.
- 6. Нажмите кнопку Сохранить.

<b>*</b>	Solar NGFW				Поиск персоны	٩	<b>£</b> ≡
ଜ	Создать роль	Создать пользователя	Права доступа / Новый по	ользователь			
	🔊 РОЛИ		Создать Отменить				
\$	🛃 ПОЛЬЗОВАТЕЛИ		Пользователь домена	•			
Ŗ	🖧 admin		Логин	iulia sinizina			
Řø							
£,	💧 ivan_ivanov		Роли	Испытательный срок ×			*
<b>(</b> E	🖧 mihaeLivanov		Пароль				
۲			Повтор пароля	Пароль обязателен. Допустимы латиница, цифры и символы: /'\"+1@#\$%A&*()_+++-			
			The second second				
Ŕ							

Рис. 8.12. Раздел «Пользователи»: создание локальной УЗ пользователя

Для создания доменной учетной записи пользователя:

- 1. В структуре раздела Пользователи нажмите кнопку Создать пользователя.
- 2. Укажите имя (**Логин**) пользователя для входа в систему (<u>Рис.8.12</u>).

#### Внимание!

Доменный логин пользователя, указанный в УЗ пользователя в Solar NGFW, должен совпадать с соответствующим доменным логином, содержащимся в AD. Иначе пользователь не сможет войти в систему.

- 3. Нажмите кнопку Создать.
- 4. При необходимости назначьте пользователю одну или несколько ролей (Рис.8.13).
- 5. Нажмите кнопку Сохранить.

<i>.</i>	Solar NGFW				Поиск персоны	٩	<b>2</b> =
ធ	Создать роль	Создать пользователя	Права доступа / <b>Новый п</b>	ользователь			
E	🛷 РОЛИ		Создать Отменить				
\$	ஜீ ПОЛЬЗОВАТЕЛИ		Пользователь домена				
Ř	🖧 admin		Логин	admin_2			
Rø			Рови	01 3-х до 100 букв латиница в нижнем регистре цифры и символы "\\"_\"\". В начале и конце буква или цифра.			
<u></u>	🔓 ivan_ivanov		голи	Chenumer harring of sourcements +			×
	👗 julia_sinizina						
	🔓 mihaeLivanov						
\$							

Рис. 8.13. Раздел «Пользователи»: создание доменной УЗ пользователя

# 8.2.3. Редактирование учетной записи пользователя

Для редактирования локальной учетной записи пользователя:

- 1. В разделе Пользователи > Пользователи выберите учетную запись пользователя.
- Отредактируйте необходимые параметры (<u>Рис.8.14</u>). В карточке пользователя можно изменить список ролей, назначенных выбранному пользователю, выбрать другой тип УЗ, а также задать новый пароль для локальной учетной записи.

#### Примечание

Для выбора/отмены выбора роли в раскрывающемся списке нажмите требуемую строку.

Для перехода к карточке роли нажмите ее название (зависит от наличия прав доступа).

3. Нажмите кнопку Сохранить.

#### Примечание

Для учетной записи, которая используется пользователем для авторизации в системе в текущей сессии, можно изменить тип УЗ с локальной на доменную, а также поменять пароль.

200	Solar NGEW				Поиск персоны Q	<b>9</b> =
*						-
<u>ଲ</u>	Создать роль	Создать пользователя	Права доступа / Новый по	рльзователь "ivan_ivanov"		
E	🔊 РОЛИ		Сохранить Удалить		Учетная запись активна	•
\$	📸 ПОЛЬЗОВАТЕЛИ		Пользователь домена	•		
Ŗ	占 admin		Логин	ivan ivanov		
Rø	🔓 admin_2					
A			Роли	Новые сотрудники ×		*
(II)	A ivan ivanov			Администратор безопасности		
~	L IVal LIVal OV			Аудитор		
۲	🔓 julia_sinizina			Системный администратор		
	🖧 mihaeLivanov			Испытательный срок		
				Новые сотрудники		~
\$						

Рис. 8.14. Раздел «Пользователи > Пользователи»: редактирование локальной УЗ пользователя, карточка пользователя

Чтобы изменить тип учетной записи пользователя, в его карточке установите/снимите флажок Пользователь домена.

#### Внимание!

При изменении типа УЗ с локальной на доменную логин пользователя должен совпадать с соответствующим доменным логином, содержащимся в АD. Иначе пользователь не сможет войти в систему.

Для локальной учетной записи можно задать новый пароль. Для этого установите флажок **Задать новый пароль**, а затем в полях **Пароль** и **Повтор пароля** укажите новый пароль для учетной записи (<u>Рис.8.15</u>).

Права доступа / пользователь "mike_vazovsky"								
Сохранить Удалить		Учетная запись активна 🛛 💽						
Пользователь домена								
Логин	mike_vazovsky							
Роли	Суперадминистратор ×	$\sim$						
	😒 Задать новый пароль							
Пароль	·····							
	Пароль обязателен. Допустимы латиница, цифры и символы: /*^-/@#\$%^&*()_+= -							
Повтор пароля								

Рис. 8.15. Раздел «Пользователи > Пользователи»: смена пароля локальной УЗ пользователя
#### 8.2.4. Блокировка/разблокировка учетной записи пользователя

Система предоставляет возможность заблокировать/разблокировать учетную запись (УЗ) конкретного пользователя. Пользователь с заблокированной учетной записью не сможет войти в систему.

Для блокировки/разблокировки учетной записи пользователя в разделе **Пользователи** > **Пользователи** откройте карточку УЗ пользователя и установите специальный переключатель в требуемое положение (<u>Рис.8.16</u>).

