SOLAR

Программный комплекс «Solar NGFW»

Версия 1.4.1

Руководство по установке и настройке

Москва, 2024

Содержание

Список иллюстраций

Список таблиц

Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
ОС	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 модифицирует 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, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
ZIP	Формат архивации файлов и сжатия данных без потерь

Использование стилей

Шрифт без форматирования	Основной текст
Моноширинный шрифт	Пользовательский ввод
Рамка	Программный вывод на экран
Курсивный шрифт	Наименования документов
Полужирный подчеркнутый фиолетовый шрифт	Внутренняя ссылка
Полужирный шрифт	Наименование элементов интерфейса

1. Введение

1.1. Область применения

Программный комплекс Solar NGFW (далее – 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.

1.2. Краткое описание возможностей

Solar NGFW представляет собой комплексную систему функциональных модулей информационной безопасности, в которую входят:

- 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 web-ресурсов на базе решения WebCat,
- потоковый антивирус на базе решения Dr.Web,
- интеграция со смежными системами по ICAP,
- мониторинг состояния системы и действий пользователей,
- кластеризация Solar NGFW с отказоустойчивостью,
- поддержка VLAN-интерфейсов,
- управление сетевыми интерфейсами.

1.3. Уровень подготовки системного администратора

Квалификация системного администратора Solar NGFW должна быть достаточной для выполнения задач по обслуживанию системы, обеспечивающих бесперебойное функционирование всех ее компонентов.

К задачам системного администратора Solar NGFW относятся:

- установка и настройка компонентов Solar NGFW;
- мониторинг функционирования процессов системы;
- реагирование на служебные уведомления системы.

Системный администратор Solar NGFW должен:

- ориентироваться в особенностях работы Solar NGFW;
- понимать работу сетевых протоколов;
- обладать знаниями в области безопасности ОС класса UNIX.

В своей работе системные администраторы Solar NGFW должны использовать внутреннюю документацию и документацию по ОС Linux.

1.4. Перечень эксплуатационной документации для ознакомления

Системный администратор Solar NGFW должен ознакомиться с эксплуатационными документами:

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

2. Назначение и возможности Solar NGFW

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. Состав Solar NGFW

Solar NGFW имеет модульную структуру на основе сервисов, которые могут работать в распределенном режиме и обеспечивают решение конкретных задач (см. ниже).

Примечание

*Большинство сервисов принимают соединение на сетевом интерфейсе 127.0.0.1. Привязать сервис к необходимому IP-адресу можно в настройках сервиса в разделе **Система**.*

Табл. 2.1. Сервисы, используемые Solar NGFW

Сервис	Решаемые задачи	Порт
Сервис Досье (abook-daemon)	Обеспечивает хранение и репликацию данных Досье: • поддержание основной БД адресной книги (создание и обновление схемы); • синхронизация с внешними источниками (Active Directory) по протоколам LDAP (TCP/389), LDAPS (TCP/636).	2269 Обеспечивает внутреннюю коммуникацию между узлами (при необходимости порт можно изменить в настройках системы)
Антивирус (antivirus)	Управляет сервисами антивируса. Обеспечивает прием трафика по протоколу ICAP и его проверку по локальным антивирусным базам.	1344 Принимает запросы на поиск вирусов по протоколу ICAP от узлов с ролью **HTTP-фильтр** (при необходимости порт можно изменить в настройках системы)
Сервис хранения статистики пользователей (clickhouse)	Хранит запросы пользователей и извлекает данные для отчетов на основе сформированных запросов	8123 Принимает данные от узлов с ролью **HTTP-фильтр**, контроль приложений, обратный прокси
Сервис синхронизации состояний соединений между узлами кластера (conntrackd)	Сервис передает данные об установленных сессиях пользователей с активного узла на пассивный	3780, 3781
Сервис хранения данных (database)	Сервис, который обеспечивает: • хранение политик для подсистемы фильтрации; • хранение данных подсистемы мониторинга; • хранение данных Досье;	5434

Сервис	Решаемые задачи	Порт
	• управление Solar NGFW.	
Сервис журналирования (dblog)	Сервис отвечает за журналирование событий в базу данных Clickhouse.	9000
Сервис построения отчетов (grafana)	Служит для построения таблиц и графиков для подсистем отчетности и мониторинга. Используется для формирования данных в разделах **Статистика** и **Мониторинг**.	3000
Сервис балансировки трафика (haproxy)	Обеспечивает распределение трафика между узлами в соответствии с настройками Solar NGFW	2344, 1010 Принимает запросы от пользователей (при необходимости порт можно изменить в настройках системы)
Сервис виртуального IP (keepalived)	Обеспечивает отказоустойчивость работы Solar NGFW, объединяя несколько узлов под одним виртуальным IP-адресом. Для автоматического переключения IP-адреса используется протокол VRRP (Virtual Router Redundancy Protocol).	–
Сервер лицензирования (license-server)	Проверяет состояние лицензии, лицензионных ограничений, а также предоставляет информацию о лицензии другим сервисам системы	3004 Принимает соединения со всех узлов
Сервис ретрансляции журнальных данных (log-streamer)	Обеспечивает взаимодействие с БД ClickHouse (отправка и архивация запросов): собирает журнальные файлы сервисов фильтрации, конвертирует их и переносит в БД сервиса хранения статистики пользователей ClickHouse. Некорректные записи журнальных файлов записываются в файл **/data/spool/skvt/access_log/invalid_log_entries**.	–
Сервис сбора данных о работоспособности системы (monitor-agent)	Сервис, который выполняет следующие функции: • проверка состояния различных ресурсов Solar NGFW; • запуск и остановка некоторых сервисов в зависимости от состояния проверяемых ресурсов.	10050 При необходимости порт можно изменить в настройках системы
Сервис анализа работоспособности системы (monitor-server)	Сервис, который выполняет следующие функции: • накопление данных от сервиса сбора; • сохранение информации о состоянии различных ресурсов Solar NGFW в БД; • отправка уведомлений о проведении заданных проверок; • выполнение действий в соответствии с заданными условиями.	10051

Сервис	Решаемые задачи	Порт
Сервис выполнения удаленных команд (monitor-ng)	Сервис, который обеспечивает: • проверку задаваемых параметров конфигурации на соответствие диапазонам допустимых значений; • выполнение удаленных команд; • получение журналов сервисов.	5555
Сервис управления сетевыми интерфейсами (network-config-agent)	Сервис-агент, который обеспечивает: • настройку сетевой конфигурации узлов в соответствии с политикой Solar NGFW; • распознание текущей сетевой конфигурации узлов; • отправку информации о текущей сетевой конфигурации узлов на сервис skvt-play-server по протоколу SSE.	5566 Skvt-play-server подключается ко всем агентам
Сервис Basic-аутентификации (skvt-auth-server)	Обеспечивает вход в систему с предоставлением идентификационных данных: запрашивает и кэширует информацию о доменных пользователях с помощью basic-аутентификации для источников LDAP (TCP/993), AD (TCP/995), IMAP (TCP/110), POP3 (TCP/143), RADIUS (TCP/1812)	2230 Skvt-auth-server ожидает запросы на аутентификацию от узлов фильтрации и/или управления (при необходимости порт можно изменить в настройках системы)
Сервис кэширования (skvt-cache)	Служит для кэширования данных, получаемых от внешних веб-серверов, и выполняет следующие функции: • кэширование (временное локальное хранение) страниц сети Интернет, запрашиваемых по протоколу HTTP; • выдача хранимых страниц из кэша по запросу пользователей рабочих станций; • перенаправление запросов пользователей рабочих станций на ресурсы сети Интернет при отсутствии соответствующих страниц в кэше. На данный момент кэшируется только HTTP-трафик.	2228 Принимает и обрабатывает HTTP/FTP/HTTPS-запросы от локального skvt-wizor (при необходимости порт можно изменить в настройках системы)
Сервис масштабируемого хранилища данных Cassandra (skvt-cassandra)	СУБД, которая хранит счетчики трафика, подтверждения, кэш привязки неаутентифицированного трафика к пользователям и кэш пользователей, получивших страницу загрузки сертификата вскрытия HTTPS. Сервис хранит: • идентификаторы аутентифицированных пользователей; • идентификаторы пользователей с ошибкой вскрытия HTTPS; • подтверждения открытия страниц;	7199, 7000, 9160 При наличии нескольких экземпляров БД Cassandra они могут обмениваться данными также по любому порту

Сервис	Решаемые задачи	Порт
	• цепочки сертификатов; • статистику по объему трафика; • информацию о загруженных файлах	
Сервис Kerberos-аутентификации (skvt-kerberos-server)	Сервис, необходимый для аутентификации пользователей рабочих станций по протоколу Kerberos (TCP/2226)	2226 Принимает запросы от узлов фильтрации (при необходимости порт можно изменить в настройках системы)
Сервис NTLM-аутентификации (skvt-ntlm-server)	Сервис, необходимый для аутентификации пользователей рабочих станций по протоколу NTLM (TCP/2225)	2225 Принимает запросы от узлов фильтрации (при необходимости порт можно изменить в настройках системы)
Веб-сервер (skvt-play-server)	Сервер управления выполняет следующие функции: • функционирование интерфейса управления; • аутентификация администраторов; • контроль действий администраторов; • передача данных и задач в другие подсистемы; • получение данных из других подсистем; • установление подлинности и действительности загруженной лицензии. Также осуществляет журналирование действий администраторов по изменению политик фильтрации и настроек конфигурации.	8443 Принимает запросы от браузеров администраторов
Сервис учета трафика (skvt-trafdaemon)	Сервис учета трафика, который обеспечивает накопление и хранение данных о количестве трафика между сервисом фильтрации и сервером назначения. Сервером назначения считается узел, с которым связывается сервис фильтрации – это может быть как узел сети Интернет, так и родительский прокси-сервер. Если система установлена на единственном узле, skvt-trafdaemon используется как библиотека сервиса фильтрации и хранит данные о трафике в файле. Если система функционирует в распределенном режиме и на одном узле или всех узлах добавлена роль **Фильтр HTTP-трафика**, в сервис фильтрации встраивается клиентская часть skvt-trafdaemon, которая отправляет данные через TCP-соединение. В этом случае данные о трафике хранятся в БД Cassandra сервиса масштабируемого хранилища данных и передаются по протоколу TLS.	2299

Сервис	Решаемые задачи	Порт
Сервис интеграции с доменом (skvt-winbind)	Сервис, организующий взаимодействие с контроллером домена. Он служит для предоставления доступа сервисам NSS (Name-Service Switch) к различным приложениям через PAM (Pluggable Authentication Modules – подключаемые модули аутентификации) и **ntlm_auth** (утилита NTLM-аутентификации), а также к Samba.	–
Сервис фильтрации (skvt-wizor)	Реализует политику безопасности для пользователей и на ее основе выполняет анализ данных, передаваемых в обоих направлениях. Сервис выполняет следующие функции: • применение политики фильтрации к запросам пользователей рабочих станций к ресурсам сети Интернет; • аутентификация пользователей. Сервис является ядром межсетевого экрана (МЭ) и находится на пути потока данных между рабочими станциями пользователей и сетью Интернет. Он может функционировать на нескольких узлах Solar NGFW.	Сервис принимает соединения на следующих портах (при необходимости порты можно изменить в настройках системы): • 2270 – порт для принятия HTTP-запросов; • 2278 – порт для принятия трафика от модуля балансировки; • 2277 – порт для получения отладочной информации о модуле; • 2281 (HTTP), 2282 (HTTPS) – порты для отображения таких внутренних ресурсов как страница подтверждения перехода, страница отложенной загрузки, страница аутентификации, страница проверки сертификата, страница инструкции по установке сертификата; • 2272 – порт для принятия сообщений в формате ICAP; • 2443 – порт для принятия HTTPS-запросов; • 2444 – порт для принятия HTTPS-запросов в прозрачном режиме.
Сервис распаковки и конвертирования данных (smaptikaserver)	Сервис выполняет следующие функции: • извлечение текста и вложений из бинарных файлов; • нормализация кодировки текстов из неизвестных источников.	9998 Принимает запросы с фрагментами сообщений от узлов фильтрации (при необходимости порт можно изменить в настройках системы)
Сервис категоризации (url-checker)	Выполняет проверку URL на соответствие категориям. Определение соответствий осуществляется согласно настройкам Solar NGFW.	2260 Принимает запросы от узлов фильтрации и управления (при необходимости порт можно изменить в настройках системы)
Система предотвращения вторжений	Выполняет проверку трафика по сигнатуре и автоматически предпринимает действия при обнаружении угрозы	–
Сервис пересылки широковещательных IGMP-пакетов (igmpproxy)	Обеспечивает пересылку IGMP-пакетов из одной сети в другую через МЭ	–

Также Solar NGFW использует дополнительные порты, представленные в таблице ниже.

Табл. 2.2. Дополнительные порты, используемые в работе Solar NGFW

Номер порта	Сервис	Назначение
Взаимодействие фильтра с внешними сервисами		
TCP/25 (можно изменить в настройках системы)	Отправка почты	Сервис отправляет: • POST-запросы правил фильтрации на запись данных в архив; • уведомления о срабатывании правил фильтрации; • уведомления о проблемах сервера мониторинга
53 (UDP)	DNS	Обеспечивает взаимодействие с DNS-серверами
22	SSH	Предоставляет доступ для подключения по SSH
80, 443	internet	Организует доступ к внешним HTTP/HTTPS/FTP-серверам

Для управления системой используется графический интерфейс пользователя (далее – GUI).

2.3. Схемы подключения Solar NGFW

Solar NGFW обеспечивает защиту периметра сети путем глубокого контроля информационных потоков, выявления и предотвращения сетевых атак, противодействия веб-угрозам (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.

Существует четыре режима работы Solar NGFW:

- Одиночный режим – один узел, на который назначены все необходимые роли.
- Распределенный режим – роли распределены между несколькими узлами. Например, роли управления Solar NGFW и межсетевого экрана расположены на одном узле, а роли прокси-сервера и контентной фильтрации – на другом.
- Режим кластера – один узел является управляющим (на него назначена роль **Сервер управления**), а два других узла выполняют роль межсетевого экрана. При этом один из узлов с ролью межсетевого экрана работает в активном режиме и обрабатывает сетевой трафик, а другой находится в пассивном режиме (режиме ожидания) и сетевой трафик не обрабатывает. При недоступности активного узла, выполняющего роль фильтрации сетевого трафика, пассивный узел становится активным.
- Режим отказоустойчивой пары на основе keepalived – два узла с независимой политикой, для которых организовано резервирование сетевого трафика по протоколу VRRP.

Примечание

*В режиме кластера или распределенного режима для узлов, на которые будет назначена роль **Межсетевой экран**, должны выполняться требования:*

- *Количество и название сетевых интерфейсов на узлах должно быть одинаковое.*
- *Интерфейсы с одинаковым названием должны быть подключены к одним и тем же сетевым сегментам.*

2.4. Порядок обработки трафика

В Solar NGFW для фильтрации трафика используется сетевой стек ОС Astra Linux (Netfilter). Обработка трафика происходит следующим образом:

1. Поступление сетевых пакетов на входящий интерфейс (для разных типов трафика входящий интерфейс может отличаться).
2. Фильтрация фрагментированных пакетов (если включена).
3. Прозрачное переопределение адреса и порта назначения пакетов (для 80/TCP и 443/TCP) с дальнейшим перенаправлением на проверку сервису wizor (если настроен прозрачный режим проксирования веб-трафика).
4. Трансляция адреса и/или порта назначения (если включен NAT).
5. Netfilter принимает решение о том, является ли трафик:
   - транзитным – в этом случае он проверяется в цепочке FORWARD с дальнейшим перенаправлением по месту назначения;
   - локальным (в том числе и проксируемый трафик в явном/прозрачном режимах) – в этом случае он проверяется в цепочке INPUT с дальнейшей передачей локальному процессу в пространство пользователя.
6. Для транзитного трафика:
   a. Фильтрация трафика в цепочке FORWARD (проверка выполняется по классическим правилам МЭ и DPI).
   b. Отправка трафика на проверку сетевым IPS средствами NetfilterQueue (если система предотвращения вторжений включена для транзитного трафика).
   c. Трансляция адреса источника (если включен NAT).
   d. Трафик отправляется по назначению.

   Для локального/проксируемого трафика:

   a. Фильтрация трафика в цепочке INPUT (проверка выполняется по классическим правилам МЭ и DPI).

b. Отправка трафика на проверку сетевым IPS средствами NetfilterQueue (если система предотвращения вторжений включена для входящего трафика).

c. Передача трафика в пространство пользователя локальному процессу (сервису) по соответствующему порту назначения.

d. Использование трафика локальным процессом (может быть служебным процессом, т.к. на этом этапе для проксируемого веб-трафика выполняется его проверка в модулях Solar webProxy).

e. Генерация исходящего трафика и передача его в пространство ядра.

f. Принимается решение о маршрутизации исходящего трафика.

g. Фильтрация трафика в цепочке OUTPUT (проверка выполняется по классическим правилам МЭ, а также по правилам DPI, однако не рекомендуется проверять исходящий трафик, т.к. он считается доверенным, пока нет явных признаков того, что решение скомпрометировано).

h. Трансляция адреса источника.

i. Трафик отправляется по назначению.

3. Требования к программному и аппаратному обеспечению

3.1. Требования к АРМ системного администратора

3.1.1. Требования к аппаратному обеспечению

АРМ системного администратора Solar NGFW должно быть оборудовано персональным компьютером. Особых требований к аппаратному обеспечению нет. Рекомендуются следующие характеристики персонального компьютера:

- процессор P-IV с тактовой частотой не менее 2 ГГц;
- объем оперативной памяти не менее 4 ГБ;
- объем жесткого диска не менее 20 ГБ.

3.1.2. Требования к программному обеспечению

В состав программного обеспечения АРМ системного администратора Solar NGFW должен входить браузер. Рекомендуемые браузеры:

- Mozilla Firefox (актуальной версии)
- Google Chrome (актуальной версии)

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 настоятельно рекомендуется разрешить выполнение JavaScript и сохранение cookies (настройка по умолчанию).

Внимание!

Если вручную увеличить размер шрифта в браузере, дизайн интерфейса Solar NGFW будет нарушен, и интерфейс станет непригодным к использованию.

3.2. Требования к серверу

3.2.1. Требования к аппаратному обеспечению

Примечание

Чтобы рассчитать индивидуальный сайзинг согласно требованиям и потребностям, обратитесь к специалистам Solar NGFW.

Для установки и корректной работы Solar NGFW требуется как минимум 150 ГБ свободного дискового пространства. Системный диск разбивается исходя из рекомендаций:

- Не менее 50 ГБ для раздела **/var** , т.к. в зависимости от политики сервис skvt-wizor по умолчанию записывает в этот каталог файлы, загружаемые из интернета.
- Не менее 30 ГБ для корневого каталога, в который будет устанавливаться операционная система.
- Не менее 70 ГБ для раздела **/opt**, в который будут установлены непосредственно рабочие файлы Solar NGFW.

Кроме того, в процессе работы Solar NGFW потребуется свободное дисковое пространство под журнальные файлы в отдельно примонтированный каталог **/data**. Рекомендуемый объем выделенного пространства под раздел **/data** не менее 100 ГБ. Выделение пространства осуществляется путем монтирования СХД к файловой системе.

Рекомендуемые характеристики аппаратного обеспечения СХД:

- Количество операций ввода-вывода в секунду (IOPS) – не менее 2000. IOPS может быть увеличен за счет использования большего количества жестких дисков меньшей емкости при сохранении общего объема СХД.
- Дисковой массив уровня RAID 10 или RAID 6.
- Интерфейс подключения жестких дисков – SAS (скорость вращения – 10000 или выше оборотов в минуту) или SSD.

Требования к СХД прямо и линейно пропорциональны сроку хранения данных в архиве, остальные требования не зависят от него.

3.2.2. Требования к программному обеспечению

Данная версия Solar NGFW функционирует под управлением ОС 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 ОС Astra Linux более новых версий (например, 1.8.1), т.к. это может нарушить штатную работу служб Solar NGFW и привести к нарушению работоспособности.

3.2.3. Требования к конфигурации ОС

Solar NGFW поддерживает работу только по протоколу IPv4. Использование ПО, работающего по протоколу IPv6, может приводить к ошибкам в работе Solar NGFW. Рекомендуется отключить использование IPv6 средствами операционной системы.

Кроме того, в процессе работы Solar NGFW необходим файл с региональными установками **ru_RU.UTF8** для корректного отображения пользовательского веб-интерфейса Solar NGFW.

Функционирование Solar NGFW зависит от наличия в ОС определенных программ и компонентов. Большинство из них являются стандартными динамическими библиотеками

ОС. Набор необходимых компонентов задается в виде зависимостей в установочном пакете Solar NGFW.

В настройках ОС должны быть открыты сетевые порты, которые используются в работе Solar NGFW. Перечень портов указан в Табл. (см. Табл.2.1).

3.2.4. Рекомендации по разделению дисков в ОС при установке Solar NGFW

По умолчанию Solar NGFW для ОС Linux настроен на использование следующих логических разделов диска:

- **/opt** – раздел, в который производится установка компонентов Solar NGFW.
- **/data** – раздел для размещения накапливаемых данных Solar NGFW.

3.2.5. Рекомендации по размещению в сетевой инфраструктуре

Аппаратное и программное обеспечение сервера должно располагаться на сетевом периметре безопасности для исключения несанкционированного доступа.

3.2.6. Требования к паролю

Solar NGFW обеспечивает стойкость паролей для доступа в систему. При создании пользователей система проверяет качество паролей, которое определяется следующими параметрами:

1. Минимально разрешенная длина пароля.
2. Известная и задокументированная максимальная длина пароля.
3. Количество различных символов в пароле:
   - заглавные буквы латиницы;
   - прописные буквы латиницы;
   - цифры;
   - служебные символы: ~ ! @ # $ % ^ & * ( ) + - = ` ' _ / \ | ".

При создании пароля система рассчитывает уровень его сложности (от 0 до 10). Система не позволит создать пароль, если он не соответствует заданному в настройках уровню сложности – например, если он содержит более двух символов подряд из одного набора. По умолчанию уровень сложности пароля должен быть не менее 6. Расчет уровня сложности пароля выполняется на основании следующих условий:

1. Если длина пароля равна или больше минимальной, прибавляется 1.
2. Если длина пароля максимальная, прибавляется 2.
3. Если пароль содержит символы из двух наборов, прибавляется 1.
4. Если пароль содержит символы из трех наборов, прибавляется 1.
5. Если пароль содержит символы из четырех наборов, прибавляется 1.

6. Если пароль не содержит более двух символов из одного набора подряд, прибавляется 1.

7. Если пароль не содержит более одного символа из одного набора подряд, прибавляется 2.

8. Если количество разных символов больше минимальной длины пароля, прибавляется 1.

9. Если пароль выполняет условия пунктов 1, 5, 7, 8, прибавляется 1.

Если сумма условий больше 10, уровень сложности пароля считается равным 10.

В настройках по умолчанию минимальная длина пароля равна 6, максимальная – 12, минимально допустимый уровень сложности пароля – 6. Таким образом, если уровень сложности меньше 6, система не позволит создать пароль.

Настройки по умолчанию можно изменить, отредактировав в GUI следующие параметры (раздел **Система > Расширенные настройки >Интерфейс**, секция **Сервер веб-интерфейса**):

- **Мин. длина пароля**;
- **Макс. длина пароля**;
- **Уровень сложности пароля**.

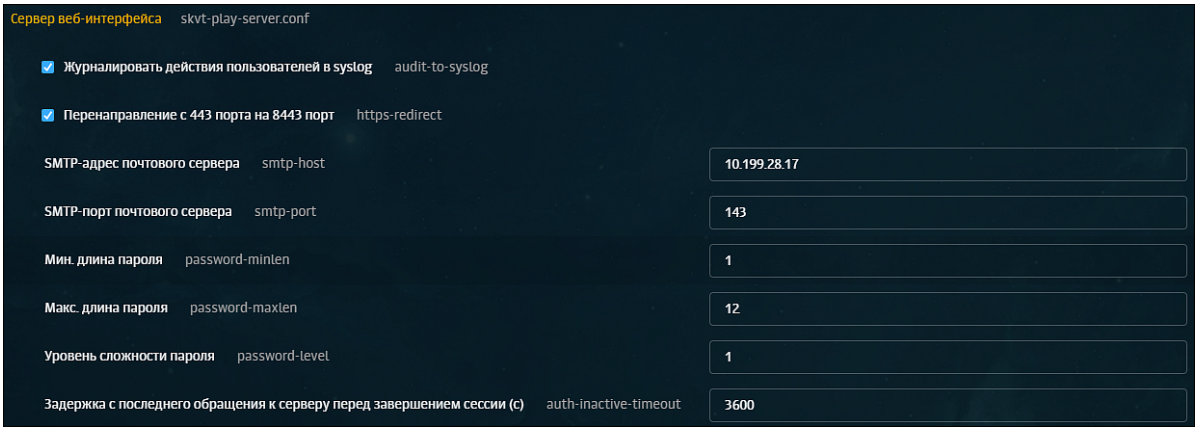


Рис. 3.1. Настройки сложности пароля

В системе реализована защита от взлома путем перебора учетных данных (брутфорс). После заданного количества неудачных попыток входа перед каждой следующей попыткой вводится временная задержка, которая увеличивается экспоненциально после каждой последующей неудачной попытки входа. Настройки защиты можно задать, используя следующие параметры конфигурации (раздел **Система > Расширенные настройки > Интерфейс**, секция **Сервер веб-интерфейса**):

- **Макс. количество неудачных попыток входа в систему до задержки**;
- **Начальное значение задержки для входа в систему (с)**;
- **Макс. значение задержки для входа в систему (с)**.

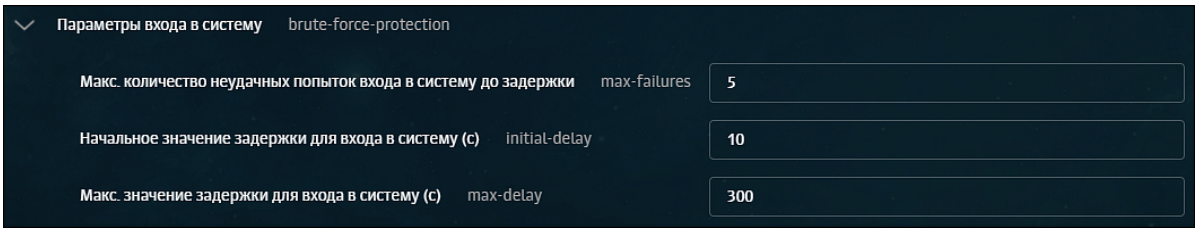


Рис. 3.2. Настройка параметров входа в систему

При неправильном вводе пароля воспользуйтесь сервисом **user-tool** для его изменения (см. раздел 11.2.3).

4. Установка и удаление Solar NGFW

4.1. Установка ОС Astra 1.8.0

Для установки ОС Astra 1.8.0 запустите сервер с использованием установочного диска или USB-носителя «Astra 1.8.0» и выполните следующие действия:

1. В окне приветствия оставьте выбор параметров программы установки по умолчанию (**Графическая установка**, **Русский**) и нажмите **Enter**.

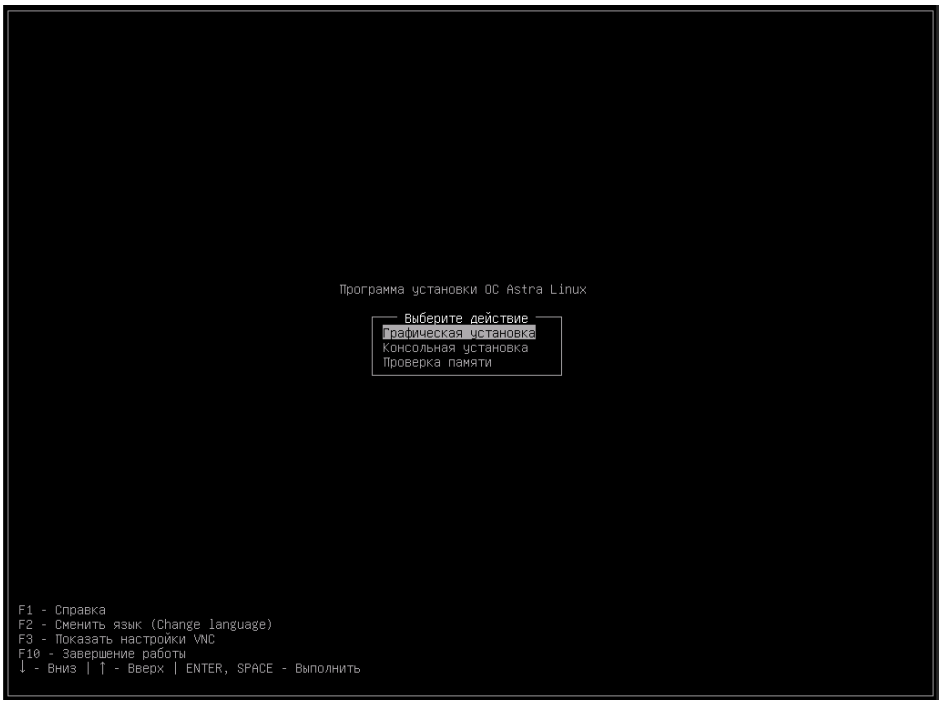


Рис. 4.1. Окно приветствия

2. Ознакомьтесь с Лицензионным солашением, выберите уровень защищенности **Максимальный («Смоленкск»)**, установите флажок **Принимаю условия лицензионного соглашения** и нажмите **Далее**.

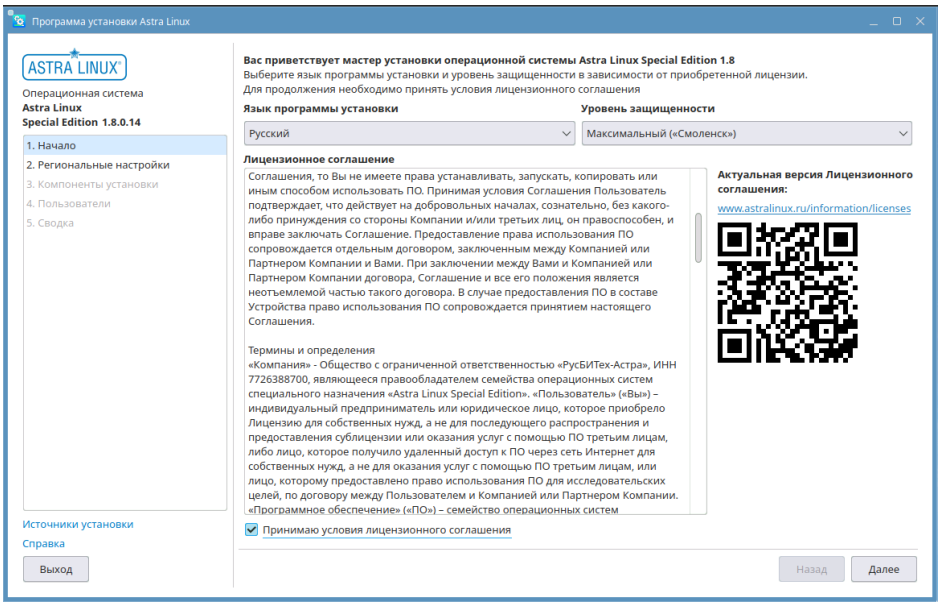


Рис. 4.2. Окно Лицензензионное соглашение

3. В окне **Региональные настройки Astra Linux** выберите регион, часовой пояс, язык ввода, язык ОС и сочетание клавиш для переключения языка. Нажмите **Далее**.

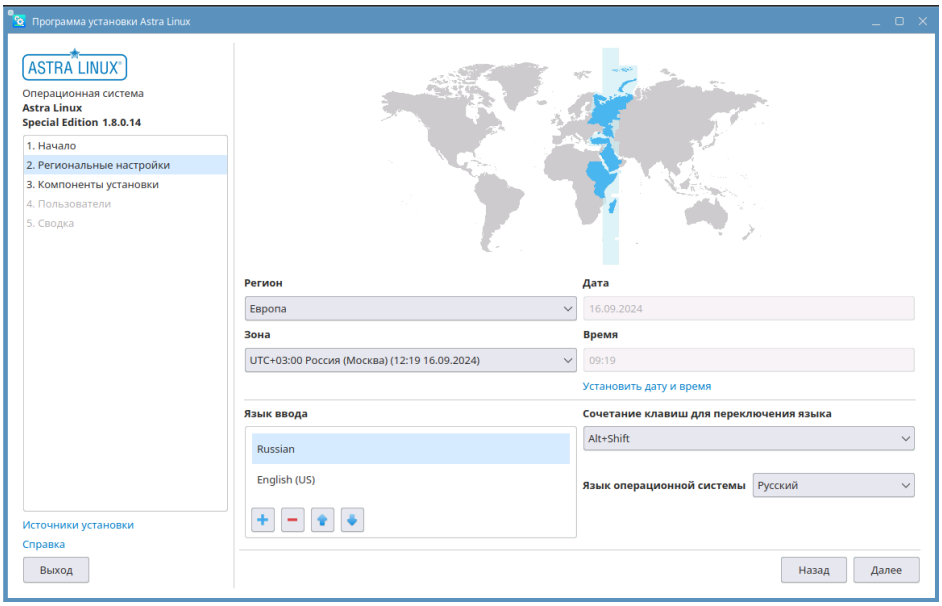


Рис. 4.3. Региональные настройки

4. В появившемся окне **Компоненты установки Astra Linux** выберите:

- **Профиль разметки диска** – **Ручная разметка**;
- **Ядро Linux** – **linux-6.1-generic**;
- **Компоненты операционной системы** – установите флажки **Средства работы в сети Интернет**, **Консольные утилиты**, **Средства удаленного подключения SSH**.

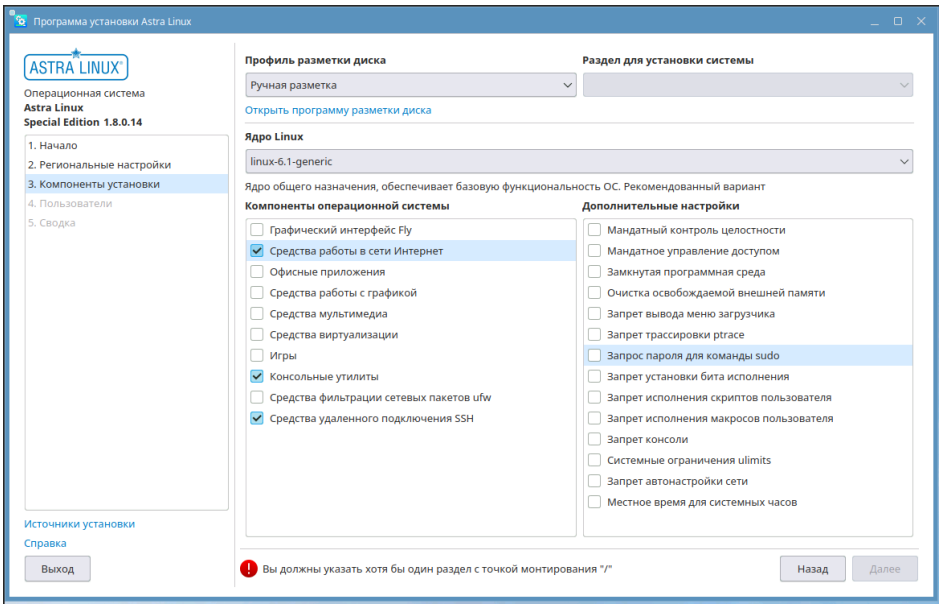


Рис. 4.4. Компоненты установки

5. Нажмите **Открыть программу разметки диска**.

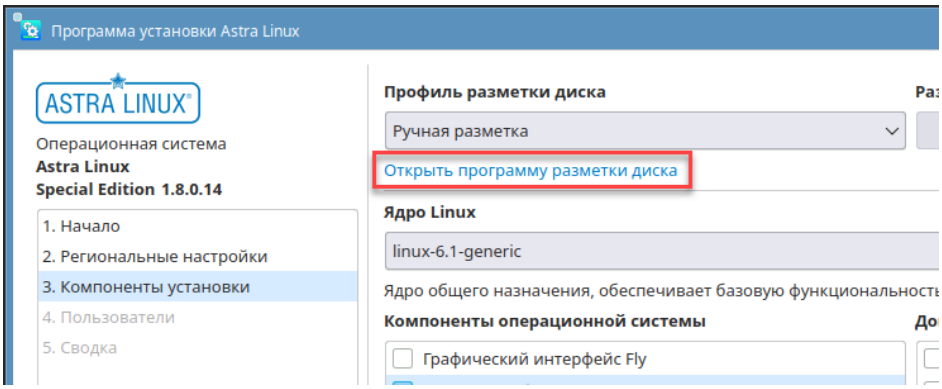


Рис. 4.5. Компоненты установки

6. В открывшемся окне **Настройки конфигурации разметки диска** удалите устройство **vda**.

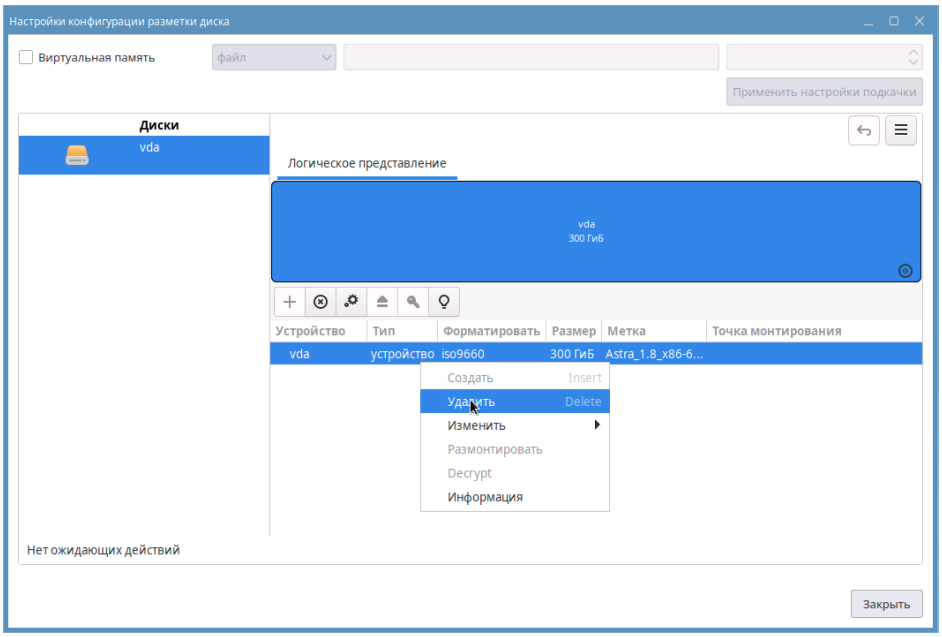


Рис. 4.6. Удаление устройства vda

.

7. Правой кнопкой мыши нажмите на строку **свободно** и в контекстном меню выберите **Создать**.

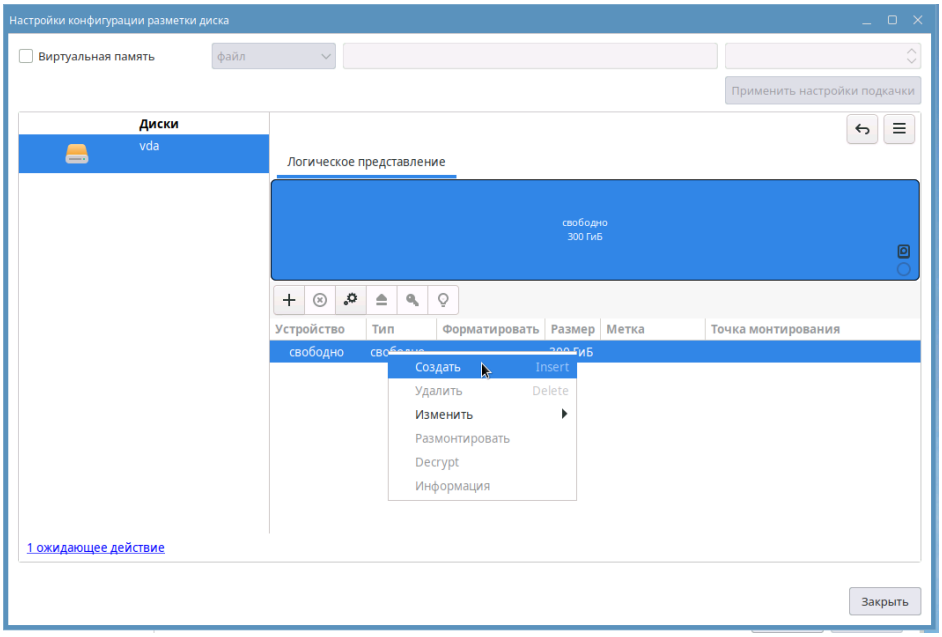


Рис. 4.7. Создание нового раздела

8. В открывшемся окне **На диске не найдена таблица разделов** в поле **Выберите тип новой таблицы разделов** выберите **gpt** и нажмите **ОК**.

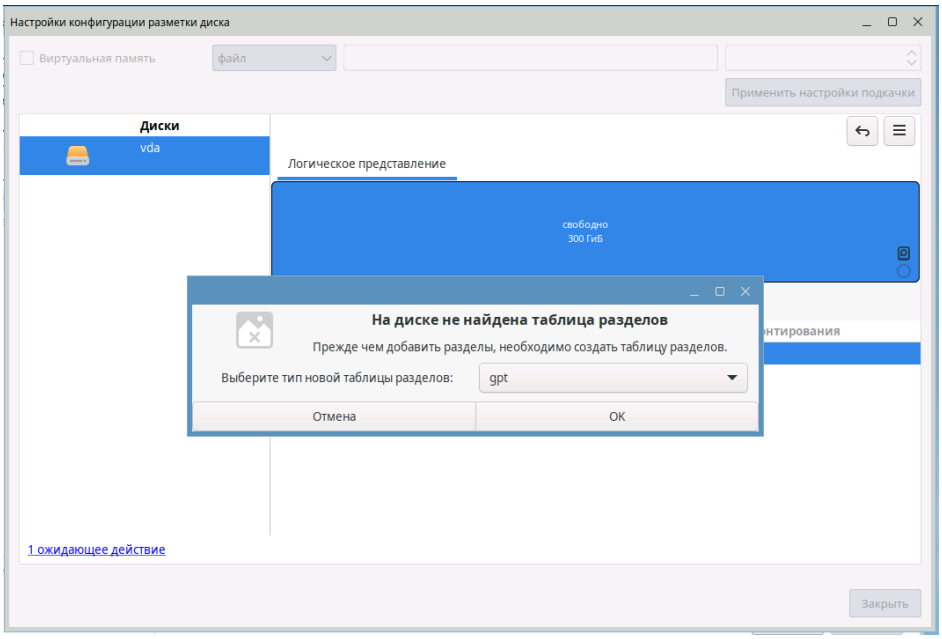


Рис. 4.8. Выбор типа новой таблицы разделов

9. В открывшемся окне **Добавить новое устройство** выберите тип устройства **Раздел** и файловую систему **BIOS Boot**. Нажмите **ОК**.

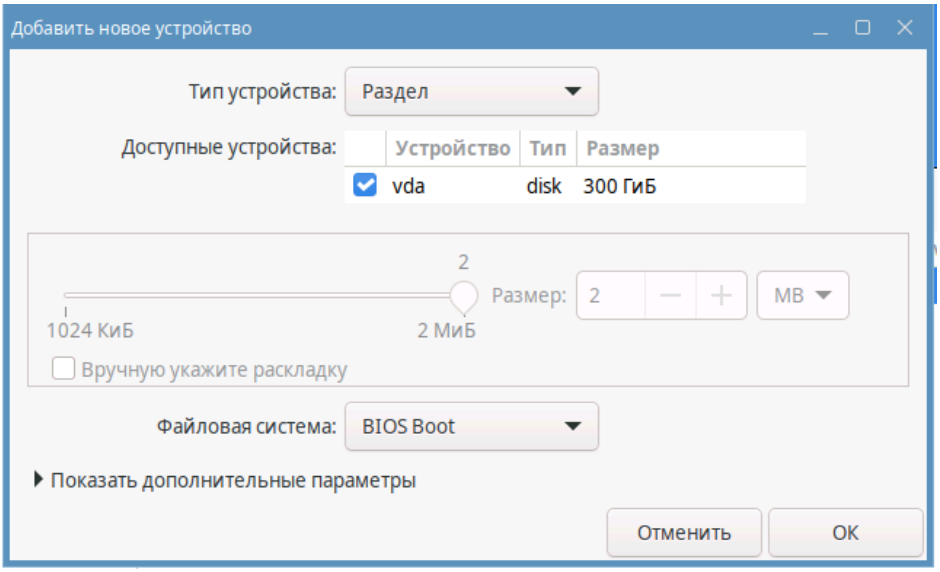


Рис. 4.9. Окно Добавить новое устройство

10. В новом окне **Добавить новое устройство** выберите максимальный объем дискового пространства и для параметра **Файловая система** выберите значение **physical volume (LVM)**. Нажмите **ОК**.

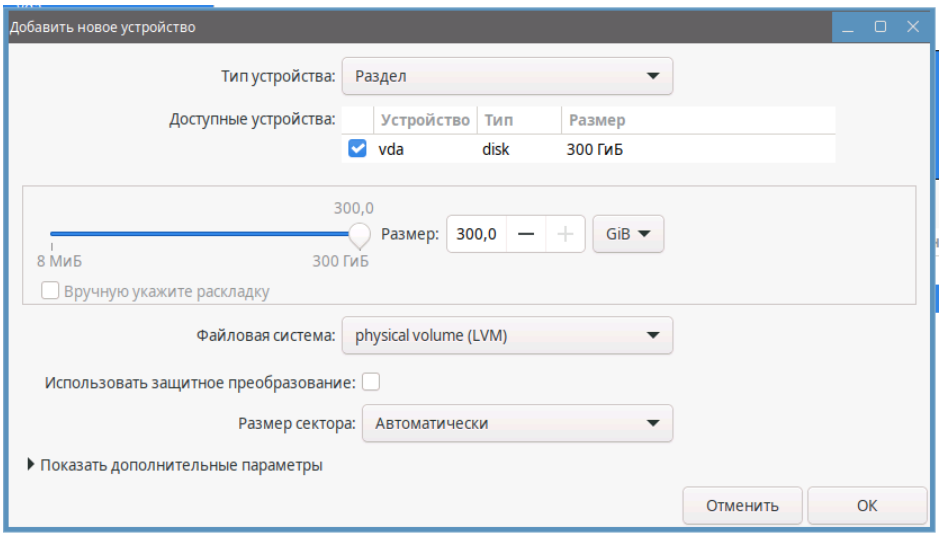


Рис. 4.10. Окно Добавить новое устройство

11. На основе LVM создайте группу томов и укажите произвольное имя, например, **ngfw**. Нажмите **OK**.

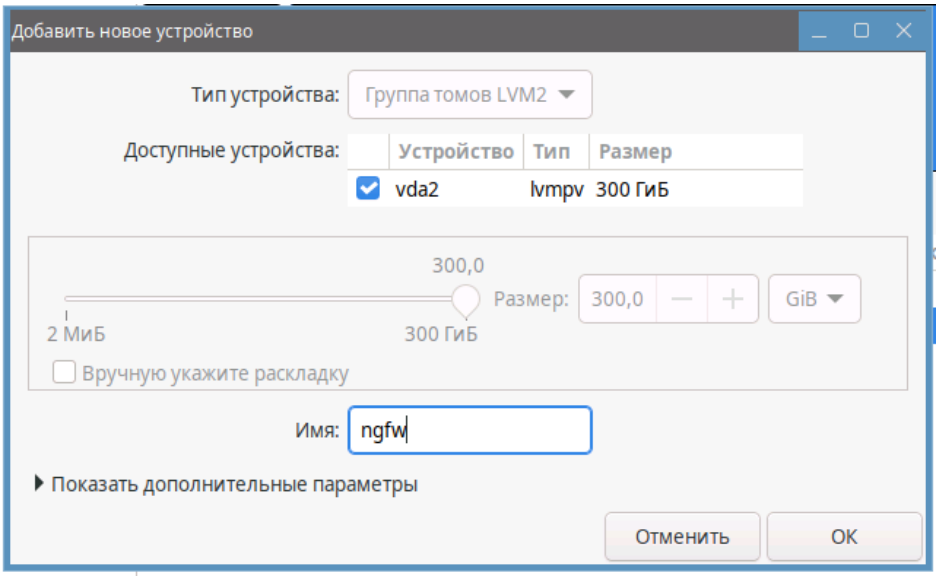


Рис. 4.11. Создание группы томов

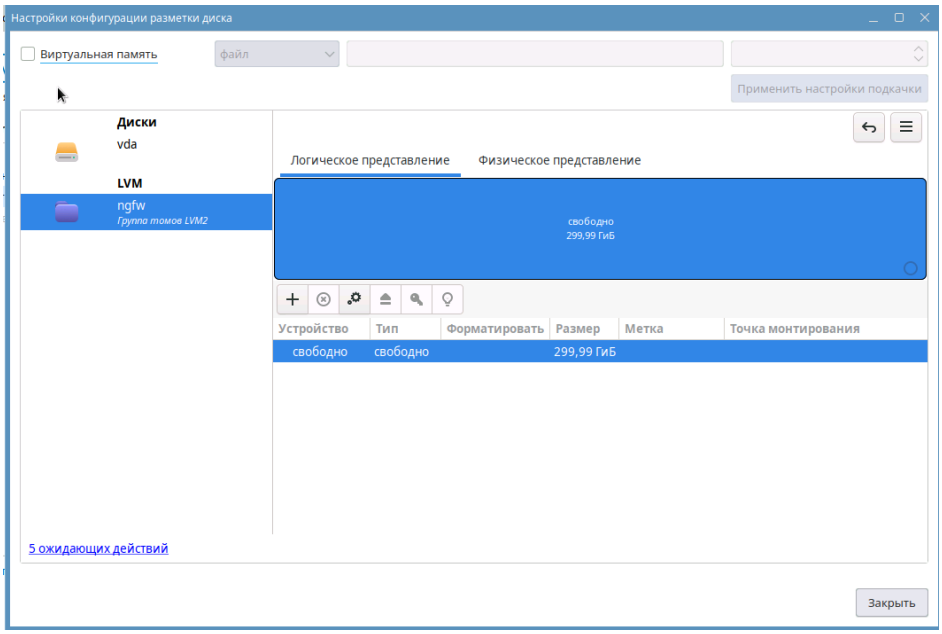


Рис. 4.12. Созданные диски vda, LVM и ngfw

12 Создайте логические тома **root**, **data**, **opt** и **var**:

- Для тома **root** выделите не менее 25 ГБ дискового пространства.

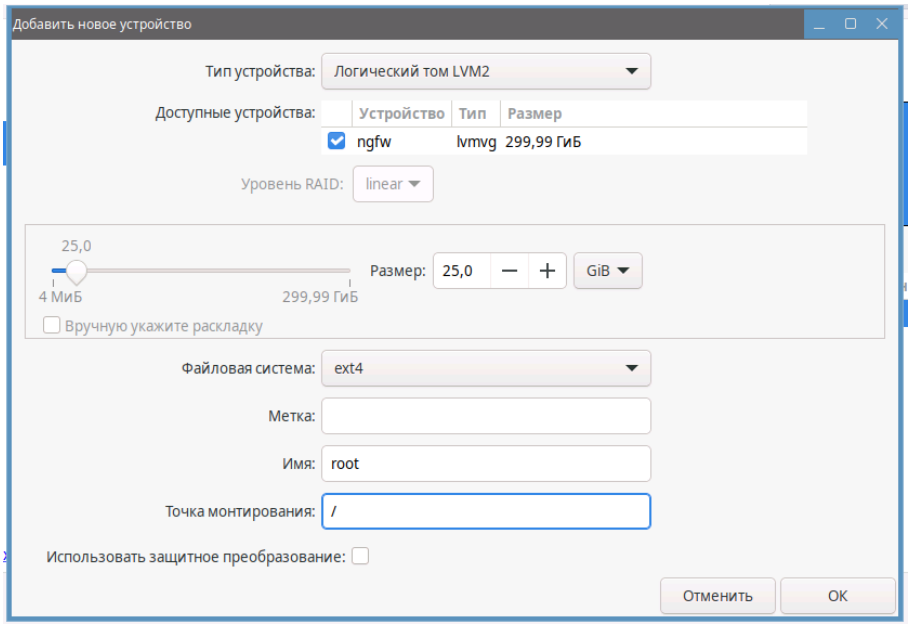


Рис. 4.13. Создание тома root

- Для тома **data** выделите не менее 100 ГБ дискового пространства.

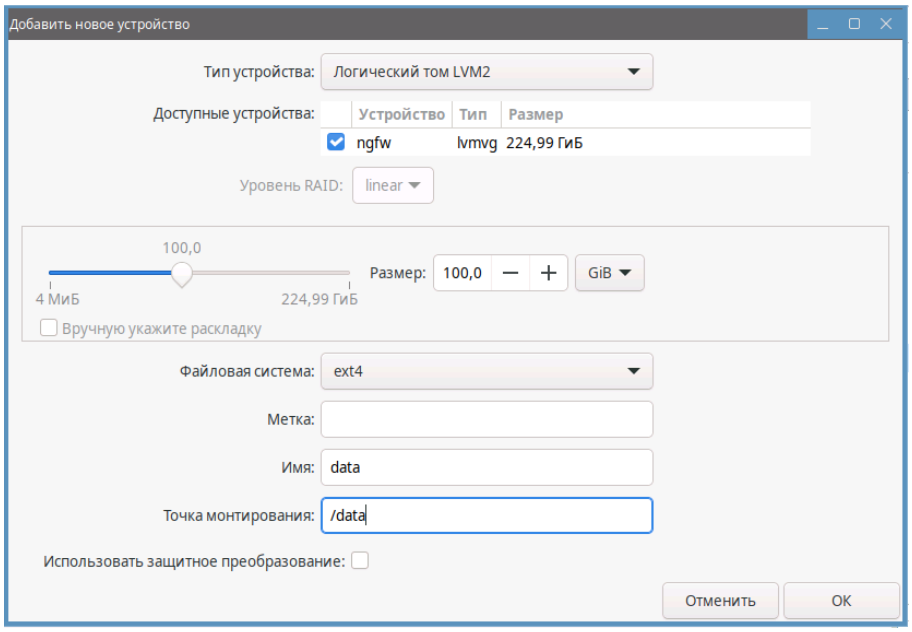


Рис. 4.14. Создание тома data

- Для тома **var** выделите не менее 50 ГБ дискового пространства.

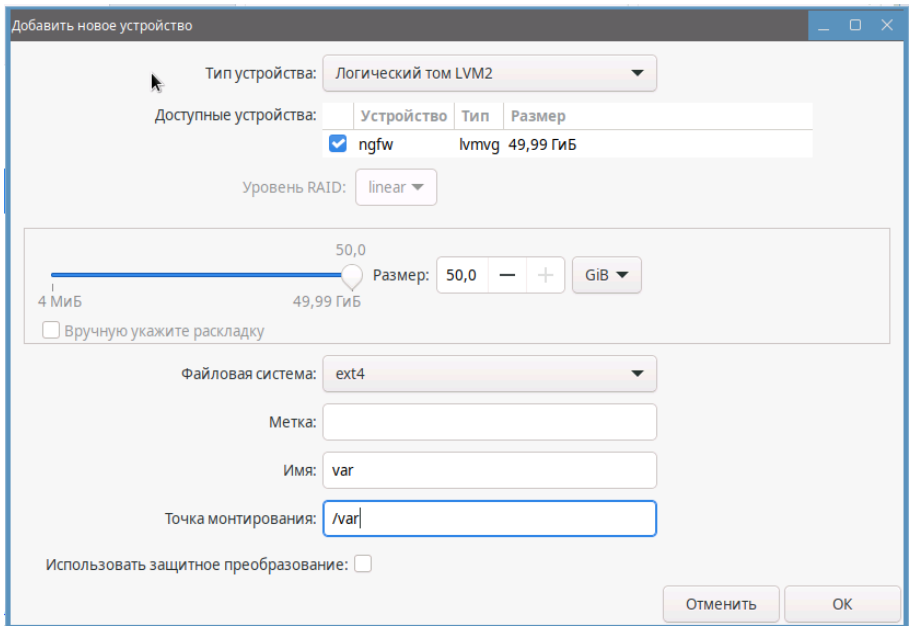


Рис. 4.15. Создание тома var

- Для тома **opt** выделите все оставшееся дисковое пространство.

Внимание!

*Крайне желательно, чтобы объем пространства, выделенного для тома **opt**, составлял не менее 40 ГБ. Этот том в процессе эксплуатации Solar NGFW активно наполняется*

данными, и исчерпание свободного места на нем приведет к аварийной остановке Solar NGFW.

