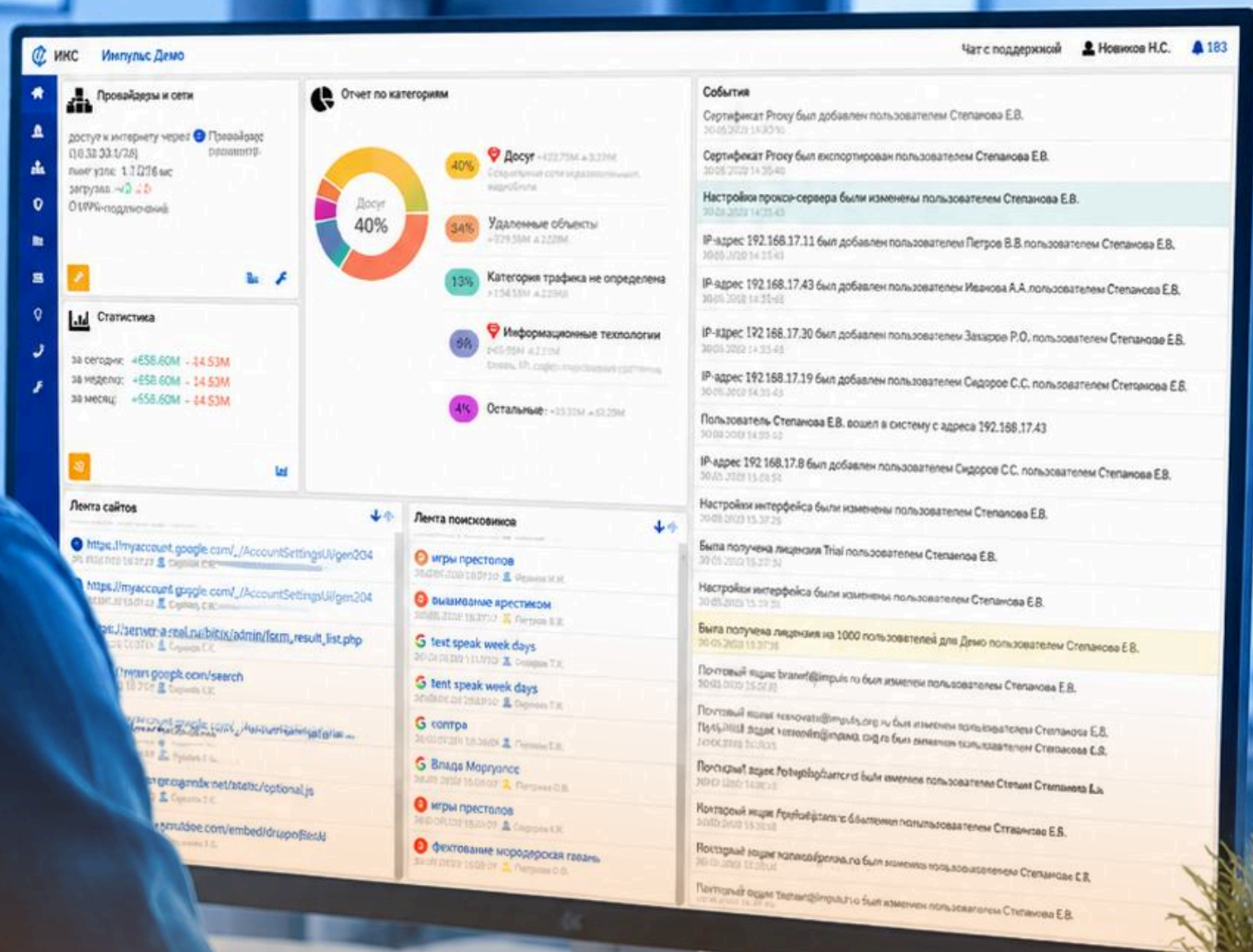




Интернет Контроль Сервер



Инструкция по настройке ИКС



Оглавление

1. [Создание локальной сети и провайдера](#)
2. [Заведение и авторизация пользователей на ИКС](#)
3. [Настройка прокси-сервера, фильтрации и правил пользователей](#)
4. [Статистика и отчеты](#)
5. [Защита сети и маршрутизация](#)
6. [Настройка удаленных подключений](#)
7. [Модуль «Телефония»](#)
8. [Почтовый сервер](#)
9. [Обслуживание, Мониторинг, Журнал и уведомления](#)