#### Примечание

Cmar	пус УЗ (ак	тивна/заб.	покирована	) отражается	в списке пол	њзователей		
<b>*</b>	Solar NGFW						Поиск персоны	۹ 💵
ធ	Создать роль	Создать пользователя						
	🔊 РОЛИ		Сохранить Удалить				Учетная запис	сь активна 🏾 💽
\$	🖧 ПОЛЬЗОВАТЕЛИ		Пользователь домена			Переключитель для		
Ŗ	🔓 admin	Неактивная УЗ п	(заблокированная) ользователя	ivan_ivanov		УЗ пользователя		
ಡ್ರ	🖧 admin_2							
<u>A</u>	🍐 helen_123		Роли	<u>Новые сотрудники ×</u>				~
(III	🔓 ivan_ivanov			📃 Задать новый пароль				
۲	🖧 julia_sinizina		Выбранная УЗ польз	зователя				
	💩 mihaeLivanov	, in the second se						
		Активная УЗ пользователя	a					
Ŵ								

Рис. 8.16. Раздел «Пользователи > Пользователи»: блокировка/разблокировка УЗ пользователя

#### 8.2.5. Удаление учетной записи пользователя

Для удаления учетной записи пользователя:

- 1. В разделе Пользователи > Пользователи откройте карточку УЗ пользователя и нажмите кнопку Удалить (<u>Рис.8.6</u>).
- 2. В открывшемся диалоговом окне подтвердите удаление.

2	Solar NGEW					<b>9</b> =
*						•
ស	Создать роль	Создать пользователя	Права доступа / Новый по			
	🔊 РОЛИ		Сохранить Удалить		Учетная запись активна	•
\$	🖧 ПОЛЬЗОВАТЕЛИ		Пользователь домена	•		
Ŗ	🔓 admin		Логин	ivan_ivanov		
Ř.	🖧 admin_2					
₽ <b>\$</b>			Роли	<u>Новые сотрудники ×</u>		~
(III)	🖧 ivan_ivanov			📄 Задать новый пароль		
۲	🔓 julia_sinizina					
	🔓 mihaeLivanov					
\$						

Рис. 8.17. Раздел «Пользователи > Пользователи»: удаление УЗ пользователя

#### 8.3. LDAP операции с доменными группами

Раздел **Пользователи > Группы LDAP** позволяет управлять доменными группами AD и связывать их с группами безопасности.

Чтобы создать группу LDAP:

<sup>1.</sup> Нажмите 🖭.

2. В поле Название заполните произвольное название группы.

#### Примечание

Название может содержать только символы латинского алфавита в нижнем регистре, арабские цифры и служебные символы: «\_», «-», «.». Оно должно начинаться и заканчиваться буквой латиницы или цифрой. Допустимая длина названия – от трех до ста символов.

3. В поле **Группа в LDAP** укажите параметры группы из LDAP (AD). В качестве значения принимается DN (отличительное имя). Например, *CN=Security Admins,OU=Company Users,DC=users,DC=domain,DC=local*.

#### Примечание

Группа LDAP должна являться атрибутом **memberOf** у пользователя AD (не должна быть первичной для него).

В качестве параметра **Группа в LDAP** должен быть указан полный путь LDAP к группе, в которую входит пользователь.

4. В поле **Роли** выберите доступные группы безопасности, для которых установлен перечень ролей.

# 5. Нажмите **Создать**. Созданная группа будет отображаться в раскрывающемся списке **Группы LDAP**.

#### Примечание

После добавления нового пользователя в группу для его аутентификации необходимо подождать примерно 5-10 минут.

Создать Отменить		
Название	group	
Группа в LDAP	CN=Security Admins, OU=Company Users, DC=users, DC=domain,DC=local	
Роли		v

Рис. 8.18. Создание группы LDAP

Для включения/выключения группы в правом верхнем углу используйте опцию **Учетные** записи группы активны.

#### 8.4. Выдача/отзыв прав доступа

Для выдачи прав доступа конкретному пользователю назначьте ему конкретную роль (для отзыва прав доступа – удалите конкретное назначение). Это можно сделать как в карточке пользователя, так и в карточке роли.

#### Настройка в карточке пользователя

Данная настройка удобна, если требуется назначить одному пользователю несколько определенных ролей или отозвать разные наборы прав доступа у одного пользователя.

Для этого:

- 1. В разделе Пользователи > Пользователи выберите учетную запись нужного пользователя.
- Задайте требуемые роли, нажав на соответствующие значения из раскрывающегося списка.
- 3. Нажмите кнопку Сохранить.

#### Примечание

Чтобы перейти к карточке роли, нажмите ссылку с ее названием (при наличии соответствующих прав).

<b>*</b>	Solar NGFW				Поиск персоны Q	2≡
ራ	Создать роль	Создать пользователя				
E.	🔊 РОЛИ		Сохранить Удалить		Учетная запись активна	•
÷	🔮 ПОЛЬЗОВАТЕЛИ		Пользователь домена	•		
Ŗ	🔒 admin		Логин	ivan ivanev		
ä,	🖧 admin_2					
Д.			Роли	<u>Новые сотрудники ×</u> Испытательный срок ×		*
đ≣				Администратор безопасности		
45	🛎 ivan_ivanov			Аудитор		
۲	💧 julia_sinizina			Системный администратор		
				Суперадминистратор		
	🔓 mihaeLivanov			Испытательный срок		~
				Новые сотрудники		~
\$						

Рис. 8.19. Раздел «Пользователи > Пользователи»: выдача/отзыв нескольких наборов прав доступа пользователю

#### Настройка в карточке роли

Данная настройка удобна при необходимости выдачи прав доступа нескольким пользователям или отзыва прав доступа у нескольких пользователей одновременно.

Для этого:

- 1. В разделе Пользователи > Роли выберите требуемую роль.
- Укажите нужных пользователей, нажав на соответствующие значения из раскрывающегося списка.
- 3. Нажмите кнопку Сохранить.