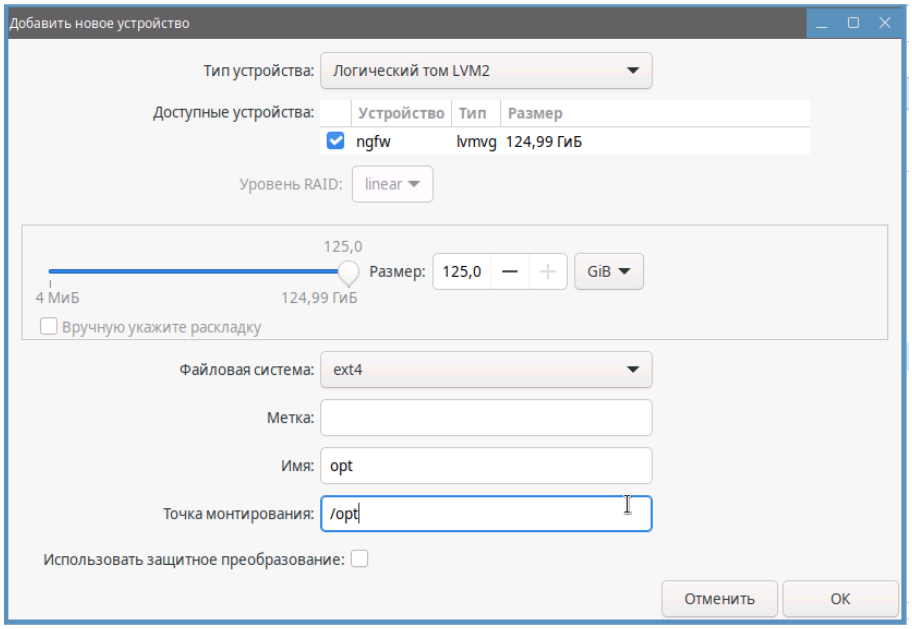


Рис. 4.16. Создание тома opt

13. В окне **Настройки конфигурации разметки диска** в правом верхнем углу нажмите ☰ и выберите **Записать изменения на диск**.

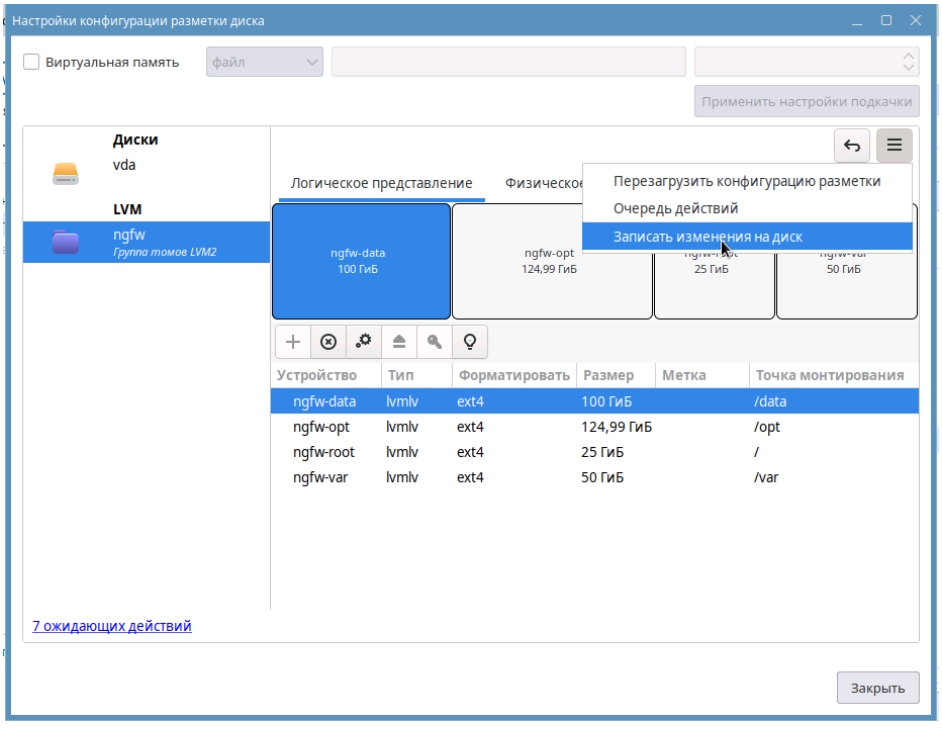


Рис. 4.17. Применение настроек конфигурации разметки диска

14. В открывшемся окне **Подтверждение плана действий** нажмите **ОК**.

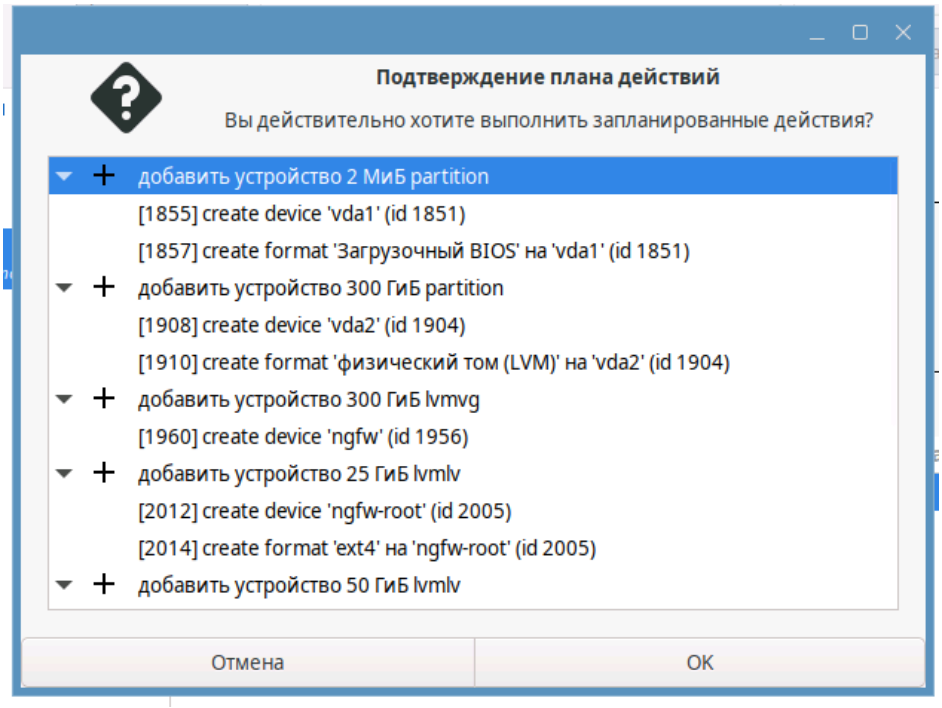


Рис. 4.18. Подтверждение применения настроек

15. Дождитесь обработки действий и нажмите **ОК**.

16. В главном меню установки Astra Linux перейдите на этап **4. Пользователи**. Укажите полное имя администратора, имя для входа в систему, имя компьютера, а также придумайте пароль. Нажмите **Далее**.

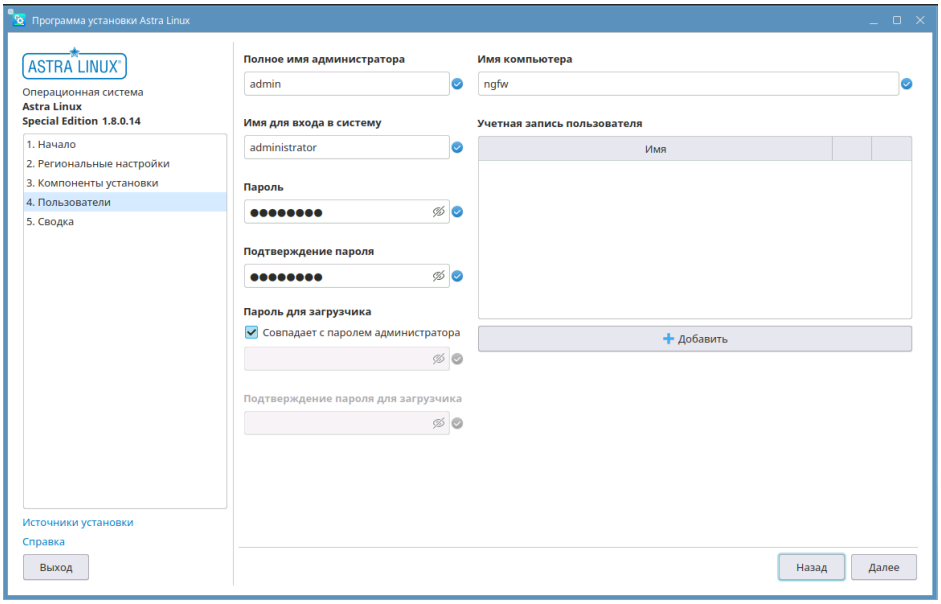


Рис. 4.19. Настройка пользователей

17. На этапе **5. Сводка** убедитесь, что вы указали все настройки правильно, и нажмите **Установить**.

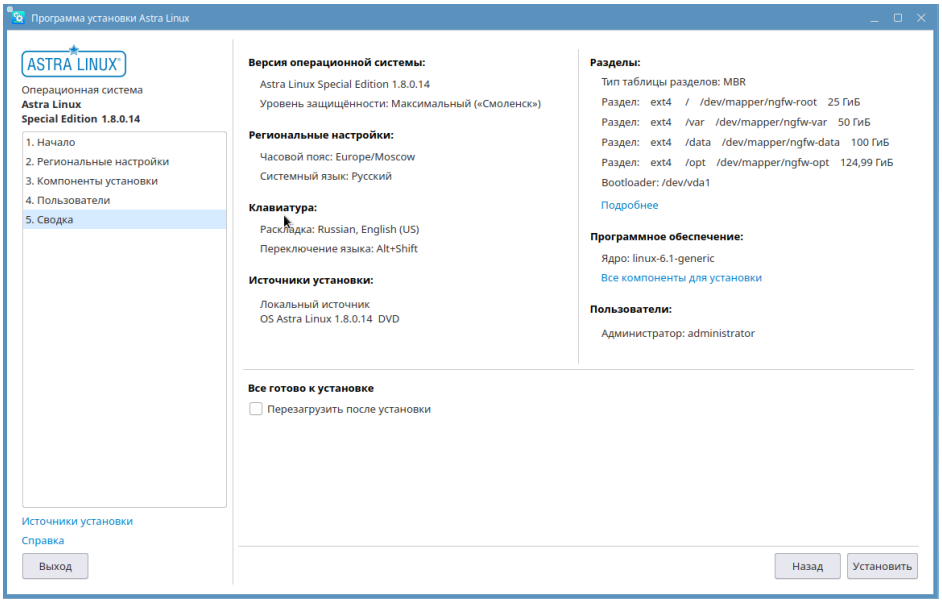


Рис. 4.20. Раздел Сводка

18. Дождитесь завершения установки и нажмите **Перезагрузить**.

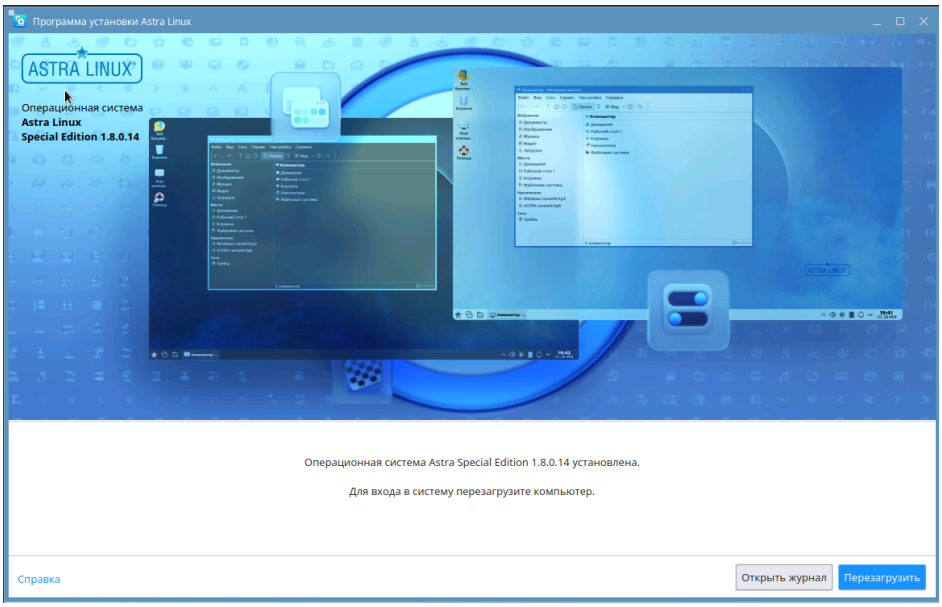


Рис. 4.21. Завершение установки

19. Перезагрузите систему и войдите под учетной записью администратора..

20. Запустите SSH-сервер, выполнив команды:

~$ sudo systemctl start ssh

~$ sudo systemctl enable ssh

Примечание

Здесь и далее команды CLI следует выполнять от имени суперпользователя, используя команду
sudo
.

21. Узнайте имя сетевого интерфейса, выполнив команду:

    ~$ ip a

    Вывод команды будет содержать пронумерованный список имен сетевых интерфейсов (включая локальную петлю под номером 1).

22. Настройте сетевые интерфейсы (см. раздел 4.1.1).

23. Перезапустите сетевую службу, выполнив команду:

    ~$ sudo systemctl restart networking

24. Выполните команды:

    ~$ sudo ufw disable

    ~$ sudo init 6

    ~$ sudo astra-mic-control disable

Примечание

Для корректной работы Журнала соединений выполните действия:

a. *Авторизуйтесь под учетной записью **root**, выполнив команду:*

   ~$ sudo su -

b. *Задайте пароль этой учетной записи, выполнив команду:*

   ~# passwd

c. *Разрешите авторизацию и вход под этой учетной записью, выполнив команду:*

   ~# echo "PermitRootLogin yes" >> /etc/ssh/sshd_config

d. *Перезапустите сервис ssh, выполнив команду:*

   ~# systemctl restart ssh

4.1.1. Настройка сетевых интерфейсов

Примечание

Рекомендуется определить перечень Ethernet-интерфейсов перед установкой Solar NGFW и не менять его в дальнейшем.

Перед установкой необходимо настроить управляющий сетевой интерфейс через службу networking. Остальными сетевыми интерфейсами можно управлять в разделе **Сеть > Сетевые интерфейсы**.

Чтобы настроить управляющий сетевой интерфейс:

1. Укажите IP-адрес и статический маршрут до сети управления администратора в конфигурационном файле **/etc/network/interfaces**, добавив строки:

   # iface <название интерфейса управления> inet static

   # address <IP-адрес с префиксом маски>

   # up /bin/ip route add <подсеть управления> via <адрес шлюза>

   Пример записи:

   ```
   root@fw1:/opt/dozor# cat /etc/network/interfaces
   source /etc/network/interfaces.d/*
   # The loopback network interface
   auto lo
   iface lo inet loopback

   # The primary network interface
   auto ens18
   allow-hotplug ens18
   iface ens18 inet static
     address 192.168.0.250/24
     up /bin/ip route add 10.255.0.0/24 via 192.168.0.1
   root@fw1:/opt/dozor#
   ```

2. Перезапустите сервис networking с помощью команды:

   # systemctl restart networking

Добавить новый VLAN-интерфейс можно в GUI в разделе **Сеть > Сетевые интерфейсы** с помощью кнопки **Добавить интерфейс**.

Примечание

*VLAN-интерфейс можно создать только на активном узле кластера. Проверить статус узла можно в разделе **Сеть > Кластеризация** в поле **Текущий статус**.*

В качестве VLAN-интерфейса не может использоваться интерфейс, который при создании кластера был выбран в качестве интерфейса синхронизации.

*При создании VLAN-интерфейса необходимо указывать его IP-адрес с помощью кнопки **Добавить IP-адрес**.*

4.1.1.1. Объединение сетевых интерфейсов в группы

Для повышения производительности и отказоустойчивости сетевых интерфейсов в Solar NGFW можно объединять физические сетевые интерфейсы в группы (bonding). Технология позволяет объединить несколько интерфейсов Ethernet в единый виртуальный интерфейс, тем самым повышая скорость передачи данных и обеспечивая отказоустойчивость.

Примечание

При выходе из строя одного из интерфейсов трафик продолжает проходить через остальные рабочие интерфейсы.

Чтобы объединить сетевые интерфейсы в группу:

1. Отключите Solar NGFW с помощью команды:

   # dsctl down

2. Добавьте в файл **/etc/network/interfaces** строки с настройками для bond-интерфейса, например:

```
auto eth1 eth2 bond0
iface eth2 inet manual
iface eth3 inet manual

iface bond0 inet manual
bond-mode 802.3ad
bond-miimon 100
bond-downdelay 200
bond-updelay 200
bond-xmit-hash-policy 1
bond-slaves eth2 eth3
```

   Примечание

   Не рекомендуется использовать в одной группе несколько интерфейсов разного типа и разной скорости.

   На одном узле может быть не более двух bond-интерфейсов.

В группу могут быть объединены от 2 до 8 интерфейсов. Рекомендуется использовать количество интерфейсов кратное 2 (2,4,6,8).

Работоспособность интерфейсов не гарантирована на разных версиях сетевых плат и модулей.

3. Добавьте физические интерфейсы, состоящие в группе, в список игнорируемых Solar NGFW в файл **/opt/dozor/etc/ignoredInterfaces.txt**.

Примечание

Если файл отсутствует, создайте его.

Каждое имя интерфейса должно быть с новой строки.

Подчиненные интерфейсы в группе должны быть исключены из управления сервисом network-agent во избежание перезаписывания настроек. При исключении интерфейсов из группы их управление должно быть возвращено к network-agent.

4. Перезагрузите устройство с помощью команды:

```
# shutdown -r now
```

Управлять группами сетевых интерфейсов можно в разделе **Сеть > Сетевые интерфейсы**.

4.2. Рекомендации к установке Solar NGFW

Приведенные в этом разделе процедуры предварительной настройки должны быть выполнены на всех серверах Solar NGFW.

До завершения установки Solar NGFW следует строго придерживаться описанных ниже процедур и не устанавливать какие-либо пакеты или обновления системы. Дистрибутив Solar NGFW содержит все необходимые для работы пакеты, и в случае его установки на ОС с дополнительно установленными пакетами и/или обновлениями не гарантируется корректная работа Solar NGFW.

4.2.1. Настройка DNS

Внимание!

Необходимо настроить FQDN на master-узле до установки Solar NGFW.

Проверьте содержимое следующих файлов настройки DNS на всех узлах Solar NGFW:

- **/etc/hostname**
- **/etc/hosts**

Файл **/etc/hostname** должен содержать единственную строку, представляющую собой краткое доменное имя сервера.

Файл **/etc/hosts** должен содержать строки для всех узлов ПК Solar NGFW, каждая из которых состоит из IP-адреса узла, FQDN (состоящего из краткого доменного имени и доменного суффикса) и краткого (домен нижнего уровня) доменного имени, например:

```
10.199.21.148 ngfw-master.company.local ngfw-master
10.199.21.149 filter1.company.local filter1
10.199.21.147 filter2.company.local filter2
```

Примечание

*При наличии адреса 127.0.1.1 в файле **/etc/hosts** необходимо его скрыть или удалить, а FQDN явно прописывать для IP-адреса, с которого происходит вход в Solar NGFW.*

IP-адрес и записи доменного имени должны быть разделены символом табуляции.

Внимание!

*Полное доменное имя (FQDN) и краткое доменное имя (hostname) могут состоять только из прописных латинских букв, цифр или служебного символа **-**. Для разделения уровней доменных зон в FQDN используйте точку. Краткое доменное имя должно начинаться только с прописной латинской буквы и не должно содержать в себе точки. При подключении Solar NGFW к NTLM-домену Windows краткое доменное имя (hostname) не должно превышать 15 символов. Пример правильного написания FQDN: **ngfw-01.example.org**, где краткое доменное имя будет **ngfw-01**.*

4.2.2. Настройка синхронизации времени

Для корректной работы Solar NGFW необходима синхронизация времени. В отсутствие контроллера домена или другого источника точного времени возникнут проблемы из-за разного времени в журналах и метках времени на данных, а также возможны проблемы с работой протокола HTTPS. Для синхронизации времени могут быть использованы один или несколько серверов точного времени, находящихся как в корпоративной сети, так и в сети Интернет.

Для настройки синхронизации времени на всех узлах Solar NGFW выполните следующие действия:

1. Найдите нужную временную зону, выполнив следующую команду:

   # timedatectl list-timezones

   Для удобства поиска можно воспользоваться сортировкой, например:

   # timedatectl list-timezones | grep Europe

2. Установите нужную временную зону, выполнив команду следующего вида:

   # timedatectl set-timezone <timezone>

где **<timezone>** – значение, найденное в предыдущем шаге.

3. Убедитесь в правильности настройки временной зоны, выполнив следующую команду:

   # timedatectl

4. Установите пакет **ntp**, выполнив команду:

   # sudo apt-get install ntp

5. Откройте для редактирования файл **/etc/ntpsec/ntp.conf** и добавьте в него одну или несколько строк следующего вида:

   ```
   server <timeserver> iburst
   ```

   где **<timeserver>** – FQDN или IP-адрес NTP-сервера (внешнего или принадлежащего организации). Параметр **iburst** является необязательным и служит для повышения точности синхронизации за счет увеличенного количества пакетов, отправляемых при обмене данными с NTP-сервером.

   Наличие нескольких записей позволяет продолжать синхронизацию в случае отказа какого-либо из NTP-серверов. Серверы опрашиваются по очереди, в порядке их перечисления в файле **ntp.conf**.

6. Запустите службу NTP и добавьте ее в автозагрузку, выполнив команды:

   # systemctl start ntp

   # systemctl enable ntp

Узнать список работающих используемых серверов точного времени можно выполнив следующую команду:

 # ntpq -p

4.2.3. Проверка и настройка БД Clickhouse (инструкции sse4_2)

Solar NGFW использует БД Clickhouse. Для корректного функционирования этой БД необходимо, чтобы процессор поддерживал набор инструкций **sse4_2**. Проверить наличие этой поддержки можно с помощью команды:

 # grep sse4_2 /proc/cpuinfo

Вывод команды не должен быть пустым.

4.2.4. Настройка функционирования под управлением systemd

По умолчанию подсистема инициализации **systemd** принудительно завершает процессы пользователя **dozor**, от имени которого впоследствии должна быть создана БД архива, а также будут выполняться некоторые другие действия. Для исправления этой ситуации выполните следующие действия:

1. Откройте для редактирования файл **/etc/systemd/logind.conf**.

2. Найдите следующие строки:

```
#KillExcludeUsers=root
#RemoveIPC=yes
```

3. Замените найденные строки на следующие:

```
KillExcludeUsers=root dozor
RemoveIPC=no
```

4. Сохраните и закройте файл.

5. Перезапустите ОС, выполнив команду:

   ~$ sudo init 6

4.3. Установка Solar NGFW

Примечание

Перед установкой Solar NGFW на виртуальных машинах определите необходимое количество физических интерфейсов. Добавлять интерфейсы в систему можно без последствий для функциональности, однако их удаление может привести к критическим последствиям, таким как некорректные настройки интерфейсов.

Для отключения отправки пакетов ICMP redirect (ICMP type 5) на узле:

1. *В CLI в файле **etc/sysctl.conf** добавьте параметры:*

   net.ipv4.conf.all.accept_redirects = 0

   net.ipv4.conf.all.send_redirects = 0

   net.ipv4.conf.default.accept_redirects = 0

   net.ipv4.conf.default.send_redirects = 0

   net.ipv6.conf.all.disable_ipv6 = 1

2. *Перезагрузите устройство.*

Для установки Solar NGFW:

1. Получите доступ к установочному файлу, выполнив команду:

   # chmod +x /var/tmp/solar-ngfw-1.4.1-86.astra1.8-1.8.0.14-signed.run

   где **/var/tmp/solar-ngfw-1.4.1-86.astra1.8-1.8.0.14-signed.run** – путь к инсталлятору.

2. На master-узле в CLI выполните команду:

   # /var/tmp/solar-ngfw-1.4.1-86.astra1.8-1.8.0.14-signed.run --install

4.4. Обновление Solar NGFW

Примечание

*Если сетевые интерфейсы в Solar NGFW называются **eth***, импорт политики МЭ на новую версию необходимо выполнять через техническую поддержку. Проверить наименование интерфейсов можно в разделе **Сеть > Сетевые интерфейсы**.*

*При обновлении данные из разделов **Досье**, **Пользователи** и **Сеть** могут быть утеряны. Во избежание утери данных зафиксируйте их любым удобным для себя способом.*

Для обновления Solar NGFW:

1. Убедитесь, что все последние настройки были применены (в разделе **Политика** необходимо нажать кнопку **Применить политику**).
2. Экспортируйте политики. Для этого перейдите в раздел **Политика** и нажмите кнопку **Экспорт** – файл с политиками будет сохранен на локальном ПК.
3. Экспортируйте сигнатуры. Для этого перейдите в раздел **Политика > Предотвращение вторжений > Наборы сигнатур** и нажмите кнопку **Экспорт сигнатур** – файл с сигнатурами будет сохранен на локальном ПК.
4. Экспортируйте настройки из раздела **Система**. Для этого:
   a. В CLI выполните команды:

      # /opt/dozor/bin/shell

      # export-config '<имя файла>.json'

      где **<имя файла>** – название файла с датой экспорта.

      Файл сохранится в директорию **/opt/dozor/**.

   b. Сохраните файл на локальном устройстве.
5. Переустановите ОС Astra Linux Special Edition версии 1.8.0 «Смоленск» (инструкция по установке ОС Astra Linux описана в разделе 4.1).
6. На master-узле в CLI выполните команды:

   # /opt/dozor/bin/shell

   # dsctl down

   # chmod +x /var/tmp/solar-ngfw-1.4.1-86.astra1.8-1.8.0.14-signed.run

   # /var/tmp/solar-ngfw-1.4.1-86.astra1.8-1.8.0.14-signed.run - -install

   где **/var/tmp/solar-ngfw-1.4.1-86.astra1.8-1.8.0.14-signed.run** – путь к инсталлятору.
7. Запустите master-узел, выполнив команду:

 # dsctl boot

8. В GUI загрузите лицензию.
9. В любом слое раздела **Политика** нажмите **Применить политику**.
10. Загрузите сохраненный файл с настройками из раздела **Система**. Для этого в CLI выполните команды:

    # /opt/dozor/bin/shell

    # import-config '<имя файла>.json'

    где **<имя файла>** – название файла с датой экспорта.
11. Импортируйте политики. Для этого:
    a. Перейдите в раздел **Политика**.
    b. Нажмите кнопку **Импорт**.
    c. Загрузите файл, сохраненный на шаге 2.
    d. Нажмите кнопку **Применить политику**.
12. Импортируйте сигнатуры. Для этого:
    a. Перейдите в раздел **Политика > Предотвращение вторжений > Наборы сигнатур**.
    b. Нажмите кнопку **Импорт сигнатур**.
    c. Загрузите файл, сохраненный на шаге 3.
    d. Нажмите кнопку **Применить политику**.
13. После обновления master-узла выполните обновление всех slave-узлов кластера. Для этого повторите выполнение шагов 6-9 на каждом slave-узле.
14. На всех узлах выполните команду:

    # reboot

4.5. Удаление Solar NGFW

Для удаления Solar NGFW:

1. Остановите процессы Solar NGFW, выполнив команду:

    # /opt/dozor/bin/dsctl down
2. Удалите Solar NGFW, выполнив команду:

    # apt purge -y solar-*

    # apt -y autoremove
3. Удалите каталоги установки Solar NGFW, выполнив команды:

 # rm -rf /opt/dozor /opt/iadmin /data

4. Если не предполагается использовать в дальнейшем пользователя **dozor**, удалите:

   - пользователя **dozor** из системы, выполнив команду:

     # userdel dozor

   - из файла **/etc/sudoers** запись:

     ```
     dozor ALL=(ALL) NOPASSWD: ALL
     ```

5. Удалите почтовый ящик пользователя **dozor**, выполнив команду:

   # rm /var/mail/dozor

6. При необходимости удалите из **/etc/krb5.conf** и **/etc/krb5.conf.save** записи вида:

   ```
   default = FILE:/opt/dozor/var/log/krb5libs.log
   kdc = FILE:/opt/dozor/var/log/krb5kdc.log
   admin_server = FILE:/opt/dozor/var/log/kadmind.log
   ```

5. Первоначальная настройка Solar NGFW

5.1. Первый запуск Solar NGFW

После установки пакетов Solar NGFW на всех узлах выберите сервер, который планируется использовать как master-узел, подключитесь к нему по SSH и назначьте ему управляющую роль, выполнив следующие команды:

 # /opt/dozor/bin/shell

 # set-role master main

 # dsctl boot

5.2. Первый вход в систему и загрузка лицензии

После первого запуска Solar NGFW смените пароль по умолчанию для доступа к GUI:

1. Откройте браузер и перейдите по адресу **https://<master-host>:8443** либо **https://<master-ip>:8443**, где:
   - **<master-host>** – полное доменное имя master-узла. Например, **proxymaster.company.local**;
   - а **<master-ip>** – IP-адрес master-узла. Например, 10.199.21.148.
2. В открывшемся окне авторизации введите имя пользователя и пароль по умолчанию: **admin/admin**. После этого система потребует изменить пароль.
3. Установите новый пароль требуемого уровня надежности (см. раздел 3.2.6) и авторизуйтесь с ним.

   После первоначальной смены пароля в верхней части экрана появится уведомление об отсутствии лицензии.

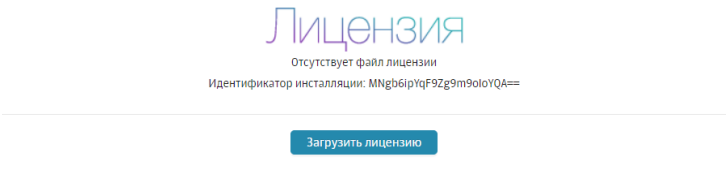


Рис. 5.1. Уведомление об отсутствии лицензии

Для загрузки лицензии:

1. В меню пользователя нажмите кнопку **Лицензия** и в окне **Лицензия** нажмите **Загрузить лицензию**.
2. В открывшемся окне укажите путь к файлу с лицензией, после чего нажмите кнопку **Открыть** (**Open**) и дождитесь загрузки лицензии. Она автоматически сохранится в файле с именем **license.xml**.

Для просмотра сведений о лицензии Solar NGFW выберите пункт меню пользователя **Лицензия**.

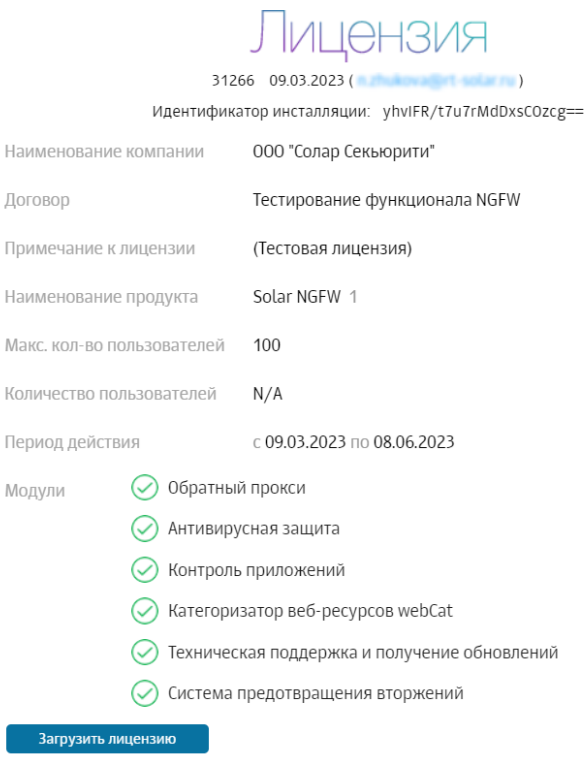


Рис. 5.2. Окно с информацией о лицензии

Постоянная лицензия Solar NGFW всегда жестко привязана к конкретной аппаратной платформе (виртуальной или физической) master-узла в Solar NGFW.

Для однозначной привязки используется идентификатор инсталляции, представляющий собой особым образом формируемый хэш, зависящий от некоторых уникальных характеристик аппаратного обеспечения master-узла. Идентификатор инсталляции формируется при первом запуске GUI Solar NGFW и передается инженерами внедрения в вендорскую службу поддержки, которая на его основе выпускает активированную лицензию для постоянного использования.

Примечание

Идентификатор инсталляции не зависит от характеристик оперативной памяти и жестких дисков. Их замена не приводит к прекращению действия лицензии.

Однако изменение хотя бы одной из характеристик master-узла, от которых зависит идентификатор инсталляции, приводит к недействительности выпущенной лицензии и неработоспособности Solar NGFW.

При функционировании master-узла в виртуальной среде миграция виртуальной машины приводит к тем же последствиям. В этих случаях необходимо обратиться в вендорскую службу поддержки для повторного выпуска лицензии.

5.3. Управление настройками системы

Управлять конфигурацией и настройками системы в интерфейсе можно в следующих разделах системы:

- **Досье** и **Политика** на вкладке **Настройки**. Это значительно упрощает настройку системы и позволяет быстро вносить изменения в конфигурацию, не покидая раздела;
- **Система > Настройки**.

Для доступа к более широкому перечню настроек перейдите в раздел **Система > Настройки > Основные настройки > Досье** (см. Рис.5.3).

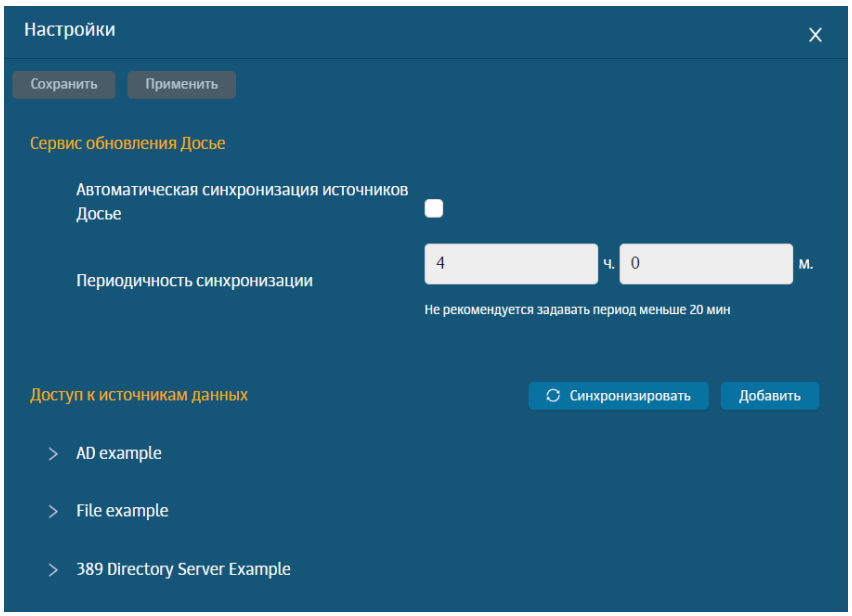


Рис. 5.3. Вкладка «Настройки» раздела «Досье»

Вкладка **Настройки** раздела **Политика** содержит те же параметры, что и раздел **Система > Настройки > Основные настройки > Работа системы** (см. Рис.5.4).

Рис. 5.4. Вкладка «Настройки» раздела «Политика»

В разделе **Система** на вкладке **Настройки** все параметры настройки сгруппированы по их назначению:

- для основных настроек системы — вкладка **Основные настройки** (см. Рис.5.5);
- для использования расширенного набора настроек — вкладка **Расширенные настройки** (см. Рис.5.6).

Табл. 5.1. Группы основных настроек

Группа	Назначение
Аутентификация	Настройки аутентификации из внешних источников для фильтрации и веб-сервера: Kerberos, NTLM, LDAP и RADIUS аутентификация
Досье	Настройки взаимодействия с внешними системами, например, Active Directory. Содержит настройки обновления Досье и доступа к источникам данных для импорта данных пользователей из Active Directory.
Журналирование	Настройка журналирования сервисов системы
Мониторинг	Определение перечня проверок и уведомлений от системы мониторинга
Отказоустойчивость	Настройки отказоустойчивости и балансировки: сервис балансировки трафика HaProxy и Сервис виртуального IP (Virtual Router Redundancy Protocol – VRRP)
Производительность	Настройки производительности системы и потребления ресурсов
Работа системы	Общая настройка работы системы: параметры фильтрации и анализа трафика системы, доступ администратора и лицензия антивируса

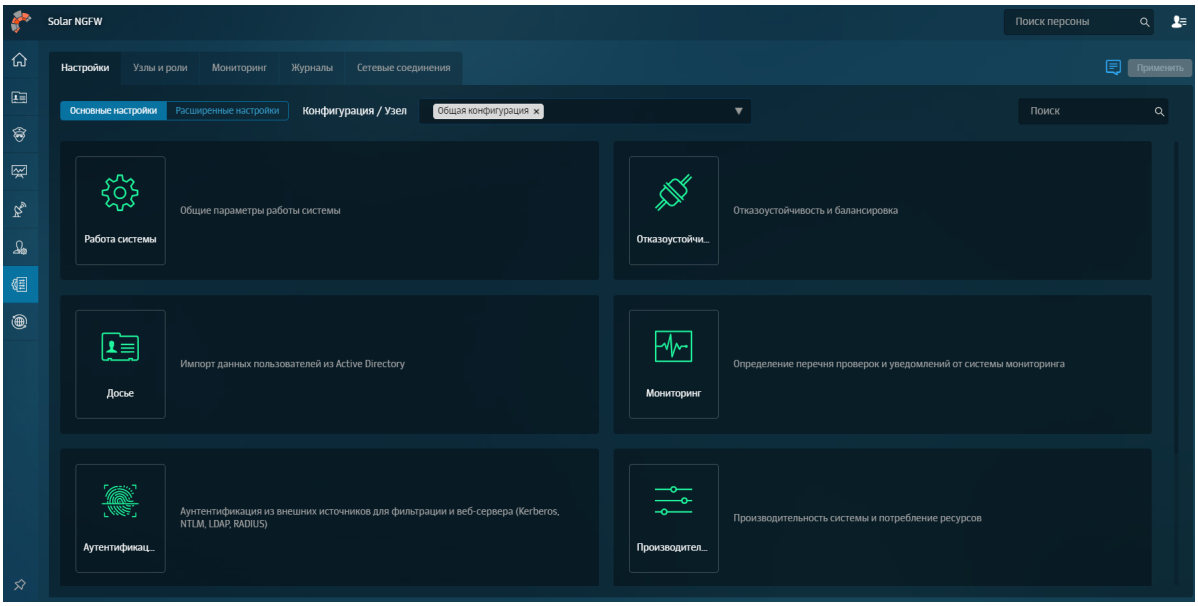


Рис. 5.5. Раздел Конфигурации: основные настройки

Для корректной работы системы в большинстве случаев *достаточно задать основные настройки*, тем более, что по умолчанию в Solar NGFW для всех параметров системы установлены рекомендуемые разработчиками значения.

Для *более детальной настройки системы* предусмотрены расширенные наборы параметров, сгруппированные по функциональным блокам системы. Следует учесть, что в основных и расширенных настройках параметры сгруппированы в разделы в зависимости от их назначения. Каждый раздел содержит секции, представляющие собой отдельные конфигурационные файлы.

Кроме того, из раздела с основными настройками можно быстро перейти по ссылке к расширенному списку параметров настройки.

Для более оперативной работы с конфигурацией предусмотрен поиск по названиям конфигурационных файлов, именам параметров и их значениям. Чтобы воспользоваться поиском, следует ввести название искомого элемента или его часть в поле **Поиск**, расположенном в правой верхней части экрана (Рис.5.7). Чтобы перейти в раздел с искомым элементом, нажмите на его имя (выделено синим).

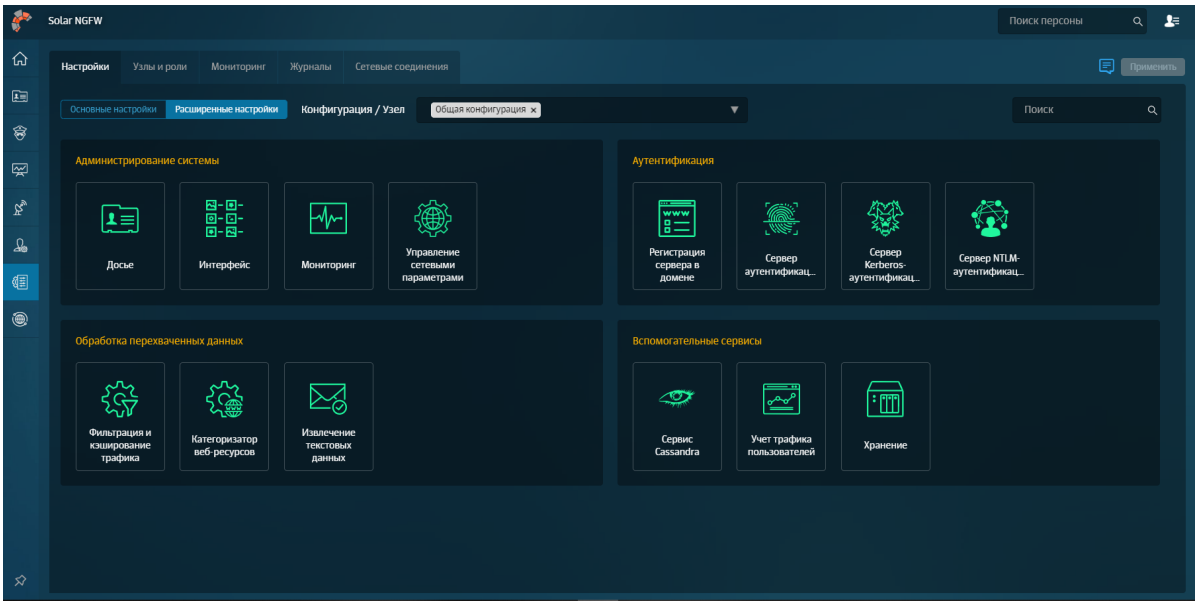


Рис. 5.6. Раздел Конфигурации: расширенные настройки

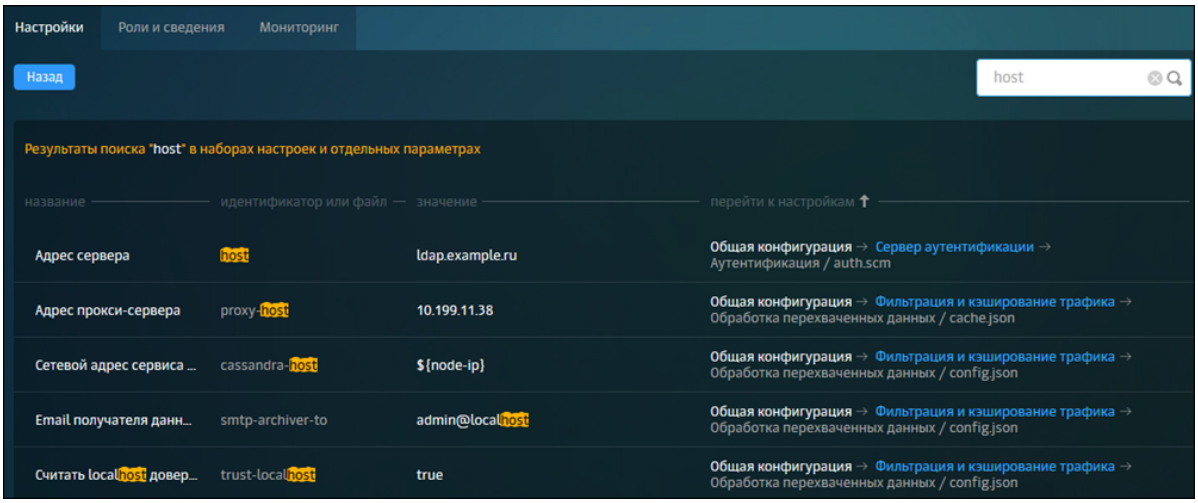


Рис. 5.7. Поиск по конфигурации

После внесения изменений в значения параметров конфигурации сохраните их или отмените с помощью соответствующих кнопок:

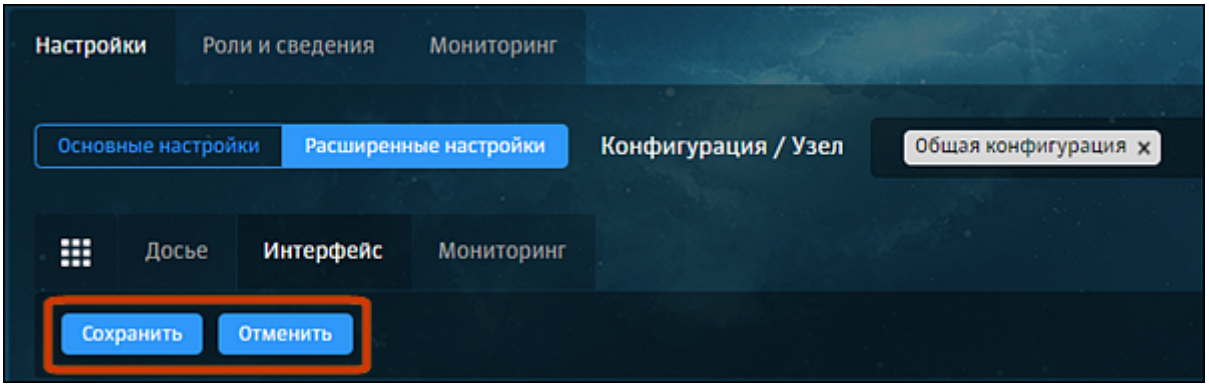


Рис. 5.8. Кнопки «Сохранить» и «Отменить»

Для применения настроек конфигурации нажмите кнопку **Применить**. Рядом с этой кнопкой расположена информационная иконка, при наведении курсора на которую появляются сведения о времени предыдущего применения настроек:

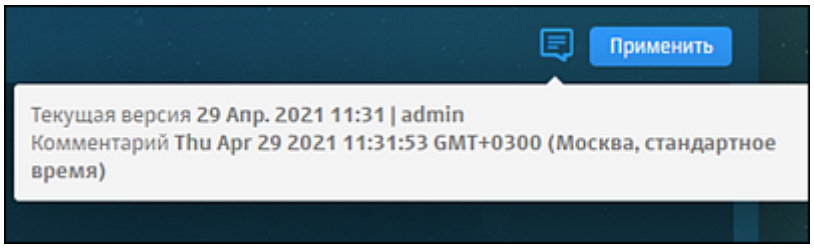


Рис. 5.9. Кнопка «Применить»

Для описания того или иного параметра можно отобразить подсказки к параметрам настройки конфигурации. Для отображения описания конкретного параметра наведите курсор мыши на его название.

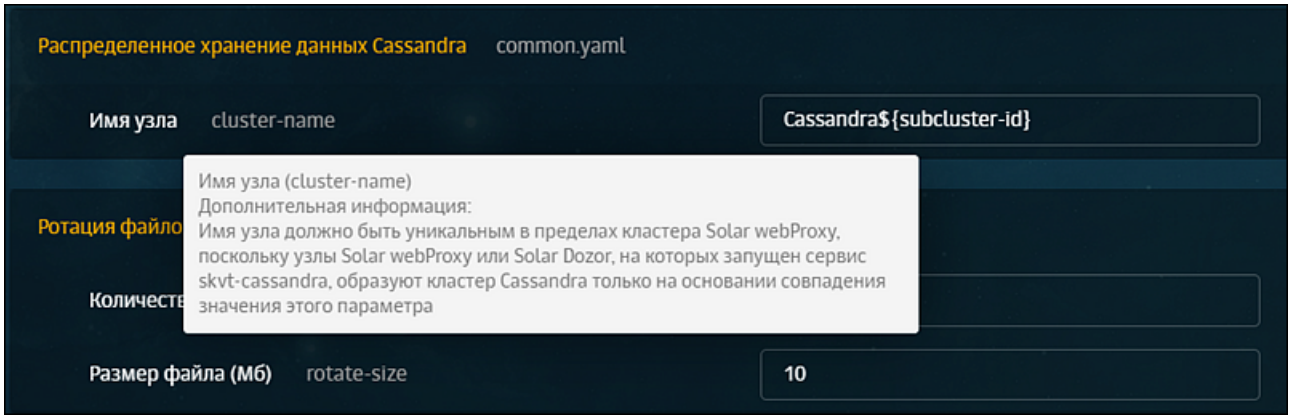


Рис. 5.10. Подсказка с описанием параметра

Для отображения всех подсказок включите **Показывать описание** в верхней части раздела.

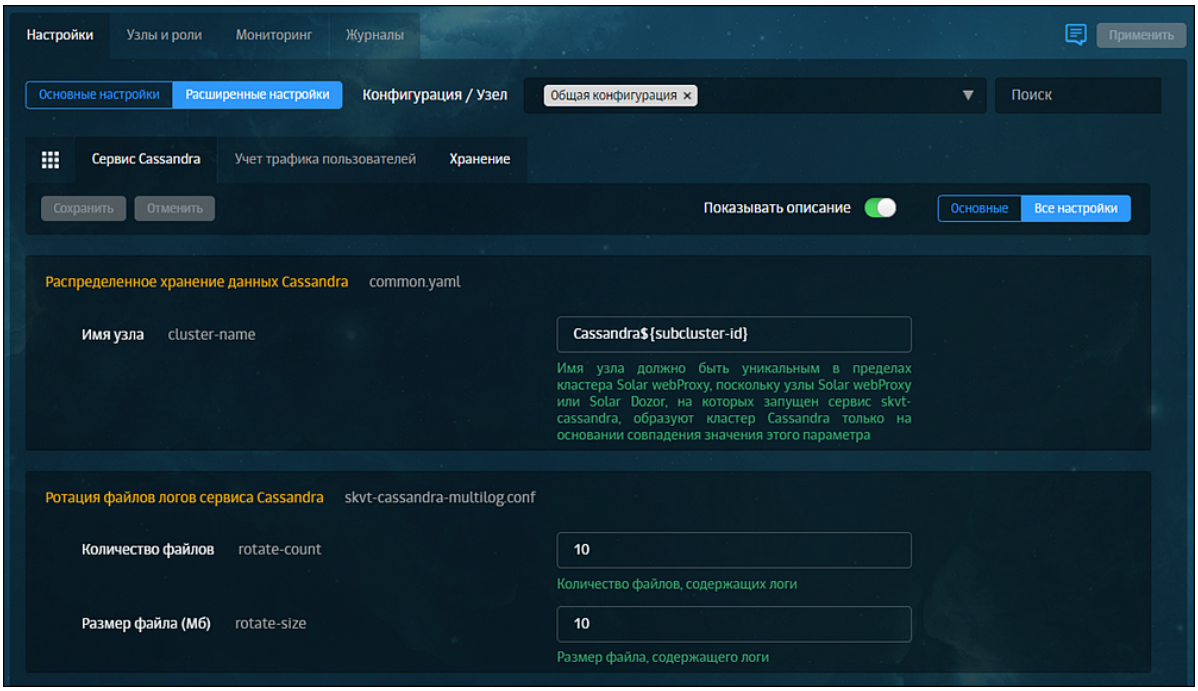


Рис. 5.11. Отображение подсказок

Чтобы задать индивидуальные параметры конфигурации для какого-либо узла, выберите этот узел в списке **Конфигурация/Узел** (Рис.5.12).

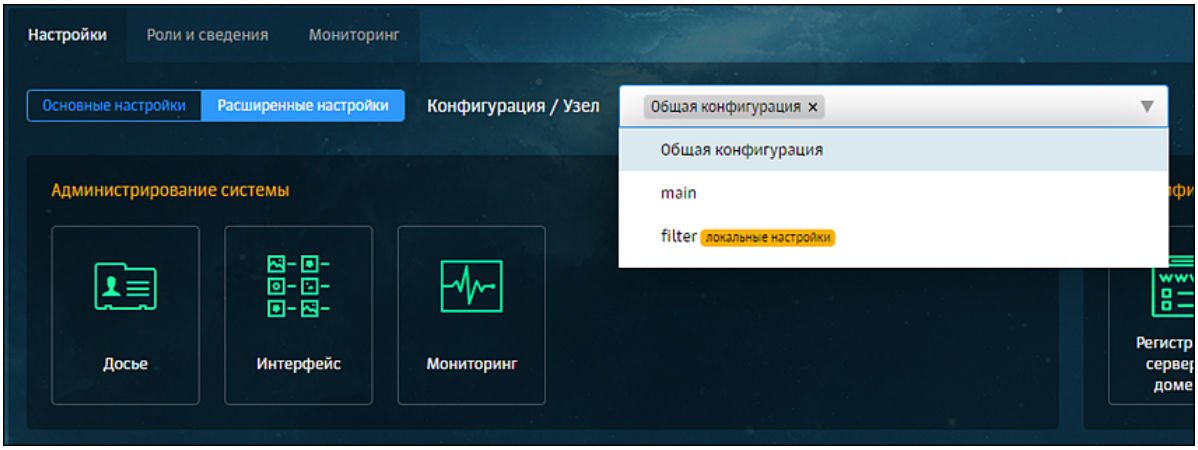


Рис. 5.12. Выбор узла

Если какой-либо узел имеет индивидуальные настройки (хотя бы один параметр), то в списке **Конфигурация/Узел** рядом с названием этого узла будет расположена метка **локальные настройки**. Такая же метка будет расположена в записи об узле на вкладке **Узлы и роли**, а также на иконках тех разделов настроек, которые имеют индивидуальные настройки, при выборе этого узла в списке **Конфигурация/Узел**.

Примечание

*Информация о состоянии системы на вкладке **Узлы и роли** автоматически обновляется каждый раз при открытии вкладки.*

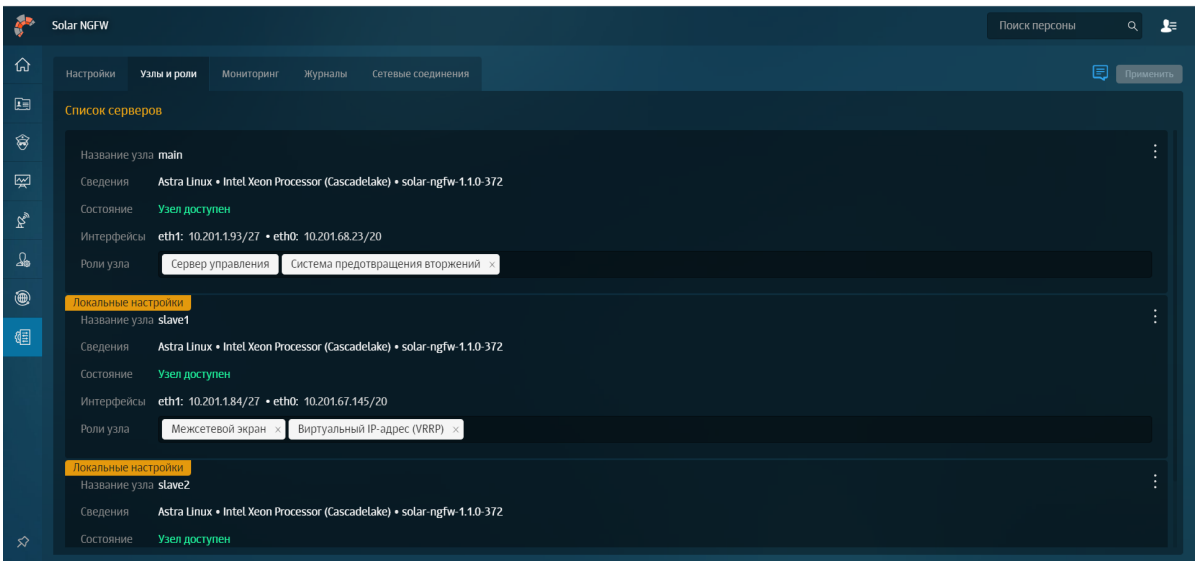


Рис. 5.13. Индикаторы индивидуальных настроек в списке узлов

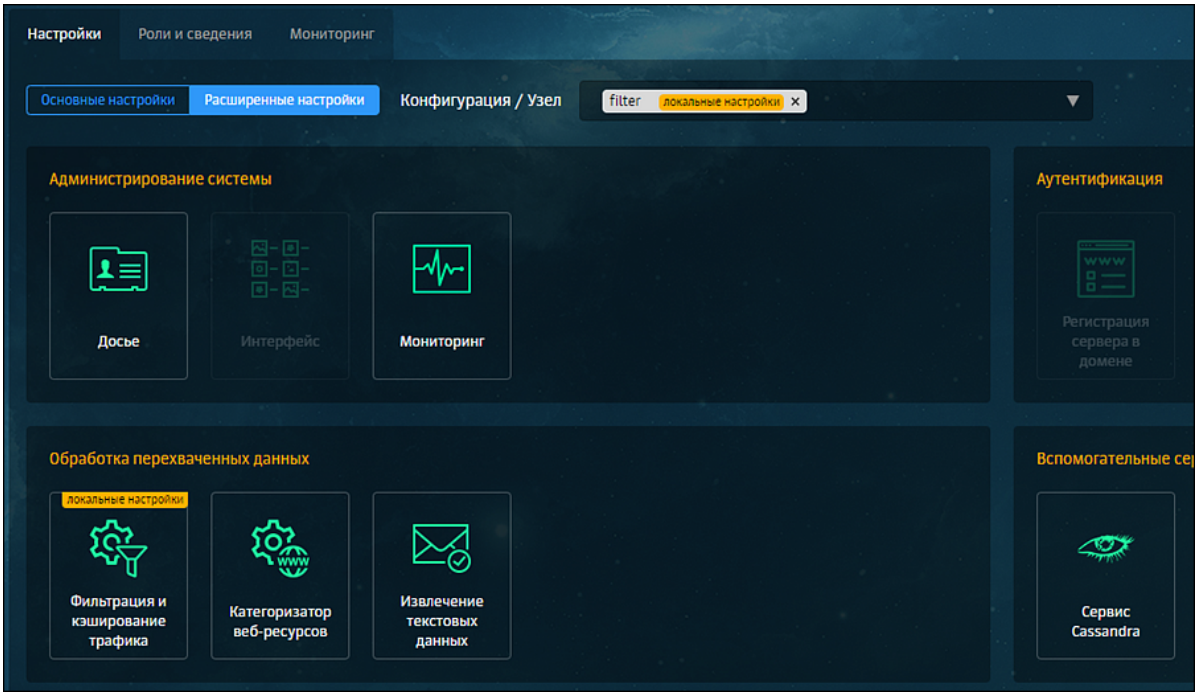


Рис. 5.14. Индикаторы локальных настроек для выбранного узла

Чтобы локальные настройки конфигурации узла вступили в силу, включите **Использовать локальные настройки** справа от названия секции параметров (Рис.5.15). Каждая секция имеет свою опцию.