1. Создание Локальной сети и Провайдера

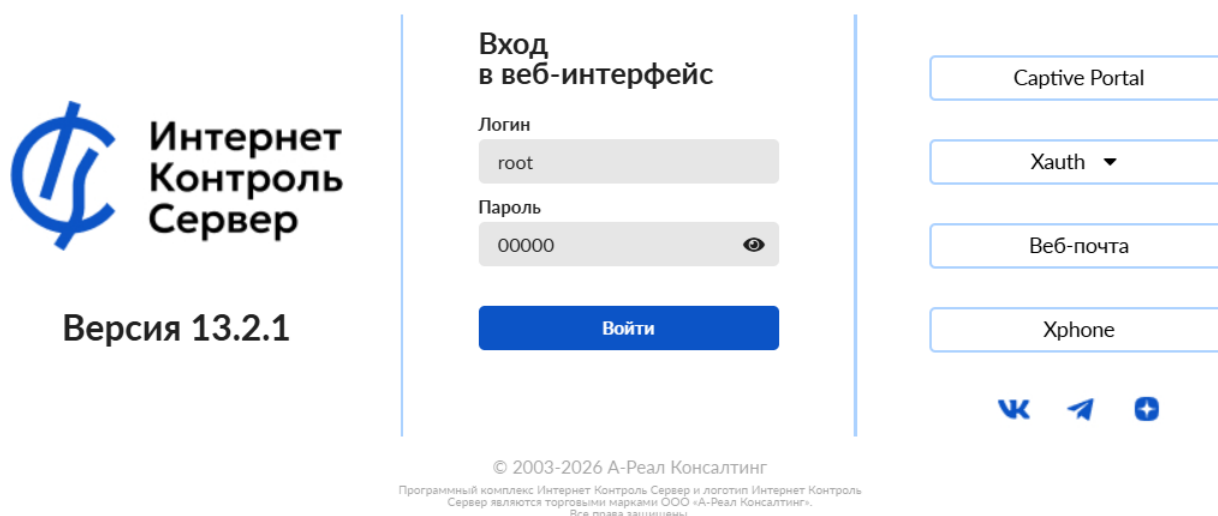
1.1 Подключение к веб-интерфейсу

После установки ИКС на сервер или виртуальную машину, необходимо подключиться к веб-интерфейсу для настройки. Для того, чтобы это сделать, вводим в строке браузера назначенный при установке ip-адрес в формате: **x.x.x.x:81**

Обратите внимание, что для входа необходимо находиться в одной сети с ИКС!

На экране появляется окно для ввода логина и пароля. По дефолту логин для входа root и пароль 00000 (пять нулей). Если вы используете версию ИКС NGFW, вам будет предложено задать пароль для администратора.

Для полноценного тестирования, необходимо активировать **Trial** версию. Тогда будут подгружены различные базы, которые необходимы для корректной работы модулей. Для регистрации **Trial** версии, переходим в меню «Обслуживание» → «О программе» и заполняем необходимые данные для запроса.



Вход
в веб-интерфейс

Логин
root

Пароль
00000

Войти

Captive Portal

Xauth ▼

Веб-почта

Xphone

Версия 13.2.1

© 2003-2026 А-Реал Консалтинг
Программный комплекс Интернет Контроль Сервер и логотип Интернет Контроль Сервер являются торговыми марками ООО «А-Реал Консалтинг». Все права защищены.

1.2 Создание Локальной сети и Провайдера

Переходим на вкладку «Сеть» → «Провайдеры и сети».

Создание Локальной сети в веб-интерфейсе является обязательным, так как настройки, сделанные при первичном входе в консоли восстановления, будут действовать до первой перезагрузки. Все управление и настройка происходит только через веб-интерфейс.

Для создания Локальной сети нажимаем кнопку «Добавить» → «Локальная сеть».

ИКС Моя тестовая > Провайдеры и сети Чат с поддержкой Администратор 11

Сеть
Мастер настройки сети
Провайдеры и сети
Сетевое окружение
Сетевые утилиты
Мониторинг экран
Маршруты
Маршрутизатор
DNS
DHCP
Прокси
VPN
ARP-таблица
Удаленное управление

Провайдеры и сети Логические интерфейсы Внешние устройства Балансировка трафика Монитор провайдеров Журнал

Добавить Удалить Выключить Редактировать Мастер настройки сети

Сети
Локальная сеть
Провайдеры
Провайдер
Туннели

кабель подключен

Указываем адрес, который выбрали для ИКС, интерфейс и разрешаем управление.