#### Примечание

Чтобы перейти к карточке пользователя, нажмите ссылку с его логином (при наличии соответствующих прав).

4.						
<b>*</b> **	Solar NGFW			Поиск персоны	۹ ۴	Ē
ඛ	Создать роль Создать пользователя					
	⊚ РОЛИ ∨	Сохранить Удалить				
\$	🐴 Администратор безопасности 🚦					
Щ	🐴 Аудитор 🗄	название роли	Испытательный срок			
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		Комментарий	Введите комментарий			
8	2. системный администратор	Пользователи	julia_sinizina × helen_123 ×			
£,	🐴 Суперадминистратор 🔹 🗄		admin			
(E	🐵 Испытательный срок 🔅		admin_2			
۲	Новые сотрудники	Разрешить лоступ	helen_123		~	
			ivan_ivanov			
	🖧 ПОЛЬЗОВАТЕЛИ >		julia_sinizina		~	
		Кроме	minaeLivanov			
Ŷ		Разрешить просмотр записей	🛢 Системных 🔲 Фильтрации 📄 Безопасности			

Рис. 8.20. Раздел «Пользователи > Роли»: выдача/отзыв прав доступа нескольким пользователям

# Приложение А. Применение MIME-типов для реализации политики безопасности доступа к веб-ресурсам в Solar NGFW

Solar NGFW позволяет фильтровать трафик по MIME-типам передаваемых/получаемых данных. Таким образом можно, например, установить запрет на просмотр определенных сетевых ресурсов, загрузку аудио- и видеофайлов и т. д. При этом для обработки MIME-типов могут использоваться регулярные выражения. Подробное описание регулярных выражений приведено в разделе <u>Приложение В, Язык описания регулярных выражений</u>.

Далее приводится пример использования МІМЕ-типов для реализации определенной политики безопасности доступа к веб-ресурсам.

Допустим, требуется запретить сотрудникам загрузку (скачивание и просмотр в оперативном режиме) файлов, содержащих музыку (аудио), изображения и/или видеоматериалы. При попытке сотрудников нарушить правила необходимо отклонить запрос на загрузку файлов и отправить на электронный адрес администратора безопасности уведомление о нарушении правил. При этом предполагается, что в Solar NGFW имеется группа **Администраторы** и задан список электронных адресов администраторов.

Для реализации данной политики администратору безопасности необходимо с помощью веб-интерфейса Solar NGFW выполнить следующие действия:

- Создать группу пользователей (например, Сотрудники) и добавить в нее пользователей, для которых должна быть запрещена загрузка файлов, содержащих музыку (аудио), изображения и/или видеоматериалы.
- 2. Для ранее созданной группы пользователей создать правило **Запрещенные данные** и при помощи расширенных настроек задать следующие типы файлов:
  - Аудио
  - Видео
  - Изображения
- 3. Выбрать шаблон страницы, которую должен видеть пользователь, нарушивший политику безопасности.
- 4. Выбрать шаблон уведомления о нарушении правил, которое должно отправляться администратору безопасности.

В данном шаблоне уведомления могут быть использованы подстановочные символы, подробное описание которых приведено в разделе <u>Приложение С, Использование</u> <u>подстановочных символов</u>.

5. Применить (обновить) политику.

Для проверки новой политики безопасности можно попробовать загрузить изображение, аудио- или видеофайл. Если политика выполняется корректно, должна появиться страница с сообщением о запрете загрузки, а на электронный адрес администратора безопасности должно прийти уведомление о нарушении правил.

Более подробную информацию о МІМЕ-типах можно просмотреть в *Приложении «Справочник МІМЕ-типов»* документа *Руководство по установке и настройке*.

### Приложение В. Язык описания регулярных выражений

Фильтры ресурсов, ключевых слов, типов данных, расширений и заголовков могут использовать для поиска не только подстроки, но и регулярные выражения. В отличие от простой строки, в регулярном выражении могут применяться для сравнения специальные символы: **\$^.\*+?[]** \. Их еще называют метасимволами.

При использовании регулярных выражений не следует указывать в них пробелы, т.к. в любом случае они не будут учитываться (в результате того, что регулярные выражения применяются после токенизации).

Метасимвол	Назначение	
. (точка)	Специальный знак, который соответствует любому одиночному символу, за ис- ключением перевода строки	
* (звездочка)	Квантификатор, который означает, что предыдущее регулярное выражение должно быть повторено столько раз, сколько это возможно. Например, выражение .* соответствует любой последовательности символов, не содержащей переводов строки	
+ (плюс)	Означает, что стоящее перед ним выражение должно появиться один или более раз. Например, выражение <b>bo+m</b> соответствует <b>bom</b> , <b>boom</b> , <b>booom</b> и т.д	
? (вопрос)	Квантификатор, который означает, что предыдущий символ или выражение (при использовании группировки) должно появиться один раз или ни одного раза. Выражение file.jpe?g будет соответствовать строкам file.jpg и file.jpeg	
() (круглые скобки)	Служат для группировки части регулярного выражения. Используется для того, чтобы квантификатор или символ применялись именно к этой группе. Например, атомарная группировка <b>a(bc b x)cc</b>	
[] (квадратные скобки)	Служат для указания набора знаков, которым может соответствовать символ. Например, <b>[abcd]</b> соответствует любому из символов <b>a</b> , <b>b</b> , <b>c</b> и <b>d</b> . Выражение <b>[ab]</b> * будет соответствовать любой комбинации подряд идущих символов a и b произвольной длины. Кроме того, в скобках могут задаваться интервалы: выра- жение <b>[a-zA-Z0-9]</b> соответствует любому из символов латинского алфавита в верхнем и нижнем регистре, а также любой десятичной цифре от 0 до 9	
{) (фигурные скобки)	Служат для указания количества символов, которые стоят перед скобками. Можно задать минимальное и максимальное количество символов (например, <b>{5;9}</b> для диапазона от 5 до 9).	
[^]	Конструкция, противоположная предыдущей. Используется для указания того, что не должно содержаться в строке. Выражение [^0-9] соответствует любому символу, кроме цифр от 0 до 9	
٨	Символ для обозначения начала строки	
\$	Символ для обозначения конца строки. Таким образом, <b>^\$</b> соответствует пустой строке, а <b>^HOME\$</b> – строке с единственным словом <b>HOME</b>	
1	Выполняет две функции: отменяет действие специальных символов, превращая их в обычные символы (данная операция называется экранированием символа), и вводит дополнительные специальные конструкции, такие как:	
	<ul> <li>\n – перевод строки;</li> </ul>	
	• \ <b>r</b> – возврат каретки;	
	• \t – табуляция;	
	<ul> <li>II – установка символа \ без функции экранирования символов</li> </ul>	
I	Означает выбор одного из вариантов. Выражение alphalbetalgamma будет со- ответствовать любой из строк alpha, beta и gamma	