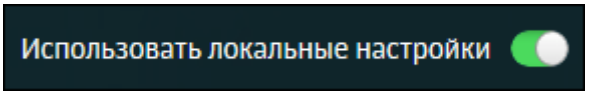


Рис. 5.15. Использовать локальные настройки

5.4. Назначение ролей

5.4.1. Назначение ролей

После загрузки лицензии и входа в систему можно назначать роли узлам с помощью GUI.

Для назначения ролей узлам используйте вкладку **Система > Узлы и роли**, содержащую информацию о состоянии и ролях всех узлов в Solar NGFW.

Для назначения роли узлу в разделе **Система > Узлы и роли** в секции с нужным узлом нажмите поле **Роли узла** и выберите в раскрывающемся списке одну или несколько ролей для него, а затем нажмите любую область за пределами списка. Назначенные узлу роли в списке выделены голубым цветом.

Чтобы снять с узла роль, нажмите:

- значок с названием этой роли;
- выбранную роль в списке.

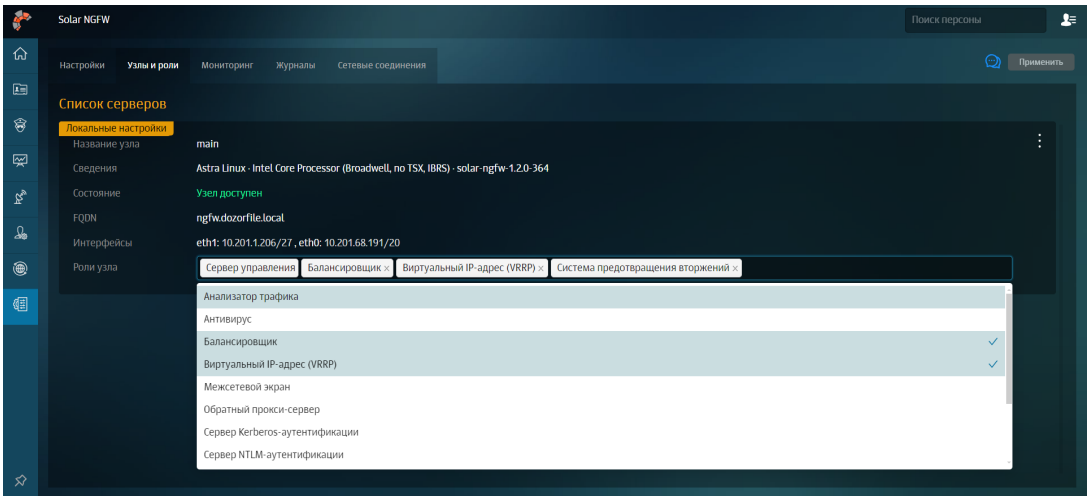


Рис. 5.16. Назначение и снятие ролей узла

Примечание

*После удаления роли **Виртуальный IP-адрес (VRRP)** со всех узлов необходимо:*

1. *В CLI выполнить команду:*

   # killall -9 keepalived

2. *Перезагрузить узел, например, с помощью команды:*

   # shutdown -r now

После установки ролей для всех узлов нажмите **Сохранить** и **Применить**.

Примечание

Если лицензия не действует на какой-либо модуль, роль будет недоступна и информация об этом отобразится: в списке ролей и в подсказке при наведении курсора мыши на роль, которую следует назначить для работы модуля. Если лицензия на модуль закончилась, роль для работы этого модуля останется назначенной узлу, но сам модуль работать не будет.

Описание всех ролей, которые можно назначить узлу, приведено далее.

Табл. 5.2. Перечень ролей

Название роли в GUI	Название роли в CLI	Описание
Анализатор трафика	analyzer	Категоризация веб-ресурсов
Антивирус	antivirus	Прием запросов на поиск вирусов по протоколу ICAP. При истечении лицензии на антивирус, модуль остановит свою работу.
Балансировщик	balancer	Распределение трафика по серверам фильтрации Solar NGFW. Роль использует сервис балансировщика HAProxy.
Виртуальный IP-адрес (VRRP)	vip	Объединение нескольких узлов под виртуальным IP-адресом
Межсетевой экран	firewall	Распределение правил межсетевого экрана по узлам
Обратный прокси-сервер	reverse-proxy	Фильтрация и кэширование трафика в обратном режиме работы системы
Сервер Kerberos-аутентификации	kerberos	Kerberos-аутентификация
Сервер NTLM-аутентификации	ntlm	Регистрация сервера в домене, NTLM-аутентификация
Сервис пересылки широковещательных igmp пакетов	igmpproxy	Пересылка IGMP-пакетов из одной сети в другую через прокси-сервер
Сервис репликации Досье на подчиненных узлах	abook-slave	Дублирование части данных Досье. Роль предназначена для повышения отказоустойчивости в ситуациях, когда связь с master-узлом (и хранящимся на нем Досье) временно отсутствует. Синхронизация Досье с внешним источником возможна только на сервере управления (master). На abook-slave загружается копия Досье с master-узла и внесенные на нем изменения. Если на внешнем источнике есть изменения, используйте master-узел для синхронизации и передачи на сервис abook-slave.
Сервер управления	master	Единая точка управления. Такая роль может быть назначена только на один Solar NGFW (см. также описание роли **Все сервисы**). На узле с этой ролью запускается веб-сервер для доступа к GUI, настраивается конфигурация, а также генерируется политика фильтрации, распространяемая на все остальные узлы.
Система предотвращения вторжений	ips	Сигнатурный анализ трафика и автоматическое предотвращение обнаруженных угроз
Фильтр HTTP-трафика	http-filter	Проксирование, фильтрация и кэширование трафика

5.4.2. Рекомендации по назначению ролей

5.4.2.1. Рекомендации по назначению ролей в одиночном режиме

Все роли должны быть расположены на одном узле, который является и узлом управления, и узлом фильтрации.

5.4.2.2. Рекомендации по назначению ролей в распределенном режиме

Роли должны быть распределены между несколькими узлами. Один узел должен обладать ролью управления. Распределение ролей по slave-узлам остается на усмотрении администратора системы. Например, роли управления и межсетевого экрана могут находиться на main-узле, а роли прокси-сервера и контентной фильтрации – на slave-узле.

5.4.2.3. Рекомендации по назначению ролей в кластере Solar NGFW

В кластере Solar NGFW рекомендуется распределять роли по узлам следующим образом:

- Slave-узлу (узлам) назначить роль **Межсетевой экран** (для применения политики межсетевого экранирования), роль **Виртуальный IP-адрес (VRRP)** (для настройки сетевых параметров сервиса keepalived), роль **Система предотвращения вторжений** (для защиты от сетевых атак).
- При назначении slave-узлам роли **Система предотвращения вторжений** эту роль необходимо назначить и на узел управления (main).

5.5. Статическая маршрутизация

Чтобы настроить маршруты, откройте раздел **Сеть** и выберите нужную вкладку:

- **Маршруты в присоединенные сети** – маршруты в сети, к которым у управляемого узла есть подключенные сетевые интерфейсы.

  На данной вкладке маршруты доступны только для просмотра. Данные представлены по следующим полям:

  - **Название маршрута**,
  - **Статус**,
  - **Адрес назначения**,
  - **Интерфейс**,
  - **Шлюз**,
  - **Кем и когда изменено**,
  - **Административная дистанция**.

  Для удобства маршруты можно отфильтровать по статусам, узлам или найти нужный маршрут с помощью поиска.

  Чтобы отредактировать название маршрута, нажмите  .

- **Маршруты по умолчанию** – маршруты, по котором будут отправлены пакеты, адрес назначения которых не совпадает ни с одним адресом назначения в таблице маршрутизации.

  Чтобы создать маршрут:

  1. В левом верхнем углу нажмите кнопку **Создать маршрут**.
  2. Заполните поля:
     - **Название**,
     - **Шлюз**,
     - **Узел** (управляемый узел, на котором необходимо создать маршрут),
     - **Административная дистанция** (приоритет).
  3. Последовательно нажмите кнопки **Сохранить** и **Применить изменения**.

  Данные представлены по следующим полям:

  - **Название маршрута**,
  - **Статус**,
  - **Адрес назначения**,
  - **Шлюз**,
  - **Кем и когда изменено**,
  - **Административная дистанция**.

- **Статические маршруты** – все остальные созданные маршруты.

  Чтобы создать маршрут:

  1. В левом верхнем углу нажмите кнопку **Создать маршрут**.
  2. Заполните поля:
     - **Тип** (узел или подсеть),
     - **Название**,
     - **Адрес**,
     - **Шлюз**,

     Примечание

     В качестве шлюза должен быть указан действующий IP-адрес. При указании в качестве шлюза адреса сети, широковещательного адреса сети или собственного адреса интерфейса статические маршруты будут неактивны.

- **Узел** (управляемый узел, на котором необходимо создать маршрут),
- **Административная дистанция** (приоритет).

3. Последовательно нажмите кнопки **Сохранить** и **Применить изменения**.

Для удобства маршруты можно фильтровать по статусам, узлам или найти нужный маршрут с помощью поиска.

Примечание

Изменения настроек статической маршрутизации после их применения вступают в силу в течение двух минут.

5.6. Управление сетевыми интерфейсами

Для управления параметрами физических сетевых интерфейсов управляемого узла используется раздел **Сеть > Сетевые интерфейсы**.

Доступ к разделу предоставляется администраторам Solar NGFW с правами **Сеть** (установленный флажок **Просмотр**). Для настройки сетевых интерфейсов необходимо обладать полным доступом прав **Сеть** (установленный флажок **Полный**). Подробнее об управлении правами доступа пользователей см. в *Руководстве администратора безопасности*.

Примечание

Перед настройкой интерфейсов рекомендуется выключить любые менеджеры сетевых настроек в ОС узла, кроме networking, и настраивать сетевые интерфейсы только при помощи менеджера интерфейсов networking.

Настройки сетевых интерфейсов рекомендуется проводить только через GUI узла управления. Вносить изменения в настройки сетевого интерфейса управляемого узла любыми другими способами не рекомендуется.

Удаление физических сетевых интерфейсов не рекомендуется, т.к. оно может вызвать смещение нумерации сетевых интерфейсов в CLI, что приведет к их некорректной настроке и работе в дальнейшем.

*При первом включении физического сетевого интерфейса в разделе **Система > Журналы** для него будет отображаться запись вида действие: создание нового интерфейса.*

Настройки считываются из конфигурационных файлов системы. При первом входе в раздел считываются настройки, выполненные средствами CLI при установке ОС и ПО.

В GUI отображаются и настраиваются только интерфейсы Ethernet и их субинтерфейсы (VLAN).

Примечание

Если с помощью GUI узла управления будет попытка изменить/удалить IP-адрес или выключить сетевой порт управляемого узла, через который осуществляется связь с узлом управления, будет показано предупреждение.

В разделе **Сеть > Сетевые интерфейсы** представлена таблица по всем созданным сетевым интерфейсам.

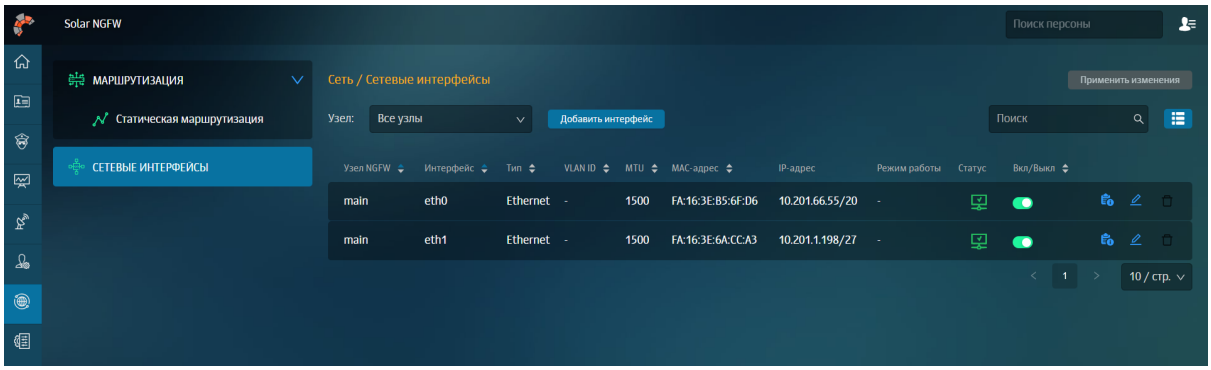


Рис. 5.17. Раздел "Сеть > Сетевые интерфейсы"

Вы можете настроить столбцы таблицы с помощью кнопки .

Для столбцов **Узел NGFW**, **Интерфейс**, **Тип**, **MTU**, **MAC-адрес** и **Вкл/Выкл** предусмотрена сортировка:

- – по возрастанию,
- – по убыванию.

Столбец **Статус** отображает статус соединения. Может принимать значения:

- – подключен (если переключатель **Вкл/Выкл** установлен в активный режим).
- – промежуточный статус (если переключатель **Вкл/Выкл** был переведен в активный режим, но подтверждение перехода интерфейса в состояние административного включения еще не получено).
- – не подключен (если переключатель **Вкл/Выкл** установлен в пассивный режим).
- – промежуточный статус (если переключатель **Вкл/Выкл** был переведен в пассивный режим, но подтверждение перехода интерфейса в состояние административного отключения еще не получено).

Столбец **Режим работы** отображает параметры настройки интерфейса: скорость соединения и режима двунаправленной передачи, в котором работает сетевой интерфейс (**Full** или **Half**). Также поддерживается автоматическое определение (значение **Auto** в списке режимов), в этом случае режим помечается как **(A)**. Примеры вывода: **1G Full**,

2.5G Full (A), **100M Half**. Если скорость или режим передачи определить невозможно, в соответствующем поле выводится значение **N/A**.

Примечание

На виртуальных машинах для Solar NGFW режим работы сетевого интерфейса может не отображаться.

Чтобы найти нужный сетевой интерфейс, воспользуйтесь полем **Поиск**.

Чтобы просмотреть подробную информацию о сетевом интерфейсе, нажмите  . Информация обновляется каждую минуту.

Примечание

Добавлять и удалять вручную можно только VLAN-интерфейсы.

Ethernet-интерфейсы доступны только для редактирования.

Рекомендуется определить перечень Ethernet-интерфейсов перед установкой Solar NGFW и не менять его в дальнейшем.

Добавить вручную можно только VLAN-интерфейсы. Ethernet-интерфейсы заводятся в системе автоматически и доступны только для редактирования.

Чтобы отредактировать параметры сетевого интерфейса, нажмите  .

При редактировании Ethernet-интерфейса открывается окно, в котором можно управлять параметрами:

- **Включено** – переключатель, отражающий состояние сетевого интерфейса.
- **Тип интерфейса** – значение, которое указывает на создание виртуального Ethernet-интерфейса. Поле нельзя отредактировать.
- **Узел NGFW** – узел, на котором доступен Ethernet-интерфейс. Поле нельзя отредактировать.
- **Интерфейс управления** – включите, если через этот интерфейс производится удаленное управление. В таблице рядом с интерфейсом управления будет значок  .

  Примечание

  Удаленное управление можно задать только для Ethernet-интерфейса.

- **Основной IP-адрес** – введите IP-адрес с маской сетевого интерфейса.
- **Добавить IP-адрес** – можно добавить до 10 дополнительных IP-адресов.

Примечание

В качестве адресов Ethernet-интерфейсов и субинтерфейсов (VLAN) нельзя указывать адреса 0.0.0.0/8, 169.254.0.0/16, 127.0.0.0/8, 240.0.0.0/4, 255.255.255.255/32 и адреса с маской /32.

IP-адрес из подсети должен использоваться только на одном интерфейсе или субинтерфейсе.

- **MTU** – MTU родительского интерфейса, который был указан в поле **Интерфейс**.

Примечание

Поле доступно для редактирования только на физических серверах.

- **MAC-адрес** – MAC-адрес родительского интерфейса, который был указан в поле **Интерфейс**. Поле нельзя отредактировать.
- **Режим работы** – выберите режим из раскрывающегося списка или укажите значение вручную.
- **Комментарий** – максимальная длина текста 500 символов.

Чтобы добавить новый VLAN-интерфейс:

1. Перейдите в раздел **Сеть > Сетевые интерфейсы**.
2. Нажмите кнопку **Добавить интерфейс**.
3. Заполните параметры:
   - **Включено** – текущее состояние сетевого интерфейса.
   - **Тип интерфейса** – значение, которое указывает на создание виртуального VLAN-интерфейса. Поле нельзя отредактировать.
   - **Узел NGFW** – выберите узел из списка доступных. Поле обязательно для заполнения.
   - **Интерфейс** – выберите физический интерфейс из списка доступных. Является родительским интерфейсом для VLAN. Поле обязательно для заполнения.
   - **VLAN ID** – число от 1 до 4094.
   - **Основной IP-адрес** – введите IP-адрес с маской VLAN-интерфейса.
   - **Добавить IP-адрес** – можно добавить до 10 дополнительных IP-адресов.

Примечание

В качестве адресов Ethernet-интерфейсов и субинтерфейсов (VLAN) нельзя указывать адреса 0.0.0.0/8, 169.254.0.0/16, 127.0.0.0/8, 240.0.0.0/4, 255.255.255.255/32 и адреса с маской /32.

IP-адрес из подсети должен использоваться только на одном интерфейсе или субинтерфейсе.

- **MTU** – MTU родительского интерфейса, который был указан в поле **Интерфейс**. Поле нельзя отредактировать.
- **MAC-адрес** – MAC-адрес родительского интерфейса, который был указан в поле **Интерфейс**. Поле нельзя отредактировать.
- **Комментарий** – максимальная длина текста 500 символов.

4. Последовательно нажмите кнопки **Сохранить** и **Применить изменения**.

Примечание

*При изменении/добавлении сетевого интерфейса временной промежуток от нажатия кнопки **Применить изменения** до фактического применения настроек может быть от 30 секунд до 2 минут.*

Чтобы удалить сетевой интерфейс, нажмите кнопку  .

Примечание

*Интерфейс управления с помощью кнопки  удалить нельзя. Чтобы удалить такой сетевой интерфейс, нажмите  и с помощью переключателя **Интерфейс управления** снимите управление с интерфейса.*

5.7. Управление маршрутизацией по протоколу OSPF

Для управления настройками маршрутизации по протоколу OSPF используется раздел **Сеть > Маршрутизация > OSPF**.

Примечание

*Управление настройками маршрутизации по протоколу OSPF возможно только при наличии полного доступа к разделу **Сеть**, а также установленной роли **Сервер управления** на узел.*

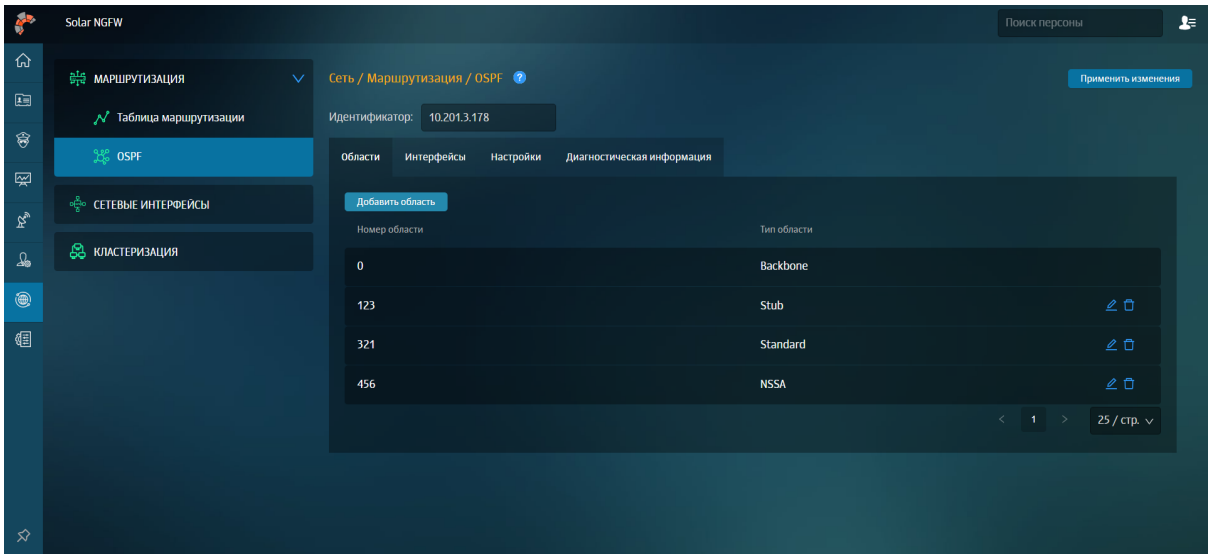


Рис. 5.18. Раздел "Сеть > Маршрутизация > OSPF"

В разделе **Сеть > Маршрутизация > OSPF** представлены вкладки:

- **Область** – таблица областей с их номерами (целое число в диапазоне от 0 до 2147483647) и типами (**Backbone** (возможно только для области с номером 0), **Standard**, **Stub** или **NSSA**). Чтобы добавить новую область, нажмите **Добавить область**.

  Примечание

  Сетевой интерфейс может быть включен только в одну область.

- **Интерфейсы** – таблица параметров существующих физических или виртуальных интерфейсов со столбцами:

  - **Номер области** – номер области (созданный на вкладке **Области**).
  - **Частота отправки Hello-пакетов** – интервал отправки Hello-пакетов в секундах, целое положительное число в диапазоне от 1 до 65535, по умолчанию – 10.
  - **Таймаут ожидания получения Hello-пакетов** – интервал ожидания получения Hello-пакетов от других участников OSPF-домена в секундах, число, кратное 4 hello-interval, целое положительное число в пределах от 1 до 65535, по умолчанию – 40.
  - **Частота повторения отправки пакетов** – интервал повторной отправки пакетов в секундах, целое положительное число в пределах от 1 до 65535, по умолчанию – 5.
  - **Стоимость** – стоимость перехода через этот интерфейс, целое положительное число в диапазоне от 1 до 65535.
  - **Приоритет** – приоритет назначенного маршрутизатора, целое положительное число в пределах от 0 до 255, по умолчанию – 1.

- **Пассивный интерфейс** – параметр отключает отправку Hello-пакетов на интерфейсе, может принимать значение **ВКЛ.** или **ВЫКЛ.**, по умолчанию – **ВЫКЛ.**.
- **Аутентификация** – тип аутентификации в области, может принимать значения **Без аутентификации**, **Пароль** и **MD5**.

Чтобы добавить новый интерфейс, нажмите **Добавить локальный интерфейс**.

- **Настройки** – настройки перераспределения статических маршрутов и маршрутов непосредственно присоединенных сетей. Вы можете установить флажки:
  - **Статические маршруты**,
  - **Маршруты непосредственно присоединенных сетей**,
  - **Маршруты ядра**.
- **Диагностическая информация** – общая информация о конфигурации OSPF (вкладка **Общая информация**), параметры интерфейса (вкладка **Интерфейсы**), информация о соседях OSPF (вкладка **Соседи**), таблица с имеющимися маршрутами (вкладка **База данных**) и таблица маршрутизации OSPF (вкладка **Маршруты**).

Возможна работа Solar NGFW в роли следующих типов маршрутизаторов протокола OSPF:

- Внутренний маршрутизатор (internal router) – маршрутизатор, все интерфейсы которого принадлежат одной области. У таких маршрутизаторов только одна база данных состояния каналов.
- Пограничный маршрутизатор (area border router, ABR) – соединяет одну или больше областей с магистральной областью и выполняет функции шлюза для межобластного трафика. У пограничного маршрутизатора всегда хотя бы один интерфейс принадлежит магистральной области. Для каждой присоединенной области маршрутизатор поддерживает отдельную базу данных состояния каналов.
- Магистральный маршрутизатор (backbone router) – маршрутизатор, у которого всегда хотя бы один интерфейс принадлежит магистральной области. Он похож на пограничный маршрутизатор, однако магистральный маршрутизатор не всегда является пограничным. Внутренний маршрутизатор, интерфейсы которого принадлежат нулевой области, также является магистральным.
- Пограничный маршрутизатор автономной системы (AS boundary router, ASBR) – обменивается информацией с маршрутизаторами, принадлежащими другим автономным системам или не OSPF-маршрутизаторами. Пограничный маршрутизатор автономной системы может находиться в любом месте автономной системы и быть внутренним, пограничным или магистральным маршрутизатором.

В Solar NGFW есть возможность работы со следующими типами областей протокола OSPF:

- Backbone – магистральная область, формирует ядро сети OSPF. Все остальные области соединены с ней. Межобластная маршрутизация выполняется через маршрутизатор, соединенный с магистральной областью. Магистральная область ответственна за распространение маршрутизирующей информации между немагистральными областями. Магистральная область должна быть смежной с другими областями, но не

обязательно физически смежной, соединение с магистральной областью может быть установлено и с помощью виртуальных каналов.

- Standard – область, которая создается по умолчанию. Эта область принимает обновления каналов, суммарные маршруты и внешние маршруты.

- Stub – конечная область, в которой не принимается информация о внешних маршрутах для автономной системы, но принимаются маршруты из других областей. Если маршрутизаторам из конечной области необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В конечной области не может находиться ASBR, исключение из этого правила – ABR может быть одновременно и ASBR. На всех маршрутизаторах области должна быть указана "конечность".

- NSSA – область, которая работает по тем же принципам, что и область Stub. Отличие в том, что в NSSA зоне может находиться ASBR. Для области NSSA предназначен специальный тип LSA – LSA type 7. LSA 7 передает внешние маршруты в области NSSA и во всем соответствует LSA 5. Когда пограничный маршрутизатор области NSSA передает LSA 7 в другие зоны, вместо LSA 7 передается стандартный LSA 5.

В Solar NGFW есть возможность работы со следующими типами объявлений о состоянии канала (Link State Advertisement, LSA):

- Type 1 LSA – Router LSA, распространяется всеми маршрутизаторами только в пределах одной области.

- Type 2 LSA – Network LSA, распространяет назначенный маршрутизатор в сетях со множественным доступом в пределах одной области.

- Type 3 LSA – Network Summary LSA, распространяется ABR, описывает маршруты к сетям вне локальной области, содержит информацию о сетях и о стоимости пути к этим сетям, но не отправляет информацию о топологии сети.

- Type 4 LSA – ASBR Summary LSA, распространяется ABR, описывает информация о пограничном маршрутизаторе автономной системы (ASBR).

- Type 5 LSA – AS External LSA, распространяется ASBR в пределах всей автономной системы, описывает внешние маршруты для автономной системы OSPF.

- Type 7 LSA – AS External LSA for NSSA, LSA 7 аналогично по содержанию LSA 5, но используется только в области NSSA. LSA 7 нужно, чтобы обойти ограничения, которые есть в области Stub. На границе области пограничный маршрутизатор преобразует type 7 LSA в type 5 LSA.

5.7.1. Перезапуск процесса OSPF

В некоторых случаях необходимо перезапустить процесс OSPF и установить соседство с другими сетевыми устройствами. Для этого в CLI выполните команды:

 # vtysh

 # clear ip ospf process

5.8. Настройка ротации журналов доступа

Для настройки ротации журналов доступа внесите в расписание планировщика **cron** следующую запись:

```
0 0 1 * * /opt/dozor/clickhouse/bin/cleanup-db.sh -d <days>
```

где **<days>** – значение времени в днях. Данные журналов доступа старше этого значения будут удаляться. В данном примере вызов скрипта **cleanup-db.sh** будет происходить первого числа каждого месяца.

5.9. Настройка синхронизации Досье

5.9.1. Синхронизация с внешним источником

Модуль **Досье** а также ряд иных функциональных областей может взаимодействовать с внешними источниками данных для синхронизации и получения данных из них.

Синхронизация с Active Directory может осуществляться по протоколам LDAP (см. раздел 5.9.2) и LDAPS (см. раздел 5.9.3).

Синхронизировать Досье с внешним источником можно в нескольких разделах системы:

- для детальной настройки – раздел **Досье** основных настроек конфигурации;
- для более быстрого доступа – раздел **Досье** > **Настройки**. Набор параметров настройки аналогичен перечню в разделе **Досье** основных настроек конфигурации.

5.9.2. Синхронизация с внешним источником по протоколу LDAP

Чтобы настроить синхронизацию данных Досье с внешним источником, используя основные настройки конфигурации:

1. В разделе **Система > Расширенные настройки > Досье > Доступ к источникам данных** нажмите кнопку **Добавить** и установите переключатель **Параметры доступа к источнику данных** в положение **ldap**.

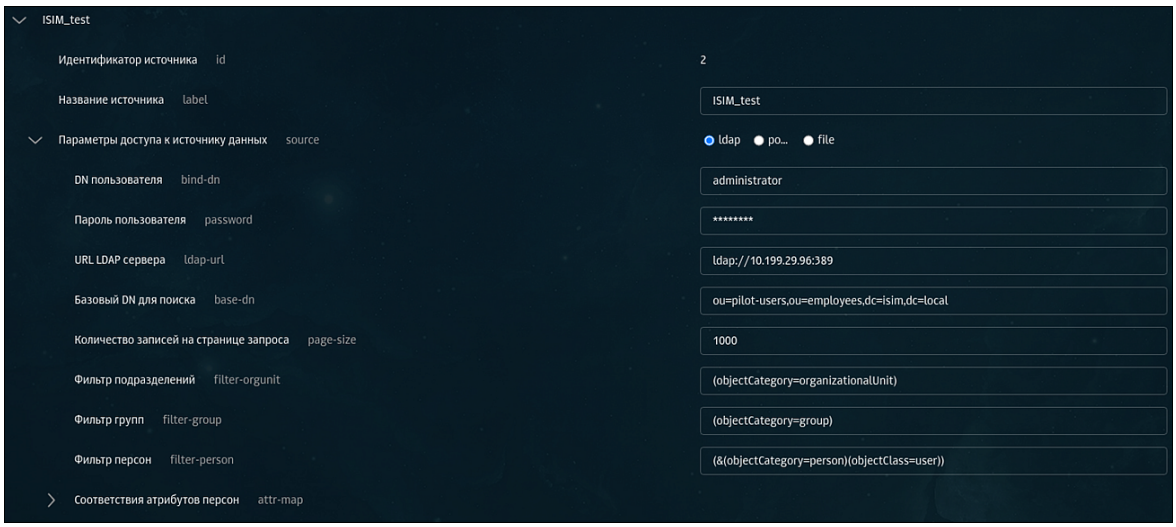


Рис. 5.19. Настройка синхронизации Досье

2. Задайте значения следующих параметров:

   - **Название источника** – укажите произвольное название источника данных AD. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
   - **DN пользователя** – имя учетной записи с правами чтения каталога AD. Имя указывается вместе с доменом (например, **admin@organization.local**).
   - **Пароль пользователя** – пароль учетной записи, указанной в предыдущем параметре.
   - **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например, **ldap://ldap.organization.local:389**).
   - **Базовый DN для поиска** – база поиска. Укажите значение в соответствии со структурой каталогов AD организации.

3. При необходимости раскройте группы параметров **Соответствия атрибутов персон**, **Соответствия атрибутов групп** и добавьте и/или исправьте соответствия между атрибутами AD и атрибутами досье.

4. Нажмите **Проверить** для проверки подключения к источнику данных. В случае неуспеха убедитесь в корректности заданных параметров.

5. Нажмите **Сохранить** и **Применить**.

6. Нажмите кнопку **Синхронизировать**. По окончании отобразится уведомление об удачной синхронизации.

7. Вернитесь в GUI и проверьте наличие оргструктуры в разделе **Досье > Организационная структура**.

По окончании задайте интервал синхронизации:

1. Откройте секцию **Сервис обновления Досье > Работа в главном режиме**.

2. Установите флажок **Автоматическая синхронизация с источниками**.

3. Задайте значение параметров **Периодичность синхронизации (ч)** и **Периодичность синхронизации (м)**.

   Примечание

   Не рекомендуется устанавливать значение периодичности синхронизации меньше 20 минут, т.к. при объемном LDAP-каталоге и большом количестве пользователей для успешного завершения обновления данного времени может быть недостаточно.

   При значении 0 часов 0 минут синхронизация работать не будет.

4. Нажмите **Сохранить** и **Применить**.

Для настройки синхронизации данных Досье с внешним источником в разделе **Досье** нажмите кнопку **Настройки** и выполните процедуру, описанную выше.

5.9.3. Синхронизация с внешним источником по протоколу LDAPS

5.9.3.1. Общий порядок настройки синхронизации

Трафик, передаваемый по протоколу LDAP, не является защищенным. Чтобы синхронизация данных была конфиденциальной и безопасной, используйте протокол LDAPS, который является защищенной версией LDAP, и в котором используется дефолтный порт 636 вместо 389, как у LDAP.

LDAPS представляет собой технологию «LDAP через SSL», которая позволяет шифровать процесс синхронизации данных и аутентификации.

Для настройки синхронизации по протоколу LDAPS:

1. Выпустите и импортируйте сертификат в центре сертификации домена (CA) – см. раздел 5.9.3.2;
2. Импортируйте сертификат центра сертификации домена (CA) в Solar NGFW – см. раздел 5.9.3.3;
3. В разделе **Досье > Доступ к источникам данных** выполните процедуру, описанную в разделе 5.9.2, предварительно заменив порт назначения на 636 (вместо 389).
4. Если вы указали FQDN в настройках URL LDAP-сервера (раздел **Система > Расширенные настройки > Досье > Доступ к источникам данных > Параметры доступа к источнику данных**), укажите этот FQDN и IP-адрес сервера в файле **/etc/hosts**.
5. После настроек проверьте связи с источником синхронизации. Для этого нажмите кнопку **Синхронизировать** на вкладке **Настройки** раздела **Досье** или в разделе **Система > Досье** основных настроек.

Примечание

*Если не работает сразу, в CLI выполните рестарт сервисов **monitor-ng** и **abook-daemon** с помощью команд:*

 # /opt/dozor/bin/shell

 # dsctl restart monitor-ng

 # dsctl restart abook-daemon

5.9.3.2. Управление сертификатом

Установка допустимого сертификата на контроллере домена позволяет службе LDAP прослушивать и автоматически принимать подключения SSL как для LDAP, так и для глобального трафика каталогов.

Для генерации сертификата:

1. На сервере с ролью **Certification Authority** (CA) запустите консоль **Certification Authority Management Console**, перейдите в раздел с шаблонами сертификатов **Certificate Templates** и в контекстном меню выберите **Manage**.

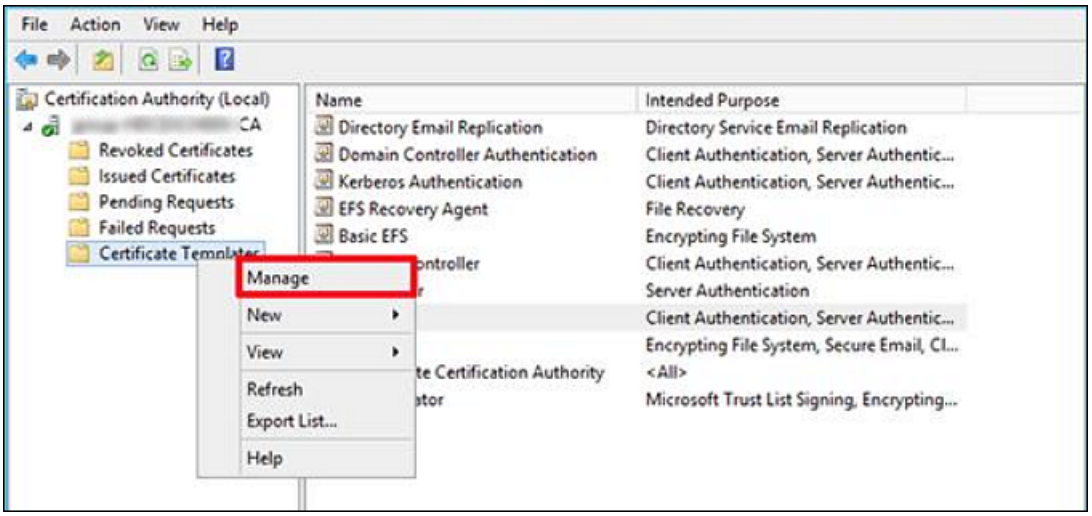


Рис. 5.20. Управление шаблонами сертификатов

2. Создайте копию шаблона **Kerberos Authentication certificate**, выбрав в контекстном меню команду **Duplicate Template**.

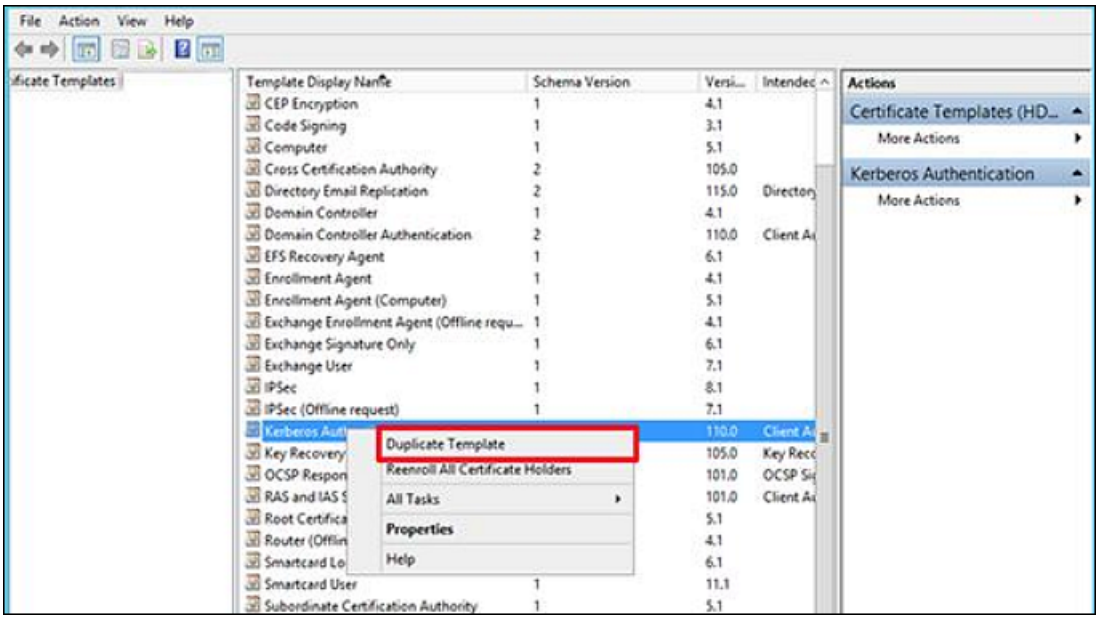


Рис. 5.21. Создание копии шаблона сертификата

3. В окне **Properties of New Template** на вкладке **General** переименуйте шаблон сертификата в **LDAPoverSSL**, указав период его действия, и опубликуйте его в AD (**Publish certificate in Active Directory**).

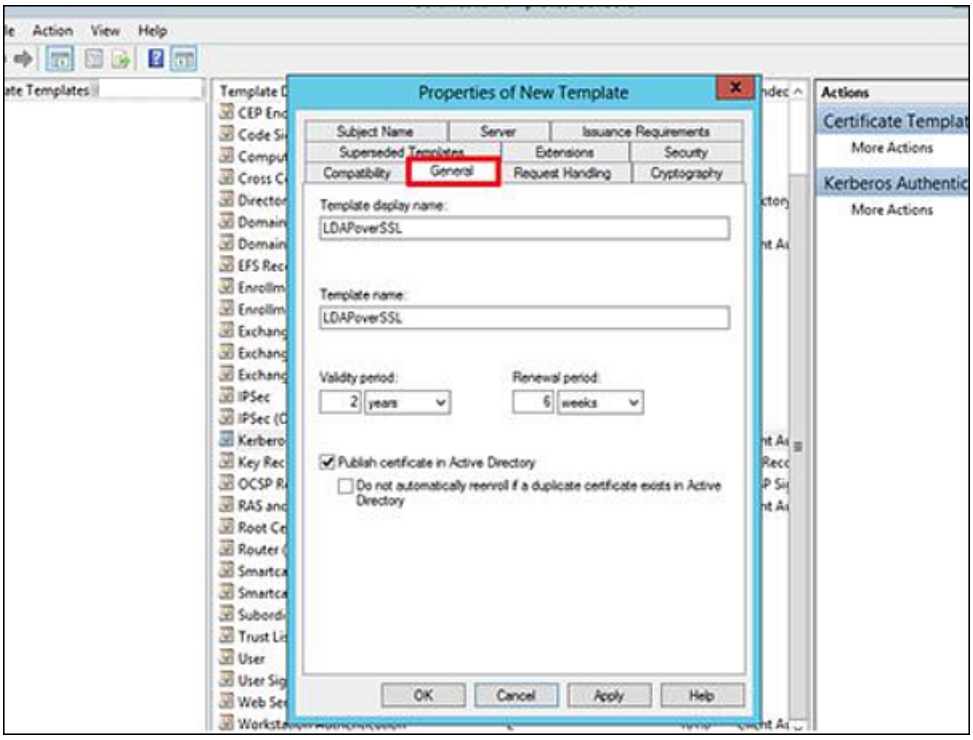


Рис. 5.22. Переименование и публикация шаблона сертификата

4. На вкладке **Request Handling** установите флажок **Allow private key to be exported** и сохраните шаблон.

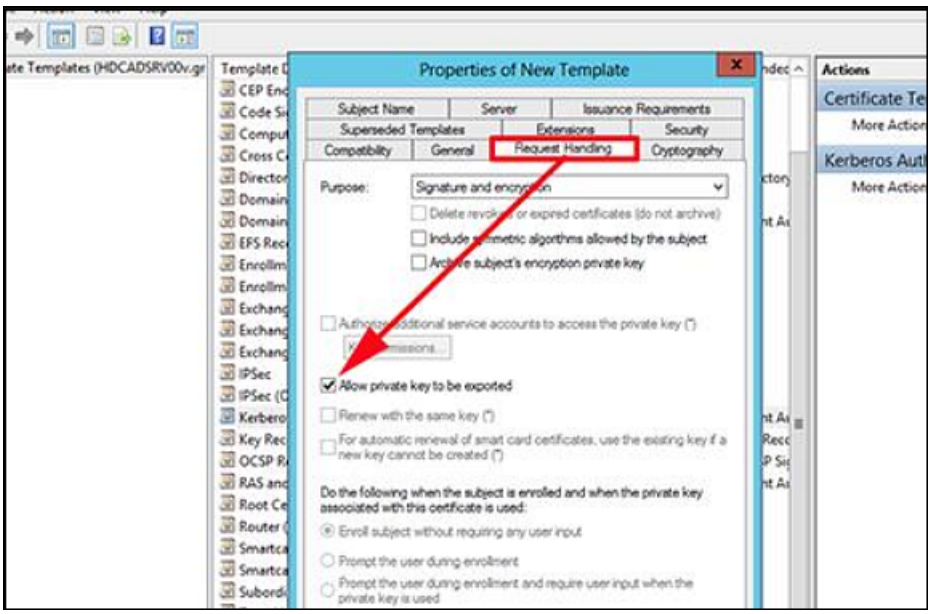


Рис. 5.23. Сохранение шаблона сертификата

5. Опубликуйте новый тип сертификата на базе созданного шаблона:

   - В контекстном меню раздела **Certificate Templates** выберите команду **New > Certificate Template to issue**.

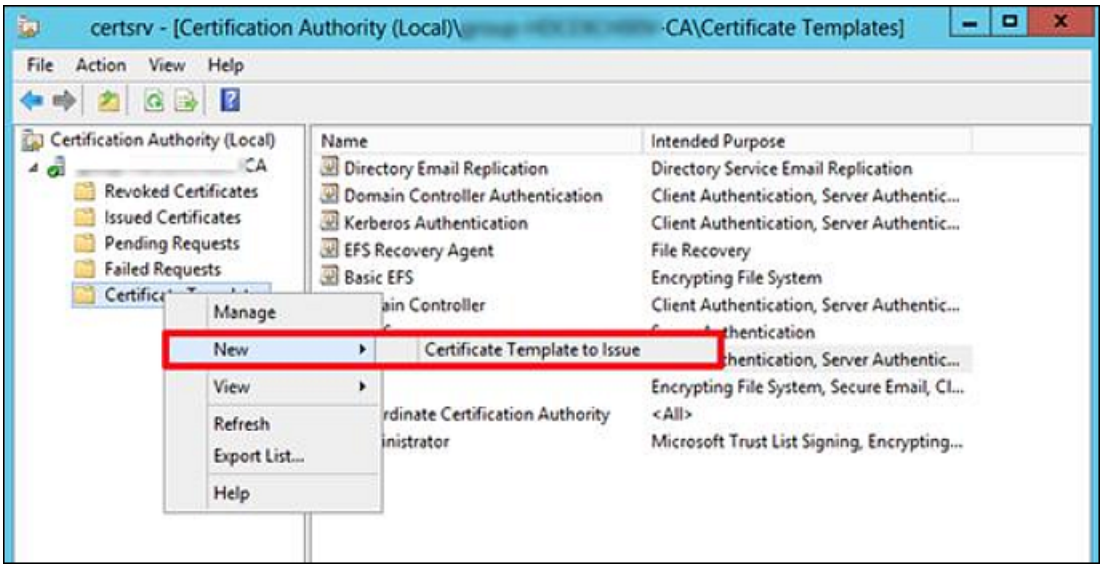


Рис. 5.24. Выбор сертификата для генерации

- В списке доступных шаблонов выберите **LDAPoverSSL** и нажмите **OK**.

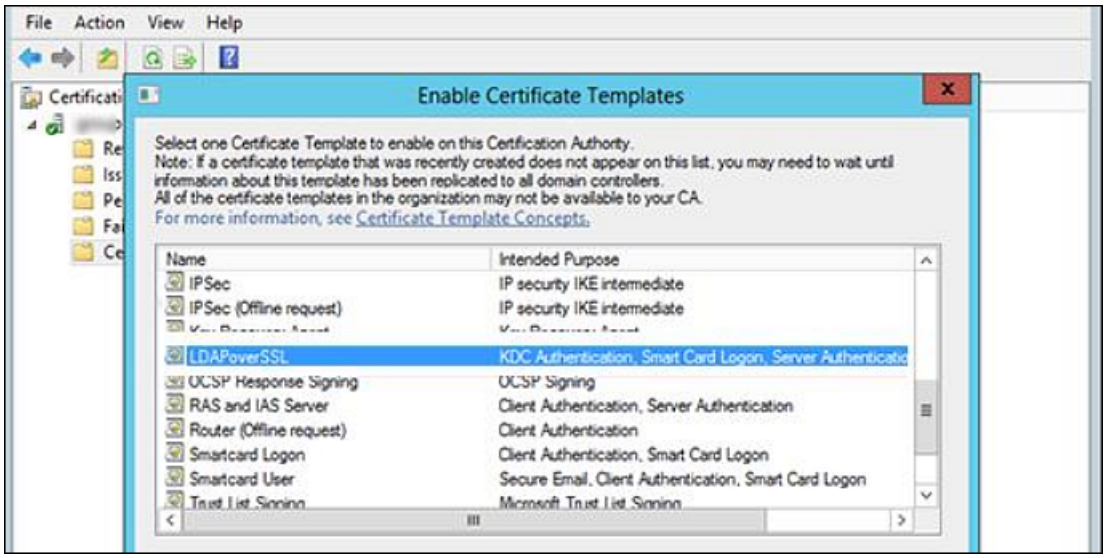


Рис. 5.25. Выбор типа сертификата LDAPoverSSL

6. На контроллере домена, для которого планируется задействовать LDAPS, откройте оснастку управления сертификатами и в хранилище сертификатов **Personal** запросите новый сертификат. Для этого в контекстном меню выберите команду **All Tasks > Request New Certificate**.

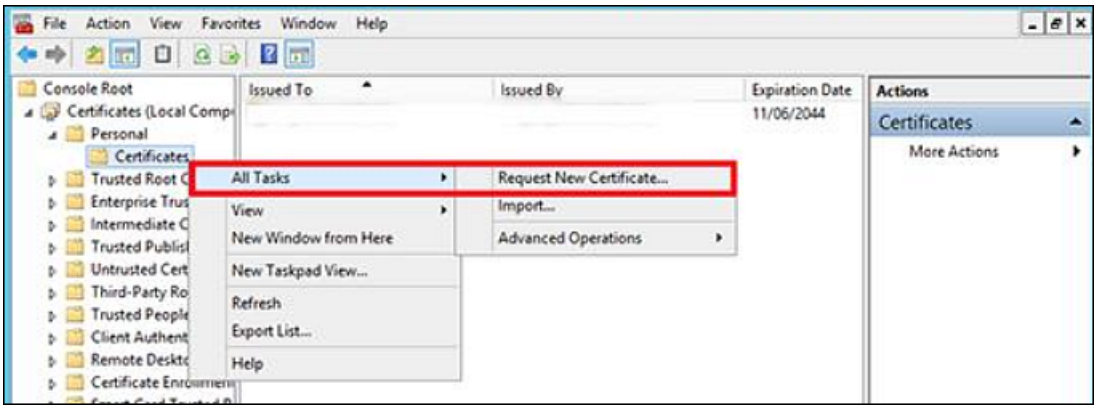


Рис. 5.26. Запрос нового сертификата

7. В списке доступных сертификатов выберите сертификат **LDAPoverSSL** и нажмите **Enroll**. Сертификат будет выпущен.

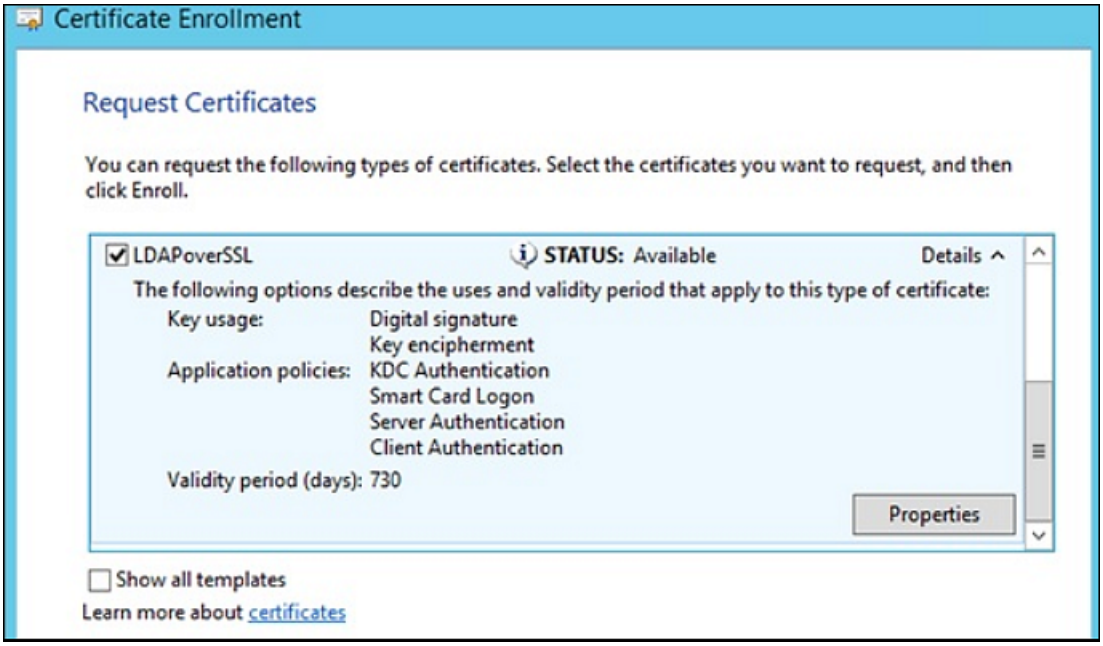


Рис. 5.27. Выпуск сертификата

8. В CLI выполните экспорт корневого сертификата удостоверяющего центра в файл, выполнив на сервере с ролью **Certification Authority** команду:
certutil -ca.cert ca_name.cer
. Файл сертификата сохранится в профиле текущего пользователя в файле формата **CER**. Например, *ca_ name. cer*.

9. Добавьте экспортированный сертификат в контейнере сертификатов **Trusted Root Certification Authorities** хранилища сертификатов на клиенте и контроллере домена, выполнив в CLI команду:
certmgr.exe -add C:\ca_name.cer -s -r localMachine ROOT
. Полностью перезагрузите DC.

5.9.3.3. Добавление сертификата в центре сертификации домена (CA) в хранилище сертификатов Solar NGFW

Добавление сертификата в центре сертификации домена (CA) позволит открывать защищенные соединения с другими устройствами, имеющими сертификат, выпущенный этим же центром сертификации.

Для импорта сертификата УЦ в хранилище сертификатов Solar NGFW:

1. Скопируйте полученный сертификат на все узлы с ролью **Фильтр HTTP-трафика**. Перейдите в каталог с сертификатом и с помощью CLI сконвертируйте его в формат PEM, выполнив команду:

   openssl x509 -inform der -in cert.cer -out cert.pem

2. Для импорта сертификата в хранилище выполните команду:

   keytool -import -v -trustcacerts -alias <cert_alias> -file /var/tmp/cert.pem -keystore /opt/dozor/etc/ldap.jks -deststoretype JKS

   где **<cert_alias>** – название сертификата в хранилище.

   Примечание

   После выполнения команды может быть запрошен пароль от ключевого хранилища. Если он не был задан ранее, придумайте новый.

3. Проверьте, что у пользователя **dozor** есть разрешение на просмотр **/opt/dozor/etc/ldap.jks**.

5.9.4. Синхронизация со сторонним Досье

Досье Solar NGFW может работать в подчиненном режиме, то есть использовать Досье Solar NGFW, Solar webProxy или Solar Dozor. Для этого внешняя система должна иметь собственное хранилище Досье. В этом режиме Solar NGFW подключается к Досье внешней системы и загружает локальную копию в оперативную память. При внесении изменений в Досье внешней системы, Досье в Solar NGFW автоматически обновляется согласно этим изменениям. В подчиненном режиме нельзя подключиться к Досье системы, также использующей подчиненный режим.

Для настройки синхронизации данных Досье Solar NGFW с Досье Solar Dozor, Solar webProxy или Solar NGFW:

1. На master-узле в CLI выполните команду:

   # /opt/dozor/abook-daemon/bin/reg-abook-slave <host>

   где **<host>** – FQDN master-узла системы, с Досье которого будет выполняться синхронизация. При выполнении команды система запросит пароль пользователя **root** удаленного master-узла.

2. В GUI в секции **Сервис обновления Досье** раздела **Досье** расширенных настроек конфигурации задать значения следующих параметров:

- **Режим работы** – **Подчиненный**.
- **Сетевой адрес** – FQDN master-узла системы, с Досье которого будет выполняться синхронизация.
- **Порт** – порт, на котором сервис **abook-daemon** ожидает соединения по HTTPS (по умолчанию – 2269).

3. Нажмите **Сохранить**, **Применить**.
4. Перезапустите сервис **abook-daemon** на локальном и удаленном master-узлах.
5. В CLI выполните следующие команды:

   # /opt/dozor/bin/shell

   # dsctl restart clickhouse

Примечание

При переходе из подчиненного режима в главный значения параметров настройки главного режима остаются неизменными, т.е. дефолтными.

5.10. Режимы работы прокси-сервера

Возможность проксирования трафика в Solar NGFW включается при использовании лицензии на функциональность Solar webProxy.

Прокси-сервер в Solar NGFW может использоваться в качестве следующих типов:

- прямой прокси,
- обратный прокси.

Примечание

Поддерживается одновременная работа прямого и обратного прокси-сервера на одном узле (с одним публичным IP-адресом). Особенности работы и описание процесса настройки прокси-сервера в обратном режиме подробно описаны в разделе 8.

Прямой прокси поддерживает следующие режимы работы:

- явный,
- прозрачный.

При использовании прокси-сервера в явном режиме работы в клиентских приложениях (например, веб-браузерах) должны быть установлены настройки прокси-сервера Solar NGFW. При использовании прокси-сервера в прозрачном режиме, данные настройки не используются, т.е. пользователь не знает о прокси-сервере Solar NGFW (подробнее о настройке прозрачного режима работы см. раздел 5.11.5).

5.10.1. Порядок обработки проксируемого трафика

5.10.1.1. Прямой прокси в явном режиме работы

Трафик проходит через Netfilter по цепочкам PREROUTING и INPUT. Поэтому фильтрация такого трафика межсетевым экраном доступна только с помощью правил, где в качестве направления трафика указано значение **Входящий**. Подробнее см. *Руководстве администратора безопасности*.

Примечание

Даже если основной трафик транзитный, веб-трафик не будет считаться транзитным и не будет попадать в цепочку FORWARD, т.к. на стороне клиентского приложения в качестве адреса назначения пакета устанавливается адрес прокси-сервера Solar NGFW.

5.10.1.2. Прямой прокси в прозрачном режиме работы

Трафик проходит через Netfilter по цепочке PREROUTING и прямо из этой цепочки перенаправляется по портам 80 и 443 в модуль прокси-сервера (skvt-wizor) для дальнейшей обработки. Поэтому фильтрация межсетевым экраном недоступна для трафика, проксируемого в прозрачном режиме (такой трафик не будет подвергаться проверкам как правилами классического межсетевого экрана, так и правилами DPI). Подробнее о настройке прозрачного режима работы см. раздел 5.11.5.

5.10.1.3. Обратный прокси

Схема обработки трафика обратным прокси аналогична схеме обработки трафика прямым прокси в явном режиме работы. Трафик проходит через Netfilter по цепочкам PREROUTING и INPUT (т.к. при публикации внутренних ресурсов с помощью обратного прокси-сервера клиентские приложения отправляют трафик именно на прокси-сервер, воспринимая его как целевой веб-сервер). Поэтому фильтрация такого трафика межсетевым экраном доступна только с помощью правил, где в качестве направления трафика указано значение **Входящий**. Подробнее о настройке обратного прокси см. раздел 8.