Редактирование локальной сети

Общие настройки

CARP

Название *

LAN

Интерфейс *

vtnet0 (fe:c3:0e:72:44:c4)

IP-адрес/префикс *

192.168.17.234/24

VLAN ID

(не использовать)

☒ NAT из локальных сетей

☒ Разрешить управление ИКС через веб

☒ Разрешить управление ИКС через SSH

☐ Задать MAC-адрес

MAC-адрес *

MAC-адрес

Скорость

Автоопределение

Режим

Автоопределение

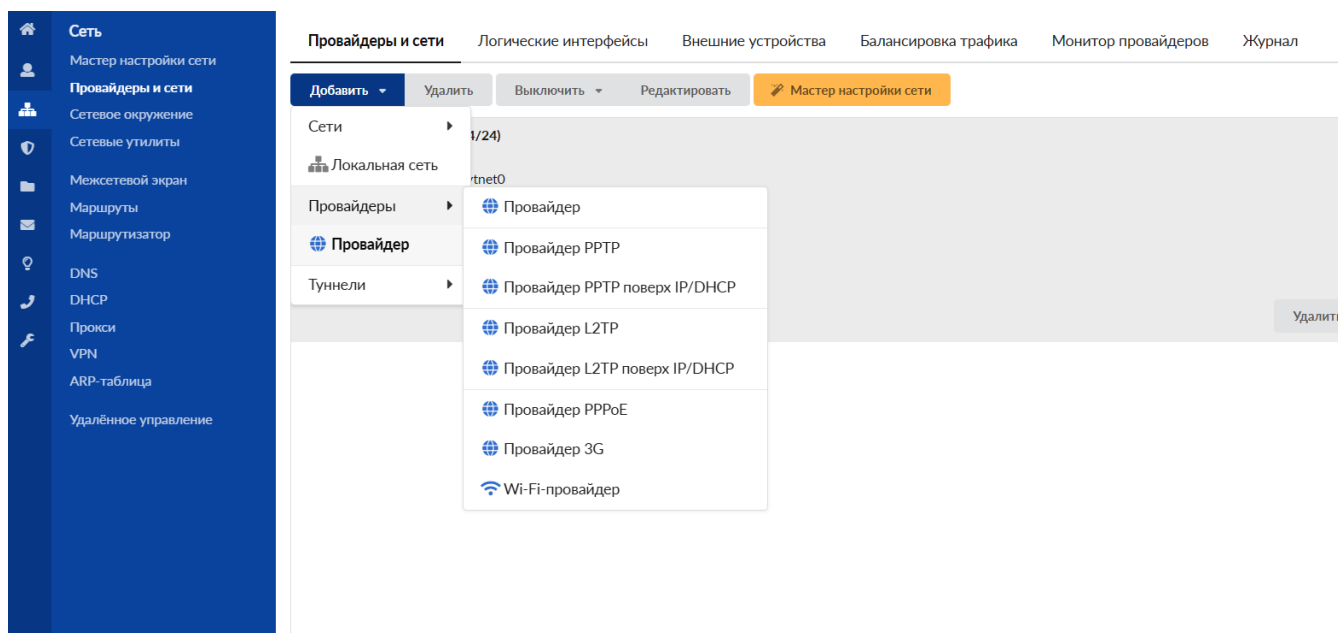
MTU

1500

Сохранить

Отмена

Далее добавляем Провайдера: Сеть → Провайдеры и сети → Добавить → Провайдер.
Заполняем поля, либо получаем адрес автоматически.



Если Провайдер не подключен на прямую, например, во время теста, и ИКС является участником сети, для выхода в интернет можно создать **Маршрут**.

В этом случае в меню «Сеть» → «Маршруты», создаем Статический маршрут. В нем указываем шлюз, через который пойдём в интернет и в поле «Назначение» прописываем 0.0.0.0/0, т.е. весь интернет.

Редактирование статического маршрута

Общие настройки

Настройки мониторинга

Описание

Назначение

☒ Через шлюз☐ Через интерфейс☐ Через провайдера

Метрика

Время действия

СохранитьОтмена

Проверить доступность интернета, можно сразу на вкладке «Сеть» → «Сетевые утилиты» → «Пинг».

Сеть

Мастер настройки сети

Провайдеры и сети

Сетевое окружение

Сетевые утилиты

Межсетевой экран

Маршруты

Маршрутизатор

DNS

DHCP

Прокси

VPN

ARP-таблица

Удалённое управление

Пинг

Трейс

Опрос DNS

Информация о домене

Дамп

Сетевые интерфейсы

Адрес *

Количество пакетов *

Провайдер

ya.ru

3

(любой)

▶ Запустить

PING ya.ru (5.255.255.242): 56 data bytes

64 bytes from 5.255.255.242: icmp_seq=0 ttl=54 time=17.159 ms

64 bytes from 5.255.255.242: icmp_seq=1 ttl=54 time=16.717 ms

64 bytes from 5.255.255.242: icmp_seq=2 ttl=54 time=17.519 ms

ya.ru ping statistics ---

3 packets transmitted, 3 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 16.717/17.132/17.519/0.328 ms

2. Заведение и авторизация пользователей на ИКС

2.1 Авторизация пользователей на ИКС

Для того, чтобы Пользователи имели доступ в интернет, их необходимо авторизовать на ИКС.