Табл. В.1. Описание м	етасимволов
-----------------------	-------------

## Приложение С. Использование подстановочных символов

При формировании шаблонов уведомительных страниц могут использоваться подстановочные символы, размещаемые среди статичного текста в шаблоне. На этапе формирования конкретного уведомления подстановочные символы заменяются реальными значениями.

Символ	Назначение
\${CATEGORY}	Описание сработавших категорий ресурса
\${CATEGORY_TRIGGRED}	Описание категорий, которые совпали с условием правила в политике безопасности. Помимо номеров передаются также описания категорий. Категории в перечне разделяются запятой
\${COMMENT}	Типы и имена совпавших элементарных проверок
\${CONDITION}	Имя сработавшего правила политики
\${CONFIRM}	Подстановочный символ, вместо которого на странице отображается кнопка с надписью «confirm»
\${DATATYPE}	Тип передаваемых данных как запроса, так и ответа. Пример: request: application/x-empty, response: image/jpeg
\${DATE}	Дата и время обработки запроса
\${GROUP}	Идентификатор группы пользователей Solar NGFW, к которой принад- лежит данный пользователь
\${IP-ADDRESS}	IP-адрес машины, с которой поступил запрос
\${LOGIN}	Имя учётной записи пользователя Solar NGFW
\${POLICY}	Название политики, используемой при обработке запроса, в поле ука- зываются все применённые политики через разделитель «/»
\${REALNAME}	Данные из источника аутентификации, если данные отсутствуют, то подставляется имя учетной записи
\${URL}	URL ресурса, запрошенного пользователем

Табл. С.1. Описание подстановочных символов

Если подстановка какого-либо из символов не может быть выполнена, возвращается значение **Отсутствует**.

Табл. С.2. Перечень подстановочных символов для показа текущих значений расхода трафика пользователя

Символ	Назначение
\${TRAFFIC_REQUEST_DAY}	Исходящий трафик в день
\${TRAFFIC_REQUEST_DAY_LIMIT}	Допустимый лимит исходящего трафика в день
\${TRAFFIC_REQUEST_HOUR}	Исходящий трафик в час
\${TRAFFIC_REQUEST_HOUR_LIMIT}	Допустимый лимит исходящего трафика в час
\${TRAFFIC_REQUEST_MONTH}	Исходящий трафик в месяц
\${TRAFFIC_REQUEST_MONTH_LIMIT}	Допустимый лимит исходящего трафика в месяц
\${TRAFFIC_REQUEST_WEEK}	Исходящий трафик в неделю
\${TRAFFIC_REQUEST_WEEK_LIMIT}	Допустимый лимит исходящего трафика в неделю
\${TRAFFIC_RESPONSE_DAY}	Входящий трафик в день
\${TRAFFIC_RESPONSE_DAY_LIMIT}	Допустимый лимит входящего трафика в день
\${TRAFFIC_RESPONSE_HOUR}	Входящий трафик в час
\${TRAFFIC_RESPONSE_HOUR_LIMIT}	Допустимый лимит входящего трафика в час
\${TRAFFIC_RESPONSE_MONTH}	Входящий трафик в месяц

Символ	Назначение
\${TRAFFIC_RESPONSE_MONTH_LIMIT}	Допустимый лимит входящего трафика в месяц
\${TRAFFIC_RESPONSE_WEEK}	Входящий трафик в неделю
\${TRAFFIC_RESPONSE_WEEK_LIMIT}	Допустимый лимит входящего трафика в неделю

# Приложение D. Методы НТТР-протокола

В этом приложении приведен перечень методов HTTP-протокола, которые поддерживает Solar NGFW, и их описание.