Примечание

В Solar NGFW есть возможность проксирования исключительно веб-трафика (протоколы HTTP, HTTPS и FTP over HTTP). При необходимости прохождения иного трафика настройте правила обработки транзитного трафика (цепочка FORWARD) и параметры трансляции адресов (NAT). Подробнее о настройке межсетевого экрана и NAT см. в Руководстве администратора безопасности.

5.11. Настройка аутентификации

5.11.1. Общие сведения

Аутентификация пользователей работает только для проксируемого трафика. При использовании другого трафика разграничение доступа пользователей в сеть будет регулироваться правилами межсетевого экрана (подробнее см. в *Руководстве администратора безопасности*).

Механизм аутентификации Solar NGFW поддерживает следующие виды источников учетных записей:

- локальный список IP-адресов и диапазонов;
- локальный список учетных записей;
- LDAP;
- LDAPS;
- RADIUS;
- IMAP;
- POP3.

При создании схемы аутентификации необходимо учитывать следующие особенности:

- Проверка по IP-адресам имеет наивысший приоритет.
- При доменной аутентификации используется только один источник в связи с уникальностью настроек **samba**, **krb5**, **winbind**.
- В тех схемах, где это нужно, следует снять флажок **abort-by-error** (**Прерывать процесс аутентификации при возникновении ошибок**) в разделе **Аутентификация > Источники Basic аутентификации** основных настроек. Параметр **abort-by-error** регулирует возможность прерывания процесса аутентификации при возникновении ошибок. Параметр предназначен для настройки разного поведения сервера аутентификации в случае возникновения ошибок с конкретным источником аутентификации. Например, если источник недоступен из-за сетевых проблем:
  - если флажок **abort-by-error** снят — поиск пользователей в БД данного источника не будет выполняться, и сервер аутентификации продолжит поиск подходящего пользователя в БД других заданных источников;
  - если флажок **abort-by-error** установлен — при появлении ошибок в процессе взаимодействия с данным источником сервер аутентификации будет выдавать ошибку, и дальнейший поиск выполняться не будет.

В Solar NGFW используются следующие методы аутентификации:

- по IP-адресам (раздел 5.11.2);
- Negotiate (раздел 5.11.3);
- NTLM (раздел 5.11.4);
- NTLM+Negotiate (примечание в разделе 5.11.3);
- Radius (раздел 5.11.6.5);
- прозрачная (раздел 5.11.5);
- basic (раздел 5.11.6).

Режимы, в которых используются эти методы аутентификации перечислены далее в Таблице.

Табл. 5.3. Режимы аутентификации

Название	Описание
Permissive	Разрешительный режим. Аутентификация не разрешается только если запись пользователя заблокирована. Используется IP-аутентификация.
Prohibitory	Запретительный режим. Аутентификация разрешается только если запись пользователя существует и не заблокирована. Используется IP-аутентификация.
Basic	HTTP-аутентификация методом basic
NTLM	Доменная аутентификация методом NTLM
Negotiate	Доменная аутентификация методом Negotiate. По выбору клиента выполняется методом Kerberos или NTLM.
NTLM+Negotiate	Доменная аутентификация методом Negotiate либо NTLM. Метод выбирается клиентом. Этот режим используется, если заранее неизвестно, поддерживает ли клиент метод Negotiate.
Radius	Basic-аутентификация для удаленного доступа к пользовательским сервисам, виртуальным частным сетям (VPN), точкам беспроводного доступа (Wi-Fi) и т.д.

5.11.2. Настройка аутентификации по IP-адресам

Аутентификация по IP-адресам может работать в одном из двух режимов:

- *Разрешительный* – доступ разрешен с любых IP-адресов без исключений.
- *Запретительный* – доступ разрешен только в соответствии с настроенным слоем политики **Доступ без аутентификации**. Подробная информация о настройке этого слоя приведена в документе *Руководство администратора безопасности*.

Режим аутентификации можно настроить:

- в разделе **Работа системы** основных настроек;
- на вкладке **Настройки** в разделе **Политика**.

Для настройки режима аутентификации:

1. В разделе **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения следующих параметров:
   - **Режим аутентификации** – **Proxy-Auth**;
   - **Метод аутентификации**:
     - **Permissive** – для разрешительного режима;
     - **Prohibitory** – для запретительного режима.
2. Нажмите **Сохранить** и **Применить**.

Для настройки режима аутентификации из раздела **Политика** нажмите кнопку **Настройки** в левом верхнем углу раздела и выполните действия, описанные выше.

5.11.3. Настройка аутентификации Negotiate

Для настройки аутентификации Negotiate:

1. Назначьте одному из узлов Solar NGFW роль **Сервер Kerberos-аутентификации**. Это будет сервер аутентификации Solar NGFW.

2. В разделе **Аутентификация > Kerberos-аутентификация** задайте значения следующих параметров:

   - **Домен** – имя домена.
   - **Адрес KDC-сервера** – IP-адрес сервера центра выдачи ключей (KDC) в сети. Можно добавлять и удалять записи о серверах, используя кнопки  и  .
   - **Адрес административного сервера** – IP-адрес контроллера домена в сети. Можно добавлять и удалять записи о серверах, используя кнопки  и  .

3. В разделе **Политика** > **Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения следующих параметров:

   - **Режим аутентификации** – **Proxy-Auth**;
   - **Метод аутентификации** – **Negotiate**.

4. Создайте и зарегистрируйте ключ. Для этого в CLI **на контроллере домена** выполните команду:

   ktpass.exe -out C:\krb5.keytab -princ HTTP/auth-skvt.solar.local@WINDOWS.DOMAIN -mapuser skvt2 -pass password -crypto All -ptype KRB5_NT_PRINCIPAL

   Примечание

   Значения для замены:

   - ***auth-skvt.solar.local*** *– FQDN сервера аутентификации Solar NGFW;*
   - ***WINDOWS.DOMAIN*** *– имя домена;*
   - ***skvt2*** *– сервисный пользователь AD, с помощью которого осуществляется аутентификация;*
   - ***password*** *– пароль пользователя.*

   В результате выполнения этой команды будет создан ключ аутентификации. Ключ будет находиться в месте, указанном после ключа **-out**, в данном примере – **C:\krb5.keytab**.

5. В GUI Solar NGFW в разделе **Аутентификация> Keytab-файл**:

   - установите переключатель **Режим использования keytab-файла** в положение **Загрузить из файла**;

- нажмите **Загрузить**, выберите в открывшемся окне файл и нажмите **Открыть**;
- нажмите **Сохранить** и **Применить**.

Примечание

В Solar NGFW есть возможность аутентификации с нескольких доменов. Для этого:

1. *На каждом домене выполните шаги из 4.*
2. *Поместите полученные файлы в любой каталог Solar NGFW с помощью SCP (Secure Copy Command).*
3. *Выполните следующие команды:*

   ktutil

   read_kt <имя_первого_ключа.keytab>

   read_kt <имя_второго_ключа.keytab>

   write_kt krb5.keytab

   quit
4. *Просмотреть содержимое итогового файла можно с помощью команды:*

   klist -k krb5.keytab

*Полученный файл **krb5.keytab** загружается на прокси-сервер (подробнее см. в разделе 5).*

При создании обоих файлов рекомендуется использовать разные пароли для учетных записей, ассоциированных с Solar NGFW.

Если серверов фильтрации несколько, ключ генерируется на общее доменное имя для всех этих серверов. Например, для двух серверов фильтрации с сетевыми именами **filter1.org.local** и **filter2.org.local** и IP-адресами 10.10.10.1 и 10.10.10.2 соответственно, выберите для них общее имя, например **proxy.org.local**. Ключ должен быть сгенерирован для имени **proxy.org.local**, и на каждом сервере фильтрации в конце файла **/etc/hosts** добавлена запись вида:

```
10.10.10.1 proxy.org.local
```

```
10.10.10.2 proxy.org.local
```

На каждом сервере фильтрации должна быть только одна из этих записей, соответствующая его IP-адресу.

Внимание!

*При добавлении записей в конец файла **/etc/hosts** не заменяйте и не удаляйте текущие.*

Для проверки корректности настроек Negotiate-аутентификации:

1. В разделе **Система > Аутентификация > Kerberos-аутентификация** в поле **Домен** укажите имя домена.
2. В качестве адреса KDC-сервера и адреса административного сервера введите IP-адрес контроллера домена.
3. Последовательно нажмите **Сохранить** и **Применить**.
4. В CLI выполните команду:

   # kinit -V -k -p HTTP/<Общий FQDN NGFW>

Отсутствие сообщений об ошибке свидетельствует об успешной настройке аутентификации.

Примечание

Для настройки аутентификации NTLM+Negotiate выполните инструкции из разделов ***5.11.4*** *и* ***5.11.3****, учитывая, что параметр* ***Метод аутентификации*** *должен иметь значение* ***NTLM+Negotiate****.*

5.11.4. Настройка NTLM-аутентификации

Для настройки NTLM-аутентификации:

1. Назначьте одному из узлов Solar NGFW роль **Сервер NTLM-аутентификации**. Это будет сервер аутентификации Solar NGFW.
2. В разделе основных настроек **Аутентификация > Подключение к Контроллеру домена (DC) для NTLM-аутентификации** укажите имя домена AD в поле **Домен**.
3. На сервере аутентификации Solar NGFW откройте для редактирования файл **/etc/resolv.conf** и добавьте в него строки следующего вида:

   ```
   nameserver <namesrvIP>
   ```

   где **<namesrvIP>** – IP-адрес контроллера домена. Если таких адресов несколько, добавьте несколько таких строк, в порядке уменьшения надежности контроллеров домена. В каждой строке может быть только один IP-адрес.
4. Добавьте сервер аутентификации в домен, выполнив на нем с помощью CLI команду следующего вида:

   # net ads join -U <admin_login>

   где **<admin_login>** – имя учетной записи пользователя с правами администратора контроллера домена.
5. В GUI в разделе **Политика** > **Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения следующих параметров:

   - **Режим аутентификации** – **Proxy-Auth**;

- **Метод аутентификации** – **NTLM**.

6. Нажмите **Сохранить** и **Применить**.

5.11.5. Настройка прозрачной аутентификации

Прозрачная аутентификация применяется, когда настройка браузеров рабочих станций пользователей невозможна, затруднена или неприемлема. При этом имеются следующие ограничения на архитектуру корпоративной сети:

- каждому IP-адресу должен соответствовать только один пользователь;
- между рабочими станциями пользователей и Solar NGFW не должно быть других прокси-серверов и оборудования, осуществляющего трансляцию адресов;
- работа терминальных серверов не поддерживается.

Режим прозрачной аутентификации заменяет обычную на прокси-сервере (HTTP 407: Proxy Authorization Required). При обращении к Solar NGFW рабочей станции пользователя, IP-адреса которой нет в хранилище Solar NGFW, ее запрос перенаправляется на служебную страницу. На этой странице пользователю предлагается ввести учетные данные (HTTP 401: Unauthorized), и в случае успешной авторизации IP-адрес добавляется в хранилище, и продолжается обработка первоначального запроса. Запросы с рабочих станций, IP-адреса которых есть в хранилище, обрабатываются без перенаправлений.

В первую очередь настройте пакетные фильтры на всех узлах фильтрации:

1. Отключите параметры настройки фильтра Linux-ядра. Для этого в файле **etc/sysctl.conf** раскомментируйте строку
   net.ipv4.conf.<название интерфейса>.rp_filter=0
   и примените изменения командой
   # /sbin/sysctl -p
   .

   Фильтрация ядром ОС отключается, когда пакет принят одним интерфейсом и должен быть передан на другой интерфейс. Если устройство стоит в разрыв, команда выполняется для всех интерфейсов, между которыми выполняется передача трафика, либо используется параметр **all**, чтобы отключить фильтрацию сразу на всех интерфейсах.

2. Включите поддержку TPROXY в подсистеме маршрутизации, выполнив команды:

   # ip -f inet rule add fwmark 1 lookup 100
   (весь трафик, поступивший на интерфейсы, помечается маркером 1 и передается в таблицу маршрутизации 100)

   # ip -f inet route add local default dev eth0 table 100
   (в таблицу маршрутизации 100 добавляется маршрут по умолчанию)

3. Подготовьте Solar NGFW к перенаправлению запросов, выполнив команды:

   # iptables -t mangle -N DIVERT

   # iptables -t mangle -A DIVERT -j MARK --set-mark 1

   # iptables -t mangle -A DIVERT -j ACCEPT

 # iptables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT

4. Настройте правила перенаправления запросов в Solar NGFW, выполнив команды:

   # iptables -t mangle -A PREROUTING -p tcp --dport 443 -j TPROXY --tproxy-mark 0x1/0x1 --on-ip 127.0.0.1 --on-port 2444

   # iptables -t mangle -A PREROUTING -p tcp --dport 80 -j TPROXY --tproxy-mark 0x1/0x1 --on-ip 127.0.0.1 --on-port 2270

   где **127.0.0.1** – IP-адрес, по которому сервис wizor принимает соединения по портам 2444 и 2270.

Примечание

При перезагрузке Solar NGFW настройки прозрачной аутентификации могут работать некорректно. Для успешного применения настроек после перезагрузки системы выполните повторно шаги 2-4.

Для включения режима прозрачной аутентификации в GUI Solar NGFW:

1. В разделе **Система > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей > Веб-сервер, предоставляющий скачанные файлы** расширенных настроек конфигурации в поле **Адрес веб-сервера** установите значение **${node-hostname}** (по умолчанию установлено значение **mitm.it**).

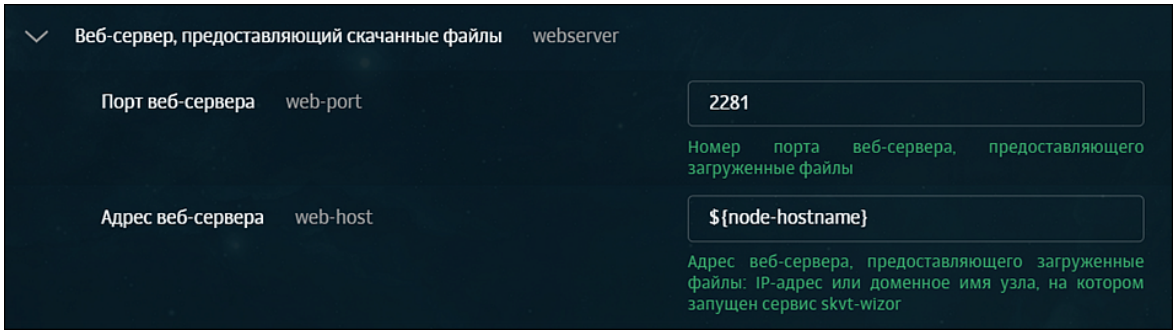


Рис. 5.28. Параметры настройки веб-сервера

2. В разделе **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации установите значение **Transparent** для параметра **Режим аутентификации**.

3. Нажмите **Сохранить**, затем **Применить** и перезапустите сервис **skvt-wizor**.

4. Убедитесь, что skvt-wizor запущен от пользователя **root**. Для этого в разделе **Политика > Настройки > Параметры запуска фильтра** или **Система > Основные настройки > Работа системы > Параметры запуска фильтра** установлен флажок **Запускать от имени пользователя root**.

5. В CLI выполните команды:

   # /opt/dozor/bin/shell

 # dsctl status

 # /opt/dozor/service/skvt-wizor:..... up (pid 3661) 63117 seconds
, где **3661** — номер процесса skvt-wizor

 # ps -ef --forest | grep 3661 -A 1

После успешного выполнения команды будет отображен вывод вида:

```
root@wp4:/opt/dozor# ps -ef --forest | grep 3661 -A 1
root      1458 31464  0 17:03 pts/0    00:00:00  |           \_ grep 3661 -A 1
root     30377  1121  0 17:02 ?        00:00:00  \_ sshd: root@notty
--
root      3661     1  0 14:56 ?        00:00:00 /bin/bash /opt/dozor/var/lib/service/skvt-wizor/run
root      3854  3661  1 14:56 ?        00:02:30  \_ /usr/lib/jvm/bellsoft-java17-full-amd64//bin/java -Djdk.tls.server.enableSessionTicketExtension=false --ad
d-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/sun.nio.ch=ALL-UNNAMED -Dfile.encoding=UTF8 -Dsun.net.client.defaultConnectTimeout=30000 -server -
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/tmp -XX:MaxJavaStackTraceDepth=1000000 -XX:MaxDirectMemorySize=4096m -Xmx2048m -Xms256m -jar /opt/dozor/s
kvt/lib/nio_proxy.jar /data/repos/dozor/config-final.git/6b34cd8d-201d-48c8-a788-088d41241248/skvt-wizor/config.xml /opt/dozor/share/url-checker/categories.js
on
```

При выводе команды убедитесь, что дочерний процесс также запущен от пользователя **root**.

6. В CLI экспортируйте сертификат УЦ Solar NGFW, выполнив команду (в одну строку):

   # keytool -exportcert -rfc -keystore /opt/dozor/skvt/var/lib/authority.jks -alias "ngfw" > ngfw.crt

   Во время выполнения команды будет запрошен пароль (по умолчанию – **secret**). Файл сертификата появится в текущем каталоге (по умолчанию – **/opt/dozor**) .

7. Сконвертируйте экспортированный сертификат в формат PEM, выполнив команду:

   # openssl x509 -in ngfw.crt -outform PEM -out ngfw.pem

8. Импортируйте полученный сертификат в списки доверенных сертификатов браузеров АРМ пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

Примечание

Если серверов фильтрации несколько, экспортируйте сертификат на всех этих серверах. После экспорта выполните импорт всех полученных сертификатов на АРМ пользователей.

Также вы можете добавить время жизни сессии прозрачной аутентификации. Для этого перейдите в раздел **Система > Расширенные настройки > Аутентификация и авторизация** и в полях **Тайм-аут неактивности прозрачной аутентификации** и **Жесткий тайм-аут прозрачной аутентификации** укажите необходимое время в секундах.

Примечание

При использовании negotiate-аутентификации совместно с прозрачным режимом необходимо на всех АРМ добавить FQDN узла Solar NGFW в "Свойства обозревателя" в список "Местная интрасеть"

1. *Откройте **Свойства браузера > Безопасность**.*
2. *Выберите **Местная интрасеть** и нажмите кнопку **Сайты**.*

3. *В открывшемся окне нажмите кнопку **Дополнительно**.*

4. *Добавьте записи **http://ngfw.example.org** и **https://ngfw.example.org**, где **ngfw.example.org** – FQDN проксирующего узла.*

5.11.6. Настройка basic-аутентификации

5.11.6.1. Типы хранилищ для basic-аутентификации

Для basic-аутентификации могут использоваться следующие типы хранилищ:

- локальный список (раздел 5.11.6.2);
- LDAP (раздел 5.11.6.3);
- LDAPS (раздел 5.11.6.4);
- RADIUS (раздел 5.11.6.5);
- Active Directory (раздел 5.11.6.6);
- IMAP (раздел 5.11.6.7);
- POP3 (раздел 5.11.6.8).

5.11.6.2. Настройка параметров для basic-аутентификации по списку пользователей

Для настройки basic-аутентификации по списку пользователей:

1. В разделе **Политика** > **Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:
   - **Режим аутентификации** – **Proxy-Auth**;
   - **Метод аутентификации** – **Basic**.
2. Нажмите **Сохранить** и **Применить**.

5.11.6.3. Настройка параметров для basic-аутентификации с LDAP-сервером

Для настройки basic-аутентификации с источником аутентификации LDAP:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **ldap**.
2. Заполните появившиеся поля, описание которых приведено в документе *Руководство администратора безопасности*.
3. В разделе **Политика** > **Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:

- **Режим аутентификации** – **Proxy-Auth**;
- **Метод аутентификации** – **Basic**.

4. Нажмите **Сохранить** и **Применить**.

Примечание

Рекомендуется использовать в качестве LDAPs-сервера только Active Directory.

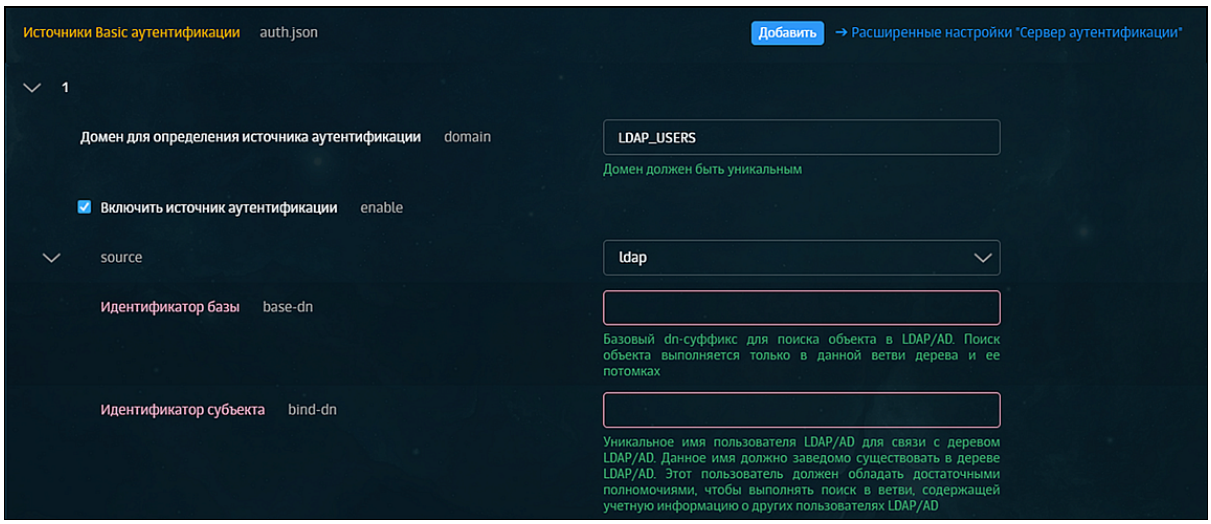


Рис. 5.29. Настройка basic- + LDAP-аутентификации

При выполнении аутентификации вы можете задать более одного домена. Для этого справа от названия секции **Источники Basic-аутентификации** нажмите **Добавить** — появится дополнительная секция для указания соответствующих параметров.

Для удаления добавленной секции используется кнопка , расположенная в выбранном сегменте.

При указании нескольких равноправных серверов (в параметре **Адрес сервера**) для одного домена срабатывает механизм **failover**: сервер аутентификации делает запрос к первому из указанных серверов, при ошибке или таймауте новый запрос будет к следующему из списка серверу. При ошибке на последнем сервере из списка выбирается первый по счету. При превышении заданного времени выполнения запроса он прерывается, даже если еще не все серверы опрошены. Состояние между запросами запоминается – при новом запросе сервер аутентификации сразу обращается к тому серверу, на котором был прерван предыдущий запрос.

Внимание!

*Механизм **failover** поддерживается только для двух равноправных контроллеров домена.*

5.11.6.4. Настройка параметров для basic-аутентификации с LDAPS-сервером

Для настройки basic-аутентификации с источником аутентификации LDAPS:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **ldaps**.

2. Заполните появившиеся поля, описание которых приведено в документе *Руководство администратора безопасности*.

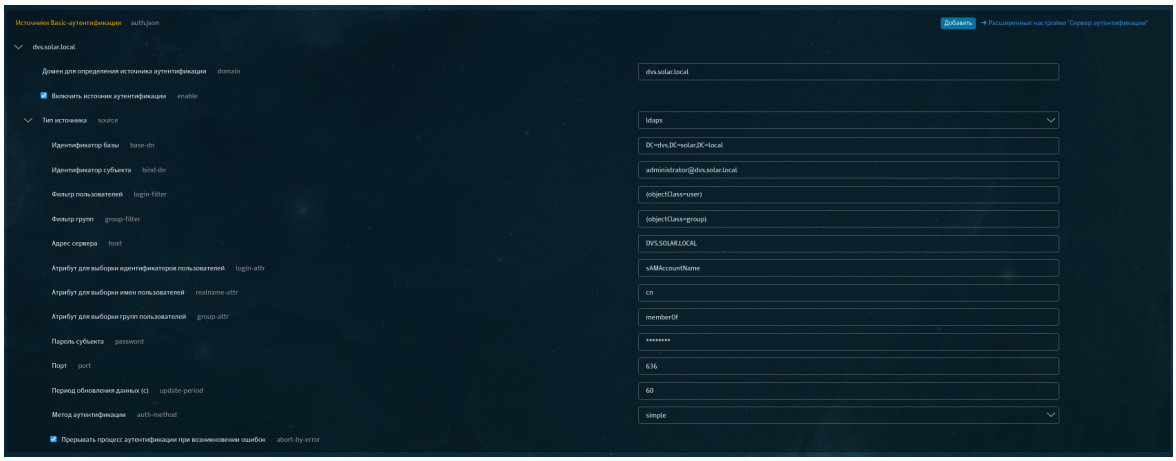


Рис. 5.30. Настройка basic- + LDAPS-аутентификации

3. В разделе **Политика** > **Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:

   - **Режим аутентификации** – **Proxy-Auth**;
   - **Метод аутентификации** – **Basic**.

4. Нажмите **Сохранить** и **Применить**.

Примечание

Рекомендуется использовать в качестве LDAPS-сервера только Active Directory.

При выполнении аутентификации вы можете задать более одного домена. Для этого нажмите **Добавить** справа от названия секции **Источники Basic-аутентификации**, в результате чего появится дополнительная секция для указания соответствующих параметров.

Для удаления добавленной секции используется кнопка  , расположенная в выбранном сегменте.

При указании нескольких равноправных серверов (в параметре **Адрес сервера**) для одного домена срабатывает механизм **failover**: сервер аутентификации делает запрос

к первому из указанных серверов, а при ошибке или таймауте новый запрос происходит к следующему из списка серверу. В случае ошибки на последнем из списка сервере выбирается первый сервер. При превышении заданного времени выполнения запроса он прерывается, даже если еще не все серверы опрошены. Состояние между запросами запоминается – при новом запросе сервер аутентификации сразу обращается к тому серверу, на котором был прерван предыдущий запрос.

Внимание!

*Механизм **failover** поддерживается только для двух равноправных контроллеров домена.*

5.11.6.5. Добавление настроек для basic-аутентификации с RADIUS-сервером

RADIUS-аутентификация — метод basic-аутентификации для удаленного доступа к пользовательским сервисам, виртуальным частным сетям (VPN), точкам беспроводного доступа (Wi-Fi) и т.д.

RADIUS-протокол реализован в виде интерфейса между NAS, который выступает как RADIUS-клиент, и RADIUS-сервером — программным обеспечением, которое может быть установлено на сервере или специализированном устройстве. Таким образом, RADIUS-сервер не взаимодействует напрямую с устройством пользователя, а только через сетевой сервер доступа.

Для настройки RADIUS-аутентификации:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации:

   - Установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **radius**.

   - В списке отобразившихся параметров укажите IP-адрес RADIUS-сервера и пароль (см. Рис.5.31).

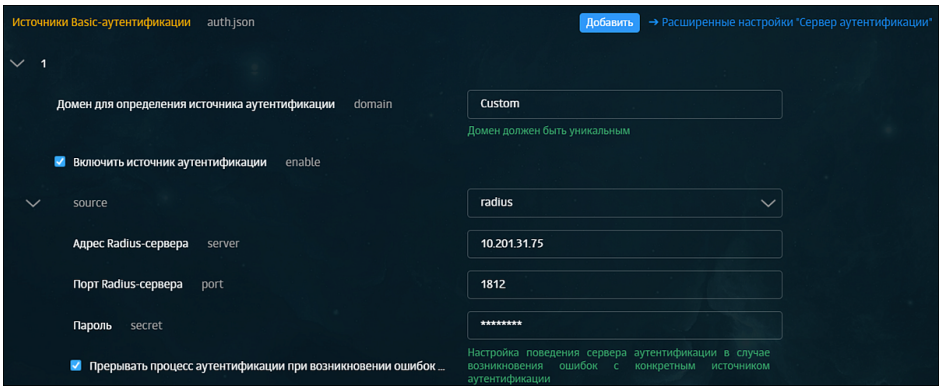


Рис. 5.31. Настройки basic-аутентификации с RADIUS-сервером

2. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:

- **Режим аутентификации – Proxy-Auth**;
- **Метод аутентификации – Basic**.

3. Нажмите **Сохранить** и **Применить**.

5.11.6.6. Добавление настроек для basic-аутентификации со службой Active Directory

Для настройки basic-аутентификации со службой Active Directory:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **ad**.

2. Заполните появившиеся поля аналогично тому, как показано на Рис.5.32:

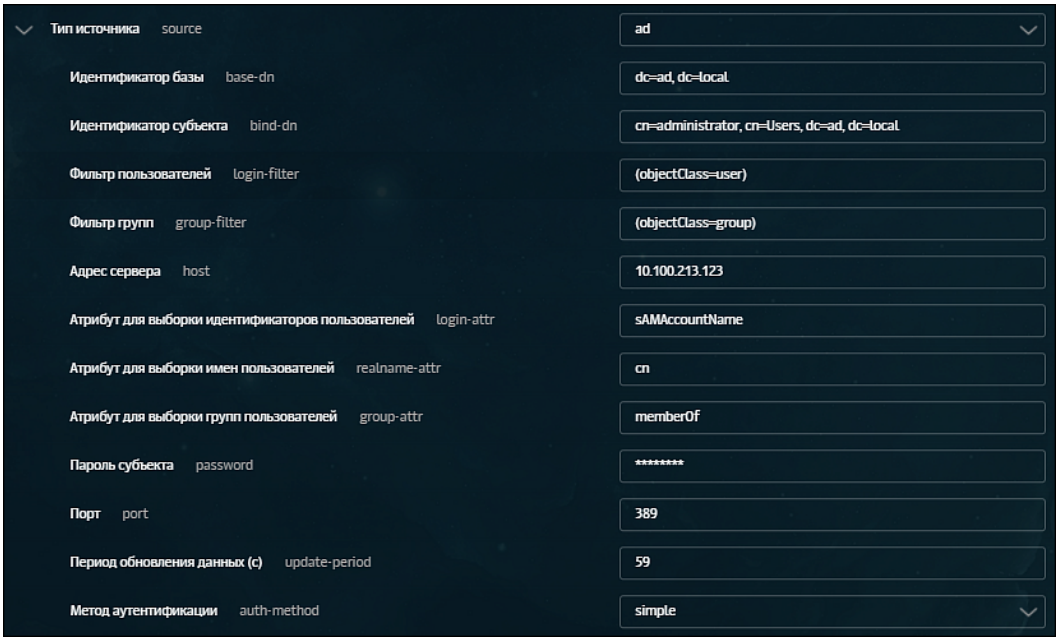


Рис. 5.32. Настройки сервера Active Directory

3. В разделе **Политика** > **Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:

- **Режим аутентификации** – **Proxy-Auth**;
- **Метод аутентификации** – **Basic**.

4. Нажмите **Сохранить** и **Применить**.

Вы можете задать более одного домена. Для этого нажмите **Добавить** справа от названия секции **Источники Basic-аутентификации**, в результате чего появится дополнительная секция для указания соответствующих параметров.

Для удаления добавленной секции используется кнопка  , расположенная в выбранном сегменте.

При указании нескольких равноправных серверов (в параметре **Адрес сервера**) для одного домена срабатывает механизм **failover**: сервер аутентификации делает запрос к первому из указанных серверов, а при ошибке или таймауте новый запрос происходит к следующему из списка серверу. В случае ошибки на последнем сервере, из списка выбирается первый сервер. При превышении заданного времени выполнения запроса он прерывается, даже если еще не все серверы опрошены. Состояние между запросами запоминается – при новом запросе сервер аутентификации сразу обращается к тому серверу, на котором был прерван предыдущий запрос.

Внимание!

*Механизм **failover** поддерживается только для двух равноправных контроллеров домена.*

5.11.6.7. Добавление настроек для basic-аутентификации с IMAP-сервером

Для настройки basic-аутентификации с источником аутентификации IMAP:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **imap**.

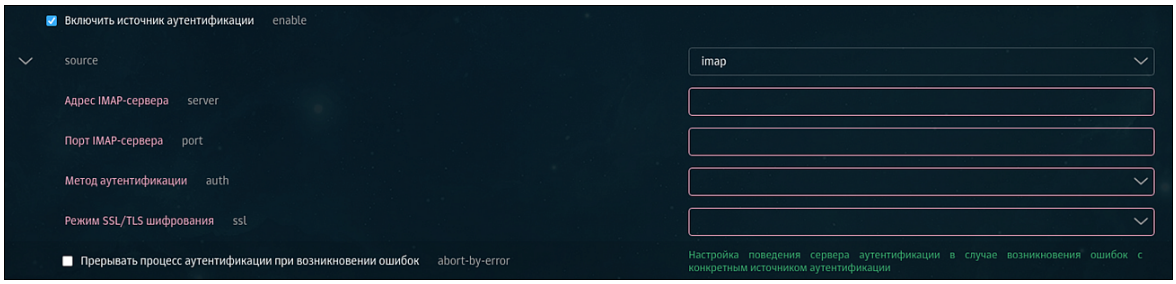


Рис. 5.33. Настройка аутентификации basic + IMAP

2. Задайте параметры:

   - **Адрес IMAP-сервера** – IP-адрес IMAP-сервера;
   - **Порт IMAP-сервера** – порт IMAP-сервера.

   Выберите метод аутентификации и режим SSL/TLS-шифрования из предложенных вариантов.

3. В разделе **Политика** > **Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:

   - **Режим аутентификации** – **Proxy-Auth**;
   - **Метод аутентификации** – **Basic**.

4. Нажмите **Сохранить** и **Применить**.

5.11.6.8. Добавление настроек для basic-аутентификации с POP3-сервером

Для настройки basic-аутентификации с источником аутентификации POP3:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **pop3**.

2. Задайте параметры (**Рис.5.34**):

   - **Адрес POP3-сервера** – IP-адрес POP3-сервера;
   - **Порт POP3-сервера** – порт POP3-сервера.

   Выберите режим SSL/TLS-шифрования из предложенных вариантов.

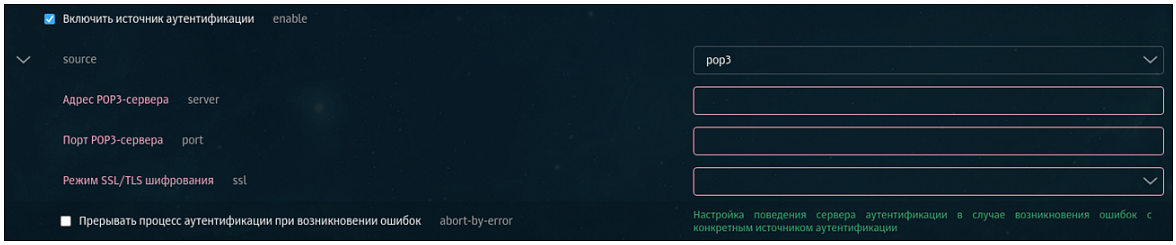


Рис. 5.34. Настройка аутентификации basic + POP3

3. В разделе **Политика** > **Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:

   - **Режим аутентификации** – **Proxy-Auth**;
   - **Метод аутентификации** – **Basic**.

4. Нажмите **Сохранить** и **Применить**.

5.12. Настройка вскрытия SSL-трафика

5.12.1. Настройка вскрытия SSL-трафика (MITM, RSA)

5.12.1.1. Настройка MITM с использованием УЦ организации

Если в организации имеется собственный УЦ, можно использовать его сертификат для вскрытия SSL-трафика. Допустимо использование сертификатов, сгенерированных алгоритмом строго выше SHA-1.

Для выпуска сертификата организации на каждом сервере Solar NGFW с ролью **Фильтр HTTP-трафика**:

1. В CLI перейдите во временный каталог (например, **/var/tmp/**), выполнив команду:

   # cd /var/tmp

2. Создайте ключ RSA, выполнив команду:

 # openssl genrsa -out wp.key -aes256 2048

Во время выполнения команды система потребует назначить пароль для ключа. Введите пароль и запомните его. После ввода подтвердите выбранный пароль.

3. Создайте в текущем каталоге файл с именем **openssl.cnf** и запишите в него данные:

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name
promt=yes
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
countryName_default             = RU

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Moscow

localityName                = Locality Name (eg, city)
localityName_default            = Moscow

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = Organization

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = Dept

commonName                  = Common Name (eg, your name or your server\'s hostname)
commonName_default              = proxy.org.com

emailAddress                = Email Address
emailAddress_default            = support@org.com

[ v3_req ]
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = proxy.org.com
IP.0 = 192.168.10.15
```

Выделенные значения параметров следует заменить на актуальные значения в организации:

- **countryName_default** – двухбуквенный код страны;
- **stateOrProvinceName_default** – регион;
- **localityName_default** – город;
- **organizationName_default** – название организации;
- **organizationalUnitName_default** – название подразделения, департамента и т. д.;
- **commonName_default** – FQDN сервера, на котором происходит настройка;

- **emailAddress_default** – контактный адрес электронной почты организации;
- **DNS.0** – значение, указанное в параметре **commonName_default**;
- **IP.0** – IP-адрес сервера, на котором происходит настройка.

4. Сгенерируйте запрос на подпись сертификата, выполнив команду:

   # openssl req -new -key wp.key -out name.csr -config openssl.cnf

   В процессе выполнения команды система потребует ввести пароль, заданный на шаге 2.

5. На сервере организации, имеющем роль CA (Certification Authority), проверьте используемый алгоритм шифрования. Для этого откройте программу **Командная строка** от имени администратора и выполните в ней команду:

   certutil -getreg ca\csp\CNGHashAlgorithm

   Если значение параметра **REG_SZ** равно **SHA1**, выполните команды:

   certutil -setreg ca\csp\CNGHashAlgorithm SHA256

   net stop CertSvc && net start CertSvc

6. Снова выпишите корневой сертификат и перезапустите службу Certificate Services, выполнив команды:

   certutil -renewCert ReuseKeys

   net stop CertSvc && net start CertSvc

7. Зайдите на портал УЦ Windows.

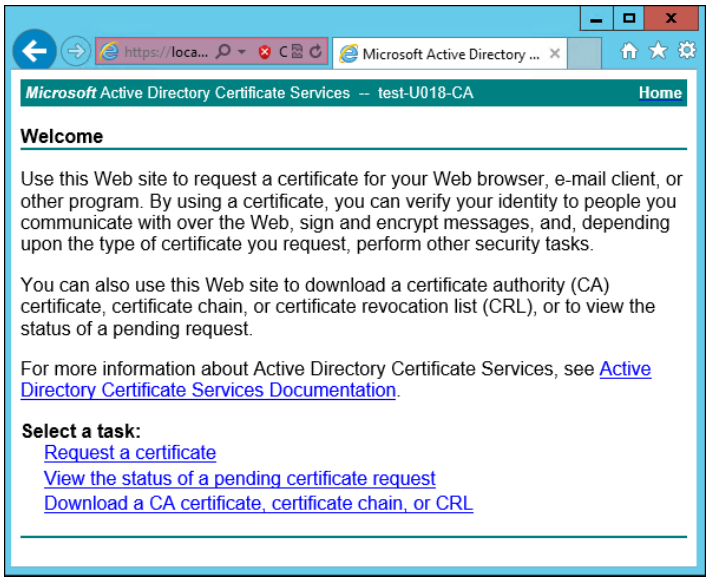


Рис. 5.35. Экран приветствия УЦ Windows

8. Нажмите **Request a certificate**.

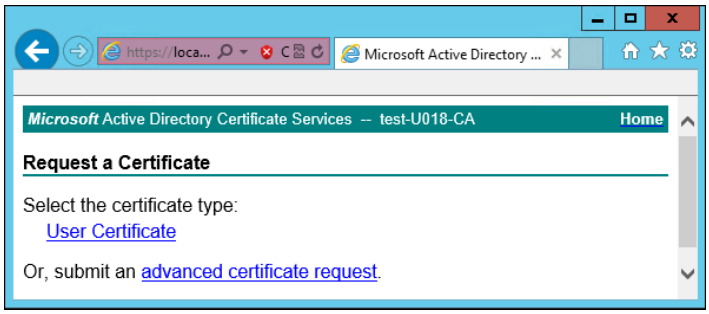


Рис. 5.36. Экран запроса сертификата

9. Нажмите **advanced certificate request**.

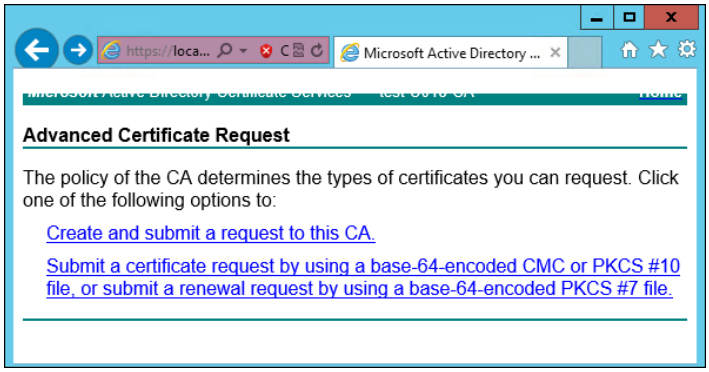


Рис. 5.37. Экран особого запроса сертификата

10. Нажмите **Submit a certificate request by using...**.

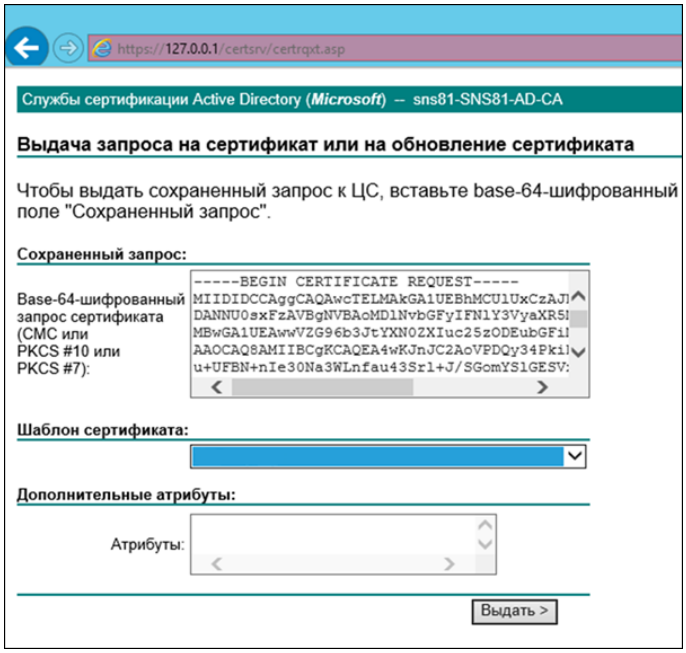


Рис. 5.38. Экран атрибутов сертификата

11. Выберите шаблон сертификата **Subordinate authority** (**Подчинённый центр сертификации**) и вставьте в поле **Base-64** содержимое файла, созданного на шаге 4. Нажмите **Выдать**.

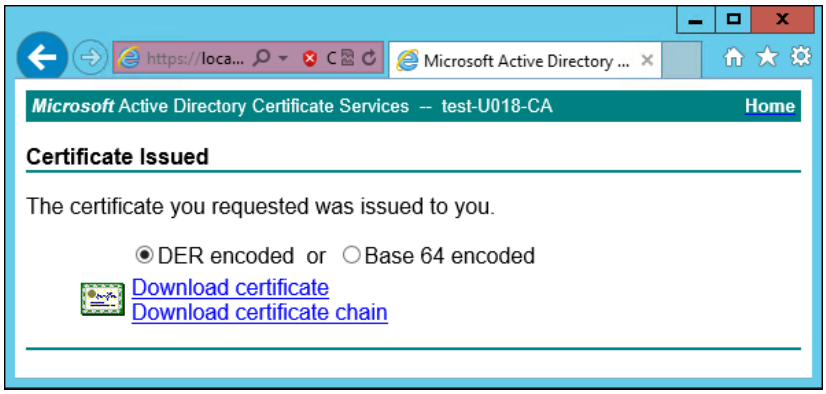


Рис. 5.39. Экран выдачи сертификата

12. Нажмите **Download certificate**. Сохраните файл сертификата с именем **wp.cer** во временный каталог, выбранный в шаге 1.

13. Перейдите на главную страницу портала УЦ и нажмите **Download a CA certificate, certificate chain or CRL**. Сохраните сертификат УЦ с именем **ca.cer** в тот же каталог.

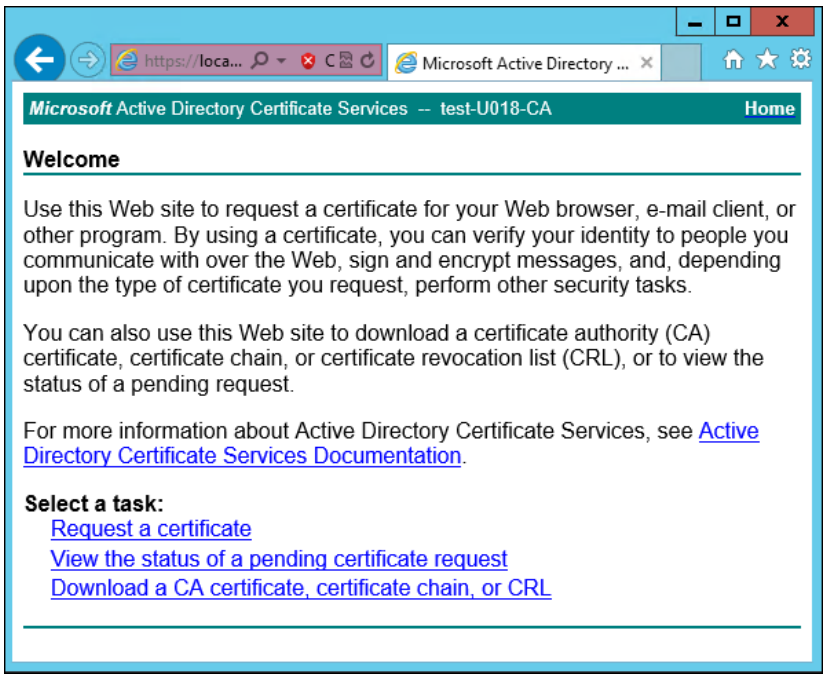


Рис. 5.40. Экран приветствия УЦ Windows

14. Вернитесь в CLI Solar NGFW, перейдите в выбранный временный каталог и сконвертируйте загруженные сертификаты в формат PEM, выполнив команды:

 # openssl x509 -inform der -in wp.cer -out wp.pem

 # openssl x509 -inform der -in ca.cer -out ca.pem

15. Объедините сертификаты и ключ в сертификат pkcs12, выполнив команду:

 # openssl pkcs12 -export -out wp.p12 -inkey wp.key -in wp.pem -certfile ca.pem

Во время выполнения команды система потребует ввести пароль.

16. Импортируйте Java-хранилище сертификатов, выполнив команду вида:

 # keytool -importkeystore -deststorepass <password> -destkeypass <password> -destkeystore <wpN>.jks -srckeystore wp.p12 -srcstorepass <password>

где **<password>** – выбранный пароль, а **<wpN>** – имя сертификата для текущего сервера (например, **wp1**).

17. Скопируйте Java-хранилище в каталог Solar NGFW, выполнив команду вида:

 # cp <wpN>.jks /opt/dozor/skvt/var/lib/

где **<wpN>** – значение, выбранное в предыдущем шаге.

18. Смените владельца хранилища, выполнив команду вида:

 # chown dozor:dozor /opt/dozor/skvt/var/lib/<wpN>.jks

19. Проверьте, что сертификат находится в хранилище, выполнив команду вида:

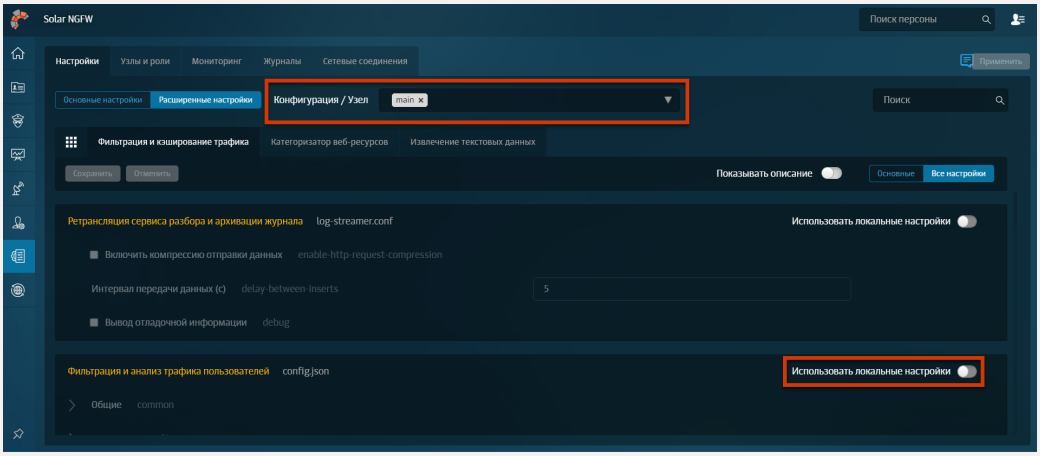
 # keytool -list -keystore /opt/dozor/skvt/var/lib/<wpN>.jks

О наличии сертификата в хранилище будет свидетельствовать вывод следующего вида:

```
1, Jul 10, 2018, PrivateKeyEntry,
Certificate fingerprint (SHA1): B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
```

20. **Примечание**

*Если для каждого фильтра необходимо выдать свой сертификат, перед выполнением данного шага в разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей** укажите в настройках соответствующий узел и используйте локальные настройки.*



Далее выполните шаг инструкции для каждого фильтра.

В GUI в разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика** > **Фильтрация и анализ трафика пользователей** раскройте группу параметров **Сертификаты** и задайте значения параметров:

- **Путь к хранилищу ключей** – **/opt/dozor/skvt/var/lib/<wpN>.jks** ;
- **Пароль к хранилищу ключей** – пароль;
- **Общее имя сертификата** – 1.

21. Перезапустите сервис **skvt-wizor**, выполнив в CLI команды:

 # /opt/dozor/bin/shell

 # dsctl restart skvt-wizor

22. Импортируйте полученный сертификат в списки доверенных сертификатов браузеров АРМ пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

Примечание

Если серверов фильтрации несколько, экспортируйте сертификат на всех этих серверах. После экспорта выполните импорт всех полученных сертификатов на АРМ пользователей.

5.12.1.2. Настройка хранилища сертификатов Windows для Mozilla Firefox

Браузер Mozilla Firefox по умолчанию использует собственное (не стандартное) хранилище сертификатов Windows. Процедура ручного добавления сертификатов Windows на АРМ пользователей, использующих этот браузер, как и процедура ручной настройки каждого браузера для использования стандартного хранилища, может быть весьма трудоемкой. Поэтому рекомендуется автоматически настроить браузеры пользователей с помощью js-скрипта, распространяемого механизмом Group Policy в домене. Для этого:

1. Создайте файл скрипта с именем **Enable sec-enterprise_roots.js** и добавьте в него строку:

```
pref ("security.enterprise_roots.enabled", true);
```

2. С помощью Group Policy распространите полученный скрипт по АРМ пользователей, использующих Mozilla Firefox. Путь, по которому должен быть размещен скрипт (в зависимости от разрядности ОС АРМ):

- **C:\Program Files\Mozilla Firefox\defaults\pref**
- **C:\Program Files(x86)\Mozilla Firefox\defaults\pref**

При запуске браузера его конфигурация будет обновлена. Проверить, что браузер настроен правильно, можно введя в адресной строке **about:config** и выполнив поиск по подстроке **roots**. Параметр **security.enterprise_roots.enabled** должен иметь значение **true**.

5.12.2. Настройка вскрытия SSL-трафика (MITM, ECDSA)

При установке Solar NGFW на новую систему будет создан JKS-контейнер, подписанный с помощью алгоритма ECDSA.

Примечание

При установке Solar NGFW автоматически будет добавлен сертификат от Минцифры РФ.

5.12.2.1. Получение сертификата

Для настройки вскрытия шифрованных соединений АРМ пользователей корпоративной сети с ресурсами сети Интернет:

1. Настройте прокси в браузере.
2. Перейдите по адресу: **http://mitm.it:2281/cert/manual**.
3. В зависимости от ОС выберите инструкцию и по ней выполните загрузку и установку сертификата.

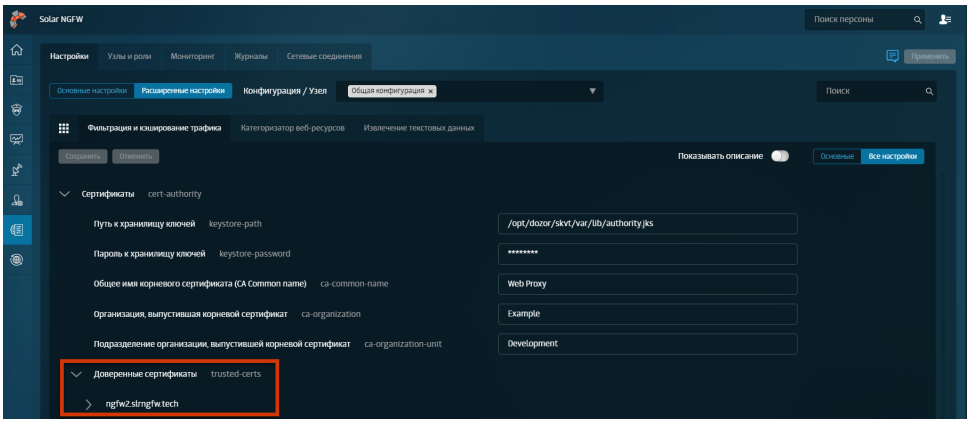
5.12.2.2. Настройка MITM без УЦ организации

В Solar NGFW предусмотрена возможность установления доверительного отношения к загруженным сертификатам в формате PEM вручную через интерфейс. Для этого в разделе **Система > Настройки > Расширенные настройки> Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей > Сертификаты > Доверенные сертификаты** нажмите кнопку **Добавить**. После добавления сертификат можно загрузить или удалить.

Примечание

Для наименования доверенного сертификата используйте только латинские буквы. С названием, написанным кириллицей, сертификат работать не будет.

Возможность скачать загруженный сертификат появляется после обновления страницы.



Для настройки вскрытия шифрованных соединений APM пользователей корпоративной сети с ресурсами сети Интернет на каждом узле с ролью **Фильтр HTTP-трафика** выполните приведенные ниже шаги:

1. В CLI экспортируйте сертификат УЦ Solar NGFW, выполнив команду (в одну строку):

   # keytool -exportcert -rfc -keystore /opt/dozor/skvt/var/lib/authority.jks -alias "ngfw" > ngfw.crt

   Во время выполнения команды будет запрошен пароль (по умолчанию – **secret**). Файл сертификата появится в текущем каталоге (по умолчанию – **/opt/dozor**) .

2. Сконвертируйте экспортированный сертификат в формат PEM, выполнив команды:

   # cd /opt/dozor

   # openssl x509 -in ngfw.crt -outform PEM -out ngfw.pem

3. Импортируйте полученный сертификат в списки доверенных сертификатов браузеров APM пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

   Примечание

   Если серверов фильтрации несколько, экспортируйте сертификат на всех этих серверах. После экспорта выполните импорт всех полученных сертификатов на APM пользователей.

5.12.2.3. Настройка MITM с использованием УЦ организации

Для настройки вскрытия SSL-трафика с использованием сертификата организации (алгоритм цифровой подписи ECDSA) на каждом сервере Solar NGFW с ролью **Фильтр HTTP-трафика**:

1. В CLI перейдите во временный каталог (например, **/var/tmp/**), выполнив команду:

   # cd /var/tmp

2. Создайте ключ ECDSA, выполнив команду:

   # openssl ecparam -name secp521r1 -genkey -noout -out wp.key

3. Создайте в текущем каталоге файл с именем **openssl.cnf** и запишите в него данные:

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name
promt=yes
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
countryName_default             = RU

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Moscow

localityName                = Locality Name (eg, city)
localityName_default            = Moscow

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = Organization

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = Dept

commonName                  = Common Name (eg, your name or your server\'s hostname)
commonName_default              = proxy.org.com

emailAddress                = Email Address
emailAddress_default            = support@org.com

[ v3_req ]
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = proxy.org.com
IP.0 = 192.168.10.15
```

Выделенные значения параметров следует заменить на актуальные значения в организации:

- **countryName_default** – двухбуквенный код страны;
- **stateOrProvinceName_default** – регион;
- **localityName_default** – город;
- **organizationName_default** – название организации;
- **organizationalUnitName_default** – название подразделения, департамента и т. д.;
- **commonName_default** – FQDN сервера, на котором происходит настройка;
- **emailAddress_default** – контактный адрес электронной почты организации;
- **DNS.0** – значение, указанное в параметре **commonName_default**;

- **IP.0** – IP-адрес сервера, на котором происходит настройка.

4. Сгенерируйте запрос на подпись сертификата, выполнив команду:

   # openssl req -new -sha256 -key wp.key -out wp.req -config openssl.cnf

5. На сервере организации, имеющем роль CA (Certification Authority), проверьте используемый алгоритм шифрования. Для этого откройте программу **Командная строка** от имени администратора и выполните в ней команду:

   certutil -getreg ca\csp\CNGHashAlgorithm

   Если значение параметра **REG_SZ** равно **SHA1**, выполните команды:

   certutil -setreg ca\csp\CNGHashAlgorithm SHA256

   net stop CertSvc && net start CertSvc

6. Снова выпишите корневой сертификат и перезапустите службу Certificate Services, выполнив команды:

   certutil -renewCert ReuseKeys

   net stop CertSvc && net start CertSvc

7. Перейдите в настройки центра сертификации и добавьте шаблон **Подчиненный центр сертификации**.