Пользователем считается единица, заведенная на ИКС. Он может быть добавлен разными способами и им может выступать как пользователь/человек, так и устройство. Каждому пользователю может соответствовать один или несколько ip-адресов.

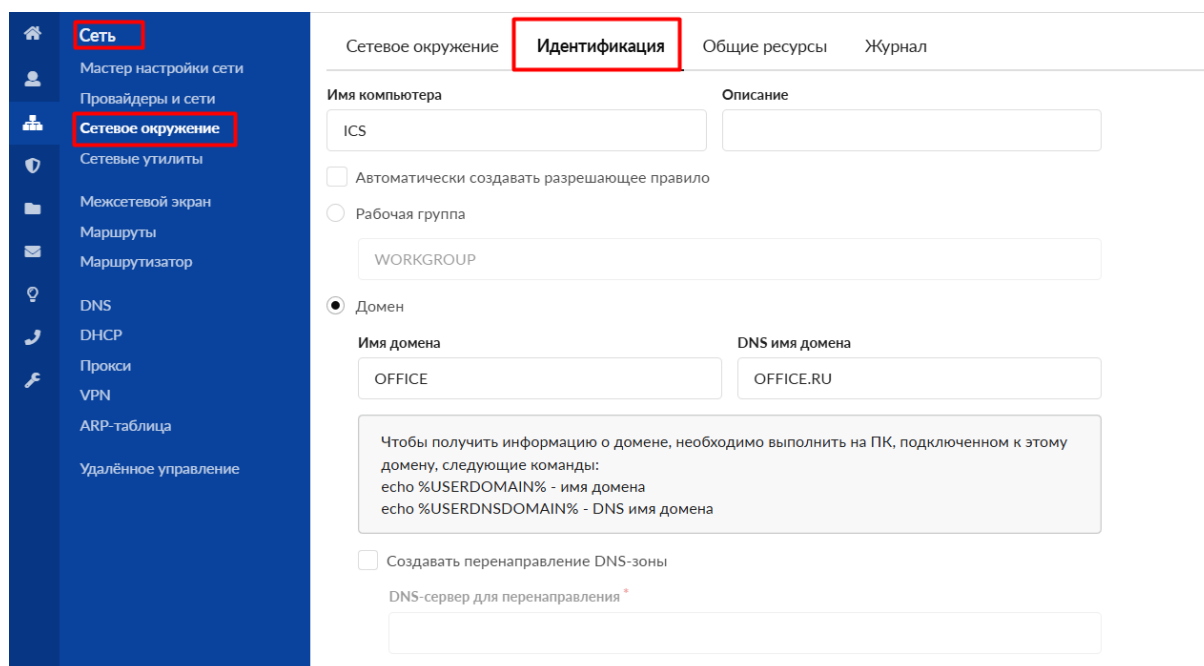
Пользователей или группы пользователей на ИКС можно добавить разными путями:

- вручную;
- импорт из файла;
- через сканирование сети;
- импортировать из домена.

Для добавления пользователя вручную, перейдите на вкладку «Пользователи и Статистика» → «Пользователи» → «Добавить» и создайте Пользователя.

В ИКС можно импортировать пользователей из домена. Есть поддержка **AD** и **ALDPro**. Если вы хотите не просто импортировать пользователей, но и настроить синхронизацию, ИКС необходимо ввести в домен.

На вкладке «Сеть» → «Сетевое окружение» → «Идентификация» указываем данные для подключения к домену.



Имя домена можно проверить через командную строку.

Вводим в ней команду: **set userdomain**

DNS имя домена проверяем командой: **set userdnsdomain**

Для ввода ИКС в домен, учетная запись должна обладать правами Администратора. После ввода ИКС в домен, можно переходить к импорту доменных пользователей.

На вкладке «Пользователи и Статистика» → «Пользователи» → «Импорт» → «LDAP» прописываем данные, подключаемся и импортируем/синхронизируем необходимые группы и пользователей.

2.2 Настройка авторизации пользователей

В ИКС предусмотрены разные варианты авторизации:

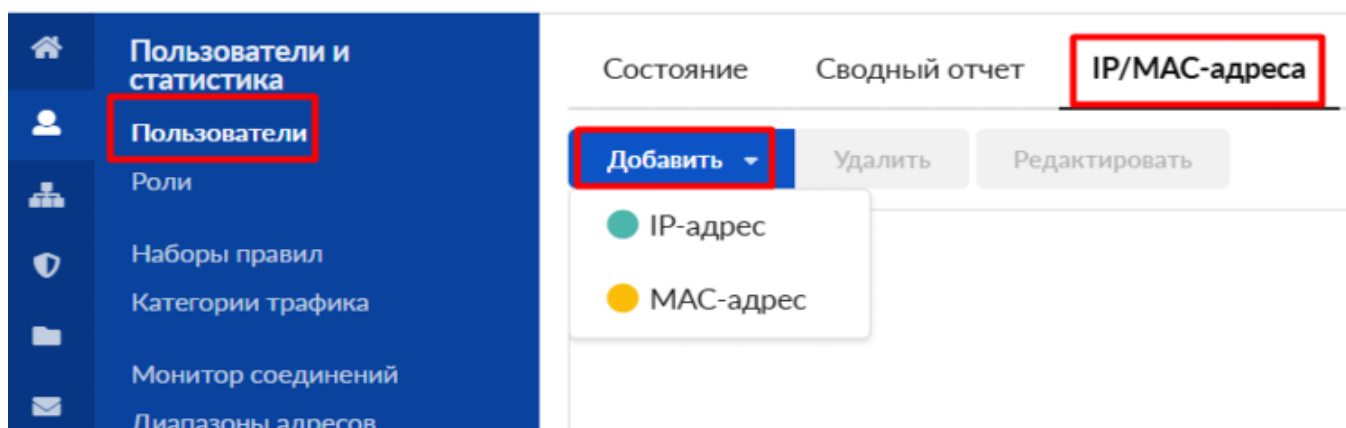
- IP или MAC адрес;
- логин/пароль;
- NTLM;
- Kerberos;
- LDAP;
- по SMS;
- по телефонному звонку;
- с использованием утилиты Xauth.

2.3 Авторизация по IP или MAC

Если у пользователя прописан статический ip-адрес, либо динамические ip-адреса, регистрируемые с привязкой по mac-адресу, то пользователь получает доступ во внешнюю сеть по всем протоколам в соответствии с глобальными и индивидуальными правилами доступа. Одному пользователю можно назначить любое количество IP-адресов.

Чтобы назначить пользователю диапазон адресов, укажите адрес в одном из двух вариантов: IP-адрес/префикс (например, 192.168.1.1/24), либо через дефис (192.168.1.1-192.168.1.254).

На вкладке «Пользователи и Статистика» → «Пользователи» выберите необходимого пользователя. В индивидуальном модуле перейдите на вкладку «IP/MAC-адреса» → «Добавить».



2.4 Авторизация по логину/паролю

На вкладке «Пользователи и статистика» → «Captive portal» установите флаг «Авторизация по логину и паролю». В этом случае в Captive portal запускается сервер веб-авторизации. При первом обращении пользователя к какому-либо ресурсу ему будет предложено ввести логин и пароль, закрепленный за его учетной записью в ИКС.

При необходимости установите флаг «Запретить множественную авторизацию с одним логином». Тогда пользователь, использующий конкретный логин, не сможет одновременно авторизоваться при помощи Captive Portal с различных устройств.

2.5 Авторизация NTLM

После импорта пользователей из LDAP, перейдите в меню «Сеть» → «Прокси» → «Настройки», выберите тип авторизации «Внешняя» → «NTLM».

2.6 Авторизация Kerberos

Для того чтобы пользователи домена авторизовывались по протоколу сетевой аутентификации Kerberos их необходимо импортировать из домена. В настройках прокси «Сеть» → «Прокси» → «Настройки» выбрать тип авторизации «Kerberos».

В меню «Пользователи и Статистика» → «Настройка авторизации» → «Kerberos» настроить соединение с доменом (создать и добавить Keytab-файл).

Керberos LDAP

Для доменной авторизации импортируйте пользователей из LDAP на странице Пользователи

Имя компьютера * DNS-имя домена *

При изменении имени компьютера и домена будет изменено имя системы в модуле Система

DNS-имя контроллера домена *

Keytab-файл *

Для создания keytab-файла необходимо выполнить следующие действия в контроллере домена:

1. Создать пользователя my с бессрчным паролем
2. Выполнить от имени администратора в командной строке:

```
ktpass -princ HTTP/my.gate.com@GATE.COM -mapuser "my" -pass "Aa123456" -crypto All -ptype KRB5_NT_PRINCIPAL -out C:\ics_01.keytab
```

-princ HTTP/my.gate.com@GATE.COM - имя принципа службы (SPN)
 -mapuser "my" - пользователь
 -pass "Aa123456" - пароль
 -out C:\ics_01.keytab - путь к файлу

2.7 Авторизация LDAP

Для того чтобы пользователи домена авторизовывались по протоколу сетевой аутентификации LDAP, необходимо импортировать пользователей из домена. Далее в настройках прокси «Сеть» → «Прокси» → «Настройка» выбрать тип авторизации «LDAP».

В меню «Пользователи и Статистика» → «Настройка авторизации» → «LDAP» настроить соединение с доменом.