CONNECT	Для использования вместе с прокси-серверами, которые могут динамически переключаться в туннельный режим SSL		
COPY	Предназначен для создания копии ресурса, заданного с помощью URI. Метод копирует как ресурсы, так и коллекции		
DELETE	Удаляет указанный ресурс		
GET	запрашивает содержимое указанного ресурса. Запрашиваемый ресурс может принимать параметры (например, поисковая система может принимать в качестве параметра искомую строку). Они передаются в строке URI (например: http://www.example.net/resource?param1=value1&param2=value2). Согласно стандарту HTTP, запросы типа GET считают идемпотентными — многократное повторение одного и того же запроса GET должно приводить к одинаковым результатам (при условии, что сам ресурс не изменился за время между запросами). Это позволяет кэшировать ответы на запросы GET		
HEAD	Аналогичен методу GET за исключением того, что он не возвращает тело ответа		
LOCK	Предназначен для блокировки доступа любого типа. Блокировка влияет и на ресурсы, и на коллекции. Если заблокирован ресурс, то и все его свойства также являются заблокированными		
MKCOL	Предназначен для создания новой коллекции. В следующем примере клиент направляет серверу запрос на создание коллекции /webdisc/xfiles/		
	MKCOL /webdisc/xfiles/ HTTP/1.1		
	Host: www.server.org		
	В ответе сервер сообщает, что коллекция создана:		
	HTTP/1.1 201 Created		
MOVE	Функционирует аналогично методу СОРҮ за исключением того, что после копирования ресурс удаляется		
OPTIONS	Возвращает методы HTTP, которые поддерживаются сервером. Этот метод может служить для определения возможностей веб-сервера		
PATCH	Аналогичен методу PUT за исключением того, что сущность содержит список различий между исходной версией ресурса, идентифицированного запрашиваемым URL, и содержимым, которое должно иметь ресурс после вызова РАТСН		
POST	Передает пользовательские данные (например, из HTML-формы) заданному ресурсу. На- пример, в блогах посетители обычно могут вводить свои комментарии к записям в HTML- форму, после чего они передаются серверу методом POST и помещаются на страницу. При этом передаваемые данные (в примере с блогами — текст комментария) включаются в тело запроса. В отличие от метода GET, метод POST не считается идемпотентным, то есть многократное повторение одних и тех же запросов POST может возвращать разные результаты (например, после каждой отправки комментария будет появляться одна копия этого комментария)		
PROPFIND	Предназначен для получения свойств ресурса, идентифицированного запрашиваемым URI. Метод можно использовать для получения структуры коллекции или дерево каталогов		
PROPPATCH	Предназначен для добавления, удаления или изменения свойств ресурсов, заданных в URI		
PUT	Загружает указанный ресурс на сервер		
TRACE	Отправляет полное сообщение, полученное веб-сервером, обратно клиенту, что позволяет увидеть конкретное содержимое, полученное веб-сервером		

Табл. D.1. Описание поддерживаемых методов НТТР-протокола

UNLOCK	Предназначен для снятия блокировки с ресурса. Для формирования запроса требуется URI ресурса и значение opaquelocktoken созданной ранее блокировки. Пример снятия блокировки:
	UNLOCK /1234.html HTTP/1.1 Host: www.host.ru Lock-Token: <opaquelocktoken:e71d4fae-5dec-22d6-fea5-00a0c91e6be4></opaquelocktoken:e71d4fae-5dec-22d6-fea5-00a0c91e6be4>
	Ответ сервера показывает, что блокировка была успешно снята:
	HTTP/1.1 204 No Content

# Приложение E. Матрица MЭ Solar NGFW

Матрица сетевого доступа нужна для настройки сетевого оборудования и доступа к/из сети предприятия на месте установки Solar NGFW. В ней отражены рекомендуемые настройки MЭ Solar NGFW и корпоративной сети.

Сеть	Описание		
Cluster int network	Внутренние подсети/диапазон адресов/VLAN для взаимодействия узлов кластера		
Cluster ext network	Знешние подсети/диапазон адресов/VLAN для доступа к сети Интернет		
Trusted networks	Защищаемые внутренние сети		
Admin hosts/net	Диапазон адресов/подсеть АРМ администраторов		
DCs	Подсеть/диапазон адресов/перечень узлов DC		
DNS servers	Подсеть/диапазон адресов/перечень DNS-серверов (может включать внешние DNS- сервера)		
DMZ	Сегмент зоны DMZ с публикуемыми веб-серверами		
SIEM	Системы SIEM для сбора и обработки журналов в целях ИБ		
Mail servers	Почтовый сервер организации		
NTP servers	Серверы времени внутри периметра сети или внешние серверы		
Internet	Сеть Интернет		
webCAT server	Сервер обновления баз категоризатора <u>wp-update.rt-solar.ru</u>		
Antivirus update server	Серверы обновления баз антивируса <u>update.geo.drweb.com</u>		

#### Табл. Е.1. Перечень сетей

#### Табл. Е.2. Общая матрица доступов для explicit-прокси

Источник	Назначение	Протокол и порт назначения	Состояние соедине- ния	Комментарий
Cluster int network	Cluster int network	ICMP, IGMP (опцио- нально), TCP/All, UDP/All	New, Established, Related	Полный взаимный доступ между узлами кластера Solar NGFW для обеспече- ния их связности и взаимо- действия
Cluster int network	Cluster int network	VRRP multicast, TCP/22, TCP/2269, TCP/2225, TCP/2226, TCP/2230, TCP/2278, TCP/5555, TCP/7001, TCP/, 8123, TCP/5434, TCP/2344, TCP/1010, TCP/3004, TCP/10051	New, Established, Related	При ограниченном доступе между узлами кластера должны быть открыты сле- дующие порты
Trusted networks	Cluster int network/vIP	ICMP, IGMP, TCP/80, TCP/443	New, Established, Related	Доступ для АРМ и устройств пользователей (первичные соединения, TCP/2281 при необходимо- сти локальной установки сертификатов пользовате- лями)
Cluster int network/vIP	DCs	TCP/389, TCP/689, TCP/3268	New, Established, Related	Доступ к контроллерам до- мена для синхронизации Досье
Cluster int/ext network/vIP	DNS	UDP/53, TCP/53	New, Established, Related	Доступ к внутренним DNS- серверам