8. Выпустите сертификат, выполнив следующую команду:

   certreq -submit -attrib "CertificateTemplate: SubCA" c:\wp.req

   В появившемся окне выберите центр сертификации и сохраните файл под именем **wp.cer**.

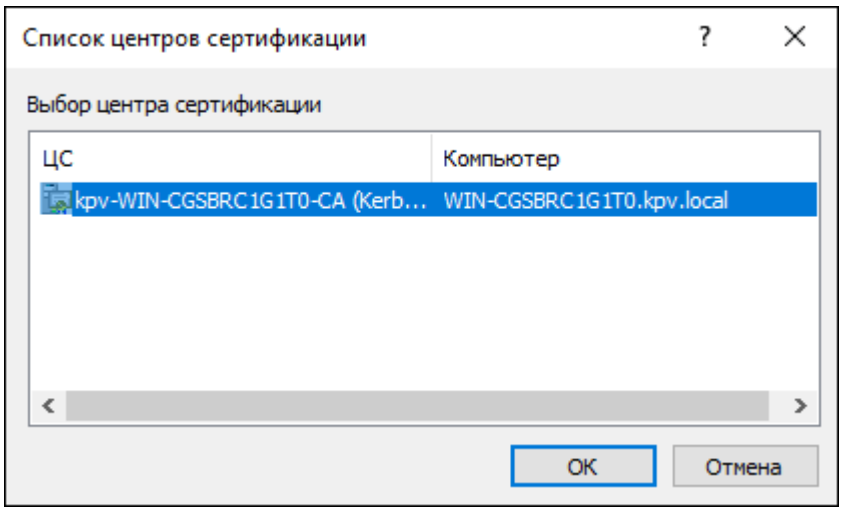


Рис. 5.41. Выбор центра сертификации

9. В CLI загрузите сертификат УЦ, выполнив команду:

certutil -ca.cert C:\ca.cer

10. Скопируйте файл **wp.cer** в каталог **/var/tmp** сервера Solar NGFW с ролью **Фильтр HTTP-трафика** и переименуйте его в **wp.pem**.

11. Сконвертируйте полученный сертификат УЦ в формат PEM, выполнив команду:

    # openssl x509 -inform der -in ca.cer -out ca.pem

12. Объедините сертификаты и ключ в сертификат pkcs12, выполнив команду:

    # openssl pkcs12 -export -out wp.p12 -inkey wp.key -in wp.pem -certfile ca.pem

    Во время выполнения команды система потребует ввести пароль.

13. Импортируйте Java-хранилище сертификатов, выполнив команду вида:

    # keytool -importkeystore -deststorepass <password> -destkeypass <password> -destkeystore <wpN>.jks -srckeystore wp.p12 -srcstorepass <password>

    где **<password>** – выбранный пароль, а **<wpN>** – имя сертификата для текущего сервера (например, **wp1**).

14. Скопируйте Java-хранилище в каталог Solar NGFW, выполнив команду вида:

    # cp <wpN>.jks /opt/dozor/skvt/var/lib/

    где **<wpN>** – значение, выбранное в предыдущем шаге.

15. Смените владельца хранилища, выполнив команду вида:

    # chown dozor:dozor /opt/dozor/skvt/var/lib/<wpN>.jks

16. Проверьте, что сертификат находится в хранилище, выполнив команду вида:

    # keytool -list -keystore /opt/dozor/skvt/var/lib/<wpN>.jks

    О наличии сертификата в хранилище будет свидетельствовать вывод следующего вида:

    ```
    1, Jul 10, 2018, PrivateKeyEntry,
    Certificate fingerprint (SHA1): B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
    ```

17. В GUI в разделе **Система > Расширенные настройки > Фильтрация и анализ трафика пользователей** раздела **Фильтрация и кэширование трафика** раскройте группу параметров **Сертификаты**. Задайте значения параметров:

    - **Путь к хранилищу ключей** – **/opt/dozor/skvt/var/lib/<wpN>.jks** ;
    - **Пароль к хранилищу ключей** – пароль;
    - **Общее имя корневого сертификата (CA Common name)** – имя удостоверяющего центра (УЦ);

- **Организация, выпустившая корневой сертификат** – название организации;
- **Подразделение организации, выпустившей корневой сертификат** – название подразделения;

18. Перезапустите сервис **skvt-wizor**, выполнив в CLI команды:

    # /opt/dozor/bin

    # dsctl restart skvt-wizor

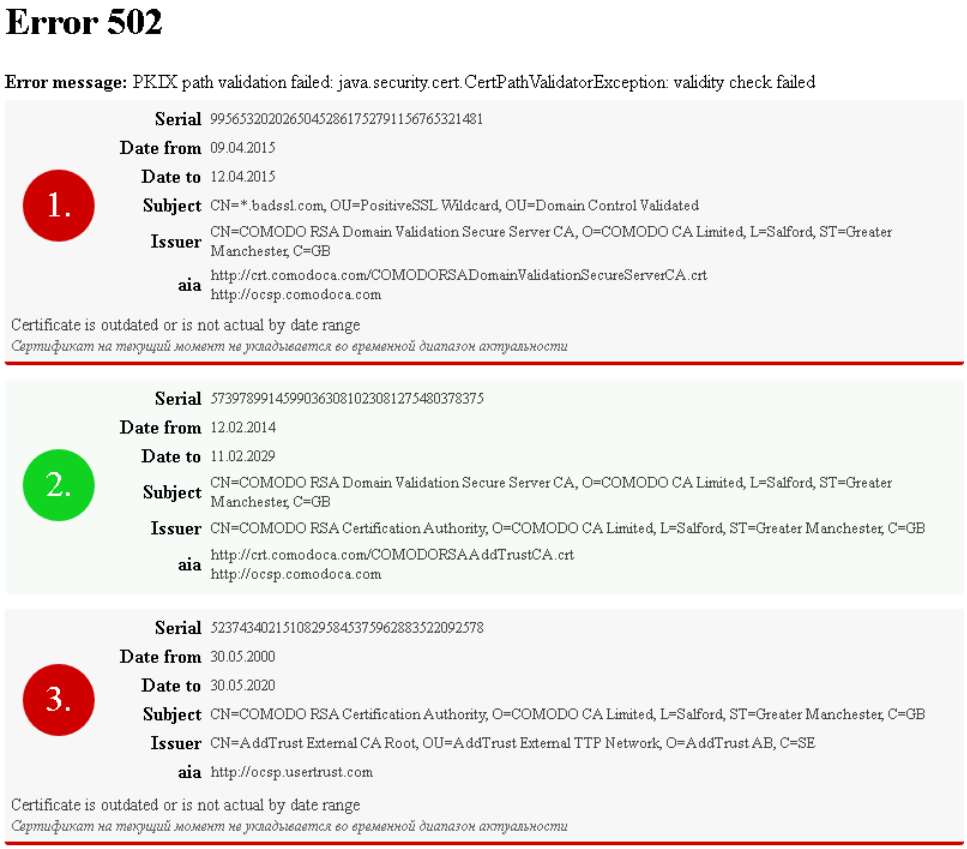
19. Импортируйте полученный сертификат в списки доверенных сертификатов браузеров АРМ пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

Примечание

Если серверов фильтрации несколько, экспортируйте сертификат на всех этих серверах. После экспорта выполните импорт всех полученных сертификатов на АРМ пользователей.

5.12.2.4. Диагностика проблем с сертификатами

При возникновении ошибок во время вскрытия сертификата или цепочки сертификатов в Solar NGFW будет отображен список с загруженными сертификатами и отчет об успехе или ошибке их загрузки. Для удобства в цепочке под каждым сертификатом с проблемой отображается текстовое описание ошибки на английском и русском языках.



Ошибка возникает, если:

- невозможно построить цепочку сертификатов;
- время действия сертификата истекло;
- имя владельца, прописанное в сертификате, не соответствует имени ресурса, предоставившего его.

В цепочке сертификатов для каждого сертификата отображаются поля:

- серийный номер,
- даты начала и окончания действия сертификата,
- имя владельца сертификата,
- имя издателя сертификата,
- адрес сервиса онлайн-получения статуса сертификата (по протоколу OCSP).

5.13. Настройка вскрытия шифрованного трафика

Для защиты локального трафика от прослушивания и MITM-атак при обращении к ресурсам сети Интернет по протоколу HTTP используется TLS-порт Solar NGFW – 2443.

Для APM, использующих TLS-порт, все передаваемые данные на участке клиент-прокси шифруются. При установлении TLS-соединения браузер APM проверяет сертификат Solar NGFW, и соединение устанавливается только при наличии доверенного сертификата. Соединение на участке прокси-назначение осуществляется в обычном режиме, шифрование не выполняется.

Для работы TLS-порта требуется следующее:

1. Solar NGFW должен обладать сертификатом, подписанным доверенным УЦ. Работа с самоподписанными сертификатами не поддерживается. Можно использовать УЦ организации, в этом случае необходимо настроить Solar NGFW на использование настроенного системным администратором ключа и сертификата (см. раздел 5.12.1.1). Системный администратор должен добавить УЦ, подписавший ключ Solar NGFW в список доверенных у пользователей APM.

   Solar NGFW по умолчанию создает свой УЦ и сертификат. Сертификат и ключ УЦ Solar NGFW находятся в файле **/opt/dozor/skvt/var/lib/authority.jks**.

   Сертификат можно экспортировать с помощью команды:

   keytool --exportcert -rfc -keystore /opt/dozor/skvt/var/lib/authority.jks -alias "ngfw" > ngfw.crt

   Во время выполнения команды будет запрошен пароль (по умолчанию – **secret**). Файл сертификата появится в текущем каталоге (по умолчанию – **/opt/dozor**).

   Полученный сертификат добавьте в список доверенных на APM, использующих TLS-порт (в случае выбора УЦ Solar NGFW).

2. Сконвертируйте экспортированный сертификат в формат PEM, выполнив команду:

openssl x509 -in ngfw.crt -outform PEM -out ngfw.pem

3. В GUI Solar NGFW в разделе **Политика > Контентная фильтрация > Вскрытие HTTPS** создайте правило для вскрытия HTTPS-трафика. Нажмите **Сохранить** и **Применить политику**.

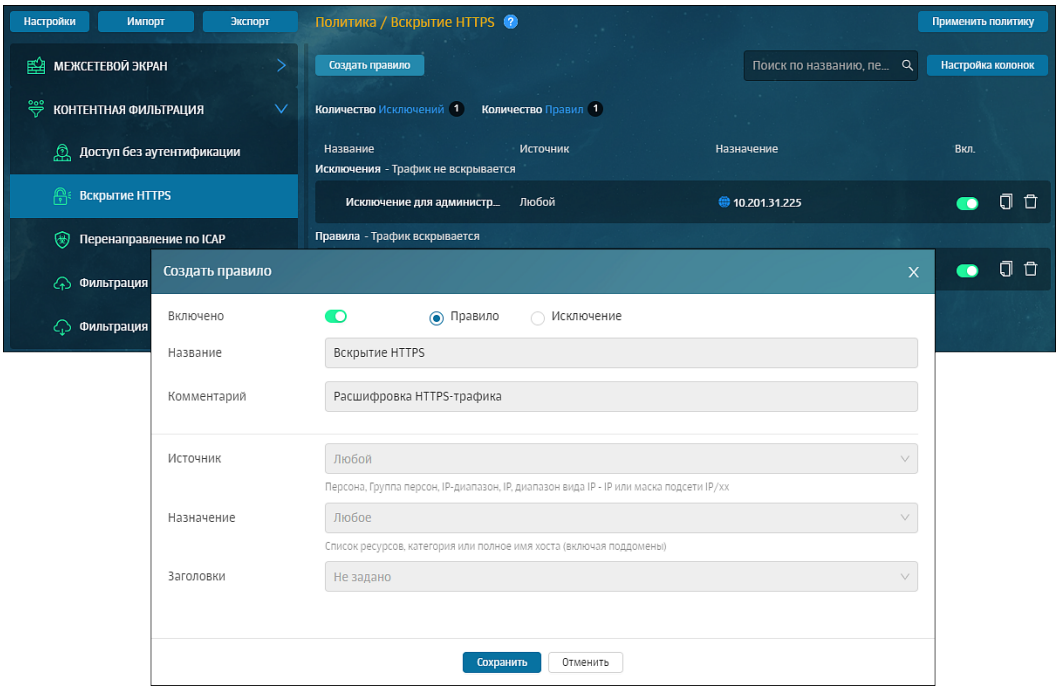


Рис. 5.42. Создание правила в слое политики «Вскрытие HTTPS»

4. Настройка прокси в браузере должна быть выполнена с помощью PAC-файла, поскольку через обычную конфигурацию такая настройка не поддерживается. В настройке прокси требуется использовать FQDN Solar NGFW. Задача создания PAC-файла ложится на системного администратора организации.

5. Работа TLS-порта поддерживается только для браузеров Mozilla Firefox и Google Chrome и для протокола HTTP.

5.14. Настройка WCCP

Перед настройкой WCCP настройте прозрачный режим работы Solar NGFW (см. раздел 5.11.5).

5.14.1. Настройка оборудования Cisco

Для настройки маршрутизатора Cisco:

1. Настройте сетевые интерфейсы маршрутизатора так, чтобы один интерфейс находился в локальной подсети организации, в которой размещен Solar NGFW, а другой – в подсети провайдера сети Интернет.

2. Авторизуйтесь в CLI маршрутизатора и создайте обратную петлю, отвечающую за GRE-туннель, выполнив команды:

cisco> enable

cisco# configure terminal

cisco(config)# interface loopback 1

cisco(config)# ip address <loopback-IP> 255.255.255.255

где **<loopback-IP>** – IP-адрес обратной петли (выбирается сетевым администратором организации на его усмотрение).

3. Создайте список управления доступом со списком адресов WCCP-клиентов, выполнив команды:

   cisco(config)# access-list 10 permit <NGFW-IP>

   cisco(config)# ip wccp web-cache group-list 10

   где **<NGFW-IP>** – IP-адрес узла фильтрации Solar NGFW.

4. Создайте список управления доступом с правилами маршрутизации трафика на Solar NGFW, выполнив команды:

   cisco(config)# ip access-list extended WCCP_ACCESS

   cisco(config-ext-nacl)# remark ACL for HTTP/HTTPS

   cisco(config-ext-nacl)# remark NGFW bypass WCCP

   cisco(config-ext-nacl)# deny ip host <NGFW-IP> any

   cisco(config-ext-nacl)# remark LAN clients proxy port 80/443

   cisco(config-ext-nacl)# permit tcp <LAN-IP> <INV-LAN-MASK> any eq www 443

   cisco(config-ext-nacl)# remark all others bypass WCCP

   cisco(config-ext-nacl)# deny ip any any

   где **<NGFW-IP>** – IP-адрес узла фильтрации Solar NGFW, **<LAN-IP>** – пространство IP-адресов локальной сети, в которой находятся АРМ сотрудников организации (например, **192.168.100.0**), **<INV-LAN-MASK>** – инверсная маска этой сети (в данном примере – **0.0.0.255**).

5. Установите правила перенаправления для WCCP, выполнив команды:

   cisco(config)# ip wccp web-cache redirect-list WCCP_ACCESS

   cisco(config)# ip wccp 70 redirect-list WCCP_ACCESS

6. Настройте перенаправление на внутреннем интерфейсе, выполнив команды:

   cisco(config)# interface <ifname>

   cisco(config-if)# ip wccp web-cache redirect in

   cisco(config-if)# ip wccp 70 redirect in

где **<ifname>** – имя интерфейса маршрутизатора Cisco, находящегося в локальной сети.

7. Завершите конфигурирование маршрутизатора и сохраните конфигурацию, выполнив команды:

   cisco(config)# end

   cisco# copy running-config startup-config

5.14.2. Настройка оборудования Solar NGFW

Для настройки Solar NGFW настройте GRE-туннель, выполнив в CLI команды:

iptunnel add wccp0 mode gre remote <CISCO-IP> local <NGFW-IP> dev eth0

ip link set wccp0 up

где **<CISCO-IP>** – IP-адрес маршрутизатора Cisco, **<NGFW-IP>** – IP-адрес узла фильтрации Solar NGFW.

5.14.3. Проверка работоспособности WCCP

Для проверки работоспособности настроенной схемы авторизуйтесь в CLI маршрутизатора и выполните команду:

show ip wccp

На экране будет отображен вывод следующего вида:

```
Global WCCP information:
    Router information:
        Router Identifier:                  192.168.30.138
        Protocol Version:                   2.0
    Service Identifier: web-cache
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           0
        Redirect access-list:               WCCP_ACCESS
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
        Group access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
    Service Identifier: 70
        Number of Cache Engines:            1
        Number of routers:                  1
        Total Packets Redirected:           0
        Redirect access-list:               WCCP_ACCESS
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
```

Если схема настроена правильно, параметр **Number of Cache Engines** для обоих потоков WCCP будет отличен от нуля.

5.15. Настройка SNMP

SNMP (Simple Network Management Protocol) – простой протокол управления сетью, базовый инструмент мониторинга сетевого оборудования. Работа протокола заключается в обмене сообщениями между компонентами систем мониторинга. SNMP-сервер часто используется как основной инструмент мониторинга оборудования в составе разных коммерческих или open source решений из-за простоты внедрения и эксплуатации.

Чтобы настроить протокол SNMP:

1. Перейдите в раздел **Система > Узлы и роли** и назначьте узлу роль **Агент SNMP**. Нажмите кнопку **Применить**.
2. В разделе **Система > Основные настройки > Мониторинг > SNMP агент мониторинга**:
   - В поле **Конфигурация / Узел** выберите узел main.
   - Включите переключатель **Использовать локальные настройки**.
   - Укажите необходимые настройки:
     - **Имя устройства** – произвольное имя отслеживаемого устройства.
     - **Местоположение** – физическое местоположение отслеживаемого устройства.
     - **Контакт** – текстовое поле, которое помогает персоналу определить, с кем необходимо связаться в случае какого-либо сбоя.
     - **IP-адрес** – IP-адрес, на котором агент будет ожидать запросы от внешних серверов мониторинга.
     - **Порт** – номер порта, на котором агент будет ожидать запросы от внешних серверов мониторинга.
     - **Протокол** – протокол, на котором агент будет ожидать запросы от внешних серверов мониторинга.
     - **Версия протокола** – при выборе SNMPv2c доступна настройка параметров: **Имя сервера**, **Сообщество**, **Адрес сервера/сети**. При выборе SNMPv3 доступна настройка параметров по уровням безопасности.

5.16. Настройка стороннего ICAP-прокси

В Solar NGFW предусмотрена возможность интеграции со сторонними прокси-серверами по протоколу ICAP.

Для настройки интеграции в настройках стороннего прокси-сервера в качестве ICAP-URI укажите значение вида **icap://<NGFW_IP>:2272/icaphandle**, где **<NGFW_IP>** – IP-адрес сервера фильтрации Solar NGFW.

Чтобы включить интеграцию по протоколу ICAP:

1. Перейдите в раздел **Система > Настройки**.

2. Откройте расширенные настройки.

3. В блоке **Обработка перехваченных данных** выберите **Фильтрация и кэширование трафика**.

4. В блоке **Фильтрация и анализ трафика пользователей** откройте **ICAP > Интерфейс ICAP-сервера**.

5. В поле **IP-адрес** введите внешний IP.

6. Последовательно нажмите кнопки **Сохранить** и **Применить**.

Описание настроек политики фильтрации приведено в документе *Руководство администратора безопасности*, раздел *Управление политиками*.

5.17. Настройка категоризаторов и стоп-листов

5.17.1. Используемые в системе категоризаторы

В Solar NGFW для фильтрации веб-трафика по умолчанию используются категоризатор **webCat**, разработанный **Ростелеком-Солар**, и пользовательский категоризатор **customlist**. Администратор также может подключить и другие внешние категоризаторы, например **iAdmin** и пр. в разделе расширенных настроек **Категоризатор веб-ресурсов**.

Примечание

Для включенных категоризаторов значение должно быть больше или равно 1.

Опрос происходит в порядке их приоритета. Чем меньше установленное значение – тем выше приоритет. Так, категоризатор со значением 1 будет опрошен раньше, чем категоризатор со значением 2.

Чтобы отключить категоризатор, установите значение 0.

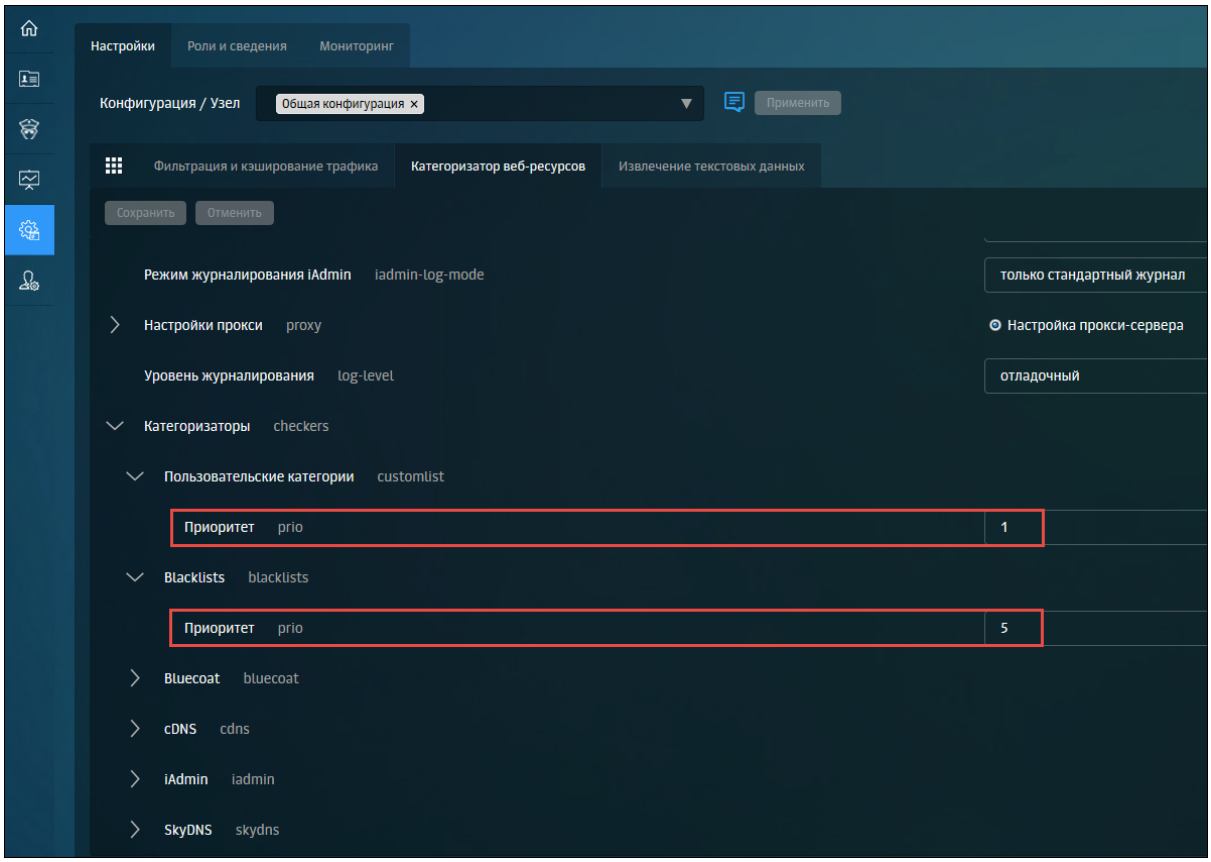


Рис. 5.43. Настройки категоризатора веб-ресурсов

Определение категории выполняется на основе URL веб-ресурса, к которому был выполнен запрос (раздел **Политика** > **База категоризации**).

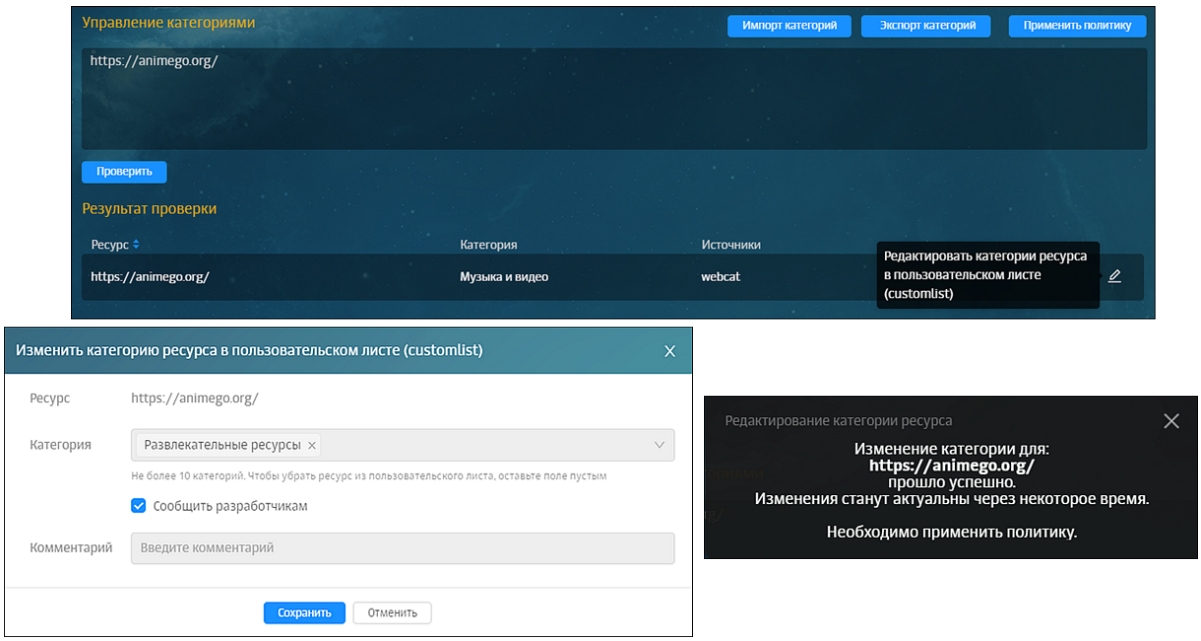


Рис. 5.44. Переопределение категории URL ресурса

Для изменения категории веб-ресурса после ее определения:

- Нажмите значок редактирования в строке ресурса и выберите новую категорию в раскрывающемся списке **Категория**.
- Установите флажок **Сообщить разработчикам** и нажмите кнопку **Сохранить**. В окне браузера отобразится уведомление об успешном переопределении категории.

5.17.2. Настройка категоризатора webCat

Для настройки категоризатора:

1. Проверьте наличие лицензии на этот модуль в окне с информацией о лицензии.
2. Назначьте узлу роль **Анализатор трафика** в разделе **Система > Узлы и роли**.
3. Нажмите кнопку **Применить**.

5.17.3. База SkyDNS

Файл базы данных записан в формате SQLite (компактная встраиваемая реляционная база данных). Встраиваемая база означает, что SQLite не использует парадигму клиент-сервер, база SQLite не является отдельно работающим процессом, с которым взаимодействует программа, а предоставляет библиотеку, с которой программа компонуется, и база становится составной частью программы. Таким образом, в качестве протокола обмена используются вызовы функций (API) библиотеки SQLite. Такой подход уменьшает накладные расходы, время отклика и упрощает программу. SQLite хранит базу данных в единственном файле базы данных.

База SQLite может работать в двух режимах:

- rollback – файл нельзя изменить, когда его кто-то читает или изменяет в данный момент;
- wal – режим позволяет одновременно читать и изменять файл базы, но при этом рядом с базой создаются служебные файлы.

Возможны два варианта подключения к базе категоризации SkyDNS:

- В интерактивном режиме через Categorization API. API не предназначено для доступа к нему конечных пользователей интегрируемой системы, а должно запрашиваться с промежуточного сервера интегрируемой системы.
- Бинарные файлы с ежедневным обновлением. Бинарные файлы содержат хэшированные файлы ресурсов и предназначены для использования в высоконагруженных системах, где требуется категоризация ресурсов в реальном времени.

Для доступа к API можно использовать адреса:

- • z.api.skydns.ru – для тестирования и анонимного доступа (количество запросов ограничено 10 запросами в минуту);
- • x.api.skydns.ru – для зарегистрированных пользователей (без ограничения числа запросов).

Примечание

Для запросов к x.api.skydns.ru необходимо использовать учетную запись, которая используется для Basic-аутентификации.

5.17.3.1. Установка контейнера Docker для доступа к локальной базе SkyDNS по Y-API

Примечание

Требуется установка контейнера Docker версии 20 и выше (работа на более ранних версиях не гарантирована).

Установка контейнера Docker должна быть на ОС Astra Linux Special Edition версии 1.7.4 и выше с максимальным уровнем защиты «Смоленск».

Архив с контейнером Docker можно запросить у представителей SkyDNS.

Чтобы установить контейнер Docker для доступа к базе SkyDNS по Y-API:

1. Отключите межсетевой экран с помощью команды:

   # systemctl stop ufw && systemctl disable ufw

2. Скопируйте файлы контейнера на узел Docker любым способом.

3. Распакуйте файл с помощью команды:

   # unzip skydns.zip

4. Установите дополнительные пакеты с помощью команды:

   # sudo apt-get install -y curl bridge-utils

   Примечание

   *Файл **y_api.tar.gz** будет разархивирован в папку /root/SkyDNS/.*

5. Установите Docker с помощью команды:

   # sudo apt install docker.io

6. Предоставьте узлу Docker прямой доступ в интернет.

7. Загрузите образ из архива с помощью команды:

   # sudo docker load -i ./SkyDNS/y_api.tar.gz

8. Проверьте список контейнеров:

   # docker container ls -a

9. Создайте отдельную подсеть Docker для данного контейнера:

   # sudo docker network create --driver=bridge --subnet=193.33.33.0/24 y-api-net

10. Запустите контейнер в данной подсети:

    # sudo docker run -it -d --net y-api-net --ip 193.33.33.33 -p 80:80/tcp -p 80:80/udp y-api:1

    Примечание

    После успешного выполнения команды запуска контейнера необходимо подождать неопределенное количество времени (зависит от скорости интернета).

    Образ Docker не хранит в себе базы, он будет их скачивать через интернет каждый раз после запуска.

    Сервис запускается на 80 порту, и он не запустится, пока не будут скачаны базы.

    Порт, на котором запускается сервис, транслируется на узел Docker с помощью параметра ***-p 80:80/tcp -p 80:80/udp****.*

11. Выполните проверку работы SkyDNS:

    # curl -v http://193.33.33.33/qwerty.com

    Примечание

    Если команда возвращает ошибку вида:

    ```
    * Expire in 0 ms for 6 (transfer 0x14ff0f0)
    *   Trying 193.33.33.33...
    * TCP_NODELAY set
    * Expire in 200 ms for 4 (transfer 0x14ff0f0)
    * connect to 193.33.33.33 port 80 failed: В соединении отказано
    * Failed to connect to 193.33.33.33 port 80: В соединении отказано
    * Closing connection 0
    curl: (7) Failed to connect to 193.33.33.33 port 80: В соединении отказано
    ```

    Подождите окончания загрузки базы и выполните предыдущую команду несколько раз, пока вывод команды не станет вида:

    ```
    * Expire in 0 ms for 6 (transfer 0x1e990f0)
    *   Trying 193.33.33.33...
    * TCP_NODELAY set
    * Expire in 200 ms for 4 (transfer 0x1e990f0)
    * Connected to 193.33.33.33 (193.33.33.33) port 80 (#0)
    > GET /qwerty.com HTTP/1.1
    > Host: 193.33.33.33
    > User-Agent: curl/7.64.0
    > Accept: */*
    >
    < HTTP/1.1 200 OK
    < Content-type: application/json
    ```

```
< Connection: keep-alive
* no chunk, no close, no size. Assume close to signal end
<
* Closing connection 0
{"category": [36, 49], "bad": false, "category_name": ["Образование и учебные учреждения",
"Компьютеры и Интернет"]}
```

После получения ответа по категории сайта qwerty.com проверьте доступность контейнера из сети узла:

 # curl http://10.201.69.124/qwerty.com

Ответ должен быть аналогичен предыдущему запросу с использованием IP-адреса контейнера SkyDNS (193.33.33.33).

12 Для упрощения дальнейшей настройки Solar Web Proxy добавьте в файл **/etc/hosts** узлов прокси сервера запись, указывающую на узел Docker:

```
# nano /etc/hosts
10.201.69.124   y.api.skydns.ru y
```

где 10.201.69.124 – адрес узла Docker с запущенным контейнером SkyDNS.

Примечание

Инкрементальное обновление локальной базы SkyDNS происходит каждые 2 часа.

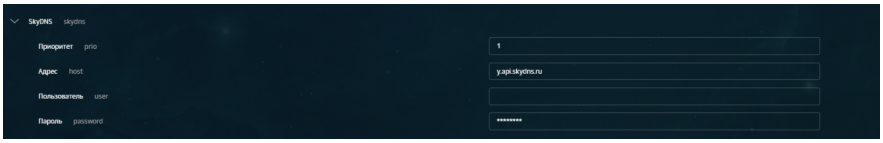
При повторном запуске контейнера база загружается заново.

Для работы Y-API требуется наличие открытого доступа в интернет (для обращения к сервисам авторизации, статистики, лицензирования, обновления). При отсутствии доступа к интернету работа сервиса прекратится частично или полностью.

5.17.3.2. Проверка работы категоризатора

Для проверки работы категоризатора:

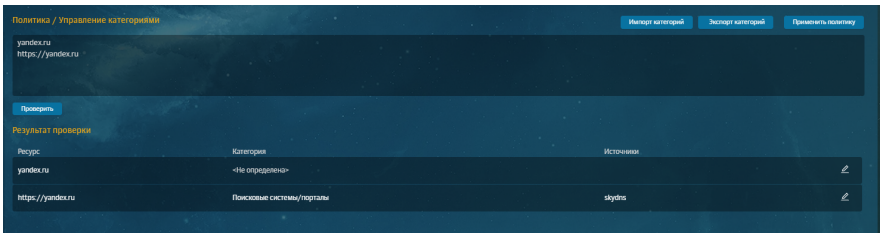
1. В разделе **Система > Расширенные настройки > Категоризатор веб-ресурсов > Категоризатор веб-ресурсов > Категоризаторы > SkyDNS** в поле **Адрес** укажите полное доменное имя или IP-адрес (10.201.69.124) хоста Docker.



Примечание

*Убедитесь, что в поле **Приоритет** установлено значение, отличное от 0. Не требуется заполнение полей **Пользователь** и **Пароль**.*

2. Проверьте работу локальной БД SkyDNS в разделе **Политика > Управление категориями**, используя префиксы (http:// или https:///) с указанием полного доменного имени (FQDN) категоризируемого ресурса.



Далее при обработке правил/исключений во всех слоях раздела **Политика > Контентная фильтрация** при наличии подкатегории/категории в атрибуте **Назначение** будет определяться категория ресурса согласно локальной базе SkyDNS.

Примечание

*При использовании локальной базы SkyDNS нет возможности проверить категорию ресурса в GUI в разделе **Политика > Проверка** по политике, т.к. в GUI есть ограничение на использование префиксов.*

6. Антивирус

6.1. Настройка антивируса

Для настройки антивируса:

1. В разделе **Работа системы** основных настроек конфигурации выберите секцию **Антивирус** и установите переключатель **Лицензия** в положение **Ключевой файл** или **Серийный номер лицензии**:

   - **Ключевой файл** – загрузите лицензионный ключевой файл, полученный от вендора;
   - **Серийный номер лицензии** – введите серийный номер лицензии, полученный от вендора.

2. Последовательно нажмите **Сохранить** и **Применить**.

3. В разделе **Система > Узлы и роли** назначьте одному из узлов роль **Антивирус**.

4. Сформируйте правило политики для перенаправления трафика на проверку антивирусом (см. далее).

6.2. Формирование политики для работы антивируса

Для окончания настройки антивируса сформируйте политику ИБ. Для этого в разделе **Политика** в слое **Перенаправление по ICAP** создайте слой с правилом на обработку трафика антивирусом, как на рисунке далее. Примените политику.

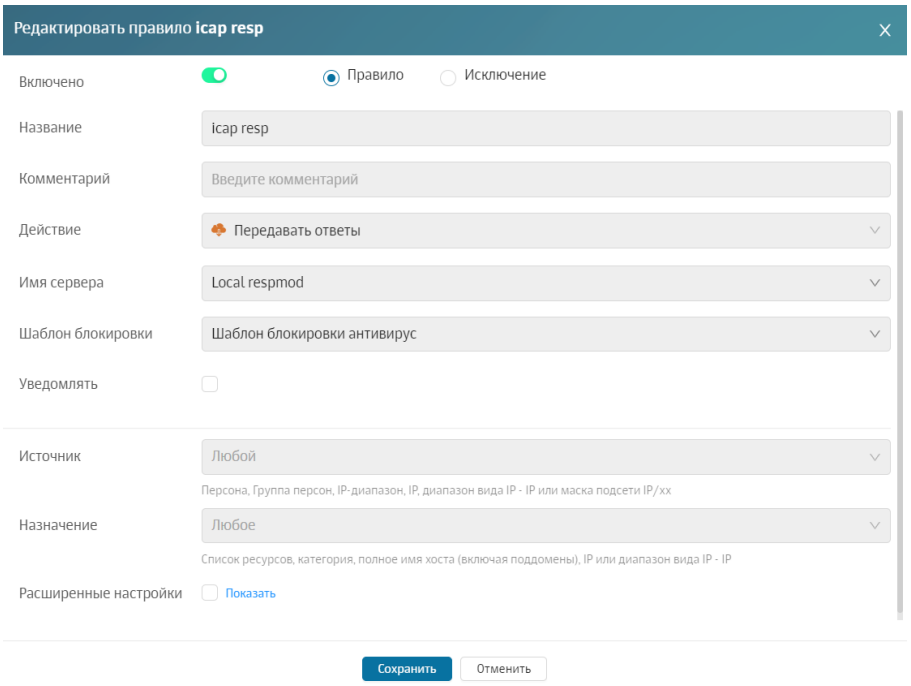


Рис. 6.1. Правило для перенаправления трафика антивирусу

7. Отказоустойчивость

7.1. Общие сведения

Для обеспечения отказоустойчивости в Solar NGFW используется технология Virtual Router Redundancy Protocol (VRRP) или виртуальный IP-адрес (Virtual IP — VIP).

Использование VRRP позволяет объединить несколько маршрутизаторов в один виртуальный с общим IP-адресом. Другими словами, технология виртуального IP-адреса — это группа интерфейсов маршрутизаторов, которые находятся в одной сети и разделяют виртуальный идентификатор (Virtual Router Identifier — VRID) и один виртуальный IP-адрес.

7.2. Настройка отказоустойчивости

7.2.1. Кластер Active/Passive

Примечание

При использовании кластера поддерживается работа исключительно VIP-адресов на data-интерфейсах. В противном случае отказоустойчивость OSPF, построенная на VRRP, может работать некорректно.

Отказоустойчивая пара состоит из двух равнозначных узлов, соединенных между собой медным или оптическим Ethernet-интерфейсом скоростью 1G или 10G, выбранным из общего набора сетевых интерфейсов устройств.

Сборке в кластер подлежат только идентичные по типу и аппаратным ресурсам системы (Virtual или Hardware).

Сборке в кластер подлежат только агенты с одинаковыми идентификаторами кластера, разными идентификаторами узла, разными постоянными ролями, одинаковым типом и именем интерфейса синхронизации.

Для корректной работы на обоих узлах должен быть включен идентичный набор функциональных ролей или компонентов.

К каждому устройству должен быть заранее настроен MGMT доступ через in-band (общий) или out-of-band (специально выделенный) интерфейс.

В кластере Active/Passive узлы регулярно обмениваются данными о своем статусе и состоянии. Основной принцип отказоустойчивости заключается в том, что при физической избыточности оборудования, когда главный (master) узел в момент времени является активным и обрабатывает трафик, резервный (slave) узел регулярно следит за активностью master-узла, и в случае сбоя забирает на себя всю работу по обработке трафика.

Отслеживать активность узлов и управлять ими можно в разделе **Сеть > Кластеризация**.

Чтобы добавить новый кластер, нажмите кнопку **Создать кластер** и укажите параметры:

- **Название** – произвольное название кластера. Можно указать значение длиной до 32 символов.
- **Тип кластера** – доступен выбор только типа кластера **Актив - Пассив**.

- **Интерфейс синхронизации** – выбор из доступных сетевых интерфейсов, имеющихся в системе. Выбранный интерфейс можно исключить из управления в разделе **Сеть > Сетевые интерфейсы**.
- **ID кластера** – значение длиной до 32 символа в шестнадцатиричном формате. Чтобы сгенерировать значение автоматически, в поле нажмите  .
- **ID локального узла** – числовое значение в диапазоне от 1 до 254.
- **Постоянная роль** – доступные значения: **Первичный** или **Вторичный**.

После добавления нового кластера будет отображена таблица с информацией о работе кластера и узлов в нем:

- **Статус кластера** – агент синхронизации статусов проводит сравнение полученных статусов от локального и смежного узлов и отображает статус общей работоспособности кластера:
  - **Normal** – кластер работает в штатном режиме. Активный узел зарезервирован.
  - **Critical** – один или оба узла в кластере находятся полностью или частично в неработоспособном состоянии.
  - **NotReady** – один из узлов находится в процессе подготовки к переходу в штатный режим.
  - **Standalone** – кластер настроен пока только на одном узле.
  - **Stopped** – кластер полностью в остановленном состоянии.
  - **Incompatible** – обнаружена несовместимость параметров узлов или агента при первой сборке и инициализации кластера. Не выполнены предусловия для сборки кластера.
- Информация о кластере:
  - **Тип кластера**,
  - **ID кластера**,
  - **Интерфейс синхронизации**,
  - **Последнее подключение**.
- Информация о локальном узле:
  - **Текущий статус**,
  - **ID узла**,
  - **Постоянная роль**,
  - **Текущая версия ПО**,
  - **Время нахождения в текущем статусе**.

- Информация о смежном узле:
  - **Текущий статус**,
  - **ID узла**,
  - **Постоянная роль**,
  - **Текущая версия ПО**.

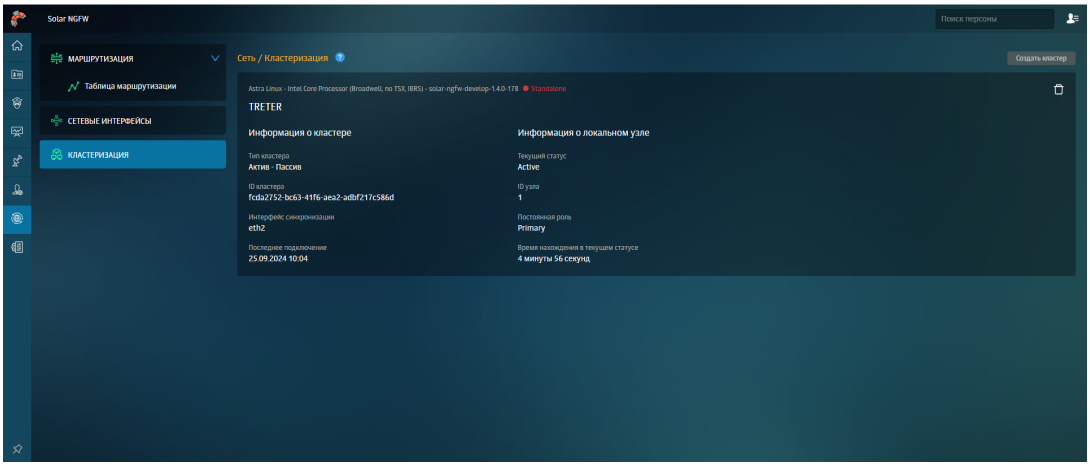


Рис. 7.1. Раздел "Кластеризация"

7.2.2. Синхронизация сессий в кластере

В Solar NGFW для отказоустойчивой пары Active-Passive реализована синхронизация сессий на базе **conntrackd**. В процессе работы кластера состояния сессий между узлами синхронизируются, и активный узел передает на пассивный информацию о состоянии проходящих через него сессий, а также об их классификации. Таким образом, при включении пассивного узла он будет обладать информацией об актуальном состоянии всех сессий и не будет их блокировать, если это не предусмотрено правилами фильтрации. Отслеживание состояния активного узла и переключение пассивного в активный выполнено на базе протокола VRRP.

Для синхронизации таблицы соединений между узлами отказоустойчивой пары используется утилита **conntrackd**, установленная на оба узла.

Для синхронизации сессий между узлами по умолчанию используются порты UDP 3780 и 3781.

Примечание

*При использовании правил трансляции (NAT) в режиме **masquerade** соединение, созданное на активном узле, не может синхронизироваться на резервный узел. При переключении на резервный узел сессия NAT должна быть создана заново.*

*Интерфейс, выбранный в качестве интерфейса синхронизации при создании кластера, не может использоваться в правилах раздела **Политика**. Это ограничение обусловлено тем, что интерфейс синхронизации предназначен исключительно для обмена служебной инфор-*

мацией между узлами кластера, и его использование в политике может нарушить работу системы.

При импорте политик запрещено импортировать правила, в которых указан интерфейс синхронизации. Перед импортом убедитесь, что во всех импортируемых правилах отсутствуют ссылки на интерфейс синхронизации, чтобы избежать ошибок и некорректной работы кластера. Эти ограничения необходимо учитывать при создании и редактировании политик, а также при импорте конфигураций для обеспечения стабильной работы системы.

8. Обратный прокси

8.1. Основные настройки

Solar NGFW обеспечивает контроль и управление трафиком пользователей не только в прямом, но и в обратном режиме (Reverse proxy).

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 их выгрузке. Можно опубликовать как один, так и несколько ресурсов. Количество ресурсов не ограничено.

Примечание

*Перед настройкой обратного прокси проверьте наличие лицензии на этот модуль. Если лицензия отсутствует, загрузите ее в окне с информацией о лицензии с помощью кнопки **Загрузить лицензию**.*

Для настройки Solar NGFW в обратном режиме:

1. Назначьте выбранному узлу роль **Обратный прокси** в разделе **Система > Узлы и роли**.
2. В разделе **Работа системы > Обратный прокси-сервер (reverse-proxy.json)** основных настроек конфигурации в секции **Настройки источника** выберите доступность по внешнему протоколу безопасности:
   - **HTTP** – при доступе извне на опубликованный внешний адрес, перенаправляемый к внутреннему ресурсу, обращение будет только по незащищенному HTTP-протоколу с использованием порта 8445 (вне зависимости от протокола открытия).
   - **HTTPS** – при доступе извне на опубликованный внешний адрес, перенаправляемый к внутреннему ресурсу, обращение будет только по защищенному HTTPS-протоколу с использованием порта 8444 (вне зависимости от протокола открытия).
   - **HTTP_AND_HTTPS** – при доступе извне на опубликованный внешний адрес, перенаправляемый к внутреннему ресурсу, допускается обращение как по протоколу HTTP (порт 8445), так и HTTPS (порт 8444).

   Примечание

   *Для каждого внутреннего ресурса в настройках обратного прокси устанавливаются свои настройки протоколов и портов, для таких ресурсов можно установить протокол HTTP или HTTPS. Для всех внешних адресов ресурсов в настройках реверс прокси устанавливаются глобальные настройки номеров портов, для таких адресов можно установить протокол **HTTP**, **HTTPS**, **HTTP_AND_HTTPS**.*

   Схема перенаправления запроса Solar NGFW при обращении к внешнему адресу ресурса при указании:

- *Номера порта для протокола HTTP для внешнего соединения и протокола HTTP для внутреннего адреса ресурса – при обращении к внешнему адресу ресурса по протоколу HTTP запрос будет перенаправлен по протоколу HTTP на внутренний адрес ресурса.*
- *Номера порта для протокола HTTPS для внешнего соединения и протокола HTTP для внутреннего адреса ресурса – при обращении к внешнему адресу ресурса по протоколу HTTPS запрос будет перенаправлен по протоколу HTTP на внутренний адрес ресурса.*
- *Номеров портов для протоколов HTTP и HTTPS для внешнего соединения и протокола HTTP для внутреннего адреса ресурса – при обращении к внешнему адресу ресурса по протоколу HTTP запрос будет перенаправлен по протоколу HTTP на внутренний адрес ресурса.*
- *Номеров портов для протоколов HTTP и HTTPS для внешнего соединения и протокола HTTP для внутреннего адреса ресурса – при обращении к внешнему адресу ресурса по протоколу HTTPS запрос будет перенаправлен по протоколу HTTP на внутренний адрес ресурса.*
- *Номера порта для протокола HTTP для внешнего соединения и протокола HTTPS для внутреннего адреса ресурса – при обращении к внешнему адресу ресурса по протоколу HTTP запрос будет перенаправлен по протоколу HTTPS на внутренний адрес ресурса.*
- *Номера порта для протокола HTTPS для внешнего соединения и протокола HTTPS для внутреннего адреса ресурса – при обращении к внешнему адресу ресурса по протоколу HTTPS запрос будет перенаправлен по протоколу HTTPS на внутренний адрес ресурса.*
- *Номеров портов для протоколов HTTP и HTTPS для внешнего соединения и протокола HTTPS для внутреннего адреса ресурса – при обращении к внешнему адресу ресурса по протоколу HTTP запрос будет перенаправлен по протоколу HTTPS на внутренний адрес ресурса.*
- *Номеров портов для протоколов HTTP и HTTPS для внешнего соединения и протокола HTTPS для внутреннего адреса ресурса – при обращении к внешнему адресу ресурса по протоколу HTTPS запрос будет перенаправлен по протоколу HTTPS на внутренний адрес ресурса.*

3. Укажите параметры настройки в разделе **Работа системы > Обратный прокси-сервер (reverse-proxy.json)** основных настроек конфигурации в секции **Настройки источника > Внутренний адрес сервиса**:

   - **Сетевой адрес (host)** – сетевой адрес внутреннего ресурса, к которому необходимо предоставить доступ. Необходимо указать IP-адрес внутреннего ресурса.
   - **Порт (port)** – порт публикуемого ресурса. Значение по умолчанию: *443*.
   - **Сертификат (certificate)** – сертификат для работы обратного прокси.

   Примечание

   Можно использовать как собственный сертификат, так и сертификат, поставляемый с продуктом.

   *Также можно сгенерировать сертификат вручную и импортировать его с помощью кнопки **Загрузить** (см. 8.2).*

При использовании своего сертификата, подписанного центром сертификации (CA), необходимо добавить его в список доверенных корневых центров сертификации. Иначе при переходе на ресурс в браузере отобразится уведомление об ошибке сертификата.

- **Порт (reverse-proxy-port)** – порт обратного прокси. Значение по умолчанию: *8444*.

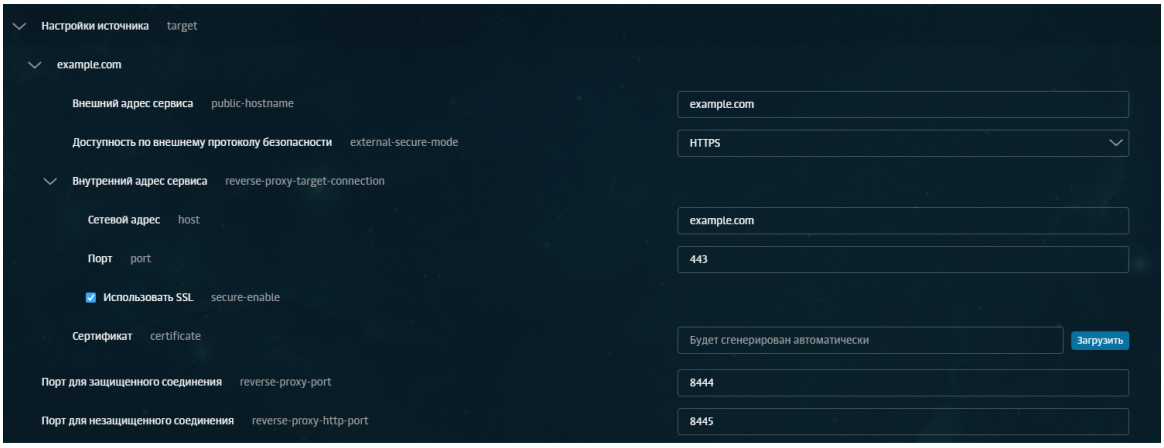


Рис. 8.1. Параметры настройки обратного прокси

4. Установите флажок **Использовать SSL**, чтобы обращение к внутреннему ресурсу было по защищенному соединению (протоколу HTTPS). При снятом флажке обращение к внутреннему ресурсу будет по незащищенному соединению (протоколу HTTP).

5. Для сохранения и применения настроек последовательно нажмите кнопки **Сохранить** и **Применить**.

6. Настройте аутентификацию.

Примечание

Режим обратного прокси поддерживает только Basic и NTLM аутентификацию.

7. Для минимальной работы с консолью, если обратный прокси запускается на мастер-узле, установите флажок **Перенаправление с 443 порта на 8443 порт** в разделе **Система > Расширенные настройки > Интерфейс**.

8. В разделе **Политики** сформируйте политику контентной фильтрации.

Примечание

Политика фильтрации для прямого и обратного режима работы системы является общей. Однако в обратном режиме по умолчанию настроено вскрытие HTTPS-трафика.

*При формировании политики для обратного прокси в разделе **Система > Работа системы > Обратный прокси-сервер** основных настроек конфигурации в секции **Настройки источника** необходимо указывать внешний адрес сервиса (public-hostname).*

9. Для проверки работы обратного прокси в браузере перейдите на адрес узла с ролью обратного прокси. Например, на корпоративную почту **webmail.rt-solar.ru**.

Добавить новый публикуемый ресурс можно одним из способов:

- нажав кнопку **Добавить**;
- скопировав уже существующий ресурс и изменив параметры настройки.

Примечание

Обычно на одном IP-адресе размещается один ресурс. Но бывают ситуации, когда несколько ресурсов размещены на одном IP-адресе. Оба случая работоспособны.

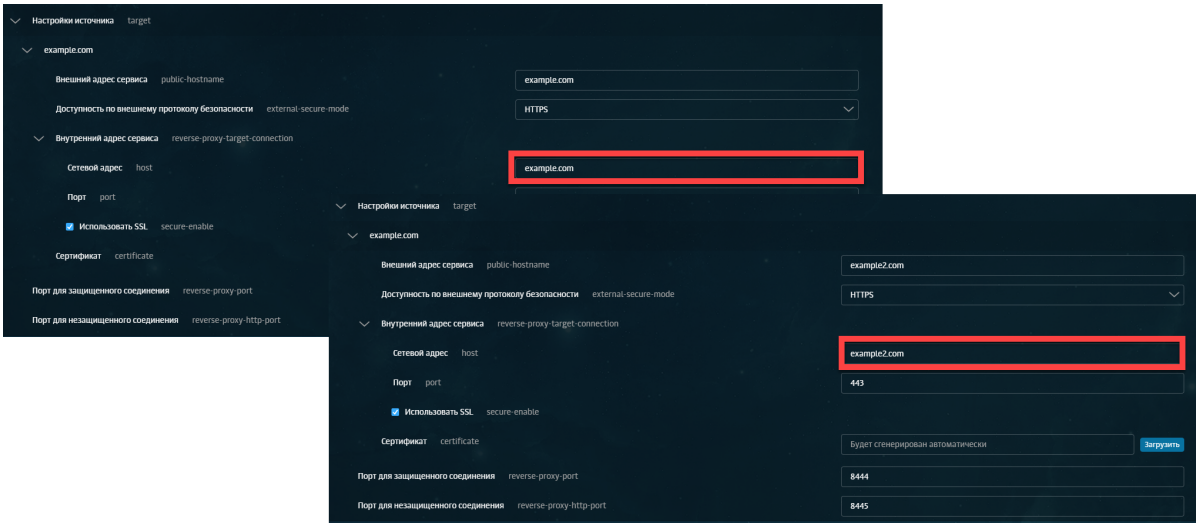


Рис. 8.2. Несколько публикуемых ресурсов

8.2. Создание сертификата для обратного прокси-сервера

Если в организации есть собственный УЦ, можно использовать его сертификат для обратного прокси.

Для выпуска сертификата с помощью УЦ Windows в CLI:

1. На АРМ с ОС Linux в CLI выполните следующие действия:

   - Сгенерируйте ключ, используя одну из команд (в зависимости от выбранного алгоритма шифрования):

     RSA:

     # openssl genpkey -out wp.key -algorithm RSA -pkeyopt rsa_keygen_bits:2048

     ECDSA:

     # openssl genpkey -out wp.key -algorithm EC -pkeyopt ec_paramgen_curve:P-256

- Сформируйте файл конфигурации **wp.cnf** для создания запроса на подпись сертификата (CSR) и заполните его данными:

```
[req]
prompt = no
distinguished_name = dn
req_extensions = ext
input_password = PASSPHRASE
[dn]
CN = webmail.rt-solar.ru
emailAddress = webmaster@rt-solar.ru
O = Solar Security
L = Moskau
C = RU
[ext]
subjectAltName = DNS:webmail.rt-solar.ru
```

  Выделенные значения параметров замените на актуальные значения в организации:

  - **CN** – FQDN сервера, на котором происходит публикация;
  - **emailAddress** – контактный адрес электронной почты организации;
  - **O** – название организации;
  - **L** – название города, в котором расположена организация;
  - **C** – двухбуквенный код страны;
  - **subjectAltName** – FQDN публикуемого ресурса: DNS.