Пользователи и статистика

Пользователи

Роли

Наборы правил

Категории трафика

Монитор соединений

Диапазоны адресов

Отчеты

Управление отчетами

Сервер авторизации (Xauth)

GSSAPI-сервер

Настройки авторизации

Captive Portal

Синхронизация

Kerberos

LDAP

Для доменной авторизации импортируйте пользователей из LDAP на странице Пользователи

LDAP-сервер

Active Directory

FreeIPA

IP-адрес/Имя сервера *

DNS-имя домена *

192.168.1.1

office.domain.ru

Тип соединения *

Plain (небезопасно)

Проверять сертификат сервера

Логин *

Пароль *

Логин

Пароль

Сеть

Мастер настройки сети

Провайдеры и сети

Сетевое окружение

Сетевые утилиты

Межсетевой экран

Маршруты

Маршрутизатор

DNS

DHCP

Прокси

VPN

ARP-таблица

Удаленное управление

Прокси-сервер

Настройки

Автоконфигурация

Родительский прокси

Исключе

Порт *

3128

Автоматически создавать разрешающее правило

Доступ к прокси

Политика доступа

IP-адрес, затем логин

Только логин

Только IP-адрес

Известные IP-адреса получают доступ без аутентификации. Остальные пользователи должны пройти аутентификацию

Аутентификация пользователей

Через ИКС

Схема аутентификации

Basic

Digest

Внешняя

NTLM

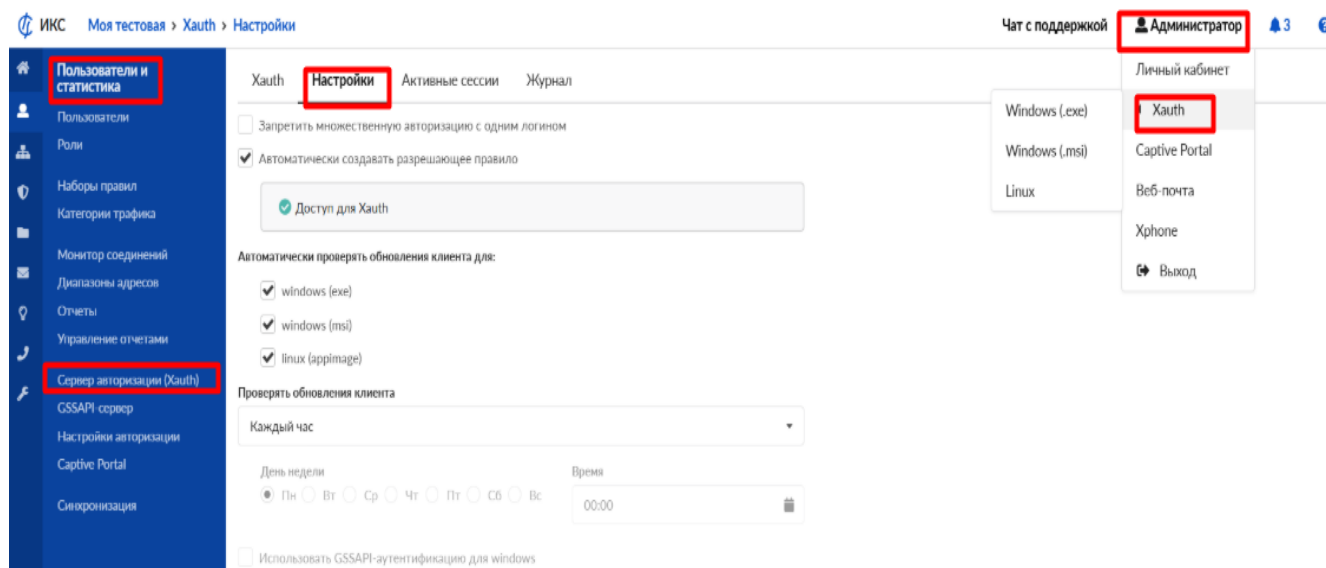
Kerberos

LDAP (не настроено)

2.8 Авторизация Xauth

Утилита для авторизации **Xauth** доступна в версии **ИКС NGFW**. Она используется для авторизации пользователей, а также добавляет возможность блокировки Приложений, запущенных на конечных устройствах.

Скачать разные варианты для утилиты для разных систем, можно включив ее на вкладке «Пользователи и статистика» → «Сервер авторизации Xauth» → «Настройки». После этого можно выбрать необходимый вариант установочника, нажав на значок «Администратора».