Источник	Назначение	Протокол и порт назначения	Состояние соедине- ния	Комментарий
Cluster int network/vIP	SIEM	TCP/514 (опциональ- но), UDP/514	New, Established, Related	Выгрузка журналов в SIEM
Cluster int network/vIP	Mail Server	TCP/25	New, Established, Related	Соединение с почтовым сервером для отправки от- четов и данных о категори- ях ресурсов
Cluster int network/vIP	Средства DLP, антивирус, пе- сочница	TCP/1344	New, Established, Related	Соединения со вспомога- тельными средствами по ICAP
Средства DLP, Антивирус, Пе- сочница	Cluster int network/vIP	TCP/2272	Established, Related	Трафик по ранее установ- ленным соединениям
Cluster int/ext network/vIP	NTP servers	UDP/123	New, Established, Related	Доступ к данным о времени по NTP
Cluster ext network/vIP	Internet	TCP/80, TCP/443, TCP/21	New, Established, Related	Доступ прокси-сервера к внешним ресурсам (вторич- ные соединения)
Admin hosts/net	Cluster int network/vIP	ICMP, IGMP, TCP/22, TCP/8443, TCP/443, TCP/80	New, Established, Related	Доступ к интерфейсу управления и службам для администрирования/досту- па в Интернет
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновле- ния БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновле- ния БД антивируса
Дополнительные доступы для узлов с ролью Реверс-прокси				
Internet	Cluster ext network/vIP	Публикуемые TCP- порты для HTTP/HTTPS (в соот- ветствии с конфигура- цией реверс-прокси)	New, Established, Related	Доступ к опубликованным портам на внешнем интер- фейсе реверс-прокси раз- дельно для протоколов НТТР и HTTPS
Cluster int network/vIP	DMZ	TCP-порты веб-серви- сов на узлах в DMZ (в соответствии с конфи- гурацией реверс-прок- си)	New, Established, Related	Вторичные соединения с веб-серверами внутри за- щищаемого периметра се- ти
DMZ	Cluster int network/vIP	ТСР-порты веб-серви- сов на узлах в DMZ (в соответствии с конфи- гурацией реверс-прок- си)	Established, Related	Ответный трафик для кли- ентов, подключенных за пределами периметра сети к реверс-прокси
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновле- ния БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновле- ния БД антивируса
	Дополнитель	ные доступы для узлое	в режиме прозрачного	прокси
Cluster int network	Cluster int network	ICMP, IGMP (опцио- нально), TCP/All, UDP/All	New, Established, Related	Полный взаимный доступ между узлами кластера Solar NGFW для обеспече- ния их связности и взаимо- действия
Cluster int network	Cluster int network	VRRP multicast, TCP/22, TCP/2269,	New, Established, Related	При ограниченном доступе между узлами кластера

Источник	Назначение	Протокол и порт назначения	Состояние соедине- ния	Комментарий
		TCP/2225, TCP/2226, TCP/2230, TCP/2278, TCP/5555, TCP/7001, TCP/, 8123, TCP/5434, TCP/2344, TCP/1010, TCP/3004, TCP/10051		должны быть открыты сле- дующие порты
Trusted networks	Cluster int network/vIP	ICMP, IGMP, TCP/80, TCP/443	New, Established, Related	Доступ для АРМ и устройств пользователей (первичные соединения)
Cluster int network/vIP	DCs	TCP/389, TCP/689, TCP/3268	New, Established, Related	Доступ к контроллерам до- мена для синхронизации Досье
Cluster int/ext network/vIP	DNS	UDP/53, TCP/53	New, Established, Related	Доступ к внутренним DNS- серверам
Cluster int network/vIP	SIEM	TCP/514 (опциональ- но), UDP/514	New, Established, Related	Выгрузка журналов в SIEM
Cluster int network/vIP	Mail Server	TCP/25	New, Established, Related	Соединение с почтовым сервером для отправки от- четов и данных о категори- ях ресурсов
Cluster int network/vIP	Средства DLP, Антивирус, Пе- сочница	TCP/1344	New, Established, Related	Соединения со вспомога- тельными средстами по ICAP
Средства DLP, Антивирус, Пе- сочница	Cluster int network/vIP	TCP/2272	Established, Related	Интеграция по ICAP с Solar NGFW
Cluster int/ext network/vIP	NTP servers	UDP/123	New, Established, Related	Доступ к данным о времени по NTP
Cluster ext network/vIP	Internet	TCP/80, TCP/443, TCP/21	New, Established, Related	Доступ прокси-сервера ко внешним ресурсам (вторич- ные соединения)
Admin hosts/net	Cluster int network/vIP	ICMP, IGMP, TCP/22, TCP/8443, TCP/443, TCP/80	New, Established, Related	Доступ к интерфейсу управления и службам для администрирования/досту- па в Интернет
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновле- ния БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновле- ния БД антивируса

# Приложение F. Перечень фильтров для формирования отчетов

Табл. F.1. Описание параметров фильтрации запросов для сбора статистики в Журнале соединений

Фильтр	Назначение филь- тра	Значение	Примечание
	•	Основные фильтры	·
Период	Позволяет выбрать временной диапазон, за который формируется отчет	Дата и время начала и окон- чания сбора информации. Временной период следует указать с помощью календа- ря, встроенного в отчет	Работа с календарем подробно описана в разделе 7.2.2.2. Для всех категорий отчетов задается по умолчанию период в 7 дней. Стати- стика для категории отчетов <b>Жур- нал соединений</b> собирается за сутки.
Запросы/Соеди- нения	Позволяет отфильтро- вать данные по опреде- ленным параметрам	Выберите значение в раскры- вающемся списке: Все, Разрешенные, Заблокированные.	В зависимости от выбранного значения фильтра можно отобразить данные по разрешенным или забло- кированным запросам, а также по всем сразу. Также вы можете отобразить дан- ные по указанным выше видам за- просов, только с исключением тех- нического трафика (плагинов соци- альных сетей, контекстной рекламы и т.д.).
	Фильтры	по категориям и типам отчето	ОВ
IP-адреса источ- ников	Позволяет указать IP- адрес или диапазон IP- адресов источника <sup>а</sup> , от которых были запросы к выбранным ресурсам, категориям ресурсов и т.д.	Значение вводится вручную.	Можно указать несколько IP-адре- сов. Статистика по каждому IP-ад- ресу источника будет отображена в отдельном наборе виджетов.
Порты назначе- ния	Позволяет указать один или несколько портов назначения	Значение вводится вручную	Вы можете указать несколько пор- тов назначения. Статистика по каждому порту будет отображена в отдельном наборе виджетов.
Узел соединений	Позволяет выбрать уз- лы соединений, через которые идет трафик	Выберите значение в раскры- вающемся списке	Вы можете выбрать несколько уз- лов соединений или их все. Стати- стика по каждому узлу будет отоб- ражена в отдельном наборе видже- тов.
Приложения	Позволяет отсортиро- вать сведения по кон- кретному приложению	Выберите значение в раскры- вающемся списке	Выберите несколько приложений. Статистика по каждому приложе- нию или протоколу будет отображе- на в отдельном наборе виджетов.
Колонки	Позволяет сформиро- вать набор колонок та- блицы <b>Журнал соедине- ний</b> : отобразить или скрыть какие-либо ко- лонки	Выберите одно или несколь- ко значений: • Адрес источника, • Адрес назначения, • Байт передано, • Байт получено,	Расположение колонок зависит от порядка их выбора. При первом построении отчета они отображают- ся по умолчанию. Чтобы располо- жить колонки в желаемом порядке, в поле <b>Колонки</b> снимите все флажки и установите их поочеред- но – колонки будут отображаться слева-направо.