- Сгенерируйте CSR:

  # openssl req -new -config wp.cnf -key wp.key -out wp.csr

2. На АРМ с ОС Windows выполните следующие действия:

   - Скопируйте CSR во временный каталог на АРМ с Windows, например, в **c:\wp.csr.**
   - Сгенерируйте сертификат из CSR:

     # certreq -submit -attrib "CertificateTemplate: WebServer" c:\wp.csr

   - Сохраните во временный каталог на АРМ пользователя сертификат с именем **wp.cer** и выберите в открывшемся окне **Получить PEM.**
   - Выгрузите сертификат Удостоверяющего центра:

     # certutil -ca.cert c:\ca.cer

3. На АРМ с ОС Linux в CLI выполните следующие действия:

   - Сконвертируйте сертификат УЦ, подчиненный УЦ (при наличии) и сертификат веб-ресурса в формат PEM:

     # openssl x509 -inform der -in ca.cer -out ca.pem

 # openssl x509 -inform der -in subca.cer -out subca.pem

 # openssl x509 -inform der -in web.cer -out web.pem

- Объедините ключ с сертификатом УЦ и подчиненным УЦ (при наличии):

  # cat wp.key wp.cer ca.pem subca.pem > webmail.pem

4. В GUI Solar NGFW выполните следующие действия:

   - В разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика** откройте секцию **Обратный прокси > Настройки источника**.
   - В строке **Сертификат** нажмите кнопку **Загрузить файл**.
   - В открывшемся окне проводника выберите файл с сертификатом и нажмите кнопку **Открыть**. Если сертификат успешно загружен, в поле **Сертификат** отобразится надпись **Загружен сертификат**.
   - Сохраните и примените настройки конфигурации, последовательно нажав кнопки **Сохранить** и **Применить**.

5. Для проверки работы обратного прокси в браузере перейдите на адрес узла с ролью обратного прокси. Например, на корпоративную почту **webmail.rt-solar.ru**.

8.2.1. Конвертация сертификатов в формат PEM

В Solar NGFW загрузить SSL-сертификат можно только в формате PEM. Если сертификат в другом формате (например, DER, P7B, PFX), его можно конвертировать в нужный формат.

8.2.1.1. Конвертация SSL-сертификатов с помощью OpenSSL

OpenSSL – надежный полнофункциональный инструмент для работы с протоколами Transport Layer Security (TLS) и Secure Sockets Layer (SSL). Конвертация с использованием библиотеки OpenSSL считается одним из самых безопасных способов: все данные будут сохранены непосредственно на устройстве, на котором будут выполняться операции по конвертированию.

Чтобы сконвертировать сертификат в формат PEM с помощью OpenSSL, на АРМ с ОС Linux в CLI выполните следующие команды:

- Для формата DER:

  # openssl x509 -inform der -in site.der -out site.pem

- Для формата P7B:

  # openssl pkcs7 -print_certs -in site.p7b -out site.pem

- Для формата PFX:

  # openssl pkcs12 -in site.pfx -out site.pem -nodes

Примечание

*Также вы можете использовать скрипт **openssl-toolkit**. Работа с этим скриптом является безопасным решением, т.к. сертификаты и их ключи используются исключительно на вашем сервере.*

Сертификаты в формате PEM могут быть с расширениями .pem, .crt, .cer, .key. Чтобы сменить расширение, в CLI выполните следующие команды:

 # openssl rsa -in server.key -text > private.pem

 # openssl x509 -inform PEM -in server.crt > public.pem

 # openssl x509 -in certificate.cer -outform PEM -out certificate.pem

8.3. Просмотр статистики по работе обратного прокси

Просмотреть информацию о работе Solar NGFW в обратном режиме можно в разделе **Статистика > Журнал запросов**. Запросы в обратном режиме помечены значком .

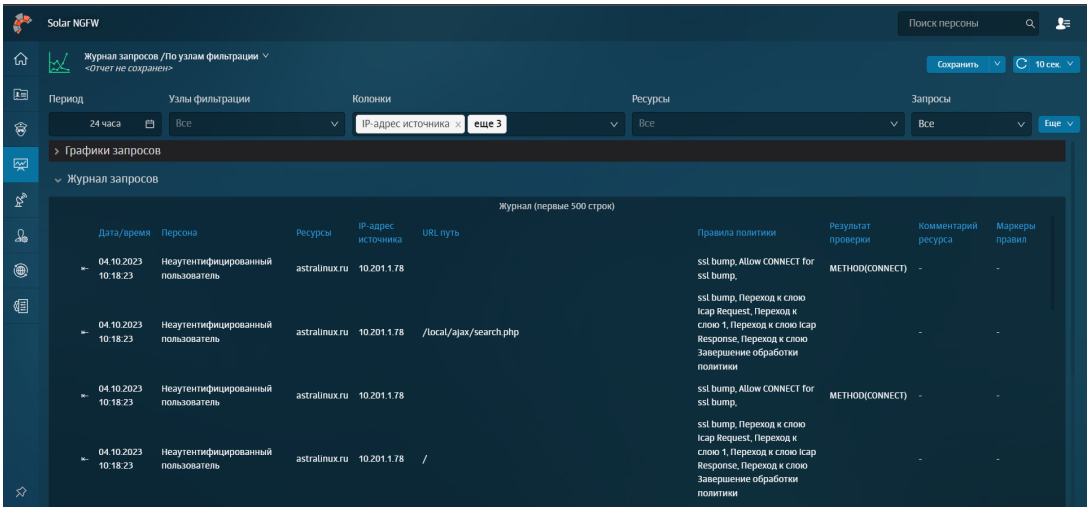


Рис. 8.3. Мониторинг работы обратного прокси в Журнале запросов

9. Система предотвращения вторжений

9.1. Общие сведения

Система предотвращения вторжений (IPS, англ. Intrusion Prevention System) – это устройство или программное приложение, которое отслеживает сеть или системы на предмет вредоносной активности или нарушений политики.

Примечание

В текущей версии Solar NGFW IPS может проверять транзитный и входящий трафик. Проксируемый пользовательский веб-трафик будет проверяться, только если включена проверка входящего трафика для IPS.

Преимущества использования системы предотвращения вторжений (IPS):

- Используемый системой сигнатурный анализ проходящего трафика позволяет идентифицировать те угрозы, которые другие средства не могут выявить.
- Фильтрация трафика происходит до того, как он успеет достичь других устройств или средств управления безопасностью. Это позволяет снизить нагрузку на эти элементы управления и повысить эффективность их работы.
- Автоматизированность системы позволяет сэкономить время администраторов безопасности на управление ею.
- Система соответствует требованиям, установленным PCI DSS, HIPAA и другим стандартам.

9.2. Настройка сервиса в веб-интерфейсе

Примечание

Перед настройкой сервиса проверьте наличие лицензии на этот модуль. Если лицензия отсутствует:

1. *В окне с информацией о лицензии нажмите кнопку **Загрузить лицензию**.*
2. *Загрузите лицензию.*
3. *Перезапустите сервис **skvt-play-server**, выполнив в CLI команды:*

   # /opt/dozor/bin/shell

   # dsctl restart skvt-play-server

Для настройки Системы предотвращения вторжений:

1. В разделе **Система > Узлы и роли** назначьте узлу роль **Система предотвращения вторжений**.

Примечание

*В режиме кластера или распределенном режиме (см. 2.3) роль **Система предотвращения вторжений** должна быть добавлена и на узел управления.*

2. В разделе **Расширенные настройки > Фильтрация и кэширование трафика > Система предотвращения вторжений** (см. Рис.9.1) укажите защищаемые сети (HOME_NET).

3. Выберите, какой трафик анализировать на наличие вредоносной активности:

   - Входящий трафик (INPUT),
   - Транзитный трафик (FORWARD) (по умолчанию),
   - Любой трафик (FORWARD и INPUT).

4. Чтобы повысить производительность, укажите количество очередей, т.е. количество обрабатываемых потоков IPS. Чем больше очередей, тем выше производительность. Задать значение можно от 1 до 10.

Примечание

При указании количества очередей учитывайте количество ЦПУ на сервере. Например, если у вас n ЦПУ, необходимо указывать n/2 очередей, чтобы все потоки не проходили по IPS. В обратном случае это может вызвать высокую нагрузку на сервер.

5. При необходимости установите флажок **Привязать очереди к ядрам CPU**. Использование идентификаторов процессора вместо хэша соединения позволяет повысить производительность. На каждую очередь выделяется ядро CPU.

6. Добавьте список проверяемых сетей в режиме транзитного трафика. Указанные сети будут отправлены на проверку в IPS. Правила обратного трафика для сетей указывать не требуется, они генерируется автоматически. Для проверки всего трафика указанной сети, необходимо второй сетью указать 0.0.0.0/0. Если необходимо проверить весь трафик в таблице FORWARD, в обоих полях нужно указать 0.0.0.0/0.

7. Нажмите **Сохранить** и **Применить**.

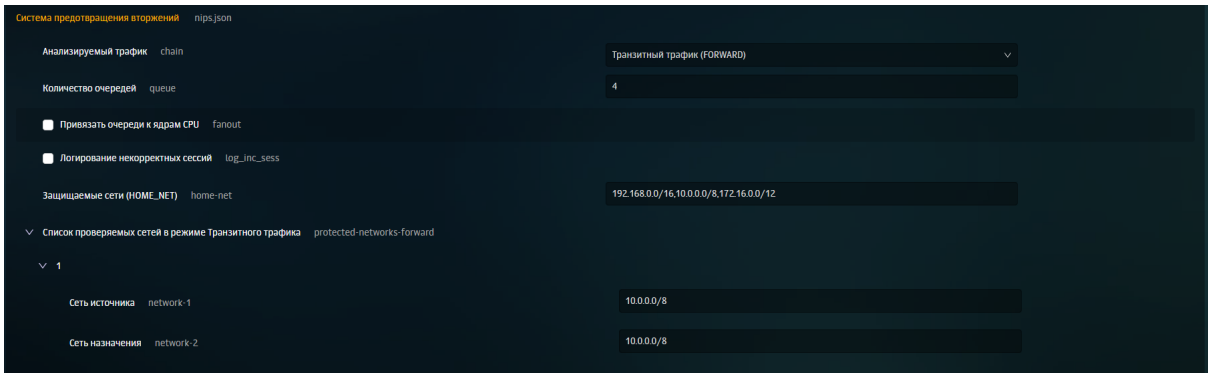


Рис. 9.1. Настройка системы предотвращения вторжений

10. Дополнительные настройки Solar NGFW

10.1. Настройка журналирования сообщений сервиса skvt-wizor

При необходимости можно организовать запись сообщений сервиса **skvt-wizor** в файл **syslog-ng** и в отдельный файл.

Примечание

*Если сервис syslog-ng не запускается, убедитесь, что в файле **/etc/syslog-ng/conf.d/mod-astra.conf** закомментирована строка **#@include "/usr/share/syslog-ng-mod-astra/mod-astra.conf"**. Если нет, закомментируйте ее и перезапустите сервис syslog-ng с помощью команды **# systemctl reload syslog-ng.service**.*

10.1.1. Настройка журналирования сообщений сервиса skvt-wizor в файл syslog-ng

Для настройки журналирования сообщений сервиса **skvt-wizor** в файл **syslog-ng** выполните следующие действия:

1. В разделе **Система > Основные настройки > Журналирование > Сервер веб-интерфейса** установите флажок **Журналировать действия пользователей в syslog**.

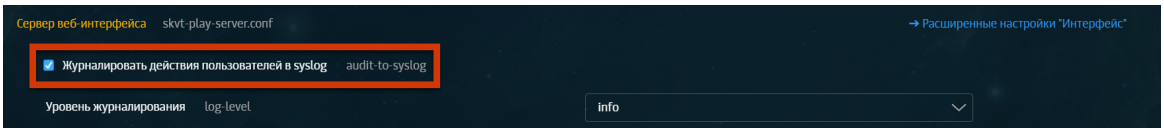


Рис. 10.1. Журналировать действия пользователей в syslog

2. Отредактируйте файл **/etc/syslog-ng/syslog-ng.conf**, добавив в него следующие записи:

   - В секции **Sources**:

```
source s_src {
      system();
      internal();
};
```

   - В секции **Filters**:

```
filter f_messages { level(info,notice,warn) or facility(local0) and
                    not facility(auth,authpriv,cron,daemon,mail,news); };
```

   - В секции **Logs**:

```
log { source(s_src); filter(f_messages); destination(d_messages); };
```

3. Перезапустите сервис журналирования **syslog-ng** с помощью команды:

   # systemctl restart syslog-ng.service

4. Выберите формат записи в системный журнал сообщений (access-log, siem-log или ip-translation-log) и установите флажок в зависимости от выбранного формата записи данных в журнал в разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика**, секция **Фильтрация и анализ трафика пользователей > Форматы записи в syslog** (см. Рис.10.2).

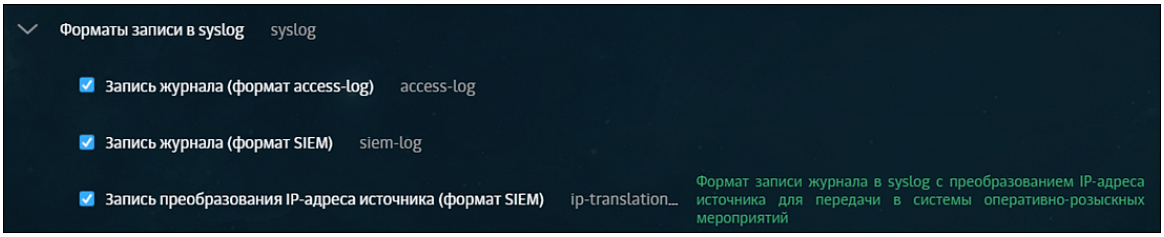


Рис. 10.2. Выбор формата записи журнала

Примечание

*Для быстрого доступа к текущим настройкам журналов используйте меню **Система** > **Основные настройки** > **Журналирование**, секция **Фильтрация и анализ трафика пользователей**.*

Далее приведено описание полей каждого формата записей в системный журнал.

Табл. 10.1. Описание полей сообщений в формате access-log

Поле сообщения	Описание
<date time>	Дата и время создания записи журнала syslog
<host>	Имя компьютера (источника)
java	Системная служба java
reqTime	Время начала запроса (float unix time)
filterTime	Общее время обработки запроса в миллисекундах
accountIP	IP-адрес источника (с учетом XFF)
filterStatus	Код состояния HTTP-узла фильтрации
responseSize	Размер тела ответа
method	HTTP-метод (GET, POST)
url	URL запроса
user	Имя авторизованного пользователя
serverHost	IP-адрес ресурса назначения
mimeType	MIME-тип ответа (если он определён) – см. Приложение D.2

Пример записи из журнала запросов в **syslog-ng**:

```
Jan 23 17:06:22 avm118 java: 1327323982.533  13 10.31.6.126 TCP_MISS/200 2779 GET
http://lenta.ru/news/2012/01/23/shortsightedness/_Printed.htm  DIRECT/81.19.85.116 text/html
```

Примечание

Настроить журналирование сообщений в формате SIEM также можно, установив флажок ***Запись журнала (формат SIEM)*** *в разделе* ***Политика > Настройки*** *или в разделе* ***Система > Основные настройки > Работа системы****.*

Табл. 10.2. Описание полей сообщений в формате siem-log

Поле сообщения	Описание
<date time>	Дата и время создания записи журнала syslog
<host>	Имя компьютера (источника)
java	Системная служба java
acc-domain	Домен источника
acc-groups	Название групп источника из Досье
acc-ip	IP-адрес источника
acc-port	Порт источника
bytes-in	Объем скачанных (полученных) данных (Б)
bytes-out	Объем загруженных (отправленных) данных (Б)
flt-categories	Категории фильтрации политики
flt-codes	Код фильтрации политики (см. Приложение *Описание HTTP-кодов фильтрации*)
flt-policy	Название сработавшего слоя политики фильтрации
flt-rules	Названия правил политики, которые были применены при фильтрации
flt-status	Код состояния HTTP-узла фильтрации
flt-time	Общее время обработки запроса в миллисекундах
req-hostname	Сетевое имя ресурса назначения
req-method	HTTP-метод запроса
req-pathname	Путь запроса
req-protocol	Идентификатор протокола запроса
req-query	Параметры запроса
req-referer	Значение HTTP-заголовка Referer
req-time	Метка времени начала запроса от источника
res-datatype	MIME-тип ответа (см. Приложение D.2)
res-ip	Числовое представление IP-адреса назначения
traf-mode	Режим направления трафика: прямой (forward)/обратный (reverse)
req-port	Порт ресурса назначения
flt-reason	Причина фильтрации

Пример записи из журнала запросов в **syslog-ng**:

```
Jul  6 12:53:23 tyur java: [acc-domain:local] [acc-groups:] [acc-ip:10.201.28.233] [acc-name:]
[acc-port:54819] [bytes-in:632] [bytes-out:893] [flt-categories:2401] [flt-codes:11,0,0,0,0]
[flt-policy:Завершение обработки политики] [flt-rules:mitm all,mitm all,Переход к слою Icap Response
 Icap Response,Переход к слою response layer, Переход к слою Завершение обработки политики]
 [flt-status:200] [flt-time:97] [req-hostname:rs.mail.ru] [req-method:GET] [req-pathname:/d66539304.gif]
 [req-protocol:https] [req-query:sz=15&_=1626173368526] [req-referer:https://mail.ru/]
[req-time:2021-07-06T09:53:23.182Z] [res-datatype:image/gif] [res-ip:10.199.30.12] [req-port:443]
[flt-reason:]
```

Табл. 10.3. Описание полей сообщений в формате ip-translation-log

Поле сообщения	Описание
<date time>	Дата и время создания записи журнала syslog
<host>	Имя компьютера (источника)
java	Системная служба java
transport-protocol	Протокол передачи данных
acc-ip	IP-адрес источника
acc-port	Порт источника
req-proxy-ip	IP-адрес прокси-сервера
req-proxy-port	Порт прокси-сервера
flt-ip	IP-адрес узла фильтрации
flt-port	Порт узла фильтрации
res-ip	IP-адрес ресурса назначения
res-port	Порт ресурса назначения

Пример записи из журнала запросов в **syslog-ng**:

```
Jul  6 12:08:08 tyur java: [sys-time:2021-07-06T09:08:08.985Z] [transport-protocol:TCP]
[acc-ip:10.199.177.212] [acc-port:53337] [req-proxy-ip:10.201.29.113] [req-proxy-port:2270]
[flt-ip:10.201.29.113] [flt-port:33824] [res-ip:10.199.30.12] [res-port:443]
```

5. Последовательно нажмите **Сохранить** и **Применить**.

10.1.2. Настройка журналирования сообщений сервиса skvt-wizor в файл

Для настройки журналирования сообщений сервиса **skvt-wizor** через **syslog-ng** в отдельный файл:

1. Создайте файл **/var/log/skvt-log**, выполнив команду:

   # touch /var/log/skvt-log

2. Для ограничения доступа к файлу **/var/log/skvt-log** выполните команду:

   # chmod 600 /var/log/skvt-log

3. Отредактируйте файл **/etc/syslog-ng/syslog-ng.conf**, добавив в него строку:

   ```
   local0.* /var/log/skvt-log
   ```

   Примечание

   *В качестве разделителя между **local0.*** и **/var/log/skvt-log** используйте символ табуляции.*

4. Перезапустите **syslog** командой:

   # systemctl restart syslog-ng.service

10.1.3. Настройка отправки syslog-сообщений

Чтобы хранить журналы в одном месте, настройте отправку сообщений с необходимыми параметрами конфигурации сервиса syslog-ng на удаленный сервер журналирования. Для этого:

1. В разделе **Система > Узлы и роли** назначьте master-узлу роль **Сервер пересылки журналов на удаленный узел**.

   Примечание

   Изменение настроек в GUI возможно только на master-узле.

2. Перейдите в раздел **Система > Расширенные настройки > Хранение** и задайте значения параметров:

   - **Имя удаленного узла** – имя сервера. Допускается указывать цифры, буквы, тире, нижнее подчеркивание. Значение не должно превышать 32 символа. Значение по умолчанию – **Host1**.

     Примечание

     При добавлении нескольких syslog-серверов значение в поле Имя удаленного узла для каждого сервера должно быть уникальным.

   - **IP-адрес удаленного узла** – IP-адрес без маски. По умолчанию значение не указано. Можно указывать любой локальный «серый» или публичный «белый» IP-адрес.
   - **Порт** – порт удаленной системы. Значение по умолчанию – 514.
   - **Протокол** – раскрывающийся список с выбором протокола TCP/UDP. По умолчанию – **udp**.
   - **Транслировать журналы обнаружения вторжений** – при установленном флажке журналы nips будут перенаправляться на удаленный узел.
   - **Транслировать журналы соединений и запросов** – при установленном флажке журналы dblog будут перенаправляться на удаленный узел.
   - **Транслировать журналы политик фильтрации** – при установленном флажке журналы wizor будут перенаправляться на удаленный узел.

3. Последовательно нажмите кнопки **Сохранить** и **Применить политику**.
4. Перезапустите систему.

10.1.4. Остановка записи данных syslog в файл messages

Сохранение журнальных записей в файл и остановка их передачи в файл **messages** определяется файлом **/etc/syslog-ng/syslog-ng.conf**.

Для прекращения передачи данных в файл **messages** пропишите в CLI правило перенаправления в отдельный файл. После него поставьте
&~
для прекращения обработки записей.

Пример записи имеет следующий формат:

```
local0.* /var/log/skvt.log
&~
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

10.1.5. Настройка журналирования NTLM-аутентификации

В разделе **Система > Основные настройки > Журналирование > Подключение к Контроллеру домена (DC) для NTLM-аутентификации** можно отрегулировать уровень журналирования при NTLM-аутентификации. Уровень ведения журнала представляет собой целое число в диапазоне от 0 до 9, где:

- **журналирование отключено** – значение 0, сообщения в журнале отображаться не будут.
- **1** – оптимальный уровень журналирования для системных администраторов, в журнале отображаются только записи об успешности соединения.

  Пример записи имеет следующий формат:

  ```
  105/25/98 22:02:11 server (192.168.236.86) connect to service public as user pcguest
  (uid=503,gid=100) (pid 3377)
  ```

- **3** – уровень журналирования для активного отслеживания проблем на сервере.

Примечание

Уровни выше 3 предназначены для использования разработчиками и позволяют получать более подробную информацию. В связи с этим выбор таких уровней приводит к быстрому заполнению свободного места на диске и замедлению работы ОС.

Выбранное значение будет отображаться в поле **help** параметра **dc-log-level** в файле **/opt/dozor/config/default/types.d/types.json**.

10.2. Настройка принудительного использования HTTPS

Для настройки принудительного использования протокола HTTPS:

1. В разделе **Система > Основные настройки > Работа системы** установите флажок **Принудительное использование HTTPS**.
2. Последовательно нажмите кнопки **Сохранить** и **Применить**.

10.3. Настройка блокировки рекламы

Для настройки применения правил блокировки рекламы:

1. В разделе **Система > Основные настройки > Работа системы** установите флажок **Блокировать рекламу**.

2. Последовательно нажмите кнопки **Сохранить** и **Применить**.

11. Сопровождение Solar NGFW

11.1. Управление сервисами

Для управления сервисами используется утилита **dsctl**. Чтобы запустить утилиту, выполните команды:

 # /opt/dozor/bin/shell

 # dsctl

(boot|down|start|stop|restart|reload|status|enable|disable|service-list|verify) [services]

Services are:

- abook-daemon
- antivirus
- clickhouse
- database
- dblog
- grafana
- haproxy
- igmpproxy
- keepalived
- license-server
- log-streamer
- monitor-agent
- monitor-httpd
- monitor-ng
- monitor-server
- ndpi-netfilter
- network-config-agent
- nips
- skvt-auth-server
- skvt-cache
- skvt-cassandra
- skvt-kerberos-server
- skvt-ntlm-server
- skvt-play-server
- skvt-trafdaemon
- skvt-winbind
- skvt-wizor
- smap-tikaserver
- url-checker

В качестве аргумента при запуске утилиты **dsctl** укажите одно из значений:

Табл. 11.1. Команды для утилиты dsctl

Роль	Описание
boot	Запуск системы управления сервисами.
down	Остановка системы управления сервисами.
start	Запуск сервиса.
stop	Остановка сервиса.
restart	Перезапуск сервиса, при выполнении команды сервис завершает работу и запускается заново, используя новую конфигурацию.

Роль	Описание
reload	Повторное считывание настроек сервисом, при выполнении команды сервис перечитывает конфигурацию и продолжает работу с новой конфигурацией.
enable	Подключение сервиса к системе управления сервисами. **Примечание** *При выборе значения необходимо указывать сервисы.*
disable	Отключение сервиса от системы управления сервисами. **Примечание** *При выборе значения необходимо указывать сервисы.*
service-list	Вывод списка сервисов, подключенных к системе управления сервисами.
status	Вывод информации о статусах сервисов.

Для вывода информации о статусе сервисов также используется скрипт **status**, который запускается командой:
 # status
.

Примечание

*Если не запущен ни один из сервисов, при запуске скрипта **status** выводится пустой список.*

Список сервисов приведен в разделе 2.2.

Примечание

При аварийном завершении работы какого-либо сервиса Solar NGFW автоматически будет предпринимать попытки перезапустить остановившийся сервис. Под аварийной причиной следует понимать остановку компонентов вследствие ошибок в ПО или наличия проблем с окружением.

11.2. Использование скриптов

11.2.1. Использование скриптов для получения информации о работе системы

Для сопровождения системы используются специальные скрипты и утилиты, расположенные в каталоге **/opt/dozor/bin**.

Перечень и назначение скриптов приведены в Табл.11.2.

Табл. 11.2. Скрипты для сопровождения работы системы

Название	Описание
Основные	
accept-settings	Утилита для управления системными настройками Solar NGFW
config	Утилита для управления кластером
dsctl	Утилита для управления сервисами
status	Скрипт для просмотра информации о статусе сервисов
user-tool	Утилита для управления учетными записями пользователей
Расширенные	
bug-report	Утилита для формирования отчета об ошибках
cassandra-optimize	Скрипт для синхронизации данных между узлами
check_skvt	Утилита для проверки целостности файлов Solar NGFW
get-config	Утилита для вывода конфигурации узла
get-role	Утилита для просмотра ролей, назначенных узлу
license-tool	Утилита для просмотра информации о лицензии
seelog	Скрипт для просмотра журнальных файлов Solar NGFW
set-config	Утилита для записи конфигурации узла
set-role	Утилита для назначения ролей узлу

Внимание!

*Если не указано иного, данные скрипты и утилиты необходимо запускать из командной оболочки Solar NGFW, имея права суперпользователя **root**. Переход в командную оболочку осуществляется с помощью команды:*

 # /opt/dozor/bin/shell

11.2.2. Запуск скриптов из веб-интерфейса

Для минимизации обращений администратора системы в консоль создан механизм запуска скриптов для узлов Solar NGFW. Запустить выполнение скрипта можно в разделе **Система > Узлы и роли** при наличии прав на работу с разделом **Система**.

Скрипты необходимы, например, инженерам поддержки Solar NGFW для получения информации о работе системы в случае сбоев в ее работе. Одним из таких скриптов является bug-report, который собирает диагностические данные с узла об ошибках.

При нажатии на значок  в правом углу секции с узлом раскрывается список доступных для выполнения на этом узле скриптов. Для запуска скрипта нажмите на его название. В верхней части экрана отобразится уведомление об успешном запуске. По окончании отобразится уведомление с предложением скачать текстовый файл с собранными журнальными записями.

Примечание

Возможен запуск только одного скрипта на одной ноде из-под одного пользователя. Если скрипт уже выполняется, его перезапуск невозможен.

На данный момент из интерфейса можно запустить следующие скрипты:

- **bug-report** – позволяет собирать и выводить информацию о системе, настройках и показателях ПО. Перечень видов информации, которую можно просмотреть с помощью утилиты **bug-report**, приведен в разделе *Приложение С, Отчет об ошибках: утилита bug-report*.

- **check-system** – позволяет проверить целостность файлов Solar NGFW на текущий момент времени (в CLI скрипт называется **check_skvt**).

Скрипт **check-system** использует стандартный механизм проверки целостности установленных файлов относительно содержащихся в исходных DEB-пакетах. Кроме того, скрипт содержит механизм, позволяющий отслеживать состояние произвольных файлов или каталогов, а также обрабатывать исключения среди установленных файлов.

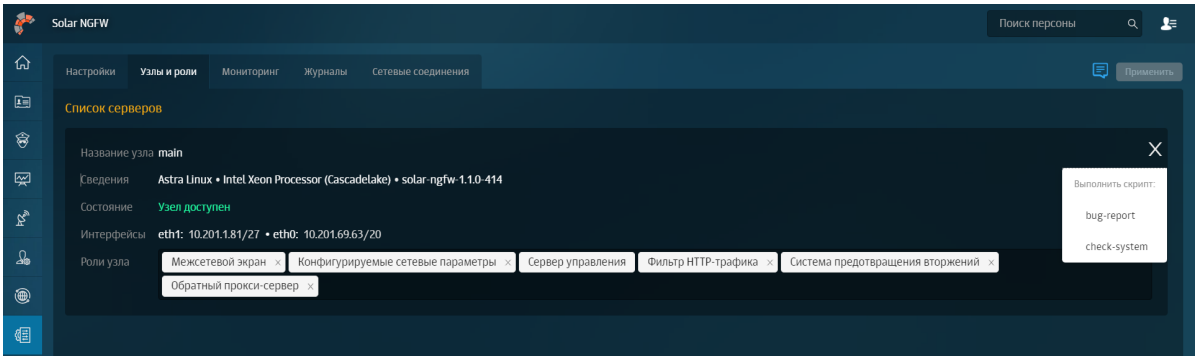


Рис. 11.1. Запуск скриптов из веб-интерфейса

11.2.3. Использование скрипта user-tool

Если пользователь забыл пароль, можно изменить его с помощью скрипта **user-tool**.

Этот скрипт также позволяет:

- заблокировать/разблокировать учетную запись пользователя;

- сменить вид авторизации пользователя. Необходимо для вывода пользователя из домена: изменения доменной авторизации на локальную.

Для запуска **user-tool** в CLI:

1. Выполните команду для запуска утилиты и вызова инструкции:

   user-tool --help

2. В зависимости от поставленной цели выберите и выполните одну из перечисленных команд.

Инструкция по действиям **user-tool** имеет следующий вид:

```
user-tool 1.0
Usage: user-tool [change-password|block-user|unblock-user|set-user-local] [options]

--help
Command: change-password [options]
```

```
change user password
-l, --login <value> login of user
-p, --password <value> password of user
Command: block-user [options]
block user
-l, --login <value> login of user
Command: unblock-user [options]
unblock user
-l, --login <value> login of user
Command: set-user-local [options]
change user auth method to local
-l, --login <value> login of user
```

Пример команды для изменения пароля от учетной записи пользователя:
ds-mode@rick /opt/dozor # user-tool change-password -l admin -p etyutqweo1w3

Примечание

После изменения пароля в CLI войдите в GUI системы для повторной смены пароля, как при первом входе в систему, и авторизуйтесь.

После выполнения других действий в GUI по умолчанию произойдут изменения:

- *после активации/блокировки учетной записи пользователя в карточке пользователя переключатель изменит свое положение;*
- *после изменения вида авторизации пользователя в его карточке исчезнет флажок **Пользователь домена**.*

11.3. Резервное копирование Solar NGFW

11.3.1. Общие сведения

Резервное копирование в Solar NGFW применяется для решения задач:

- восстановление после сбоя;
- полное обновление операционной системы.

Процедура восстановления после сбоя зависит от характера сбоя, и в ряде случаев сводится к полному восстановлению ранее зарезервированных данных. Ниже описана процедура полного резервирования и восстановления данных. Эту процедуру, с небольшими изменениями, можно использовать для обновления операционных систем на серверах комплекса (в случае использования распределенной конфигурации).

11.3.2. Резервное копирование данных

11.3.2.1. Резервное копирование программного обеспечения

Создайте копию установочных DEB-пакетов и сохраните ее на надежном носителе данных. Это необходимо проделать один раз, сразу после установки или обновления, настройки и ввода комплекса в эксплуатацию.

11.3.2.2. Резервное копирование конфигурации системы

Резервное копирование конфигурации системы необходимо делать в случае внесения существенных изменений в конфигурацию комплекса, либо по расписанию.

Для резервного копирования конфигурации предназначены утилиты командной строки (скрипты) **export-config** и **import-config**, которые позволяют «одним движением» экспортировать и импортировать конфигурацию.

Примечание

*Следует отметить, что утилиты работают только на **master-узле** и только от пользователя **dozor** или **root**.*

Для экспорта всей конфигурации в файл на master-узле в CLI выполните команду:

 # export-config <output-file.json>

Для импорта конфигурации из файла в CLI на master-узле:

1. Выполните команды:

   # /opt/dozor/bin/shell

   # import-config <input-file.json>

2. Примените настройки с помощью команды:

   # accept-settings

11.3.2.3. Резервное копирование политики

Для оптимизации резервного копирования политики фильтрации предназначены команды утилиты **policy-tool**, которые позволяют экспортировать и импортировать политику фильтрации. При этом файл с резервной копией политики имеет меньший объем на диске, чем дамп БД.

Для экспорта политики на **master-узле** в CLI выполните команды:

1. Зайдите в **shell**: **/opt/dozor/bin/shell**

2. Экспортируйте политику:

   policy-tool export

   или

   policy-tool export -f /var/tmp/test_policy_export.json.

Для импорта политики:

1. На **master-узле** в CLI выполните команды:

   /opt/dozor/bin/shell

policy-tool import -f policy_for_import_policytool.json

2. В GUI перейдите в раздел **Политика** и нажмите кнопку **Применить политику**.

Для сброса всех правил политики к дефолтным настройкам:

1. На **master-узле** в CLI выполните команды:

   /opt/dozor/bin/shell

   policy-tool reset

2. В GUI перейдите в раздел **Политика** и нажамите кнопку **Применить политику**.

Поскольку политика может довольно часто изменяться, то ее резервное копирование лучше делать по расписанию: раз в день и раз в неделю.

Перед копированием также необходимо временно отключить веб-интерфейс администратора.

11.3.3. Восстановление зарезервированных данных

При восстановлении зарезервированных данных необходимо учесть следующее:

- На master-узле следует установить программное обеспечение заново и восстановить конфигурацию. Процедура восстановления программного обеспечения заключается в установке или переустановке набора DEB-пакетов.
- Процесс восстановления конфигурации осуществляется на каждом из узлов, где есть необходимость в этом. В случае обновления операционной системы необходимо восстановить все узлы.
- После установки новой операционной системы и установки набора пакетов Solar NGFW каждый узел будет работать в режиме **master-узла**.
- Процесс восстановления политики начинается с восстановления данных на **master-узле**.
- Восстановление политики на **slave-узлах** осуществляется после ее восстановления на **master-узле**.

11.3.4. Плановое резервное копирование

Плановое резервное копирование производится встроенными в Solar NGFW или внешними программными средствами, работающими на основе описанных выше процедур резервного копирования Solar NGFW .

11.4. Просмотр журнальных файлов Solar NGFW

Для просмотра журнальных файлов сервисов используется скрипт **seelog**. Для его запуска необходимо выполнить команду:

seelog <service-name>

где **<service-name>** – имя сервиса, журнальный файл которого требуется просмотреть.

Скрипт позволяет просматривать журнальные файлы в реальном времени. Файлы формируются с использованием значений, выводимых в стандартный поток вывода сообщений и в стандартный поток вывода ошибок. После выполнения команды запуска скрипта, например, для просмотра журнального файла сервиса **skvt-wizor**:

 # seelog skvt-wizor

на экран выводится информация вида:

```
2009-10-19 14:05:09.280829500 5268523 [Reactor-18] DEBUG nio_proxy  - proc@15999328: writing
290 bytes
2009-10-19 14:05:09.280832500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328: writing
done
2009-10-19 14:05:09.280835500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328:
clientWriteDone, state=WRITE_GENERATED_PAGE readingPreview=false download=false
serverDone=true
2009-10-19 14:05:09.280851500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328: Changing
 state to NEW_REQUEST
2009-10-19 14:05:09.280855500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328:
fireRequestFinished
2009-10-19 14:05:09.280885500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328: Running
 NEW_REQUEST filters; threaded=false
2009-10-19 14:05:09.280889500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328: Running
 FilterHelper:su.msk.jet.nioproxy.auth.AuthFilter@5db5ae
2009-10-19 14:05:09.280893500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328: Running
 FilterHelper:su.msk.jet.nioproxy.rule.engine.RuleEngineFilter@1efe475
2009-10-19 14:05:09.280926500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328: Changing
 state to READING_REQUEST_LINE
2009-10-19 14:05:09.280930500 5268524 [Reactor-18] DEBUG nio_proxy  - proc@15999328: expectInput
```

В таблице ниже приведен перечень существующих уровней детализации информации в журнальных файлах.

Табл. 11.3. Уровни детализации информации журнальных файлов

Уровень	Описание
DEBUG	Отладочная информация (для разработчиков)
INFO	Дополнительная информация, относящаяся к процедуре обработки данных
TRACE	Подробная отладочная информация (для разработчиков)
WARN	Уведомления о том, что некоторые компоненты не работают (без нарушения обработки данных)
ERROR	Сообщения об ошибках, способных нарушить обработку данных
FATAL	Критическая ошибка

Уровень детализации информации в журнальных файлах можно указать в веб-интерфейсе:

- на вкладке **Система > Основные настройки** > **Журналирование**;
- на вкладке **Система > Расширенные настройки**.

Далее приведен перечень уровней детализации информации, которые можно задать.

Табл. 11.4. Уровни детализации информации

Роль	Описание
Уровень отладки (log-level)	Задает уровень журналирования для тех подсистем фильтра, для которых отсутствуют дополнительные настройки уровня журналирования.
Уровень отладки аутентификации (log-auth)	Задает уровень журналирования подсистемы аутентификации.
Уровень отладки политики (log-policy)	Задает уровень отладки выполнения политики. Сюда же входит работа с внешними сервисами, необходимыми для работы политики – url-checker, антивирус и др.
Уровень отладки сетевого ввода-вывода (log-network)	Задает уровень журналирования подсистемы проксирования HTTP-протокола, управления сокетами, работы мультиплексированного ввода-вывода.
Уровень отладки архивации данных (log-archive)	Задает уровень журналирования подсистемы архивации POST-запросов и их передачи в Solar Dozor.

Перечисленные параметры можно найти с помощью поиска по конфигурации. Все настройки журналирования имеют стандартные уровни (ERROR, WARN, INFO, DEBUG, TRACE) – за исключением **Уровень отладки архивации данных** и **Уровень отладки аутентификации** – отсутствует TRACE. Кроме того, для других сервисов в веб-интерфейсе задается уровень журналирования VERBOSE (подробная информация) и DEBAG (отладочная информация).

Примечание

Наиболее объемным является журналирование процессов сетевого ввода-вывода (log-network), поэтому уровни DEBUG и TRACE включать в штатном режиме функционирования Solar NGFW не рекомендуется.

В распределенном режиме просмотр журнальных файлов осуществляется с помощью скрипта **seelog** для каждого узла по отдельности.

Действия администраторов по настройке политик фильтрации и конфигурации Solar NGFW, такие как создание, редактирование, удаление и просмотр правил/ресурсов/параметров, фиксируются в журнальном файле сервиса **skvt-play-server**. Пример записи из журнала:

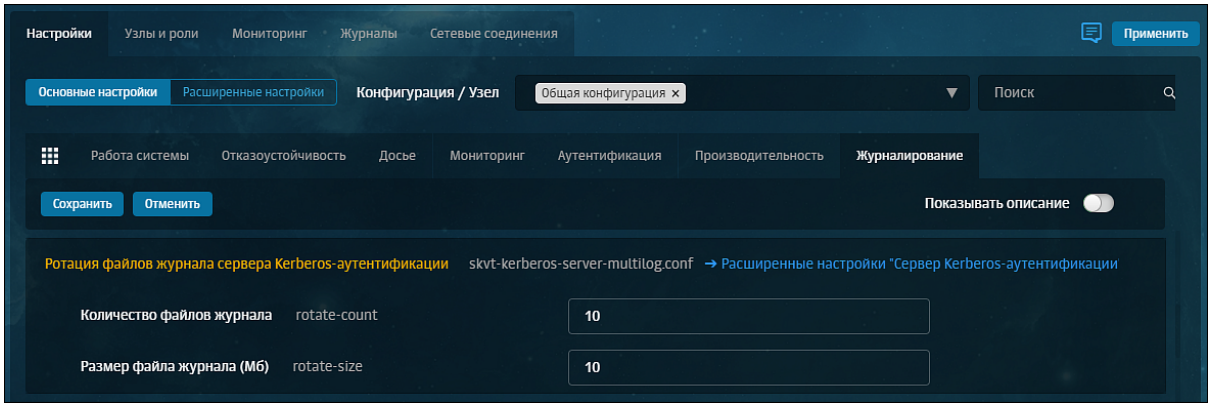
```
2018-04-13 14:29:40.379898500 INFO  application - Read item of type 'ruleset' with name 'a'
(41275174-c3e2-492a-ac1c-bbe29ac128b1) by user 'admin'
2018-04-13 14:30:04.803325500 INFO  application - Connected to Address book daemon realtime
stream
2018-04-13 14:30:09.092094500 INFO  application - Update item of type 'ruleset' with name 'a'
(41275174-c3e2-492a-ac1c-bbe29ac128b1) by user 'admin':
Add rule Rule(4f7df7b2-77cc-4c52-b49f-a98db6d54487,Правило
1,true,List(And((MatchUser(Some(3d4ffa9a-de30-4ee6-a60b-bece8c1d5acf),")),")),
List(Notify(840fc4c3-3a7c-4441-b49f-df4c4a55be3a,4a17763c-59a4-4fd2-99f3-1992d331f87c,")),Some())
```

11.5. Настройки журналирования

Для настройки журнальных файлов через GUI:

1. В меню **Система** > **Основные настройки** > **Журналирование** для секции настроек ротации журналов конкретного сервиса установите необходимые значения.

2. Нажмите **Сохранить** и **Применить**.



Текущие настройки журналирования идентичны тем, которые используются в расширенных настройках системы. Для удобства использования раздела в каждом блоке настроек предусмотрен переход по ссылке к расширенным настройкам соответствующего сервиса.

12. Настройка авторизации в web-интерфейсе с учетной записью в домене

Для настройки аутентификации с доменной учетной записью (речь идет о любом виде basic-аутентификации):

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Источник** выберите значение **ldap**.

2. Заполните появившиеся поля аналогично тому, как показано на **Рис.12.1**:

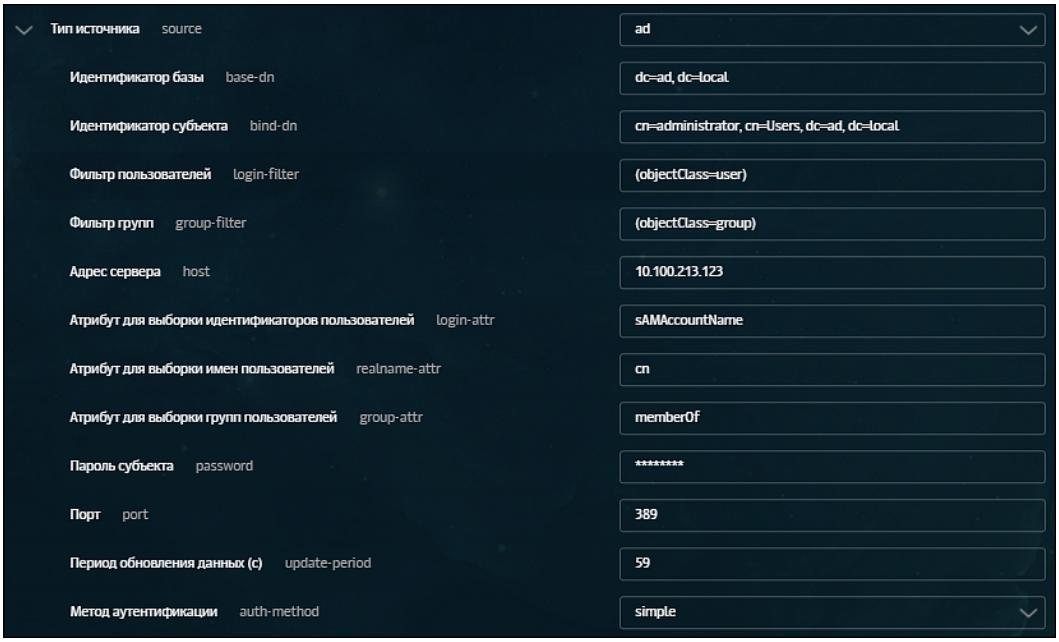


Рис. 12.1. Настройки сервера Active Directory

Параметр **Идентификатор субъекта** также можно задать в формате **administrator@ad.local**.

3. Создайте доменную учетную запись пользователя согласно инструкции раздела *Создание учётной записи пользователя* документа *Руководство администратора безопасности*. Имя создаваемой учетной записи должно совпадать с именем учетной записи в Active Directory.

Внимание!

Функция смены пароля для доменных учетных записей недоступна в веб-интерфейсе.

13. Выпуск сертификата организации для web-интерфейса

Если в организации имеется собственный УЦ, можно использовать его сертификат для установления соединения с GUI Solar NGFW. Для выпуска сертификата организации на master-узле Solar NGFW:

1. В CLI перейдите во временный каталог (например, **/var/tmp/**), выполнив команду:

   # cd /var/tmp

2. Создайте ключ ECDSA, выполнив команду:

   # openssl genrsa -out wp.key -aes256 2048

   Во время выполнения команды система потребует назначить пароль для ключа. Введите пароль и запомните его. После ввода подтвердите пароль.

3. Создайте в текущем каталоге файл с именем **openssl.cnf** и добавьте в него данные:

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name
promt=yes
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
countryName_default             = RU

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Moscow

localityName                = Locality Name (eg, city)
localityName_default            = Moscow

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = Organization

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = Dept

commonName                  = Common Name (eg, your name or your server\'s hostname)
commonName_default              = proxy.org.com

emailAddress                = Email Address
emailAddress_default            = support@org.com

[ v3_req ]
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = proxy.org.com
IP.0 = 192.168.10.15
```

   Выделенные значения параметров замените на актуальные значения организации:

- **countryName_default** – двухбуквенный код страны;
- **stateOrProvinceName_default** – регион;
- **localityName_default** – город;
- **organizationName_default** – название организации;
- **organizationalUnitName_default** – название подразделения, департамента и т. д.;
- **commonName_default** – FQDN master-узла;
- **emailAddress_default** – контактный адрес электронной почты организации;
- **DNS.0** – FQDN master-узла;
- **IP.0** – IP-адрес master-узла.

4. Сгенерируйте запрос на подпись сертификата, выполнив команду:

   # openssl req -new -key wp.key -out name.csr -config openssl.cnf

   В процессе выполнения команды система потребует ввести пароль, заданный на шаге 2.

5. На сервере организации, имеющем роль CA (Certification Authority), проверьте используемый алгоритм шифрования. Для этого откройте программу **Командная строка** от имени администратора и выполните в ней следующую команду:

   certutil - getreg ca \ csp \ CNGHashAlgorithm

   Если значение параметра **REG_SZ** равно **SHA1**, выполните команды:

   certutil -setreg ca\csp\CNGHashAlgorithm SHA256

   net stop CertSvc && net start CertSvc

6. Перевыпишите корневой сертификат и перезапустите службу Certificate Services, выполнив следующие команды:

   certutil -renewCert ReuseKeys

   net stop CertSvc && net start CertSvc

7. Зайдите на портал УЦ Windows.

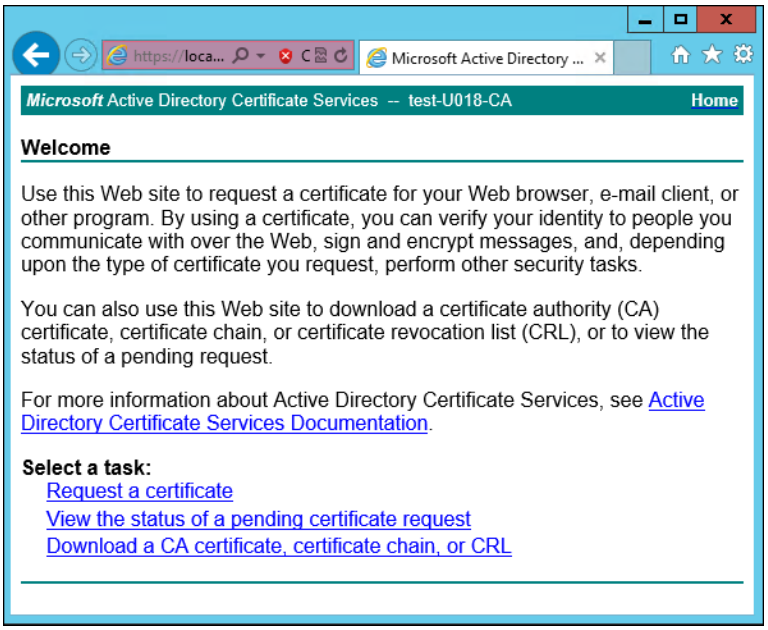


Рис. 13.1. Экран приветствия УЦ Windows

8. Нажмите **Request a certificate**.

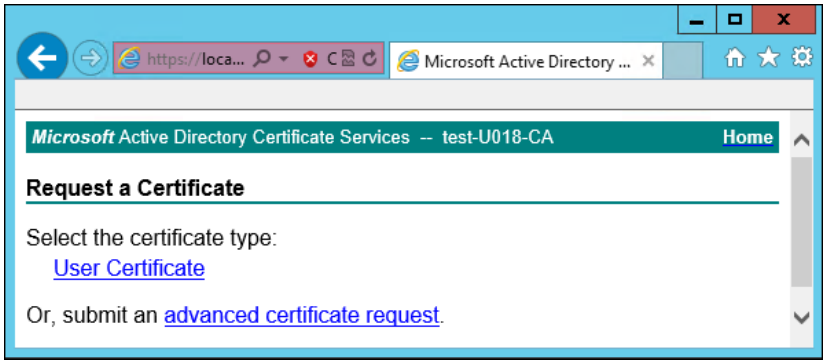


Рис. 13.2. Экран запроса сертификата

9. Нажмите **advanced certificate request**.

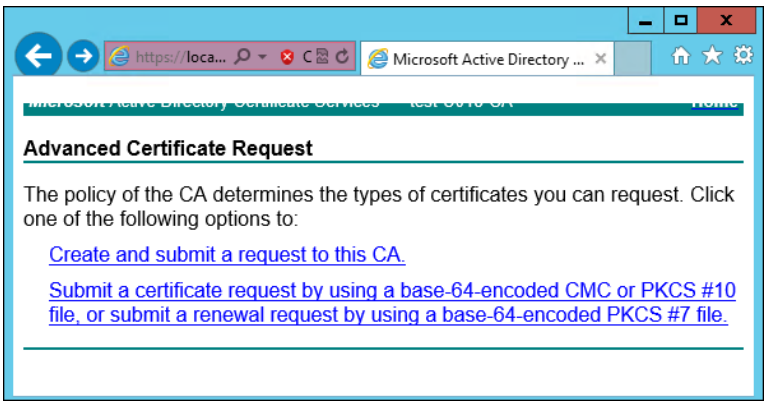


Рис. 13.3. Экран особого запроса сертификата

10. Нажмите **Submit a certificate request by using...**.

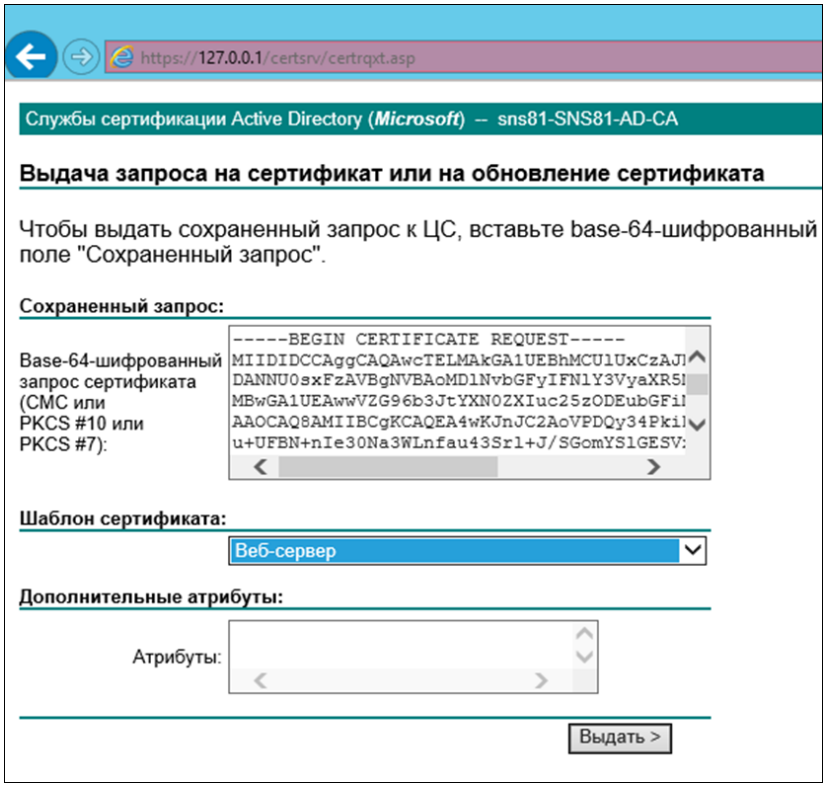


Рис. 13.4. Экран атрибутов сертификата

11. Выберите шаблон сертификата **Веб-сервер** и вставьте в поле **Base-64** содержимое файла, созданного на шаге 4. Нажмите **Выдать**.

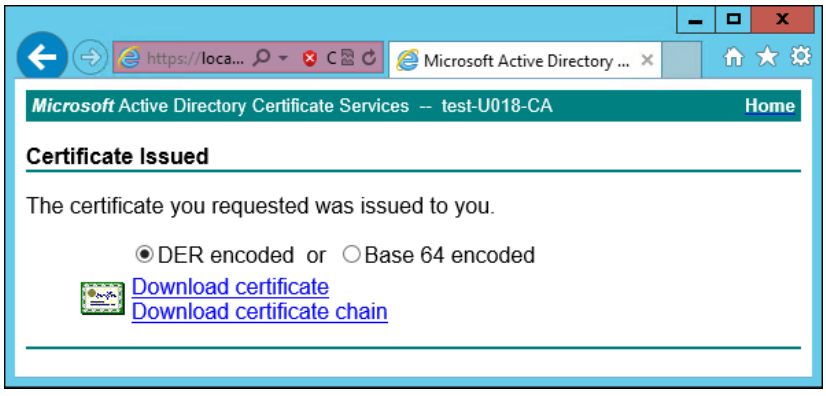


Рис. 13.5. Экран выдачи сертификата

12. Нажмите **Download certificate**. Сохраните файл сертификата с именем **wp.cer** во временный каталог, выбранный на шаге 1.

13. Перейдите на главную страницу портала УЦ и нажмите **Download a CA certificate, certificate chain or CRL**. Сохраните сертификат УЦ с именем **ca.cer** в тот же каталог.

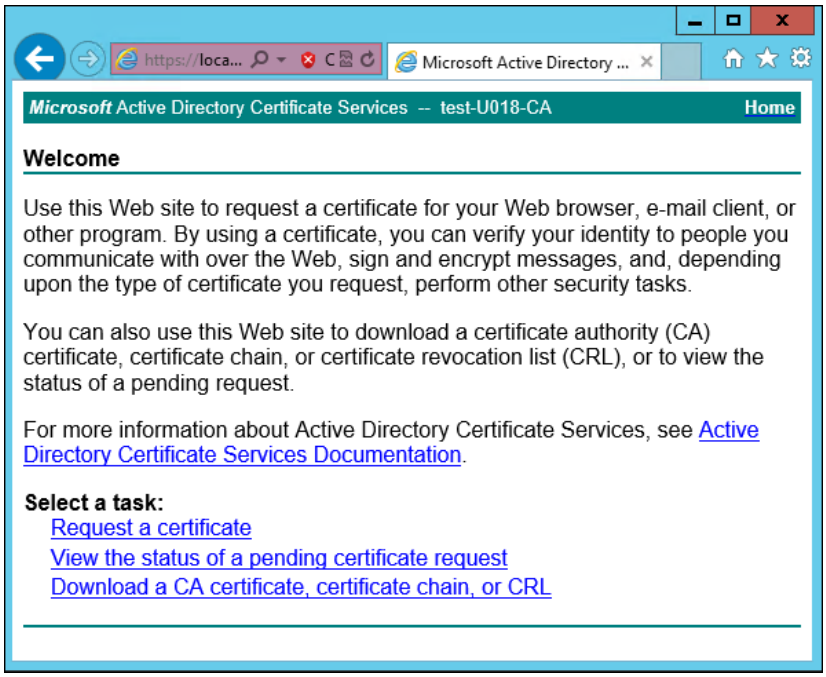


Рис. 13.6. Экран приветствия УЦ Windows

14. Вернитесь в CLI Solar NGFW, перейдите в выбранный временный каталог и сконвертируйте загруженные сертификаты в формат PEM, выполнив команды:

    # openssl x509 -inform der -in wp.cer -out wp.pem

    # openssl x509 -inform der -in ca.cer -out ca.pem

15. Объедините сертификаты и ключ в сертификат pkcs12, выполнив команду:

    # openssl pkcs12 -export -out wp.p12 -inkey wp.key -in wp.pem -certfile ca.pem

    Во время выполнения команды система потребует ввести пароль.

16. Импортируйте Java-хранилище сертификатов, выполнив команду вида:

    # keytool -importkeystore -deststorepass <password> -destkeypass <password> -destkeystore WEB.jks -srckeystore wp.p12 -srcstorepass <password>

    где **<password>** – выбранный пароль.