The screenshot displays the web interface of the Internet Control Server. The breadcrumb navigation at the top reads: ИКС > Моя тестовая > Xauth > Настройки. The left sidebar contains a menu with the following items: Пользователи и статистика (highlighted with a red box), Пользователи, Роли, Наборы правил, Категории трафика, Монитор соединений, Диагнозы адресов, Отчеты, Управление отчетами, Сервер авторизации (Xauth) (highlighted with a red box), GSSAPI сервер, Настройки авторизации, Captive Portal, and Синхронизация. The main content area is titled 'Настройки' (highlighted with a red box) and includes tabs for Xauth, Активные сессии, and Журнал. Under the Xauth tab, there are checkboxes for 'Запретить множественную авторизацию с одним логином' (unchecked) and 'Автоматически создавать разрешающее правило' (checked). A green status bar indicates 'Доступ для Xauth'. Below this, a section titled 'Автоматически проверять обновления клиента для:' contains three checked options: 'windows (exe)', 'windows (msi)', and 'linux (appimage)'. The 'Проверять обновления клиента' section features a dropdown menu set to 'Каждый час', a 'День недели' selector with 'Пн' selected, and a 'Время' field set to '00:00'. At the bottom, there is an unchecked checkbox for 'Использовать GSSAPI-аутентификацию для windows'. On the right side, a user profile dropdown for 'Администратор' is open, showing options: 'Личный кабинет', 'Xauth' (highlighted with a red box), 'Captive Portal', 'Веб-почта', 'Xphone', and 'Выход'. Above this dropdown, there is a link for 'Чат с поддержкой' and a notification bell icon with the number '3'.

3. Настройка прокси-сервера, фильтрации и правил пользователей

Для того, чтобы была возможность фильтровать трафик пользователей, необходимо настроить его расшифровку.

Есть два режима для настройки фильтрации: **Полная расшифровка с подменой сертификата**, в этом случае происходит полная расшифровка содержимого страницы, виден весь путь обращения, запрос который пользователь вводил в браузере и будет доступна возможность блокировки по словам и выражениям. В этом случае необходима установка сертификата в **Доверенные корневые центры** на конечном устройстве.

Второй вариант – **Фильтровать без подмены сертификата**. В этом случае будет виден только домен обращения. Установка сертификата на конечное устройство не требуется. Чтобы настроить фильтрацию HTTPS-трафика, в первую очередь необходимо создать сертификат.

Переходим в меню «Защита → «Сертификаты» → «Добавить» → «Корневой сертификат (CA)».

Добавляем «Корневой сертификат» со стандартными настройками.

Тип сертификата	Закрытый ключ	Создан
Open	не зашифрован	15.12.2023
Autogenerated Asterisk_65705d0c755b96.99141202	не зашифрован	06.12.2023
Autogenerated Default Web_66fcbcb0f5ba552.37153935	не зашифрован	02.10.2024
Autogenerated GUI_65705d08b70de3.13774070	не зашифрован	06.12.2023
Autogenerated MailServer_65705d09666551.45669145	не зашифрован	06.12.2023
CA	не зашифрован	18.12.2023
dfdg	не зашифрован	22.07.2024
https	не зашифрован	07.12.2023

Добавление сертификата

Общие Настройки Использование ключа Netscape расширение

Название *

https

Код страны *

RU - Russian Federation

Город Область

Город Область

Организация E-mail

Организация E-mail

Имя или адрес хоста *

test.ru

Список дополнительных доменов и поддоменов

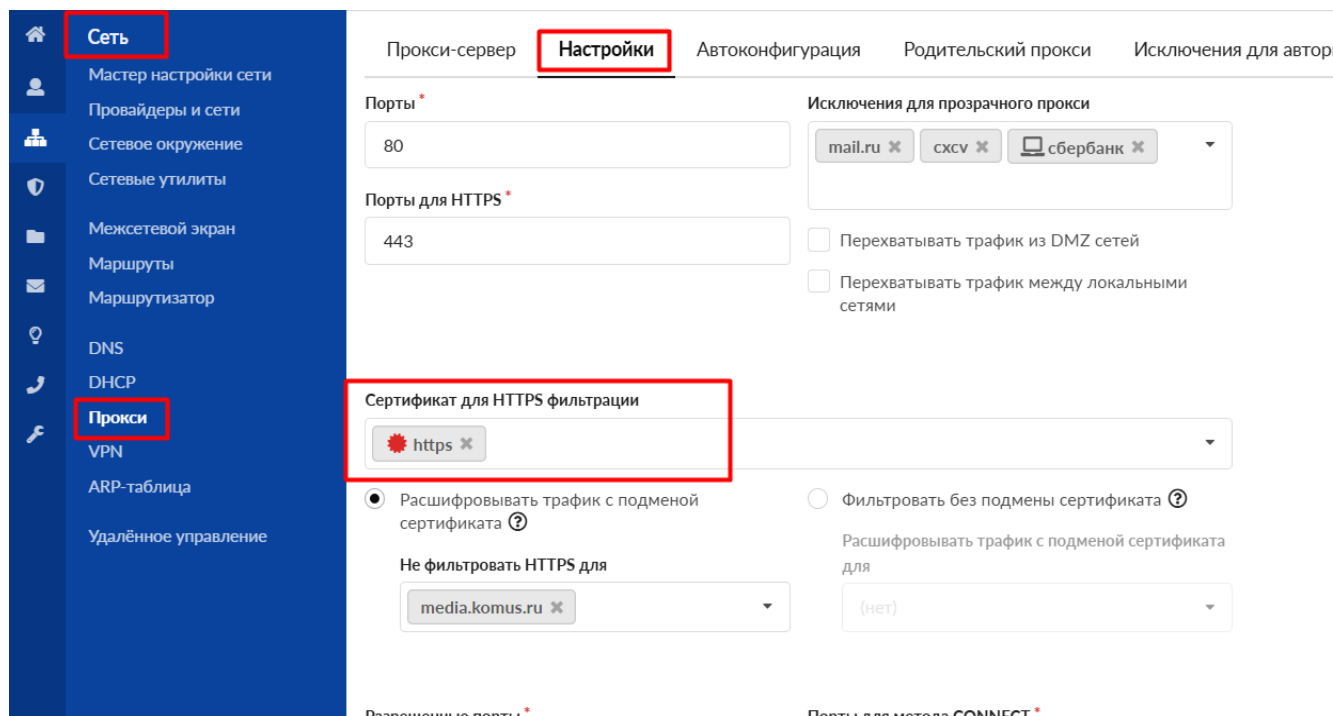
Список дополнительных доменов и поддоменов