Фильтр	Назначение филь- тра	Значение	Примечание
		<ul> <li>Время завершения сес- сии,</li> </ul>	
		• Время начала сессии,	
		• Входящий интерфейс,	
		<ul> <li>Действие с пакетом по правилу,</li> </ul>	
		• Идентификатор сессии,	
		• Исходящий интерфейс,	
		<ul> <li>Наименование правила МЭ,</li> </ul>	
		• Пакетов передано,	
		• Пакетов получено,	
		• Порт источника,	
		• Порт назначения,	
		• Приложение,	
		• Протокол,	
		• Протокол L7 DPI,	
		• Родительская сессия,	
		<ul> <li>Узел фильтрации.</li> </ul>	
Лимит	Позволяет ограничить количество отображае- мых объектов в интере-	Укажите число вручную или с помощью счетчика	Минимальное количество отобра- жаемых результатов — 1.
	фейсе системы		Максимальное количество отобра- жаемых результатов — 10 000.
			Значение по умолчанию — 500.

<sup>а</sup>Под источником подразумевается локальная машина пользователя, с которой он выходит в интернет.

Табл. F.2. Описание параметров фильтрации запросов для сбора статистики в Журнале запросов

Фильтр	Назначение филь-	Значение	Примечание
	тра		
		Основные фильтры	
Период	Позволяет выбрать временной диапазон, за который формируется отчет	Дата и время начала и окон- чания сбора информации. Временной период следует указать с помощью календа- ря, встроенного в отчет.	Работа с календарем подробно описана в разделе 7.2.2.2. Для всех категорий отчетов задается по умолчанию период в 7 дней. Стати- стика для категории отчетов <b>Жур- нал запросов</b> собирается за сутки.
топ	Позволяет ограничить количество объектов, по которым формируется статистика	Укажите число вручную или с помощью счетчика.	Значение по умолчанию — 25.

Фильтр	Назначение филь- тра	Значение	Примечание
Сортировать по	Позволяет сортировать данные по различным параметрам	С помощью счетчика можно отсортировать информацию в отчете по возрастанию или убыванию. Вы можете отсортировать информацию в отчете, в раскрывающемся списке вы- брав одно из значений: • Количеству запросов, • Объему исходящего трафика, • Объему входящего тра- фика.	Сортировка количества запросов, объема исходящего или входящего трафика по возрастанию или убы- ванию. По умолчанию сортировка установлена по убыванию.
Запросы	Позволяет отфильтро- вать данные по опреде- ленным параметрам	<ul> <li>Выберите значение в раскрывающемся списке:</li> <li>Все,</li> <li>Разрешенные,</li> <li>Заблокированные,</li> <li>Все (без технического трафика),</li> <li>Разрешенные (без технического трафика),</li> <li>Заблокированные (без технического трафика),</li> </ul>	В зависимости от выбранного зна- чения фильтра можно отобразить данные по разрешенным или забло- кированным запросам, а также по всем сразу. Также вы можете отобразить дан- ные по указанным выше видам за- просов, только с исключением тех- нического трафика (плагинов соци- альных сетей, контекстной рекламы и т.д.).
	и Фильтры	по категориям и типам отчето	)B
Ресурсы	Позволяет указать ре- сурсы (подробнее см. раздел <u>6.5.5.3</u> ), посеща- емые пользователями	Введите значение вручную	Вы можете указать несколько ресур- сов или даже список ресурсов, ко- торые перечислены через запятую. Например, скопировать список из текстового редактора. Каждый ре- сурс определяется как отдельный элемент. Статистика по каждому ресурсу будет отображена в отдель- ном наборе виджетов.
Категории ресур- сов	Позволяет указать кате- гории ресурсов, на кото- рые были выполнены запросы от указанных персон/групп персон или IP-адресов источников	Выберите значение в раскры- вающемся списке	Можно выбрать несколько катего- рий ресурсов. Статистика по каж- дой категории ресурсов будет отображена в отдельном наборе виджетов.
Персоны	Позволяет указать пер- сон, по которым следует собрать статистику	Введите значение вручную или выберите его в раскрыва- ющемся списке	Поиск запускается при вводе пер- вого символа и ведется аналогично поиску в поле <b>Поиск</b> (подробнее см. раздел <u>5.6</u> ). При этом ищутся только те персоны, в данных кото- рых имеется совпадение <b>началь-</b> <b>ных</b> символов с введенными. На- пример, в фамилии, имени и/или должности.