17. Скопируйте Java-хранилище в каталог Solar NGFW, выполнив команду:

    # cp WEB.jks /opt/dozor/skvt/var/lib/

18. Смените владельца хранилища, выполнив команду вида:

    # chown dozor:dozor /opt/dozor/skvt/var/lib/WEB.jks

19. Проверьте, что сертификат находится в хранилище, выполнив команду вида:

    # keytool -list -keystore /opt/dozor/skvt/var/lib/WEB.jks

О наличии сертификата в хранилище будет свидетельствовать вывод:

```
1, Jul 10, 2018, PrivateKeyEntry,
Certificate fingerprint (SHA1): B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
```

20. В GUI в разделе **Система > Расширенные настройки > Интерфейс > Сервер веб-интерфейса** задайте значения параметров:

- **Путь к хранилищу ключей** – **/opt/dozor/skvt/var/lib/WEB.jks** ;
- **Пароль к хранилищу ключей** – пароль.

21. Перезапустите сервис **skvt-play-server**, выполнив в CLI команды:

 # /opt/dozor/bin/shell

 # dsctl restart skvt-play-server

14. Мониторинг системы

Мониторинг системы доступен на вкладке **Мониторинг** раздела **Система**.

14.1. Состояние узлов кластера Solar NGFW

На вкладке **Состояние** представлена информация о состоянии узлов кластера Solar NGFW.

В верхней части расположен список узлов для отображения. По умолчанию отображаются все узлы. Для отображения определенного набора узлов откройте список узлов и выделите курсором все требуемые узлы. Сбросить группировку можно с помощью значка .

Состояние узла отображается как **OK**, если в настоящий момент на нем нет проблем с уровнем критичности **Средняя** или выше. Если на узле есть проблемы с уровнем критичности **Средняя** или выше, в соответствующем прямоугольном блоке отображается их количество.

В нижней части расположены списки проблем всех выбранных узлов: слева – с уровнем критичности **Средняя** и выше, справа – с уровнем критичности **Низкая**.

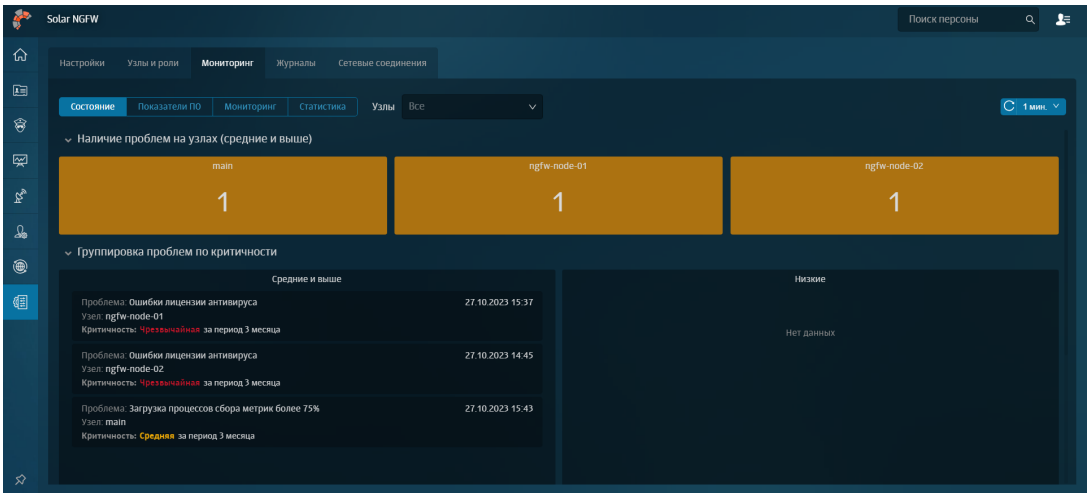


Рис. 14.1. Вкладка «Состояние»

14.2. Мониторинг показателей Solar NGFW

На вкладке **Рабочий стол** представлена актуальная информация о работе Solar NGFW на узлах. Статистику за прошедший период можно посмотреть на вкладке **Система > Мониторинг**.

В верхней части расположен список узлов для отображения и инструмент для выбора временного отрезка, за который необходимо получить данные.

Ниже расположены блоки с названиями узлов. Принцип их отображения такой же, как и на вкладке **Состояние**.

В нижней части расположены графики:

- **Наличие проблем на узлах (средние и выше)**;

- **Количество уникальных персон на узлах фильтрации (в минутах)**;
- **Время загрузки сайтов напрямую (без прокси)**;
- **Время загрузки сайтов через узлы фильтрации**;

Примечание

*Из-за отключенной проверки доступа в интернет для агентов мониторинга на графике **Время загрузки сайтов через узлы фильтрации** может не быть данных. Чтобы данные отображались, в разделе **Система > Основные настройки > Мониторинг > Агенты мониторинга** для параметра **Тип проверки доступа в интернет** установите значение, отличное от **OFF** (например, **Simple**).*

- **Коды загрузки сайтов**;
- **База статистики**.

На каждом графике можно выбрать определенный интервал для отображения на всю длину шкалы. Для этого поместите курсор в один из концов требуемого интервала и с зажатой левой кнопкой мыши переместите курсор к другому концу интервала, а затем отпустите кнопку мыши.

14.3. Мониторинг показателей аппаратного обеспечения

На вкладке **Мониторинг** представлена информация о состоянии аппаратного обеспечения узлов Solar NGFW.

В верхней части расположен список узлов для отображения и инструмент для выбора временного отрезка, за который необходимо получить данные.

Ниже расположены блоки с названиями узлов (см. далее). Принцип их отображения такой же, как и на вкладке **Состояние**.

Табл. 14.1. Блоки данных вкладки "Мониторинг"

Блок	Описание
Время работы	Время непрерывной работы узла, прошедшее с момента последней перезагрузки (включения)
Средняя загрузка (load average)	Значение **Load average** за последнюю минуту в выводе команды **top** на узле
Количество ядер ЦПУ	Количество ядер процессора на узле
Доступно памяти	Объем свободной оперативной памяти на узле

Ниже расположена группа графиков для каждого выбранного узла, отображающих следующие данные (см. далее).

Табл. 14.2. Группа графиков выбранного узла

График	Описание
ЦПУ	История загрузки процессора
Память	История потребления оперативной памяти

График	Описание
Свободное место для разделов	Свободное пространство на жестком диске в процентах
Свободные индексные дескрипторы для разделов	Количество свободных индексных дескрипторов для разделов на файловой системе в процентах
Свободное место для разделов	Свободное пространство на жестком диске в абсолютном исчислении
Активное время дисков	Процент, отражающий время, которое жесткий диск занят чтением/записью
Количество операций чтения/записи на дисках в секунду	Количество операций ввода-вывода в секунду, выполняемых системой хранения данных
Время ожидания чтения/записи дисков	Время, затрачиваемое на операции ожидания чтения и записи дисков в миллисекундах
Объем чтения/записи на дисках в секунду	Объем жесткого диска, занимаемый операциями чтения/записи
Сетевой трафик	История скорости передачи данных через сетевые интерфейсы узла

14.4. Статистика

В разделе **Система > Мониторинг > Статистика** системный администратор может построить отчеты по необходимым статистическим показателям, выбрав определенный набор узлов и период времени.

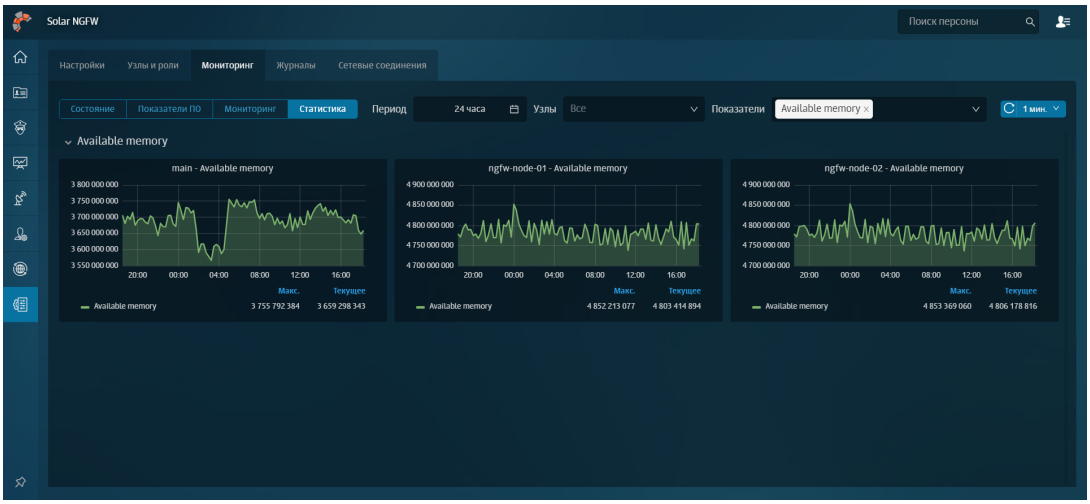


Рис. 14.2. Вкладка «Статистика»

Для построения отчетов по конкретным показателям в выпадающем списке выделите курсором необходимые показатели.

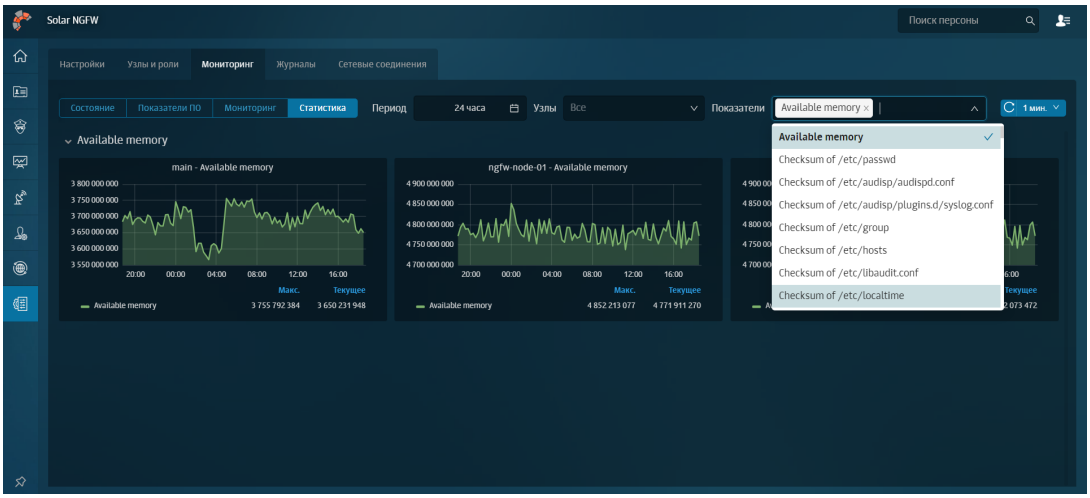


Рис. 14.3. Выбор показателей для построения отчетов

14.5. Журналы событий: просмотр записей журнальных файлов в интерфейсе

Журналы событий содержат информацию о действиях пользователей и работе системы, которая представлена в интерфейсе в форме записей журнальных файлов на вкладке **Журналы** раздела **Система**.

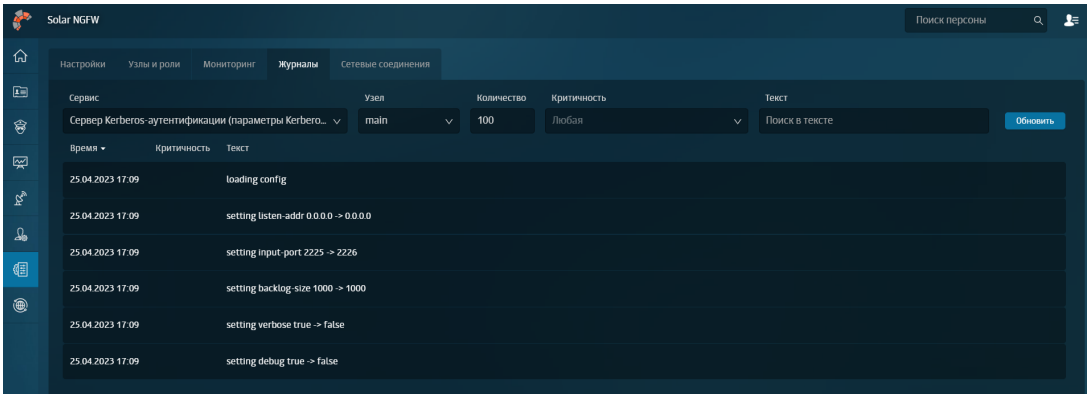


Рис. 14.4. Журнал событий

На вкладке **Журналы** можно просмотреть информацию по следующим сервисам и категориям информации о работе системы:

- **Сообщения журнала обнаружения вторжений**: события, полученные от системы предотвращения вторжений;
- **Проверка URL-адресов**: состояние категоризатора и его лицензии;
- **Сервер Kerberos-аутентификации**: параметры аутентификации и ошибки генерации ключа для аутентификации;
- **HTTP-фильтр**: состояние фильтрации трафика и возникшие ошибки взаимодействия;
- **Сервер NTLM-аутентификации**: параметры NTLM-аутентификации и возникшие при настройке аутентификации ошибки;

- **Веб-сервер**: активность администратора и внесенные в политику изменения;
- **Сервер аутентификации**: параметры доменной аутентификации;
- **Системные сообщения**: события, произошедшие в системе с момента ее запуска;
- **Проверка целостности системы**: контрольные суммы файлов (установочных пакетов) и ошибки при их подсчете;
- **Безопасность операционной системы**: сообщения об угрозе безопасности;
- **Трансляция сетевых адресов**: срабатывание правил трансляции сетевых адресов.

Отобразить информацию по конкретной категории можно, выбрав соответствующий фильтр из списка в поле **Сервис**.

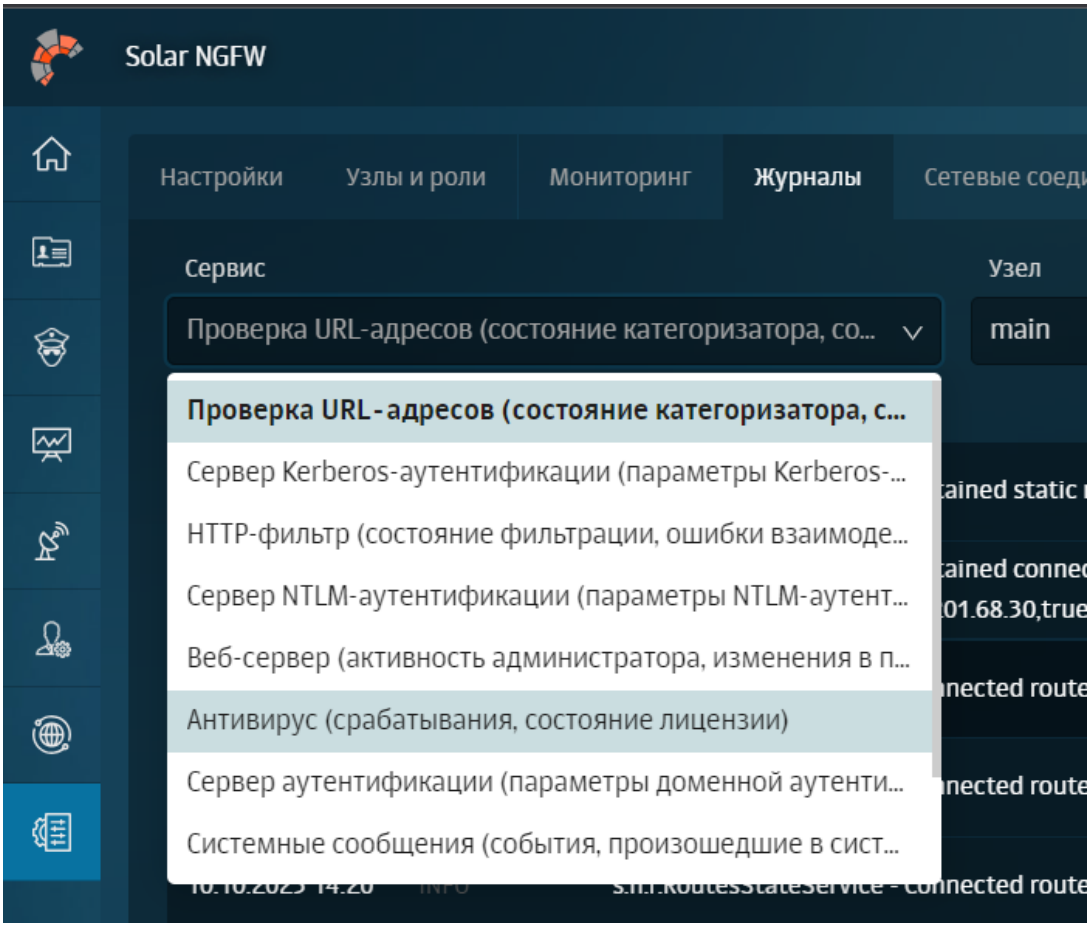


Рис. 14.5. Фильтры журнала событий

Для настройки более детального отображения сведений воспользуйтесь другими фильтрами в верхней части раздела, с помощью которых можно выбрать:

- узел, для которого будут отображаться журнальные записи;
- число выводимых записей журнальных файлов;
- критичность отображаемого события:

- **Info** – информационная запись,;
- **Warning** – предупреждение, выводится в том случае, если обнаружено некое несоответствие ожидаемому поведению;
- **Error** – запись об ошибке, позволяющей продолжить нормальное функционирование подсистемы;
- **Debug** – отладочная информация.

По умолчанию события, произошедшие раньше, отображаются сверху.

Также вы можете воспользоваться поиском по тексту, указав искомое слово в поле **Текст**.

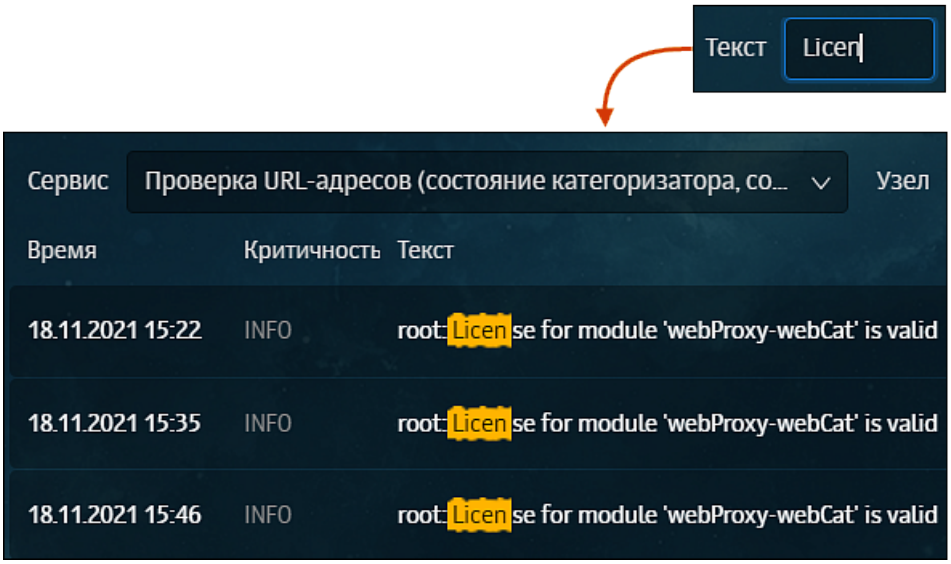


Рис. 14.6. Поиск по тексту в журнале событий

Для работы с журналами событий реализована правовая модель доступа, которая основана на разграничении данных по категориям журналов событий:

- *системные* (сведения о работе сервиса управления, кэш-сервиса, сервиса фильтрации трафика, сервиса проверки URL по категориям и системного файла «messages»);
- *фильтрации* (сведения о срабатывании правил политики: слои **Фильтр транзитного трафика**, **Фильтр входящего трафика**, **Фильтр исходящего трафика** и **Трансляция адресов**);
- *безопасности* (сведения о работе сервиса управления, кэш-сервиса, сервисов NTLM- и Kerberos-аутентификации, сервиса аутентификации).

Пользователь может просмотреть записи только тех категорий журналов, права на которые ему выданы. Все доступные для просмотра журналы отображаются в списке фильтров поля **Сервис**.

Подробная информацию приведена в документе *Руководство администратора безопасности*.

14.6. Журнал соединений

В разделе **Журнал соединений** отображается статистика сетевых соединений через узлы фильтрации. Например, количество сетевых пакетов между определенными IP-адресами, по определенному протоколу, порту или приложению за конкретное время.

Статистику в отчете можно отфильтровать по:

- приложению,
- узлам фильтрации,
- IP-адресу,
- протоколу.

По умолчанию данные в таблице отображаются по столбцам: **Дата/время**, **ID**, **Состояние, IP-адрес источника**, **IP-адрес назначения**, **Протокол**, **Результат проверки**. Чтобы изменить состав таблицы, откройте раскрывающийся список фильтра **Колонки** и выберите названия столбцов, которые нужно отобразить в таблице. Можно отобразить все колонки из списка.

Чтобы изменить состав фильтров в отчете категории **Журнал соединений**, добавьте или скройте неиспользуемые фильтры с помощью раскрывающегося меню **Еще**.

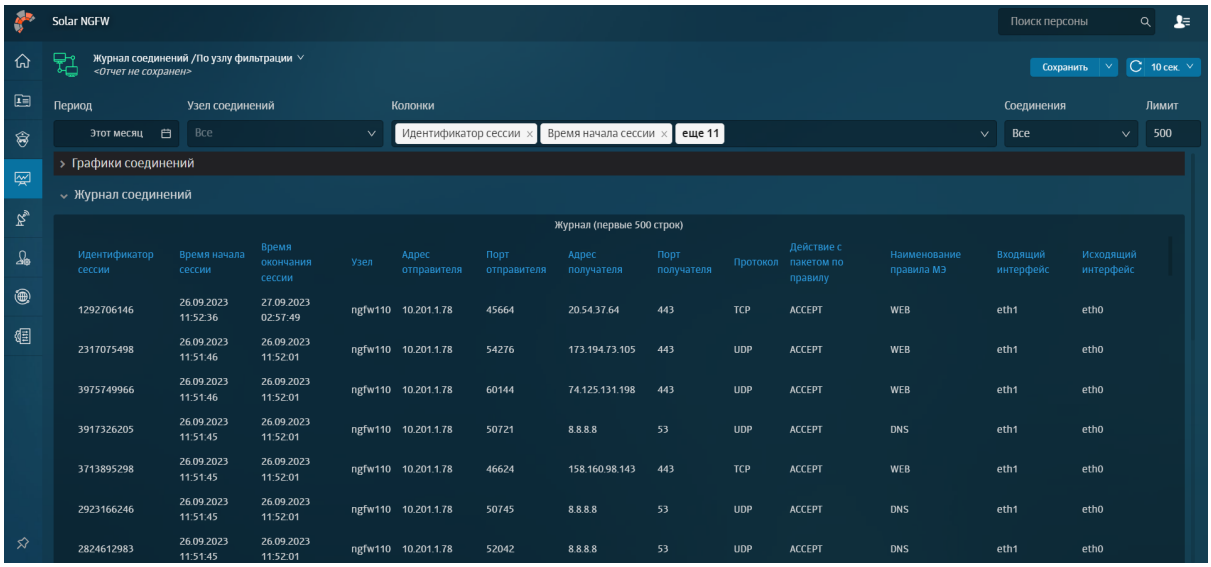


Рис. 14.7. Журнал соединений

Примечание

*Активные сессии могут обрабатываться несколькими правилами МЭ, поэтому в разделе **Журнал соединений** они отображаются в виде нескольких записей, где одна из них характеризует прохождение некоторого количества пакетов по определенному правилу. После завершения сессии все данные по ней агрегируются, и сессия отображается в виде одной записи, содержащей информацию о результате обработки данной сессии.*

Статистика соединения приложения, которое распознается DPI, отображается в виде двух строк с данными:

- *До детектирования приложения – информация о начальной фазе TCP-соединения и нескольких пакетов, необходимых DPI для выполнения распознавания.*
- *После детектирования приложения – запись об основной части соединения, соответсвующего распознанному приложению.*

Данным фазам соединения соответствует один и тот же идентификатор, который позволяет получить полную информацию о соединении.

15. Проверка работоспособности настроенного Solar NGFW

Для успешной работы настроенного Solar NGFW выполните проверки, перечисленные в Табл.15.1.

Табл. 15.1. Проверки работоспособности системы

№	Проверка	Действия
1.	Состояние узлов и назначение ролей	В разделе **Система > Узлы и роли** проверьте наличие условий: • отображаются все узлы Solar NGFW; • состояние каждого узла: **Узел доступен**.
2.	Наличие уведомлений и работа мониторинга	В разделе **Система > Мониторинг** проверьте наличие условий: • на виджетах не отображаются ошибки; • на странице отсутствуют надписи: **Нет данных**.
3.	Интеграция Досье с внешними источниками	В разделе **Досье > Персоны** проверьте наличие условий: • список персон организации актуален; • отсутствуют ошибки связи с источником.
4.	Работа категоризатора	В разделе **Политика > База категоризации** проверьте отображение результатов проверки ресурсов на корректность: • название категоризатора; • категория ресурса.
5.	Вскрытие HTTPS	1. В разделе **Политика > Вскрытие HTTPS** создайте правило на вскрытие. 2. Проверьте соблюдение условий: • При посещении ресурса через прокси-сервер сертификат на пользовательском АРМ должен совпадать с сертификатом, указанным в конфигурации системы. • В **Журнале запросов** раздела **Статистика** должен быть виден мониторинг URL ресурсов (параметр **URL путь**). Следует учесть, что внешнее ПО, например DLP-система Solar Dozor, может использовать свой самоподписанный сертификат.
6.	Работа антивируса	1. В разделе **Политика > Перенаправление по ICAP** проверьте или сформируйте правило для перенаправления трафика в антивирус (см. раздел 6.2). 2. Проверьте работу вскрытия HTTPS-трафика (см. выше). 3. Перейдите с клиента через прокси-сервер с ролью балансировщика (порт 2270) по адресу https://www.eicar.org/download-anti-malware-testfile/ и скачайте тестовый вирус *eicar*: • если в браузере отображается страница блокировки, антивирус успешно работает; • если тестовый вирус загружается на компьютер, проверьте мониторинг URL ресурсов (параметр **URL путь**) в **Журнале запросов**.

16. Аварийные ситуации

16.1. БД Clickhouse

БД Clickhouse в некоторых ситуациях может занимать всю предоставленную оперативную память и приостанавливать свою работу в ожидании освобождения дополнительного объема памяти. Это связано с внутренними значениями лимита на использование памяти по умолчанию, которые могут превосходить объем доступной памяти на конкретном узле Solar NGFW.

Для решения этой проблемы:

1. Откройте конфигурационный файл **/data/repos/dozor/config-final.git/<идентификатор узла>/clickhouse/** для редактирования.
2. В разделе **<yandex> <profiles> <default>** отредактируйте значение параметра **max_memory_usage**, задав для него значение лимита памяти в байтах.
3. В том же разделе создайте параметры **max_memory_usage_for_user** и **max_memory_usage_for_all_queries** и задайте для них то же значение.
4. Сохраните и закройте файл.
5. Перезапустите процесс **clickhouse**, выполнив команды:

   # /opt/dozor/bin/shell

   # dsctl restart clickhouse

17. Получение технической поддержки

Для получения консультации по техническим вопросам можно обратиться по адресу **support@rt-solar.ru**.

С условиями поддержки можно ознакомиться на сайте компании **«Ростелеком-Солар»** (по адресу: **http://solar-rt.ru/support/**). При оформлении запроса укажите номер контракта на техническую поддержку, опишите проблему, укажите свое полное имя, адрес электронной почты и номер телефона.

Приложение А. Коды фильтрации политики

В данном приложении приведено описание возможных кодов фильтрации политики и их значений, которые можно увидеть в записях журнала **syslog**. Например, **FilterCodes=[11, 0, 0, 31]**
.

Табл. А.1. HTTP-коды фильтрации

Код фильтрации	Значение	Описание действий
0	CONTINUE	Ничего не делать и продолжить обработку политикой дальше
1	ALLOW	Разрешить запрос/ответ
2	DENY	Заблокировать запрос/ответ и отобразить страницу с шаблоном блокировки
3	NOTIFY	Уведомить системного администратора
4	ARCHIVE	Архивировать логи в сервис Clickhouse
5	CONFIRM	Запросить подтверждение
6	DETECT_MIMETYPE	Определить MIME-типа данных (см. D.2)
7	DETECT_CATEGORY	Определить категорию ресурса
8	MODIFY_HEADERS	Изменить заголовков на правиле значение
10	REDIRECT	Перенаправить на указанный в правиле URL
11	MITM	Вскрыть трафик
12	CHECK_CERT	Проверить сертификат
30	FORBIDDEN_NETWORK	Запрещенная сеть
31	NOATH	Не аутентифицировать пользователя
32	BLOCKED	Заблокировать запрос/ответ

Приложение В. Поддерживаемые протоколы DPI

В данном приложении приведен перечень поддерживаемых протоколов DPI и описание их.

Табл. В.1. Поддерживаемые протоколы DPI

Категория	Приложение	Номер в статистике	Описание протокола
Unrated	Unknown	0	Нераспознанный протокол.
	FTP_CONTROL	1	Протокол передачи файлов по сети. Использует разные сетевые соединения для передачи команд и данных между клиентом и сервером. При использовании протокола FTP можно пройти аутентификацию, передавая логин и пароль открытым текстом, или подключиться анонимно (если разрешено).
	POP3	2	Интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP-соединению. POP3-сервер прослушивает общеизвестный порт 110. Шифрование связи для POP3 запрашивается после запуска протокола с помощью либо команды STLS (если она поддерживается), либо POP3S, которая соединяется с сервером, используя TLS или SSL по TCP-порту 995.
	IMAP	4	Протокол прикладного уровня для доступа к электронной почте. Протокол IMAP работает только с сообщениями и не требует каких-либо пакетов со специальными заголовками. IMAP предоставляет широкие возможности для работы с почтовыми ящиками, находящимися на почтовом сервере. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя.
	eDonkey	36	Клиент файлообменной сети, построенный по принципу P2P на основе сетевого протокола прикладного уровня MFTP.
	IRC	65	Протокол прикладного уровня для обмена сообщениями в режиме реального времени. Разработан в основном для группового общения, также позволяет общаться через личные сообщения и обмениваться данными, в том числе файлами. IRC использует транспортный протокол TCP и криптографический TLS (опционально).
	Telnet	77	Текстовый протокол, используемый для подключения (при помощи транспорта TCP) к удаленным устройствам для доступа к CLI. При подключении данные передаются в открытом виде.
	RSH	294	Протокол, позволяющий подключаться удаленно к устройству и выполнять команды на нем.
	FTPS	311	Протокол, используемый для передачи файлов между компьютерами.
Acceptable	SMTP	3	Сетевой протокол, предназначенный для передачи электронной почты между сервером отправителя и почтовым клиентом/сервером получателя.
	DNS	5	Протокол преобразует удобочитаемые имена компьютеров, например, www.example.ru, в числовые IP-адреса, необходимые для работы в сети.

Категория	Приложение	Номер в статистике	Описание протокола
	IPP	6	Сетевой протокол прикладного уровня для передачи документов на печать.
	HTTP	7	Протокол передачи гипертекста.
	MDNS	8	Протокол MDNS переводит доменные имена в IP-адреса в небольших сетях, которые не включают локальный сервер имен.
	NTP	9	Сетевой протокол, используемый для синхронизации даты и времени через интернет. Один из наиболее широко используемых протоколов.
	NetBIOS	10	Протокол позволяет компьютерам в небольшой локальной сети взаимодействовать друг с другом.
	NFS	11	Протокол используется для создания служб обмена файлами в основном для систем UNIX/Linux. Как правило, протокол служит для предоставления центрального хранилища по локальной сети.
	SSDP	12	Сетевой протокол, основанный на наборе протоколов интернета, служащий для объявления и обнаружения сетевых сервисов.
	BGP	13	Протокол динамической маршрутизации. Относится к классу протоколов маршрутизации внешнего шлюза. На текущий момент является основным протоколом динамической маршрутизации в сети Интернет.
	SNMP	14	Протокол, который используется для управления сетевыми устройствами.
	XDMCP	15	Протокол аутентификации между X-сервером и X-клиентом. Задача XDMCP – предоставление стандартного механизма для запроса сервиса входа в систему автономным дисплеем. XDMCP не рекомендован к использованию в сетях общего доступа, поскольку по умолчанию передает данные в не зашифрованном виде, но при подключении модулей шифрования его использование бывает вполне оправданным. Основан на передаче информации посредством UDP/IP дейтаграмм, по умолчанию использует 177 порт.
	Syslog	17	Стандарт отправки и регистрации сообщений о происходящих в системе событиях, использующийся в компьютерных сетях, работающих по протоколу IP.
	DHCP	18	Сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.
	PostgreSQL	19	Свободная объектно-реляционная система управления базами данных.
	MySQL	20	Свободная реляционная система управления базами данных. Обычно MySQL используется в качестве сервера, к которому обращаются локальные или удаленные клиенты, однако в дистрибутив входит библиотека внутреннего сервера, позволяющая включать MySQL в автономные программы.
	VMware	28	Протокол используется для подключения клиентов к серверным системам VMware.
	BitTorrent	37	Протокол для обмена файлами через интернет. Обычно он используется для загрузки больших файлов, а также фильмов, музыки и других медиафайлов.

Категория	Приложение	Номер в статистике	Описание протокола
	Memcached	40	Программное обеспечение, реализующее сервис кэширования данных в оперативной памяти на основе хеш-таблицы.
	SMBv23	41	Сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам.
	Modbus	44	Открытый коммуникационный протокол, основанный на архитектуре «ведущий - ведомый». Широко применяется в промышленности для организации связи между электронными устройствами.
	MongoDB	60	Система управления базами данных, не требующая описания схемы таблиц.
	VXLAN	64	Технология виртуализации сети, которая решает проблемы масштабируемости, связанные с большими облачными вычислениями.
	MerakiCloud	66	Протокол предоставляет сервис туннелирования устройств Meraki для подключения к облачной инфраструктуре Cisco.
	Jabber	67	Открытый, основанный на XML, свободный для использования протокол для мгновенного обмена сообщениями и информацией о присутствии в режиме, близком к режиму реального времени.
	Nats	68	Протокол представляет собой текстовый протокол обмена сообщениями публикации/подписки. Его можно использовать для построения распределенных систем, связи устройств и т.д.
	VRRP	73	Сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию.
	STUN	78	Сетевой протокол, позволяющий клиенту, находящемуся за сервером трансляции адресов, определить свой внешний IP-адрес, способ трансляции адреса и порта во внешней сети.
	RTP	87	Протокол передачи данных, работает на прикладном уровне и используется при передаче трафика реального времени.
	RDP	88	Проприетарный протокол прикладного уровня, использующийся для обеспечения удаленной работы пользователя с сервером, на котором запущен сервис терминальных подключений.
	VNC	89	Система удаленного доступа к рабочему столу компьютера.
	SSH	92	Сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений.
	Usenet	93	Компьютерная сеть, используемая для общения и публикации файлов.
	MGCP	94	Протокол, предназначенный для управления шлюзами между системами традиционной телефонии (PSTN) и VoIP-системами.
	IAX	95	Протокол используется для транспортировки сеансов VoIP-телефонии между серверами и оконечными устройствами.
	TFTP	96	Простой протокол, используемый для передачи файлов. Обычно он используется в локальной сети для начальной загрузки систем VoIP и других сетевых устройств.

Категория	Приложение	Номер в статистике	Описание протокола
	AFP	97	Сетевой протокол представительского и прикладного уровней сетевой модели OSI, предоставляющий доступ к файлам в Mac OS X.
	SIP	100	Протокол сигнализации VoIP, используемый для инициирования, поддержания и завершения сеансов в реальном времени, которые включают приложения для передачи голоса, видео и обмена сообщениями.
	DHCPV6	103	Сетевой протокол для конфигурации узлов версии 6 (IPv6) протокола интернет с IP-адресами, префиксами IP и другими данными конфигурации, которые необходимы для работы в сети IPv6.
	Kerberos	111	Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними.
	LDAP	112	Протокол, определяющий методы, посредством которых осуществляется доступ к данным каталогов Microsoft (ActiveDirectory) для операционных систем Windows.
	MsSQL-TDS	114	Протокол прикладного уровня, используемый для передачи данных между сервером базы данных и клиентом.
	PPTP	115	Туннельный протокол, позволяющий компьютеру устанавливать защищенное соединение с сервером за счет создания специального туннеля в стандартной, незащищенной сети.
	RPC	127	Класс технологий, позволяющих программам вызывать функции или процедуры в другом адресном пространстве (на удаленных узлах или в независимой сторонней системе на том же узле). Обычно реализация RPC-технологии включает два компонента: сетевой протокол для обмена в режиме клиент-сервер и язык сериализации объектов или структур для необъектных RPC.
	NetFlow	128	Технология, разработанная Cisco для мониторинга трафика в сетях передачи данных. Обычно он встроен в коммутаторы и маршрутизаторы.
	sFlow	129	Стандарт для мониторинга компьютерных сетей, беспроводных сетей и сетевых устройств.
	HTTP_Connect	130	Метод запускает двустороннюю связь с запрошенным ресурсом. Метод можно использовать для открытия туннеля.
	HTTP_Proxy	131	Прокси-сервер, позволяющий работать в интернете по HTTP.
	CHECKMK	138	Используется для мониторинга серверов, приложений, сетей, облачных инфраструктур, контейнеров, хранилищ, баз данных и датчиков среды.
	AJP	139	Бинарный протокол, который может проводить входящие запросы с веб-сервера до сервера приложений, который находится за веб-сервером.
	Radius	146	Протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах
	LotusNotes	150	Платформа для автоматизации совместной деятельности рабочих групп. Используется с различными локальными и совместными серверными приложениями, включая электронную почту, календари и менеджеры личной информации.

Категория	Приложение	Номер в статистике	Описание протокола
	SAP	151	Протокол используется для широковещательных передач сеансов многоадресных данных и связи. Например, его можно использовать для представления пользователю списка доступных аудиопотоков.
	GTP	152	Группа протоколов соединения на основе IP, используемая в сетях GSM, UMTS и LTE.
	WSD	153	Протокол для автоматического обнаружения, настройки и управления. Реализует Plug and Play для сетевых устройств.
	LLMNR	154	Протокол позволяет IPv6 и IPv4 клиентам за счет широковещательных запросов в локальном сегменте сети L2 разрешать имена соседних компьютеров без использования DNS сервера.
	H323	158	Стандарт, используемый для организации VoIP-телефонии и видеоконференцсвязи.
	NOE	160	Протокол, обеспечивающий автоматизацию управления и виртуализацию сетей. Позволяет создавать несколько виртуальных сетей (используя одну физическую) для каждой категории устройств и создать оптимальную конфигурацию и изоляцию для каждой виртуальной сети.
	CiscoVPN	161	Проприетарный вариант протокола IPSec, разрабатываемый компанией Cisco.
	CiscoSkinny	164	Определяет набор сообщений между клиентом Skinny для взаимодействия проводных и беспроводных IP-телефонов Cisco 7900 серии, таких как Cisco 7960, 7940, 7920, с сервером голосовой почты Cisco Unity и Cisco CallManager.
	RTCP	165	Протокол управления передачей в реальном времени. Используется совместно с протоколом RTP.
	RSYNC	166	Программа, которая эффективно выполняет синхронизацию файлов и каталогов в двух местах с минимизированием трафика.
	Oracle	167	Протокол доступа к базам данных.
	Corba	168	Протокол предназначен для облегчения связи систем, развернутых на различных операционных системах, языках программирования и аппаратных платформах.
	Whois-DAS	170	Предназначен для получения регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем.
	SD-RTN	171	Технология построения программно-определяемых сетей для доставки информации с высоким уровнем сервиса (QoS).
	SOCKS	172	Сетевой протокол, который позволяет пересылать пакеты от клиента к серверу через прокси-сервер прозрачно
	RTMP	174	Протокол используется для передачи потокового видео и аудиопотоков с веб-камер через интернет.
	FTP_DATA	175	Связанное с FTP_CONTROL соединение в рамках подключения по протоколу FTP, отвечающее за передачу данных.
	ZeroMQ	177	Библиотека асинхронного обмена сообщениями.
	Megaco	181	Протокол, используемый между элементами телекоммуникационных сетей: шлюзом (Media Gateway) и контроллером шлюзов (Media Gateway Controller).

Категория	Приложение	Номер в статистике	Описание протокола
	Redis	182	Хранилище баз данных в памяти, используемое в серверной инфраструктуре. Протокол используется для подключения клиентов к хранилищам данных Redis.
	QUIC	188	Позволяет мультиплексировать несколько потоков данных между двумя компьютерами.
	EAQ	190	Редко использующийся протокол, служащий для замера скорости в широкополосных сетях передачи данных.
	AMQP	192	Протокол используется для передачи сообщений между компонентами системы с низкой задержкой и на высокой скорости.
	KakaoTalk_Voice	194	Мобильное приложение для мгновенного обмена аудио сообщениями.
	BJNP	204	Настраиваемый протокол обнаружения служб локальной сети, используемый принтерами и сканерами Canon. Компьютерные системы используют этот протокол для автоматического обнаружения устройств Canon в сети.
	SMPP	207	Протокол предназначен для передачи сообщений между внешними устройствами.
	TINC	209	VPN, позволяющий создавать безопасные виртуальные частные сети, по которым серверы могут взаимодействовать так, будто они работают в локальной сети.
	Teredo	214	Сетевой протокол, предназначенный для передачи IPv6 пакетов через сети IPv4.
	IMO	216	Веб-сервис для мгновенного обмена сообщениями и VoIP-звонков.
	MQTT	222	Протокол для легкого обмена сообщениями публикации/подписки. Это полезно для соединений с удаленными местами, где требуется небольшой объем кода.
	RX	223	Позволяет компьютерным программам вызывать функции или процедуры в другом адресном пространстве.
	DRDA	227	Набор протоколов, обеспечивающих возможность связи между программами и системами баз данных на разных платформах и позволяющих распределять реляционные данные по нескольким платформам.
	SOMEIP	229	Транспортный протокол, ориентированный на масшабируемое промежуточное ПО (т.е. он находится на уровне приложений и имеет свои собственные уровни протокола общего назначения для работы с более специфическими операциями и приложениями).
	LISP	236	Стандарт для разделения IP-адреса на два отдельных пространства имен для разделения отображения местоположения и идентификатора IP.
	Diameter	237	Сеансовый протокол, созданный для преодоления некоторых ограничений протокола RADIUS. Обеспечивает взаимодействие между клиентами в целях аутентификации, авторизации и учета различных сервисов.
	TargusDataspeed	243	Протокол, используемый для измерения пропускной способности сетей.
	DNP3	244	Протокол передачи данных, используемый для связи между компонентами АСУ ТП (Автоматизированной системы управления технологическим процессом).

Категория	Приложение	Номер в статистике	Описание протокола
	IEC60870	245	Протокол телемеханики, предназначенный для передачи сигналов в систему верхнего уровня, регламентирующий использование сетевого доступа по протоколу TCP/IP. Чаще всего применяется в энергетике для информационного обмена между энергосистемами, а также для получения данных от измерительных преобразователей (вольтметры, измерительные преобразователи и т.д.).
	CAPWAP	247	Стандарт, позволяющий центральным контроллерам беспроводного доступа управлять точками беспроводного доступа.
	Zabbix	244	Протокол является частью программного инструмента с открытым исходным кодом, который отслеживает IT-инфраструктуру, такую как сети, серверы, виртуальные машины и облачные сервисы.
	s7comm	249	Протокол связи, используется для обмена данными между программируемыми логическими контроллерами, которые обычно используются в производстве.
	WebSocket	251	Технология, позволяющая открывать сеанс двусторонней интерактивной связи между браузером и сервером.
	SOAP	253	Протокол обмена сообщениями, используемый для обмена информацией между различными машинами и компьютерными сетями.
	HP_VIRTGRP	256	Протокол, используемый в системе виртуализации от компании HP. Обычно использует порт 5223 (TCP/UDP).
	Z3950	260	Клиент-серверный протокол для поиска и получения информации с удаленных компьютерных баз данных.
	Cassandra	264	Протокол кластера базы данных. Он был разработан для Apache Cassandra – распределенной системы управления базами данных NoSQL с открытым исходным кодом, предназначенной для обработки больших объемов данных.
	GTP_U	271	Протокол используется для передачи пользовательских данных внутри мобильных сетей.
	GTP_C	272	Протокол используется на уровне управления внутри базовых мобильных сетей.
	GTP_PRIME	273	Протокол используется для передачи данных о взимании платы внутри опорных сетей мобильной связи.
	EthernetIP	278	Промышленный сетевой протокол, который адаптирует общий промышленный протокол к стандартному Ethernet. Один из ведущих промышленных протоколов в США, который широко используется в различных отраслях, включая заводские, гибридные и технологические.
	HSRP	282	Протокол Cisco, используемый для обеспечения избыточности между несколькими маршрутизаторами в сети.
	collectd	298	Программа Unix, которая собирает, передает и хранит данные о производительности компьютеров и сетевого оборудования.
	UltraSurf	304	Протокол предоставляет решение прокси/VPN, предназначенное для обхода межсетевых экранов веб-цензуры.
	AliCloud	306	Семейство протоколов, использующихся при работе с Alibaba Cloud (поставщик облачных услуг на рынке Китая).
	Kismet	309	Протокол удаленного захвата используется для отправки данных беспроводного мониторинга (анализа) на центральный сервер.

Категория	Приложение	Номер в статистике	Описание протокола
	NAT-PMP	312	Протокол используется для автоматической установки параметров преобразования сетевых адресов (NAT) и конфигураций переадресации портов.
	Line	315	Приложение для моментального обмена сообщениями на смартфонах и ПК.
	LineCall	316	Семейство протоколов, используемых в телефонии VoIP.
	Munin	329	Протокол является частью программного инструмента с открытым исходным кодом, который отслеживает IT-инфраструктуру, такую как сети, серверы, виртуальные машины и облачные сервисы.
	Elasticsearch	330	Двоичный протокол, используется для связи между узлами: выборы мастеров, оркестровка узлов, управление сегментами и другое.
	TuyaLP	331	Протокол, который используется в технологиях устройств умного дома. Поддерживается компанией Tuya.
	TPLINK_SHP	332	Протокол, который используется в технологиях устройств умного дома.
	OICQ	335	Мессенджер мгновенных сообщений, популярный в Китае
Dangerous	SMBv1	16	Сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам.
	Tor	163	Система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания.
	HotspotShield	215	ПО для организации виртуальной частной сети, обеспечивающей безопасную передачу данных по шифрованному соединению, защищенному от прослушивания.
	Pastebin	232	Веб-приложение, которое позволяет загружать отрывки текста, обычно фрагменты исходного кода, для возможности просмотра окружающими.
Email	Outlook	21	Персональный почтовый и информационный сервис корпорации Microsoft.
	POPS	23	Зашифрованный протокол, используемый почтовыми клиентами для получения почты с удаленного сервера.
	SMTPS	29	Протокол используется для отправки электронных сообщений.
	YandexMail	33	Бесплатная служба электронной почты от компании Яндекс. **Примечание** *Для работы YandexMail требуется включение следующих протоколов: Yandex, YandexMail, YandexAuth, YandexMetrika, YandexImages (для отображения аватара в почте). Для блокировки достаточно установить YandexMail.*
	IMAPS	51	Протокол используется почтовыми клиентами для синхронизации почты с удаленного сервера.
	GMail	122	Электронная почта от компании Google.
SocialNetwork	VK	22	ВКонтакте – российская социальная сеть.
	TikTok	49	Сервис для создания и просмотра коротких видео, принадлежащий пекинской компании ByteDance.

Категория	Приложение	Номер в статистике	Описание протокола
	GooglePlus	72	Социальная сеть, принадлежавшая компании Google и позволявшая выстраивать социальные взаимоотношения в интернете.
	Tumblr	90	Служба микроблогов, включающая в себя множество картинок, статей, видео и gif-изображений по разным тематикам и позволяющая пользователям публиковать посты.
	Facebook	119	Крупнейшая социальная сеть в мире, которой владеет компания Meta Platforms.
	Twitter	120	Американский сервис микроблогов и социальная сеть, в которой пользователи публикуют сообщения и взаимодействуют с ними.
	Pinterest	183	Социальный интернет-сервис, фотохостинг, позволяющий пользователям добавлять в режиме онлайн изображения, помещать их в тематические коллекции и делиться ими с другими пользователями.
	Snapchat	199	Мобильное приложение для обмена сообщениями с прикрепленными фото и видео.
	Sina(Weibo)	200	Китайский сервис микроблогов.
	Reddit	205	Сайт, сочетающий черты социальной сети и форума, на котором зарегистрированные пользователи могут размещать ссылки на какую-либо понравившуюся информацию в интернете и обсуждать ее.
	Instagram	211	Американская социальная сеть для обмена фотографиями и видео.
	LinkedIn	233	Американская социальная сеть для поиска и установления деловых контактов.
	Likee	261	Социальная сеть, пользователи которой могут создавать и распространять короткие музыкальные видеоклипы с возможностью добавления спецэффектов и дополненной реальности.
	Badoo	279	Социальная сеть знакомств, поддерживающая множество языков и работающая с пользователями всех стран мира.
	Tencent	285	QQ – наиболее распространенный в Китае сервис мгновенного обмена сообщениями.
VPN	Tailscale	24	Простой, быстрый и современный VPN на основе WireGuard.
	OpenVPN	159	Реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа «точка-точка» или «сервер-клиенты» между компьютерами.
	WireGuard	206	Протокол реализует методы виртуальной частной сети для создания защищенных соединений «точка-точка»
	FortiClient	259	Комплексное решение безопасности, предназначенное для защиты компьютеров и ноутбуков.
	iCloudPrivateRelay	277	VPN от Apple, который позволяет пользователям с iOS 15, iPadOS 15 или macOS Monterey на своих устройствах и подпиской iCloud+ подключаться к интернету и просматривать страницы с помощью Safari более безопасным и конфиденциальным способом.
	Softether	290	Бесплатная кроссплатформенная многопротокольная VPN-программа с открытым исходным кодом.
	TunnelBear	299	Простой в использовании VPN-сервис на Android. Находится в продаже только на территории некоторых стран.

Категория	Приложение	Номер в статистике	Описание протокола
	CloudflareWarp	300	VPN, который не скрывает исходный IP-адрес, а шифрует трафик и использует службу DNS Cloudflare 1.1.1.1.
	Psiphon	303	Бесплатный VPN с открытым исходным кодом, в котором используется сочетание технологий защищенной связи и обфускации.
Web	Yandex	25	Поисковая система и интернет-портал.
	DataSaver	46	Расширение, позволяющее экономить трафик. Решение предназначено специально для браузера Google Chrome и дает возможность экономить трафик при загрузке страницы в глобальной сети.
	YandexMetrika	98	Бесплатный интернет-сервис компании Яндекс, предназначенный для оценки посещаемости веб-сайтов и анализа поведения пользователей.
	GoogleMaps	123	Набор приложений, построенных на основе бесплатного картографического сервиса.
	Google	126	Веб-ресурсы компании Google.
	Apple	140	Веб-ресурсы компании Apple.
	AppleiCloud	143	Сервис компании Apple для облачного хранения данных.
	Wikipedia	176	Интернет энциклопедия.
	Amazon	178	Веб-ресурсы компании Amazon.
	CNN	180	Официальный новостной сайт телеканала CNN.
	Cloudflare	220	Веб-ресурсы компании Cloudflare.
	OpenDNS	225	Интернет-служба, предоставляющая общедоступные DNS-серверы.
	GoogleServices	239	Системное приложение от Android, которое позволяет следить за тем, чтобы все установленные на устройстве приложения всегда были последней версии.
	Alibaba	274	Веб-ресурсы компании Alibaba Group.
	AccuWeather	280	Веб-ресурсы компании AccuWeather Inc. (частная американская медиа-компания, предоставляющая коммерческие услуги по прогнозированию погоды по всему миру).
	Xiaomi	287	Веб-ресурсы компании Xiaomi.
Network	ntop	26	Приложение для исследования компьютерной сети.
	CPHA	53	Протокол, обеспечивающий работу служб высокой доступности в оборудовании от компании Check Point.
	OCSP	63	Интернет-протокол, используемый для получения статуса отзыва цифрового сертификата X.509.
	GRE	80	Протокол туннелирования низкого уровня, используемый различными реализациями VPN: Cisco, IPsec, PPTP и другими. Протокол может использоваться для передачи IPv4, IPv6, многоадресной рассылки и других протоколов низкого уровня.
	ICMP	81	Протокол, предоставляющий услуги диагностики, устранения неполадок, управления и сообщений об ошибках.
	IGMP	82	Протокол связи, используемый узлами и соседними маршрутизаторами для многоадресной связи с IP-сетями. Обычно он используется IPTV и другими многоадресными приложениями.
	EGP	83	Протокол маршрутизации, который использовался для соединения различных автономных систем в интернете с се-

Категория	Приложение	Номер в статистике	Описание протокола
			редины 1980-х до середины 1990-х годов, пока не был заменен протоколом BGP.
	SCTP	84	Протокол, обеспечивающий передачу сообщений. Используется в телекоммуникационных сетях.
	OSPF	85	Протокол маршрутизации, который используется для поиска наилучшего пути между исходным и целевым маршрутизаторами. Используется среди маршрутизаторов для оптимизации потока трафика.
	IP_in_IP	86	Протокол IP-туннелирования, который инкапсулирует один IP-пакет в другой IP-пакет.
	ICMPV6	102	Межсетевой протокол управляющих сообщений для межсетевого протокола версии 6, реализация ICMP для IPv6.
	Citrix	132	Комплексное решение для виртуальных приложений и десктопных устройств, которое помогает доставлять приложения Windows, Linux, веб-приложения и приложения SaaS либо полные виртуальные десктопы из любого облака (общедоступного, локального или гибридного).
	Ookla	191	Инструмент для измерения пропускной способности интернет-провайдера
	DoH_DoT	196	Технологии DNS-over-TLS (DoT) и DNS-over-HTTPS (DoH) предназначены для защиты DNS-трафика (запросов и ответов) от перехвата и подмены.
	DNScrypt	208	Протокол, который аутентифицирует связь и передачу данных между DNS-клиентом и DNS-преобразователем.
	Bloomberg	246	Веб-ресурсы компании Bloomberg L.P.
	AVASTSecureDNS	263	Служба, защищающая пользователя от просмотра вредоносного контента в интернете.
	PGM	296	Многоадресный транспортный протокол компьютерной сети, который обеспечивает надежную последовательность пакетов для нескольких получателей одновременно.
	IP_PIM	297	Набор протоколов для передачи мультикаста в сети между маршрутизаторами.
Safe	COAP	27	Протокол предназначен для взаимодействия простых устройств, например, датчиков малой мощности, выключателей, клапанов, которые управляются или контролируются удаленно через сеть Интернет.
	DTLS	30	Коммуникационный протокол, обеспечивающий безопасность приложений, основанных на дейтаграммах, который предотвращает прослушивание, фальсификацию и подделку сообщений.
	UBNTAC2	31	Приложение для централизованного управления сетью устройств Ubiquiti.
	IPSec	79	Набор защищенных протоколов, которые аутентифицируют и шифруют сетевой трафик для служб VPN. Широко используемый протокол VPN.
	TLS	91	Протокол защиты транспортного уровня.
	Git	226	Система управления исходным кодом, используемая при разработке ПО.
	FIX	230	Протокол передачи данных, международный стандарт для обмена данными между участниками биржевых торгов в режиме реального времени.

Категория	Приложение	Номер в статистике	Описание протокола
	AVAST	307	Семейство антивирусных программ, разработанных компанией Avast для операционных систем Windows, Mac OS, Android и iOS.
	FastCGI	310	Протокол для взаимодействия интерактивных программ с веб-сервером.
	BACnet	334	Сетевой протокол, применяемый в системах автоматизации зданий и сетях управления.
Potentially	Kontiki	32	Протокол передачи видео и контента.
	Gnutella	35	Протокол обмена файлами.
Music	YandexMusic	34	Российский музыкальный стриминговый сервис, разработанный Яндексом.
	LastFM	134	Веб-ресурс по музыкакльной тематике.
	Spotify	156	Сервис для прослушивания музыки.
	Vevo	186	Музыкальный видеосайт и видеохостинг.
	Deezer	210	Приложение для прослушивания музыки.
	SoundCloud	234	Платформа для распространения оцифрованной звуковой информации, обладающая функциями социальной сети.
	IHeartRadio	325	Американская платформа бесплатного вещания, подкастов и потокового радио.
	Tidal	326	Веб-сервис подписки на музыку, подкасты и потоковое видео, сочетающий в себе звук без потерь и музыкальные видеоролики высокой четкости с эксклюзивным контентом и специальными функциями для музыки.
	TuneIn	327	Американский аудио-потоковый сервис, транслирующий новости, эфиры радиостанций, спортивные мероприятия, музыку и подкасты.
	SiriusXMRadio	328	Американская радиовещательная компания в сфере спутникового радио и онлайн-радио, расположенная в нью-йоркском Мидтауне.
VoIP	Skype_TeamsCall	38	Функция звонков в Skype_Teams.
	WhatsAppCall	45	Звонки в приложении Whatsapp.
	TruPhone	101	Сервис для совершения VoIP звонков.
	Skype_Teams	125	ПО для совместной работы, чата, звонков и собраний от компании Microsoft.
	Webex	141	Приложение для веб-конференций.
	Viber	144	Мессенджер, позволяющий обмениваться сообщениями и медиафайлами.
	Tuenti	149	Испанская социальная сеть.
	GoogleHangoutDuo	201	DUO – приложение для видеосвязи. Hangout – приложение для переписки (чат).
	SnapchatCall	255	Звонки в приложении Snapchat.
	FacebookVoip	268	VoIP звонки в социальной сети Facebook.
	SignalVoip	269	VoIP звонки в приложении Signal.
	Fuze	270	Масштабируемое облачное решение для проведения видеоконференций и совместной работы с просмотром роликов, текстовых документов и изображений.
	GoTo	293	Индонезийская компания, разрабатывающая программное обеспечение для видеоконференций.