Фильтр	Назначение филь- тра	Значение	Примечание
			Можно указать несколько персон. Статистика по каждой персоне бу- дет отображена в отдельном набо- ре виджетов.
Группы персон	Позволяет указать груп- пы персон, по которым можно собрать статисти- ку	Введите значение вручную или выберите его в раскрыва- ющемся списке	Поиск запускается при вводе пер- вого символа и ведется аналогично поиску в поле <b>Поиск</b> (подробнее см. раздел <u>5.6</u> ). Поиск идет только по тем группам персон, в данных которых имеется совпадение <b>на- чальных</b> символов с введенными. Например, в названии группы. Вы можете указать несколько групп. Статистика по каждой группе
			ном наборе виджетов.
IP-адреса источ- ников	Позволяет указать IP- адрес или диапазон IP- адресов источника <sup>а</sup> , от которых были запросы к выбранным ресурсам, категориям ресурсов и т.д.	Введите значение вручную	Можно указать несколько IP-адре- сов. Статистика по каждому IP-ад- ресу источника будет отображена в отдельном наборе виджетов
Исключить ресур- сы	Позволяет исключить из отчета ресурсы и сведе- ния о них для минимиза- ции полученных данных	Введите значение вручную	Вы можете указать несколько ресур- сов
Типы данных	Позволяет указать типы передаваемых или полу- чаемых пользователем данных	Выберите значение в раскры- вающемся списке	Вы можете выбрать несколько ти- пов данных. Статистика по каждому типу данных будет отображена в отдельном наборе виджетов.
Узлы фильтра- ции	Позволяет выбрать уз- лы фильтрации, через которые идет трафик	Выберите значение в раскры- вающемся списке	При наличии нескольких узлов фильтрации вы можете выбрать их все. Статистика по каждому узлу будет отображена в отдельном на- боре виджетов.
Колонки	Позволяет сформиро- вать набор колонок та-	Выберите одно или несколь- ко значений:	Отображение в отдельных колон- ках таблицы следующих сведений:
	блицы <b>Журнала запро-</b> сов: отобразить или	• НТТР-код,	<ul> <li>код ответа НТТР-протокола;</li> </ul>
	скрыть какие-либо ко- лонки	<ul> <li>НТТР-протокол,</li> </ul>	<ul> <li>НТТР-протокола;</li> </ul>
		• HTTP-referer,	• заголовка запроса;
		<ul> <li>IP-адрес источника,</li> </ul>	<ul> <li>IP-адреса источника;</li> </ul>
		<ul> <li>URL запрос,</li> </ul>	<ul> <li>URL запроса;</li> </ul>
		• URL параметры,	<ul> <li>URL параметрам;</li> </ul>
		• URL путь,	• URL пути;
		<ul> <li>User-Agent,</li> </ul>	<ul> <li>User agent;</li> </ul>
		• Группы,	• группам персон;
		<ul> <li>Правила Политики,</li> </ul>	<ul> <li>правилам политики;</li> </ul>
		• Результат проверки,	<ul> <li>результата проверки;</li> </ul>

Фильтр	Назначение филь- тра	Значение	Примечание
		• Слои Политики,	• слоям политики;
		• Статусы фильтрации.	• статусам фильтрации.
			По умолчанию фильтру присвоены значения URL путь, URL парамет- ры, URL запрос. Удалить их не- льзя.
НТТР-код	Позволяет отсортиро- вать сведения по кон- кретному коду НТТР-от- вета	Введите значение вручную	Отображаются сведения по конкрет- ному HTTP-коду.
Тип проверки	Позволяет отсортиро- вать сведения о запро- сах по конкретному типу проверки	Выберите значение в раскры- вающемся списке: • Тип данных, • Метод, • Заголовки, • Порт, • Протокол, • URL ресурса, • Категория ресурса, • Ключевое слово в URL ресурса, • Расписание, • Размер, • Антивирус, • Лимит трафика, • ІР источника, • Пользователь, • Группа, • Запрос подтверждение, • Архивирование,	В зависимости от выбранного значения фильтра можно отобразить данные по типу проверки запросов. Например, выбрав значение фильтра Антивирус, в журнале запросов будут отображаться све- дения о запросах, которые относят- ся только к этому типу проверки.
Лимит	Позволяет ограничить количество отображае- мых объектов в интере- фейсе системы	Укажите число вручную или с помощью счетчика	Максимальное количество отобра- жаемых результатов — 10 000. Значение по умолчанию — 500.
Режим прокси	Позволяет отсортиро- вать сведения о запро- сах, в зависимости от	Выберите значение в раскры- вающемся списке: • Все,	В зависимости от выбранного зна- чения фильтра, можно отобразить данные при работе прокси-сервера

Фильтр	Назначение филь-	Значение	Примечание
	Тра		
	режима работы прокси-	<ul> <li>Прямой режим,</li> </ul>	в прямом или в обратном режиме,
	сервера		а также по всем сразу.
		<ul> <li>Обратный режим.</li> </ul>	
			По умолчанию выбрано значение
			Bce.
Приложение/про-	Позволяет отсортиро-	Выберите значение в раскры-	Выберите несколько приложений
токол	вать сведения по кон-	вающемся списке	и/или протоколов. Статистика по
	кретному приложению		каждому приложению или протоко-
	или протоколу передачи		лу будет отображена в отдельном
	данных		наборе виджетов.
ІР-адрес сервера	Позволяет указать IP-	Введите значение вручную	Укажите несколько ІР-адресов.
назначения	адрес или диапазон IP-		Статистика по каждому IP-адресу
	адресов серверов назна-		сервера назначения будет отобра-
	чения, которым были		жена в отдельном наборе видже-
	направлены запросы		тов.

<sup>а</sup>Под источником подразумевается локальная машина пользователя, с которой он выходит в Интернет.

# Лист контроля версий

10/02/2025-13:34