Категория	Приложение	Номер в статистике	Описание протокола
Chat	Signal	39	Приложение для обмена мгновенными сообщениями.
	eXpress	338	Платформа корпоративных коммуникаций и мобильности, которая объединяет видеоконференции, корпоративный мессенджер, почтовый клиент, а также корпоративные приложения Smart Apps для мобильного доступа к информационным системам и сервисам компании.
	QQ	48	Сервис мгновенного обмена сообщениями.
	WhatsApp	142	Мессенджер, позволяющий обмениваться сообщениями и медиафайлами.
	Messenger	157	Приложение для общения (чат).
	Telegram	185	Мессенджер, позволяющий обмениваться сообщениями и медиафайлами.
	KakaoTalk	193	Мобильное приложение для мгновенного обмена сообщениями.
WeChat	WeChat	197	Мессенджер, позволяющий обмениваться сообщениями и медиафайлами.
Mining	Mining	42	Протоколы майнеров Bitcoin, Monero, ZCash, Ethereum.
Cloud	NestLogSink	43	Протокол обновления журнала Google Nest Protect используется детекторами дыма.
	YandexDisk	57	Облачный сервис, созданный Яндексом, который позволяет пользователям хранить файлы на «облачных» серверах и делиться ими с другими пользователями в интернете.
	YandexCloud	62	Публичная облачная платформа от компании Яндекс.
	Dropbox	121	Файловый хостинг компании Dropbox Inc., включающий персональное облачное хранилище, синхронизацию файлов и программу-клиент.
	UbuntuONE	169	Онлайн-хранилище, предназначенное для обмена файлами и синхронизации между компьютерами и мобильными устройствами.
	Microsoft	212	Веб-ресурсы компании Microsoft.
	GoogleDrive	217	Сервис для хранения, редактирования и синхронизации файлов, разработанный компанией Google.
	MS_OneDrive	221	Облачное хранилище, предоставляемое компанией Microsoft.
	ApplePush	238	Позволяет сторонним разработчикам отправлять уведомления на устройства Apple.
	AmazonVideo	240	Веб-видеосервис Amazon.
	AmazonAWS	265	Коммерческое публичное облако, поддерживаемое и развиваемое компанией Amazon.
	Salesforce	266	Американская компания, разработчик одноименной CRM-системы, предоставляемой заказчикам исключительно по модели SaaS.
	Azure	276	Облачная платформа компании Microsoft.
	GoogleCloud	284	Набор облачных служб, которые выполняются на той же самой инфраструктуре, которую Google использует для своих продуктов, предназначенных для конечных потребителей, таких как Google Search и YouTube.
	Edgecast	288	Американская компания в сфере Content Delivery Network.
	Cachefly	289	Поставщик сети доставки контента.

Категория	Приложение	Номер в статисти-ке	Описание протокола
Game	Xbox	47	Веб-ресурсы компании Xbox.
	AmongUs	69	Многопользовательская 2D игра от третьего лица с видом сверху, рассчитаная на 4-15 человек.
	Steam	74	Онлайн-сервис цифрового распространения компьютерных игр и программ.
	WorldOfWarcraft	76	Онлайн-игра.
	MapleStory	113	Онлайн-игра.
	Nintendo	173	Веб-ресурсы компании Nintendo.
	Playstation	231	Сервис цифровой дистрибуции компании Sony для пользователей консолей PlayStation.
	Activision	258	Американская компания по изданию и разработке компьютерных игр.
Fun	RTSP	50	Прикладной протокол, в котором описаны команды для управления видеопотоком.
	IceCast	52	ПО для организации потокового цифрового аудио- и видеовещания.
	HalfLife2	75	Компьютерная игра.
	Armagetron	104	Компьютерная игра.
	Dofus	106	Онлайн-игра.
	Guildwars	109	Онлайн-игра.
	Warcraft3	116	Онлайн-игра.
	WorldOfKungFu	117	Онлайн-игра.
	TocaBoca	106	Шведский разработчик детских мобильных видеоигр.
	TeamSpeak	162	Программа, предназначенная для голосового общения в сети Интернет посредством технологии VoIP.
	VHUA	184	Устаревший протокол, который использовался для сервисов, подобных Skype, в Китае.
	MPEG_TS	198	Протокол для передачи аудио- и видеоданных.
	Starcraft	213	Онлайн-игра.
	CSGO	235	Онлайн-игра.
	GenshinImpact	257	Компьютерная игра в жанре action-adventure с открытым миром и элементами RPG, разработанная китайской компанией miHoYo Limited.
	RakNet	286	Кроссплатформенное ПО, разработанное Oculus VR, для использования в игровой индустрии.
	i3D	301	Протокол с малой задержкой, которое в основном используется игровыми серверами.
	RiotGames	302	Американская компания, разработчик видеоигр, издатель и организатор киберспортивных турниров.
	Threema	305	Протокол используется одноименным приложением – платной службой обмена мгновенными сообщениями со сквозным шифрованием.
	TiVoConnect	308	Протокол обеспечивает автоматическое обнаружение двух или более медиаплееров Tivo, работающих в одной сети.
	Syncthing	313	Протокол используется для синхронизации файлов между двумя или более компьютерами в режиме реального времени.

Категория	Приложение	Номер в статистике	Описание протокола
	CryNetwork	314	Игровой протокол, используемый на платформе CryEngine. Используется для подключения игровых клиентов, синхронизации событий, подбора игроков и т.д.
	Source_Engine	333	Игровое ПО, разработанное компанией Valve Corporation и используемое ею для создания собственных компьютерных игр.
	Heroes_of_the_Storm	336	Онлайн-игра.
Streaming	PPStream	54	Китайская сеть для показа фильмов, сериалов и т.д.
	DisneyPlus	71	Американский сервис потокового вещания на основе подписки, управляемый отделом Media and Entertainment Distribution компании The Walt Disney Company.
	Hulu	137	Сервис, предлагающий доступ к потоковому видео: телевизионным шоу, фильмам, трейлерам, съемкам за сценой и другим продуктам от компаний NBC, Fox, ABC, TBS и других студий и телеканалов.
	AppleiTunes	145	Сервис компании Apple для прослушивания музыки.
	Pandora	187	Служба потоковой передачи музыки на основе подписки, принадлежащая Sirius XM Holdings.
	Vimeo	267	Американский видеохостинг.
	Dazn	292	Спортивный стриминговый сервис. Сервис транслирует спортивный контент в прямом эфире и по запросу в более чем 200 странах.
	1kxun	295	Китайский видеохостинг.
	AppleTVPlus	317	Американский стриминговый сервис, принадлежащий и управляемый компанией Apple.
	DirecTV	318	Сервис, предоставляющий просмотр онлайн телевидения, спорта и фильмов с помощью смартфона, планшета, компьютера, смарт-телевизора или потокового устройства.
	HBO	319	Американская сеть платного телевидения, которая является флагманским активом одноименной материнской компании Home Box Office, Inc.
	Vudu	320	Американский магазин цифрового видео и потоковый сервис, принадлежащий Fandango Media.
	Showtime	321	Американский платный кабельный и спутниковый телеканал.
	Dailymotion	322	Французский видеохостинг.
	Livestream	323	Американский платный кабельный и спутниковый телеканал.
	Tencentvideo	324	Китайская стриминговая платформа, принадлежащая Tencent.
Video	Zattoo	55	Платформа для показа телевизионных каналов.
	TVUplayer	59	Программа для просмотра бесплатных интернет телеканалов.
	Pluralsight	61	Американская частная онлайн-образовательная компания, которая предлагает на своем веб-сайте различные обучающие видеокурсы для разработчиков программного обеспечения, IT-администраторов и творческих профессионалов.
	NetFlix	133	Сервис для просмотра фильмов и сериалов.
	Zoom	189	Программа, предназначенная для конференцсвязи.
	Twitch	195	Видеостриминговый сервис, специализирующийся на тематике компьютерных игр.

Категория	Приложение	Номер в статистике	Описание протокола
	IFLIX	202	Малайзийский бесплатный видеосервис по подписке, ориентированный на развивающиеся рынки.
Shopping	YandexMarket	56	Электронная торговая площадка, сервис для покупки товаров.
	eBay	179	Официальный сайт компании Ebay (интернет-магазин).
Collaborative	Discord	58	Кроссплатформенная система мгновенного обмена сообщениями с поддержкой VoIP и видеоконференций, предназначенная для использования различными сообществами по интересам.
	Slack	118	Корпоративный мессенджер.
	Github	203	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки.
	Microsoft365	219	Программный продукт от компании Microsoft, объединяющий набор веб-сервисов, который распространяется на основе подписки по схеме «программное обеспечение как услуга».
	GoogleDocs	241	Приложение для создания текстовых файлов, таблиц, презентаций и.т.д.
	Teams	250	Microsoft Teams – корпоративная платформа, объединяющая в рабочем пространстве чат, встречи, заметки и вложения.
	GitLab	262	Веб-инструмент жизненного цикла DevOps с открытым исходным кодом, представляющий систему управления репозиториями кода для Git.
	GoogleClassroom	281	Бесплатный веб-сервис, разработанный Google для школ, который призван упростить создание, распространение и оценку заданий безбумажным способом.
Advertisement	YandexDirect	99	Сервис для размещения объявлений контекстной рекламы на Яндексе и на сайтах-партнерах его рекламной сети.
	ADS_Analytic_Track	107	Сервис контекстной рекламы от компании Google.
RPC	Crossfire	105	Система удаленного управления, отличающаяся большим радиусом действия, невосприимчивостью к бортовым помехам, малой задержкой.
AdultContent	AdultContent	108	Взрослый контент.
VirtAssistant	AmazonAlexa	110	Виртуальный ассистент, разработанный компанией Amazon.
	AppleSiri	254	Облачный персональный помощник и вопросно-ответная система от компании Apple.
Media	MpegDash	291	Технология адаптивной потоковой передачи данных, предоставляющая возможность доставки потокового мультимедиа-контента через интернет по протоколу HTTP.
	YouTube	124	Видеохостинг, предоставляющий пользователям услуги хранения, доставки и показа видео.
	YouTubeUpload	136	Протокол отвечает за загрузку видео с Youtube.
	OCS	218	Протокол для интеграции веб-сообществ и веб-сервисов.
SoftwareUpdate	WindowsUpdate	147	Центр обновления Windows.
	AppleStore	224	Магазин приложений Apple.
	PlayStore	228	Магазин приложений Google.
RemoteAccess	TeamViewer	148	ПО для удаленного контроля компьютеров.
	AnyDesk	252	Приложение для удаленного доступа и управления компьютерами под управлением Windows, MacOS и Linux.

Категория	Приложение	Номер в статисти-ке	Описание протокола
Download	WhatsAppFiles	242	Передача файлов в приложении WhatsApp.
DataTransfer	Crashlytics	275	Программа, которая помогает собирать, анализировать и систематизировать отчеты о сбоях приложений.
Cybersecurity	Cybersec	283	Функция безопасности, которая блокирует рекламу и веб-сайты, которые, как известно, содержат вредоносные программы.

Приложение С. Отчет об ошибках: утилита bug-report

Для формирования отчета об ошибках используется утилита **bug-report**.

В отчете отображается следующая информация:

- информация о лицензии;
- системные журнальные файлы и журнальные файлы Solar NGFW;
- запущенные процессы и установленные сетевые соединения;
- информация об аппаратном обеспечении и используемых ресурсах
- информация о запущенных процессах;
- основные конфигурационные файлы Solar NGFW;
- файлы **crontab** суперпользователя root, пользователя skvt и общие;
- информация о наличии и состоянии пакетного фильтра;
- информация о системном окружении;
- данные последних 100 пользователей, которые входили в систему.

С содержанием отчета можно ознакомиться далее в Табл.С.1.

Табл. С.1. Информация отчета об ошибках: bug-report

Тип информации	Примеры вывода данных
Информация о лицензии	license-info license.xml
Системные журнальные файлы и журнальные файлы Solar NGFW	tail -n1000 /var/log/maillog tail -n1000 /var/log/mail.err tail -n1000 /var/log/messages dmesg dmesg.err
Запущенные процессы и установленные сетевые соединения	ps -fax netstat -nap netstat -nlp
Информация об аппаратном обеспечении и используемых ресурсах	iostat -N 5 vmstat -s 5 top -b -n20 -d03 free -m cat /proc/meminfo cat /etc/hosts uname -a df -h cat /etc/hostname dpkg -l cat /etc/resolv.conf

Тип информации	Примеры вывода данных
	fdisk -l ifconfig lsof mount route -n
Информация об установленной ОС	/etc/os-release
Основные кофигурационные файлы Solar NGFW	/opt/dozor/config /data/repos/dozor/policy-base.git /data/repos/dozor/policy-final.git /data/repos/dozor/config-base.git /data/repos/dozor/config-final.git
Файлы **crontab** суперпользователя **root**, пользователя skvt и общие	cat /var/spool/cron cat /etc/crontab
Информация о наличии и состоянии пакетного фильтра – файлы	iptables -L -v -n iptables -L -v -n -t nat
Информация об окружении	Содержимое файла **env**
Данные последних 100 пользователей, которые входили в систему. Ниже приведен пример таких данных	root pts/0 pc-ifadeev6.lpr. Thu Feb 10 17:45 - 15:34 (21:48) reboot system boot 2.6.18-238.el5 Thu Feb 10 17:45 (15+20:20) reboot system boot 2.6.18-238.el5 Thu Feb 3 17:12 (00:14) root tty1 Thu Feb 3 16:53 - 16:54 (00:00) reboot system boot 2.6.18-238.el5 Thu Feb 3 16:38 (00:19) reboot system boot 2.6.18-238.el5 Thu Feb 3 16:36 (00:00)

Приложение D. Справочник MIME-типов

D.1. Краткое описание стандарта MIME

Для передачи данных по сети Интернет был принят стандарт MIME (Multipurpose Internet Mail Extension – многоцелевое расширение интернет-почты). Этот стандарт определяет способы передачи и кодирования данных.

Типичное применение стандарта MIME – пересылка графических изображений, аудио- и видеофайлов, документов MS Word и MS Excel, программ, а также текстовых файлов. Другими словами, MIME-типы были введены чтобы обеспечить присоединение к сообщениям электронной почты файлов различных типов; задание типа файла позволяет почтовой программе определить, какое ПО должно использоваться для просмотра вложенного файла. Позже MIME-типы стали использоваться не только почтовыми службами, но и другими программами для унификации действий по обработке файлов. Например, по MIME-типу принятого файла веб-браузер определяет, что с ним требуется делать: если это HTML-документ, то он отображается как веб-страница, а если это файл формата MPEG, то он исполняется подключаемым модулем обозревателя, предназначенным для показа видеофильмов.

Согласно стандарту MIME, в передаваемых данных должен указываться специальный заголовок, определяющий тип передаваемой информации. Этот заголовок характеризуется парой тип/подтип. Поле подтип уточняет используемый тип.

В настоящее время стандартом MIME определяется 8 основных типов содержимого:

Табл. D.1. Типы содержимого

Уровень	Описание
text	Используется для передачи текстовой информации в разных кодировках, а также форматированного текста.
multipart	Используется для объединения нескольких различных взаимонезависимых типов, таких как текст, изображение, аудио и видео.
application	Используется для передачи приложений или бинарных данных.
model	Используется для передачи многомерных структур, состоящих из объектов. Такими многомерными структурами могут быть, например, трехмерные модели.
message	Используется для передачи вложенного почтового сообщения, состоящего из вложенных сообщений. Рекурсия в данном случае не ограничивается, и составные части также могут состоять из вложенных сообщений.
image	Используется для передачи изображений.
audio	Используется для передачи звуковых файлов.
video	Используется для передачи видеоинформации.

В отличие от типов, подтипы не имеют жесткой спецификации в стандарте, и при создании нового формата данных могут быть добавлены соответствующие новые подтипы. Подтипы могут образовывать деревья вида **тип/корень.подтип**. MIME определяет три стандартных корня:

- личные подтипы (personal tree), начинающиеся с prs;
- корпоративные подтипы (vendor tree), начинающиеся с vnd;

- подтипы индексации (index tree), начинающиеся с index.

Для локального и корпоративного использования допускаются незарегистрированные MIME-типы. При этом имя подтипа должно начинаться с **x-**. Например, скриптлеты Microsoft Internet Explorer 5.x имеют тип **text/x-scriptlet**.

С большинством MIME-типов связаны соответствующие форматы файлов. Например, тип **text/css** задает стили (файлы формата *.css), тип **text/html** – html-данные (файлы формата *.htm,*.html), тип **text/xml** – xml-данные (файлы формата *.xml) и т.д. Однако необходимо учитывать, что данные разных типов не обязательно должны быть в отдельных файлах, то есть в одном файле могут быть разнотипные данные. Например, html-документы позволяют использовать как внешние файлы с определением стилей, так и внедрять данные этого типа непосредственно на страницу.

D.2. Описание MIME-типов

При формировании политики безопасности в системах класса Solar Dozor используются MIME-типы, представленные в таблицах ниже. Каждой таблице соответствует определенный тип файлов, который можно выбрать при создании правила или исключения.

Табл. D.2. MIME-типы, относящиеся к типу файлов «Служебные файлы»

MIME-тип	Описание	Расширения
ФАЙЛЫ ПРИЛОЖЕНИЙ		
application/x-1c-metadata	Файл метаданных 1С	CF, CFU
application/x-freelance-presentation	Файл Lotus Freelance Presentation	PLZ
application/vnd.ms-works	Файл MS Works	WCM, WDB, WKS, WPS
application/x-installshield	Файл InstallShield	WIS
application/x-repligo.vpf	Файл данных RepliGo для конвертации файлов для мобильных устройств	RGO
application/x-notes-id	ID-файл Lotus Notes	ID
application/x-bittorrent	Файл BitTorrent	TORRENT
ОБРАЗЫ НАКОПИТЕЛЕЙ ДАННЫХ И ДАМПЫ ПАМЯТИ		
application/x-iso9660	ISO-образ диска	ISO
application/x-coredump	Дамп памяти	DMP, ELF
application/x-binary-image	Образ флоппи-диска (3.5" дискеты)	IMG, ISO, FLP
ИСПОЛНЯЕМЫЕ ФАЙЛЫ И ДИНАМИЧЕСКИЕ БИБЛИОТЕКИ		
application/palmos	Приложение Palm OS	PRC, PDB
application/vnd.ms-installer	Пакет инсталляции (обновления) приложений MS Windows	MSI, MST, MSM, WIM
application/x-executable-binary	Приложение MS Windows	EXE
application/x-g3	Программа процессора G3	
application/x-scr.samsung.c100	Программа-скринсейвер для телефонов Samsung	SCS
application/macos.x	Приложение MacOS X	APP
АРХИВЫ И СЖАТЫЕ ФАЙЛЫ		
application/x-compressed-simple	Архив SCZ	SCZ
application/x-compressed-alz	Архив ALZip	ALZ

MIME-тип	Описание	Расширения
application/x-compressed-bza	Архив BZA	BZA
application/x-compressed-lha	Архив LHA	LHA
application/x-sfx-7z	Самораспаковывающийся архив типа 7Z для MS Windows	SFX, EXE
application/x-sfx-zip	Самораспаковывающийся архив типа Zip для MS Windows	SFX, EXE
application/x-compressed-yz	Архив YZ1	YZ1
application/x-composite-rar-jpeg	Архив RAR	RAR
application/x-composite-rar-msword		
application/x-composite-rar-pdf		
application/x-compressed-rar		
application/x-rar-compressed		
application/x-compressed-zip	Архив ZIP	ZIP
application/zip		
application/x-compressed-pae	Зашифрованный архив PowerArchiver	PAE, PAE2
application/x-svr4-package	Установочный пакет в формате PKG для Mac OS X	PKG
application/x-debian-package	Пакет Debian	DEB
application/x-compressed-gzip	Архив GZIP	GZ, RAR
application/gzip		
application/x-zip-bomb	Архив типа zip-бомба	ZIP
application/x-compressed-arj	Архив ARJ	ARJ
application/x-compressed-xz	Архив LZMA	XZ
application/x-rpm	Установочный пакет в формате RPM (Red Hat Package Manager)	RPM
application/x-iscab	Архив CAB	CAB
application/x-mscab		
application/vnd.ms-cab-compressed		
application/x-compressed-bzip2	Архив BZIP2	BZ2
application/x-compressed-ace	Архив WinAce	ACE
application/x-compressed-sit	Архив Stuffit	SIT
application/x-compressed-7zip	Архив 7-Zip	7Z
application/x-cpio	Архив POSIX CPIO	CPIO
application/x-tar	Архив Tar	TAR
application/x-compressed-bh	Архив BlackHole	BH
application/x-sfx-rar	Самораспаковывающийся архив типа RAR для MS Windows	SFX, EXE
СИСТЕМНЫЕ ФАЙЛЫ		
application/x-empty	Пустой файл или файл, превышающий допустимый размер	
application/x-folder.info	Описание каталога MacOS X	DS_STORE
image/vnd.microsoft.icon	Пиктограмма в формате ICO	ICO
image/x-icon		
application/x-mschm	Файл контекстной справки MS Windows	CHM
application/vnd.ms-htmlhelp		

MIME-тип	Описание	Расширения
image/x-animated-cursor	Анимированный курсор Windows	ANI
application/x-thumbs	Кэш эскизов предварительного просмотра (Windows Thumbnail Cache)	DB
application/x-not-regular-file	Директория, очередь или другой нерегулярный файл в UNIX-системах	SOCK
application/x-ms-shortcut	Ярлык MS Windows	LNK
application/x-mshelp	Файл справки MS Windows	HLP
ЖУРНАЛ СОБЫТИЙ		
application/bug-report	Диагностический отчет Solar Dozor	
application/log-data	Файл журнала	LOG
application/gzipped-bug-report	Сжатый диагностический отчет Solar Dozor	GZIP, GZ
ИСПОЛНЯЕМЫЕ ФАЙЛЫ И ДИНАМИЧЕСКИЕ БИБЛИОТЕКИ		
application/java-archive	Java-архив	JAR

Табл. D.3. MIME-типы, относящиеся к типу файлов «Информационные технологии»

MIME-тип	Описание	Расширения
БЕЗОПАСНОСТЬ		
application/x-hp-arcsight:arb	Пакет HP ArcSight	ARB
СКРИПТЫ		
text/javascript	Файл скрипта на языке JavaScript	JS
application/javascript		
application/json		
application/x-javascript		
application/x-executable-script	Скрипты BASH и SHELL	SH, CSH
application/x-windows-batch	Пакетный файл для выполнения команд в Windows Command Prompt	BAT
ВЕБ-СТРАНИЦЫ		
text/html	Веб-страница	HTML, ACGI, HTM, HTMLS, HTX, SHTML, STM
text/css	Каскадная таблица стилей	CSS
application/x-mht	Архив веб-страницы, сохраненной в Internet Explorer	MHT, MHTML
ИСХОДНЫЕ КОДЫ		
application/x-msvba	Код программы на языке BASIC	BAS
БАЗЫ ДАННЫХ (БД)		
application/x-sql-light.journal	Журнал транзакции СУБД SQLite	DB-JOURNAL
application/vnd.oasis.opendocument.base	БД OpenDocument	ODB
application/x-dbf	Файл БД dBASE	DBF
application/x-paradox-idx	Индексный файл типа IDX для СУБД Paradox и других программ	IDX
application/access-2007	БД MS Access	ACCDB, MDB
application/msaccess		

MIME-тип	Описание	Расширения
text/x-oracle-trace-dump	Файл трассировки СУБД Oracle	TRC
application/x-sql-light.database	Файл БД SQLite	SQLITE, SQLITEDB, SQLITE3, DB3
application/x-paradox-db	Файл БД СУБД Paradox	DB, DBC, DBF, DBX
text/x-pgsql-db-dump	Дамп БД PostgreSQL	DUMP
ЗАШИФРОВАННЫЕ ДАННЫЕ		
application/pgp-signature	Сигнатуры PGP	ASC, SIG, PGP
application/agent.enc	Зашифрованные данные в формате ENC	ENC
application/pgp-encrypted	Зашифрованные данные в формате PGP	PGP, GPG
application/pgp-keys	Ключи PGP	PGP
application/mac-binhex40	Зашифрованные данные в формате BinHex 4.0	HQX

Табл. D.4. MIME-типы, относящиеся к типу файлов «Графика»

MIME-тип	Описание	Расширения
ПЕЧАТЬ		
application/pjl	Файл HP Printer Job Language	PGL
ИЗОБРАЖЕНИЯ		
image/x-bitmap	Растровое изображение в формате BMP	BMP
image/x-bitmap-corrupt		
image/x-msw3bmp		
application/x-adobe-illustrator	Векторное изображение в формате Adobe Illustrator	AI
application/pdf		
drawing/cmx	Векторное изображение с метаданными Corel	CMX
application/x-msimage-obj	Векторное изображение (метафайл графики Windows)	WMF, WMZ, EMF
image/msemf		
image/mswmf		
image/x-emf		
image/x-wpg	Векторное изображение в формате WordPerfect	WPG
image/tiff	Растровое изображение в формате TIFF без сжатия	TIFF, TIF
application/photoshop	Растровое изображение в формате Adobe Photoshop и PhotoDeluxe	PSD, PDD
image/x-adobephotoshop		
image/xcf	Растровое изображение в формате GIMP	XCF
drawing/corel-symbol.library	Внешняя библиотека символов Corel Graphics Suite	CSL
image/x-coreldraw	Векторное изображение в формате CorelDRAW	CDR, CDT
image/pcx	Растровое изображение в формате PCX	PCX
image/targa	Растровое изображение в формате Targa Graphic	TGA, VDA, ICB
drawing/corel-rave	Проект Corel R.A.V.E	CLK

MIME-тип	Описание	Расширения
image/gif	Растровое изображение в формате GIF	GIF
image/psp	Растровое изображение в формате Paint Shop Pro	PSP, PSPIMAGE
image/fig	Векторное изображение в формате Xfig	FIG
image/jpeg2000	Растровое изображение в формате JPEG 2000	JP2, J2K
image/x-j2k		
image/x-cgm	Векторное изображение в формате CGM	CGM
image/x-portable-bitmap	Растровое изображение в формате Portable Pixmap	PPM, PBM, PGM
image/x-portable-graymap		
image/x-portable-pixmap		
image/jpeg	Растровое изображение в формате JPEG	JPEG, JPG, JPE, JFIF, JIF, JFI, JFIF-TBNL
application/x-msphotoedit	Растровое изображение в формате MS Photo Editor	WDP
image/png	Растровое изображение в формате PNG без сжатия	PNG, X-PNG, 9.PNG, PNS, APNG
image/x-corelphotopaint	Растровое изображение в формате Corel Photo-Paint	CPT
image/svg+xml	Масштабируемая векторная графика	SVG
ШРИФТЫ		
application/ms-embedded-font-source	Встроенный шрифт MS Office	
application/x-font-type1	Шрифт Type	PFA, PFB, PFM, AFM
application/x-font-ttf	Шрифт в формате TTF (TrueType)	TTF, TTC
application/x-screenfont.data		
font/woff	Шрифт в формате WOFF	WOFF, WOFF2
font/woff2		
application/font-woff		
ВЕРСТКА И ПУБЛИКАЦИИ		
application/x-macromedia-freehand-doc	Документ Adobe FreeHand	FH, FHC, FH4, FH5, FH7
application/postscript	Описание страниц на языке Adobe PostScript	PS, EPS
application/x-pagemaker	Документ разметки страницы в формате Adobe PageMaker	PM4, PM5, PM7
image/dcx	Изображение в формате FAXserve	DCX
application/x-mspublisher	Документ MS Publisher	PUB
application/quarkxpress-mime	Файл QuarkXPress	QXD, QXT, QWD, QWT, QXL, QXB
application/x-pfr-fax	Факсимильное сообщение Пенсионного фонда РФ	
application/x-dvi	Документ DVI системы TeX	DVI

Табл. D.5. MIME-типы, относящиеся к типу файлов «Документы»

MIME-тип	Описание	Расширения
ПРЕЗЕНТАЦИИ		
application/vnd.oasis.opendocument.presentation	Презентация OpenDocument	ODP
application/vnd.openxmlformats-officedocument.presentationml.presentation-write-protected	Презентация OpenOffice, недоступная для редактирования	PPTX
application/mspowerpoint-2007	Презентация MS PowerPoint	PPT, PPTX, PPS, PPSX, POT, POTX, PPA
application/vnd.ms-powerpoint		
application/vnd.openxmlformats-officedocument.presentationml.slideshow		
application/vnd.openxmlformats-officedocument.presentationml.template		
application/vnd.openxmlformats-officedocument.presentationml.presentation	Презентация OpenOffice	PPTX, THMX
application/vnd.stardivision.impress	Презентация StarOffice	SDP, SXI
application/vnd.sun.xml.impress		
ДАННЫЕ ДОКУМЕНТОВ		
application/vnd.oasis.opendocument.image	Изображение OpenDocument	ODI
application/vnd.sun.xml.impress.template	Шаблон презентации StarOffice	STI
application/vnd.ms-officetheme-write-protected	Тема MS Office, недоступная для редактирования	THMX
application/x-msclipart	Упакованная галерея изображений в формате MS Clip Gallery	CIL
application/vnd.oasis.opendocument.chart	Диаграмма OpenDocument	ODC
application/x-msdraw	Файл MS Draw	
application/x-msole-broken	Поврежденная библиотека OLE-объектов для MS Office	OLB
application/vnd.stardivision.draw	Графика StarOffice	SDA
application/vnd.sun.xml.draw		
application/vnd.sun.xml.draw.template	Шаблон графики StarOffice	STD
application/vnd.stardivision.math	Формула StarOffice	SMF, SXM
application/vnd.sun.xml.math		
application/vnd.oasis.opendocument.formula	Формула OpenDocument	ODF
application/x-msole.data	Библиотека OLE-объектов для MS Office	OLB
application/vnd.oasis.opendocument.graphics	Графика OpenDocument	ODG
application/msole-word.picture	Графический OLE-объект в MS Word	
application/vnd.sun.xml.calc.template	Шаблон таблицы StarOffice	STC
application/x-msequation	Файл MS Equation	
application/vnd.sun.xml.writer.template	Шаблон документа StarOffice	STW
application/ms-graph.x-ms-excel	Диаграмма MS Graph	
application/x-vnd.oasis.opendocument.formula-template	Шаблон для создания формул в формате OTF	OTF
application/x-msole-encrypted	Зашифрованная библиотека OLE-объектов для MS Office	OLB
application/vnd.ms-officetheme	Тема MS Office	THMX

MIME-тип	Описание	Расширения
application/x-ole-storage	OLE хранилище	DAT, WID
application/x-msole-unknown	Неизвестная библиотека OLE-объектов для MS Office	OLB
application/msole-excel.picture	Графический OLE-объект в MS Excel	
ТЕКСТОВЫЕ ФАЙЛЫ		
text/x-fouled-text	Файл, в котором встречаются не-текстовые символы	TXT
text/plain	Текстовый файл	TXT
ТЕКСТОВЫЕ ДОКУМЕНТЫ		
application/x-rocketbook	Электронная книга в формате Rocket eBook	RB
image/x-djvu	Электронная книга или пакет изображений DjVu	DJV, DJVU
application/x-wordperfect-text	Текстовый документ в формате Corel WordPerfect	WPD
application/ms-office.x-vba-project	Файл MS Office с поддержкой макросов (VBA)	DOCM, DOTM, XLAM, XLSM, XLTM, POTM, PPSM, PPTM
application/vnd.ms-excel.addin.macroenabled.12		
application/vnd.ms-excel.template.macroenabled.12		
application/vnd.ms-powerpoint.presentation.macroenabled.12		
application/vnd.ms-powerpoint.slideshow.macroenabled.12		
application/vnd.ms-powerpoint.template.macroenabled.12		
application/vnd.openxmlformats-officedocument.wordprocessingml.document-write-protected	Документ MS Word, недоступный для редактирования	DOC, DOCX, DOT, DOTX, DOCM
application/vnd.oasis.opendocument	Документ OpenDocument	ODT, OTT
application/vnd.oasis.opendocument.text		
application/vnd.oasis.opendocument.text-template		
application/pdf-with-forms	Документ PDF с формой	PDF
text/ms-word-xml	Документ MS Word в формате XML	XML
application/vnd.stardivision.writer	Документ StarOffice	SDW, SGL, SXW, SXG
application/vnd.stardivision.writer-global		
application/vnd.sun.xml.writer		
application/vnd.sun.xml.writer.global		
application/pdf	Документ PDF	PDF
application/x-palm	Электронная книга в формате Palm Doc или БД Palm OS	PRC, PDB
application/msword	Документ MS Word	DOC, DOCX, DOT, DOTX, DOCM
application/msword.6		
application/msword-2007		
application/vnd.ms-word2006ml		
application/vnd.openxmlformats-officedocument.wordprocessingml.document		

MIME-тип	Описание	Расширения
application/vnd.openxmlformats-officedocument.wordprocessingml.template		
application/vnd.ms-word.document.macroenabled.12		
application/vnd.ms-word.template.macroenabled.12		
application/vnd.ms-wordml		
application/rtf	Документ в формате RTF	RTF, DOC
ТАБЛИЦЫ		
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Таблица OpenOffice	XLSX, XLTX
application/vnd.openxmlformats-officedocument.spreadsheetml.template		
application/vnd.ms-excel.sheet.binary.macroEnabled.12	Двоичная книга MS Excel	XLSB
application/msexcel	Книга MS Excel	XLS, XLM, XLA, XLC, XLT, XLW, XLSX
application/msexcel-2007		
application/msexcel-before-97		
application/msexcel-old		
application/vnd.ms-excel		
application/vnd.stardivision.calc	Таблица StarOffice	SDC, SXC
application/vnd.sun.xml.calc		
application/x-pivottables	Сводная таблица	XLS
application/x-123	Таблица Lotus 1-2-3	WK1, WKS
application/vnd.openxmlformats-officedocument.spreadsheetml.sheet-write-protected	Таблица OpenOffice, недоступный для редактирования	XLSX
application/vnd.oasis.opendocument.spreadsheet	Таблица OpenDocument	ODS

Табл. D.6. MIME-типы, относящиеся к типу файлов «Мультимедиа»

MIME-тип	Описание	Расширения
АНИМАЦИЯ		
application/x-shockwave-flash	Анимация в формате Adobe Flash	SWF, SWFL
video/x-flc	Анимационные видеофайлы формата FLIC	FLC, FLI
video/x-fli		
ВИДЕО		
video/x-shockwave-flash	Видео в формате Adobe Flash	FLV
application/x-unknown-mv2	Видео в формате MPEG, MPEG-4, MPEG-TS	MPEG, MPG, MPE, M1V, M2V, MP2, MP3, MPA, MPV2, TS, TSV, TSA, MV2
video/mpeg		
video/mp4		
video/x-msvideo	Видео в формате AVI	AVI
video/asf	Мультимедийные файлы формата ASF	ASF, ASX, ASR
video/x-ms-asf		
video/quicktime	Видео в формате Apple QuickTime	QT, MOV, MOOV
video/vnd.rn-realmedia	Видео в формате RealMedia	RM
АУДИО		
audio/x-mod	Звуковой модуль в формате MOD или близком к нему	MOD, PSM, XM, XMZ, 669

MIME-тип	Описание	Расширения
audio/x-ape	Звукозапись в формате Monkeys Audio со сжатием без потери качества	APE, APL
audio/x-monkeys		
audio/x-monkeys-audio		
audio/x-wav	Звукозапись в формате WAV без сжатия	WAV, WAVE
audio/midi	Файл в формате MIDI	MID, MIDI, KAR, RMI
audio/basic	Звукозапись, используемая в ОС Unix, Mac OS, Akai MPC, Amiga и пр.	AU, SND
audio/voxware	Звукозапись в формате VoxWare Dialogic для хранения человеческой речи	VOX
audio/ac3	Звукозапись в формате AC-3 (Dolby Digital)	AC3
audio/vnd.rn-realmedia	Звукозапись в формате RealMedia	RM
audio/x-nice-aud	Звукозапись компьютерных игр в формате NICE Media Player	AUD
audio/aiff	Звукозапись в формате AIFF	AIF, AIFF, AIFC
audio/amr	Звукозапись в формате AMR со сжатием	AMR
audio/x-voc	Звукозапись в формате Creative Labs	VOC
audio/x-s3m	Звуковой модуль в формате ScreamTracker 3.0 и выше	S3M
audio/x-oggmedia	Звукозапись в формате Ogg Vorbis	OGA, OGG
audio/x-flac	Звукозапись в формате FLAC со сжатием без потери качества	FLAC
audio/x-pat	Звуковой модуль в формате Gravis UltraSound GF1	PAT
audio/x-creative-sf-bank	Звуковой модуль в формате SoundFont 2	SF2
audio/x-twinvq	Звукозапись в формате TwinVQ	VQF
audio/mpeg	Звукозапись в форматах MPEG, MPEG-2, MPEG-4	MP2, MP2A, M2A, MPA, MPG, MPEGA, M4A, MPGA, MP3
audio/mpeg2		
СПИСКИ ВОСПРОИЗВЕДЕНИЯ		
audio/x-mpegurl	Список воспроизведения аудио- и видеофайлов	M3U, M3U8

Табл. D.7. MIME-типы, относящиеся к типу файлов «Бизнес»

MIME-тип	Описание	Расширения
ФАЙЛЫ ДАННЫХ		
text/csv	Файл данных, разделенных запятыми	CSV
text/sgml	Файл данных SGML	SGML, SGM
text/xml	Файл данных XML	XML
ИНЖЕНЕРНЫЕ И НАУЧНЫЕ ПАКЕТЫ		
application/x-autocad	Файл AutoCAD	DWG, LIN, CUI, ADT, MVI

MIME-тип	Описание	Расширения
application/x-dwg		
application/vnd.visio	Документ MS Visio	VSD, VSDX, VST, VSTX, VSS, VSX, VSW
application/vnd.ms-visio.drawing		
application/vnd.ms-visio.drawing.macroenabled.12		
application/vnd.ms-visio.stencil		
application/vnd.ms-visio.stencil.macroenabled.12		
application/vnd.ms-visio.template		
application/vnd.ms-visio.template.macroenabled.12		
application/x-matlab-binary	Файл MatLab	MAT
application/x-AT-mathcad	Файл MathCAD	MCD
application/vnd.mcd		
ФИНАНСЫ		
application/x-1c.data	Файл данных 1С	1CD, DT
text/x-ptk-pzd	Документ банковской отчетности в формате ПТК ПСД	
СПРАВОЧНИКИ		
application/x-consultant	Файл Консультант Плюс	KUB, DT
ЭЛЕКТРОННАЯ ПОЧТА		
application/vnd.ms-attachment-tnef	Файл данных MS Exchange	DAT, MS-TNEF, TNEF
application/vnd.ms-tnef		
application/x-pkcs7-mime	Зашифрованное сообщение электронной почты или сертификат	P7M, P7C
application/x-sensor-m-box	Почтовый ящик электронной почты	MBOX
message/news	Файл почтовых сообщений или новостей Windows Live Mail	NWS
application/x-microsoft-rpmsg-message	Сообщение MS Outlook с ограниченным доступом	RPMSG
application/vnd.ms-outlook	Файл MS Outlook	DBX, EMAIL, EML, BCMX, DBX, ECF, IDX, MBX, NCH, OFT, PRF, SRS, MSG
application/x-pkcs7-signature	Цифровая подпись (без сообщения, которое подписано)	P7A, P7S
message/rfc822	Сообщение электронной почты	EML, MHT, MHTML, MIME, NWS
УПРАВЛЕНИЕ		
application/msproject	Проект MS Project	MPP, MPT
application/ms-project-2007-workspace		
application/x-ibm-requisitepro	Файл IBM Rational Requisite Pro	RQS

D.3. Язык описания регулярных выражений

При задании MIME-типов могут использоваться регулярные выражения. В регулярных выражениях применяются специальные символы (метасимволы): **$ ^ . * + ? [ ]** .

Табл. D.8. Описание метасимволов

Метасимвол	Назначение
. (точка)	Специальный знак, который соответствует любому одиночному символу, за исключением перевода строки.
***** (звездочка)	Постфиксный оператор, 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)	Оператор, который означает, что стоящее перед ним выражение должно появиться один или более раз. Например, выражение **bo+m** соответствует **bom**, **boom**, **booom** и т.д.
? (вопрос)	Оператор, 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**.
[] (квадратные скобки)	Служат для указания набора знаков, которым может соответствовать символ. Например, **[abcd]** соответствует любому из символов **a**, **b**, **c** и **d**. Выражение **[ab]*** будет соответствовать любой комбинации подряд идущих символов a и b произвольной длины. Кроме того, в скобках могут задаваться интервалы: выражение **[a-zA-Z0-9]** соответствует любому из символов латинского алфавита в верхнем и нижнем регистре, а также любой десятичной цифре от 0 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.
^	Символ для обозначения начала строки.
$	Символ для обозначения конца строки. Таким образом, **^$** соответствует пустой строке, а **^HOME$** — строке с единственным словом **HOME**.
\	Выполняет две функции: отменяет действие специальных символов, превращая их в обычные символы (данная операция называется экранированием символа), и вводит дополнительные специальные конструкции, такие как: • **\n** – перевод строки; • **\r** – возврат каретки; • **\t** – табуляция; • **** – установка символа \ без функции экранирования символов.
|	Означает выбор одного из вариантов. Выражение **alpha|beta|gamma** будет соответствовать любой из строк **alpha**, **beta** и **gamma**.

Приложение Е. Категории контентной фильтрации

Табл. Е.1. Категории контентной фильтрации

Номер	Дочерние подкатегории	Описание	Примеры сайтов
0	**Неопределенная категория**		
2100	**Хобби, отдых и развлечения или Досуг**		
2101	Еда и напитки (гурманство)	Супермаркеты, рестораны, кейтеринг, услуги доставки еды, организация банкетов, рецепты, домашняя еда	eda.ru, diets.ru, eda.yandex
2102	Мода, стиль, красота	• Высокая мода, подиум, хот кутюр, журналы о моде и красоте (женские, мужские), косметика, ювелирные изделия, пластическая хирургия • Сайты популярных людей и посвященные таким людям	• zaitsev.info, sofafashionweek.com, faberlic.kz • spletnik.ru
2103	Спорт	Виды спорта, спортивные состязания, спортивные товары и услуги, клубы, ассоциации, комитеты, новости спорта, обучение и тренировки, активные спортивные игры (например, пейнтбол), боевые искусства, форумы о спорте	sportrbc.ru, olympic.ru, baltikadiving.ru, bcrostovdon.ru, canoesport.ru, vmma.ru, paintballmfp.ru
2105	Строительство и ремонт	• Частное строительство, ремонт, услуги, инструменты, товары для дачи и садоводства, обустройство дома, домашняя мебель и техника • Экстерьер, интерьер зданий, сервис, разработка, проектирование	leroymerlin.ru, ikea.ru allegroclassica.ru, uar.ru, ardik.ru, a-garden.ru
2106	Авто, мото	Виды механической транспортной техники (в том числе летная и водная техника), автомобильные журналы, авто/мото-товары, сервисы и другие услуги, услуги по перевозке грузов, производители и дилеры, ремонт, запчасти, обучение вождению, авто форумы	audi-sever.ru, autoreview.ru, autosecurity.ru, bmw.ru, auto.ru, ilarauto-avia.ru, intermoto.ru, pddavto.ru, plenkacarbon.ru, prokat74.ru
2107	Природа, животные	Животные и уход за ними	wallpets.ru
2108	Юмор	Юмористические развлекательные сайты	anekdot.ru
2109	Фотография	Архивы фотографий, фотостоки, услуги фотостудий	300dpi.ru, kamakaev.ru aphoto.ru
2110	Сайты для детей	Сайты для детей	zakraski.ru
2111	Путешествия, туризм	Авиакомпании, поиск и бронирование туров, билетов, гостиниц, туроператоры, турагентства, отели и гостиницы, гиды и описания путешествий	travel.ru, lufthansa.com, aeroflot.ru, australia.ru, aviasales.ru
2113	Развлекательные ресурсы	• Отдых, досуг, фестивали, концерты, шоу, жизненные интересы, веб-журналы о жизни, развлечения, красота, устройство быта, развлекательные блоги	afisha.mail.ru, kudago.com, yaplakal.com, mdmpalace.ru, ticketland.ru,

Номер	Дочерние подкатегории	Описание	Примеры сайтов
		• Непрофессиональные увлечения, коллекционирование, рукоделие, охота, рыбалка • Сайты кафе, ресторанов • Прочая информация о досуге и развлечениях	kinoprostor.ru, xlbowling.ru, novostidom2.ru, belcoins.com, beloshveika.su, cactusok.ru, ohotniki.ru, hobby365.ru
2114	Культура	Музеи, музыка, культурные учреждения, театры, классическая литература, музыка, живопись	bolshoi.ru, teatr.ru, vavilon.ru, 21art.r
2200	**Мультимедиа**		
2201	Музыка и видео	• Сайты для загрузки, прослушивания, просмотра музыки, фильмов, видеороликов, картинок и изображений • Сайты компаний, музыкальных групп, организаций, баз данных, относящихся к производству музыки и фильмов, торренттрекеры с этими материалами • Сайты клубов, диджеев, концертов • Сайты для фанатов аниме и косплеев	• kinopoisk.ru, youtube.com, ivi.ru, rutor.info, music.yandex.ru, kirkorov.ru • animenime.ru, animefan.ru, chiwassu.ru
2202	ТВ или видео стриминг	Онлайн трансляции, стриминговые видео сервисы, прямой эфир, сайты телеканалов	sport-stream.ru, 1tv.ru
2203	Радио/аудио стриминг	Радиотрансляции в интернете, сайты радиостанций, музыкальные архивы	nashe.ru
2204	Файловые обменники, хостинг файлов	Файловые архивы ПО, файлообменники, сайты для загрузки бесплатных и условно бесплатных программ, включая программы для мобильных устройств	softportal.com
2300	**Непристойное содержание**		
2301	Порнография	Порнография, проституция, сайты для взрослых, секс знакомства, рекламные сети с порно	
2302	Эротика, нудизм, интимная одежда	Эротические сцены, фильмы, секс без порнографии, стриптиз, секс магазины, нижнее белье, изображения и фотографии обнаженных и полуобнаженых тел	bur-club.ru, sex-shopintim.com
2303	Половое воспитание	Сексуальное образование для детей	uroweb.ru, allcondoms.com
2304	Плохая репутация, аморальные, мат	Сайты, содержащие избыточное количество нецензурной лексики, либо немодерируемые форумы	yahooeu.ru, yebanko.ru
2305	Запрещенные сайты	Сайты, страницы и адреса, доступ к которым в России запрещен на основании закона и других нормативных актов	
2400	**Интернет-коммуникация**		
2401	Веб-почта	Бесплатная почта в интернет через веб-браузер	e.mail.ru, mail.yandex.ru
2402	Форумы, блоги	Форумы, вопросы и ответы, блоги, частные сайты, системы массового хостинга	spbtalk.ru, otvet.mail.ru, vbazar.mybb.ru
2403	Чат, SMS	Сайты чатов и мессенджеров, управляющие серверы систем обмена сообщениями	agent.mail.ru

Номер	Дочерние подкатегории	Описание	Примеры сайтов
2404	Интернет-телефония	Телефонные сервисы, VoIP (Voice over Internet Protocol) или IP-телефония	freecall.com, voice.google.com, justvoip.com
2405	Социальные сети	Социальные сети, сайты знакомств, чаты, мессенджеры	vk.com, skype.com, love.mail.ru, chatvdvoem.ru
2406	Сайты знакомств и брачные агентства	Сайты знакомств и брачные агентства	badoo.com
2500	**ИТ-Угрозы**		
2501	Хакинг и крэкинг	Взлом сетей и программ (услуги, руководства, обучение), в том числе для исследования защищенности, несанкционированный доступ к данным	
2502	Онлайн мошенничество, фишинг	• Оплата за клики, серфинг, просмотр рекламы • Поддельные сайты для выуживания паролей и номеров банковских карт путем подделки дизайна оригинального сайта • Архивы рефератов, ответов на ЕГЭ и т.д.	5-kopeek.ru, rabotnikonline.ru
2503	Незаконное распространение программ	Warez, кодгены, патчи, нелегальное ПО	cracklab.ru
2504	Анонимные прокси или VPN	Анонимные прокси серверы через веб, IP-адреса TOR узлов входа и выхода, программ и плагинов для анонимного выхода в интернет, IP-адреса VPN прокси сервисов	hidemy.name, proxy6.net
2506	Шпионское ПО, спам	Трояны, кейлогеры и другие программы скрытного удаленного управления компьютером	
2507	Вредоносное ПО, вирусы	Вредоносные компьютерные программы, зараженные веб сайты	
2600	**Преступная деятельность**		
2601	Насилие, убийства, суицид	Сайты, посвященные расовой дискриминации, вражде между людьми, насилию	kukluxklan.bz, resist.com
2602	Оружие	Военные ведомства и предприятия, каталоги, магазины оружия, включая гражданское оружие	mil.ru, guns.ru, tempgun.ru
2603	Терроризм, экстремизм	Сайты, посвященные пропаганде агрессии, расизма, терроризма	
2604	Криминал, мошенничество	Криминальные новости, справочники, правила, продажа или изготовление оружия, взрывчатки	bratva.koptevo.ru, gopnic.ru, allcrime.ru
2605	Запрещенные лекарства, наркотики	Пропаганда употребления наркотических средств, продажа и изготовление наркотиков	cannabiscafe.net
2700	**Игры**		
2701	Азартные игры, онлайн-казино	Игры на деньги, справочники, правила по таким играм, игровое оборудование, онлайн казино	ligastavok.ru, kingvulcan.com, gaminator.com
2702	Игры, онлайн-игры	• Компьютерные игры, производство, продажа, фанклубы, форумы, возможности скачать игру с официального сайта, онлайн покупка игр, игровые журналы, рейтинги, премии и награды • Онлайн игры через веб-браузер	playground.ru, free-games.ru, gta.ru, xboxrussia.ru, games.rambler.ru, flashworld.ru, lotr.ru
2800	**Бизнес, коммерция**		

Номер	Дочерние подкатегории	Описание	Примеры сайтов
2801	Экономика, финансы	• Коммерческие компании, производители товаров/услуг вне других категорий, предпринимательство, консалтинговые услуги, корпоративные сервисы, бизнес менеджмент, B2B • Рынки, инвестиционные фонды, акции, биржи, банки, кредиты, займы • Страховые компании, агентства, услуги	• sberbank.ru, moex.com • vtbins.ru, zettains.ru, inskasko.ru
2802	Машиностроение, промышленность	• Промышленные предприятия, заводы, добывающие компании, производство и продажа промышленных материалов, техники, оборудования • Отрасли сельского и лесного хозяйства, техника, товары	rosenergoatom.ru, bz.ru, zmz.ru, belaz.by
2803	Электронные денежные системы, криптовалюта	• Платежные системы, электронные деньги, процессинговые центры платежей по банковским картам • Услуги купли продажи различных крипто валют, правила работы, новости и другая информация об этом	• webmoney.ru, elecsnet.ru, uniteller.ru • coingate.com, bitcoin.com, bitcoin.org
2804	Аукционы	Онлайн-аукционы	molotok.ru
2805	Торговля, интернет-магазины	• Товары народного потребления, предоставление услуг и сервисов частным лицам, розничная торговля, продавцы, торговые сети, центры, магазины, рынки, присутствие интернет-магазина как раздел сайта • Покупка товаров онлайн, платформы и сервисы, реализующие полный цикл онлайн продаж, оплата по банковской карте, доставка, интернет-магазины	mvideo.ru, fotolab.ru, 220-volt.ru
2806	Недвижимость	Сайты застройщиков, купли продажи и аренды недвижимости, управления недвижимостью и риелторы	1dom.ru, cian.ru
2807	Веб-реклама и аналитика	• Рекламные сервисы, баннерные сети, биржи, агентства, услуги, сувенирная продукция, брендинг, выставки, маркетинг, продвижение сайтов • Счетчики посещаемости и статистики сайтов • Сайты, временно размещенные у регистратора доменов с тестовой страницей-заглушкой, чаще всего рекламной	ad.adriver.ru, reklamy.ru, adwords.google.com, googleadservices.com, http://www.freedomart.ru/
2808	Поиск работы и карьера	Поиск работы, услуги подбора персонала, кадровые агентства	hh.ru, rabota.ru, superjob.ru, rabota.mail.ru, zarplata.ru, personagency.ru, triumphhr.ru
2900	**Здравоохранение**		

Номер	Дочерние подкатегории	Описание	Примеры сайтов
2901	Здоровье	Медицинские услуги, товары, забота о здоровье, сайты больниц, поликлиник и прочих медицинских учреждений, описания заболеваний и методов лечения, лекарства, аптеки	medison.ru, rigla.ru, gkb13.ru, mosgorzdrav.ru, rlsnet.ru, pharmamed.ru
2902	Алкоголь, курение	Сайты производителей алкоголя и табака, а также сайты, призывающие к их употреблению	russamogon.ru, amigo cigarro.ru, smokewoman.org
21000	**Технологии**		
21001	Производители ПО и оборудования	Сайты производителей ПО и оборудования	azure.com, citrix.com, vmware.com, teleport.media
21002	Web-хостинг	• Домены с просроченной оплатой и удерживаемые регистратором для продажи • Платформы, позволяющие бесплатно размещать веб-сайты, блоги. Бесплатные сервисы облачного хранения данных, рисунков, файлов с возможностью дать ссылку на скачивание, файлообменники • Сайты, которые обобщают и предоставляют доступ к многочисленным веб-сервисам, являющимся, как правило, отдельными сайтами данного портала с единой системой аутентификации. Бывают общего назначения или узкой тематической направленности, предоставляющие различные сервисы по определенным интересам и ориентированные на полный охват определенной тематики, например, региональный портал	narod.ru, ucoz.ru, radikal.ru, disk.yandex.ru mail.ru, rambler.ru, nn.ru
21003	Удаленное управление	Программное обеспечение для онлайн управления удаленным компьютером, его рабочим столом для технической поддержки	teamviewer.com
21004	Интернет	IT-компании, производители компьютерной техники и программного обеспечения, услуги в сфере IT, автоматизация предприятий, специализированные IT-магазины. Мобильная связь, операторы, гаджеты. Новостные или справочные сайты, программирование, системное администрирование, сети, сервера, компьютеры, программные онлайн сервисы, облака, высокие технологии	microsoft.com, softline.ru, stackoverflow.com, westerndigital.com
21005	Сети доставки контента	• Сайты торрент-трекеров и P2P систем • Сети доставки (и дистрибуции) содержимого	yastatic.net, www.gstatic.com
21100	**Информация**		
21101	Справочная информация	• Сайты со справочной информацией, карты, словари, переводчики, каталоги, статистика, расписание транспорта • Онлайн библиотеки, прослушивание аудиокниг онлайн, краткие содержания книг, краткие описания книг	altay-krai.ru, gvozdik.ru, allsoch.ru, slovari.ru, translate.yandex.ru, yandex.ru/maps/213/moscow, rasp.yandex.ru

Номер	Дочерние подкатегории	Описание	Примеры сайтов
21102	Образование	• Образовательные и научные учреждения, образовательные сайты по дисциплинам, научные данные и исследования • Книги, библиотеки, тексты песен, аккорды, ноты • Развивающие игры, пазлы, настольные игры, головоломки	• msu.ru • gramota.ru, danetka.ru, brainapps.ru, puzzles.in.ua
21103	Новостные сайты	Средства массовой информации, новостные агентства, интернет-издания, журналы, газеты, крупные частные блоги, прогноз погоды	ria.ru, rcb.ru, gismeteo.ru
21104	Поисковые системы/порталы	Поисковые системы/порталы	yandex.ru, google.ru, go.mail.ru
21105	Афиши, доски объявлений	Сайты с объявлениями частных лиц о купли продаже услуг и товаров	avito.ru
21106	Белый список	Разрешенные ресурсы	kassa.rambler.ru, soft.rambler.ru
21108	Офисные/бизнес приложения	Ресурсы офисных приложений и программ	miro.com, myoffice.ru, ilovepdf.com, docs.google.com
21200	**Общество**		
21201	Религия	• Религия и религиозные организации. Гадания, магия, гороскопы и другие потусторонние вещи. Псевдонаучные данные, догадки • Межнациональные отношения, народности	patriarchia.ru, horo.mail.ru, arhangel.ru
21202	Секты	• Сайты религиозных сект, нестандартные религиозные учения, ответвления от основных религий • Сайты, посвященные оккультизму и астрологии, сайты астропрогнозов	drevolife.ru, golgotha.ru,raelpress.org
21203	Государство и закон	• Официальные веб-сайты государственных учреждений, политических партий, судов, адвокатов и юриспруденции • Сайты политических новостей, политических партий • Справочники законов	kremlin.ru, ldpr.ru, mosgorsud.ru
21204	Негосударственные организации, фонды	• Благотворительные организации, фонды помощи • Некоммерческие организации, межгосударственные организации и другие организации, не связанные напрямую с бизнесом	fondotv.ru, rusfond.ru
21205	Семья, дети	• Сайты для детей и сделанные самими детьми, сайты школ и для школьников • Сайты о домоводстве, семье, различных хобби	parents.ru, detochka.ru, lyceum87.narod.ru

Лист контроля версий

02/11/2024-17:04