Добавить Отмена

При добавлении выбираем «Не шифровать закрытый ключ».

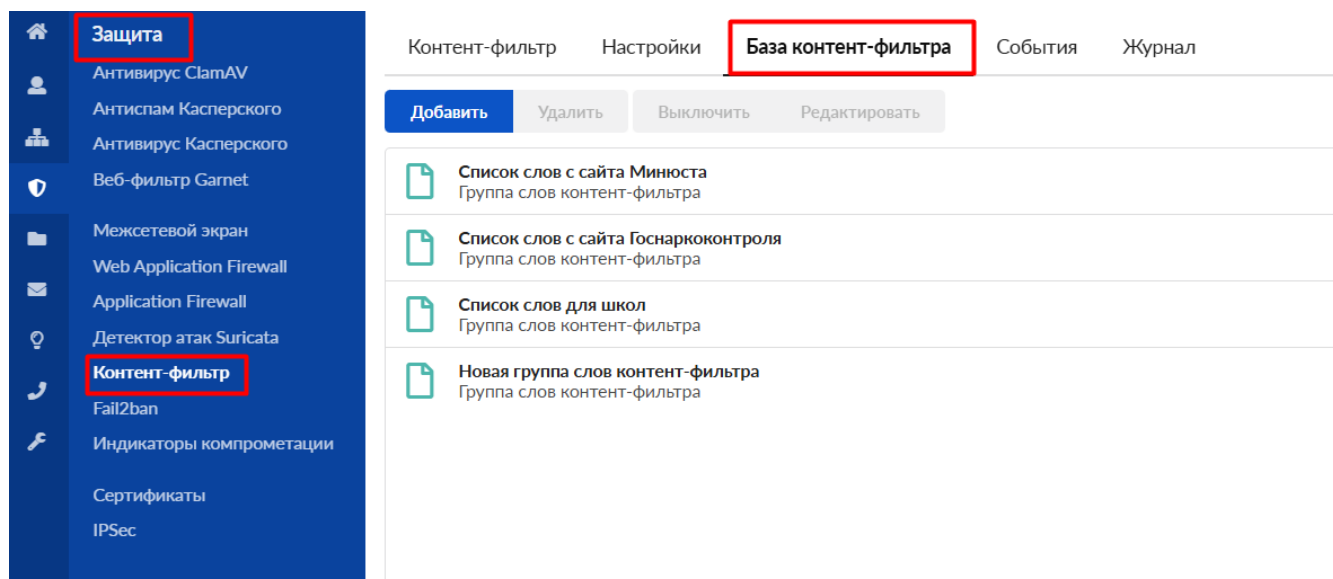
Далее мы можем его использовать для настройки режима работы Прокси-сервера.

Переходим на вкладку «Сеть» → «Прокси» → «Настройки» и выбираем необходимый режим.



3.1 Контент-фильтр

Модуль «Контент-фильтр» доступен с первого дня тестирования и используется для блокировки по словам и выражениям. Для его настройки перейдите на вкладку «Защита» → «Контент-фильтр». Здесь мы можем выбрать базы, которые будут использоваться для фильтрации, либо добавить свои, для блокировки по Шаблонам и Ключевым словам. Далее правила Контент-фильтра мы можем использовать при добавлении правил для пользователя или группы.

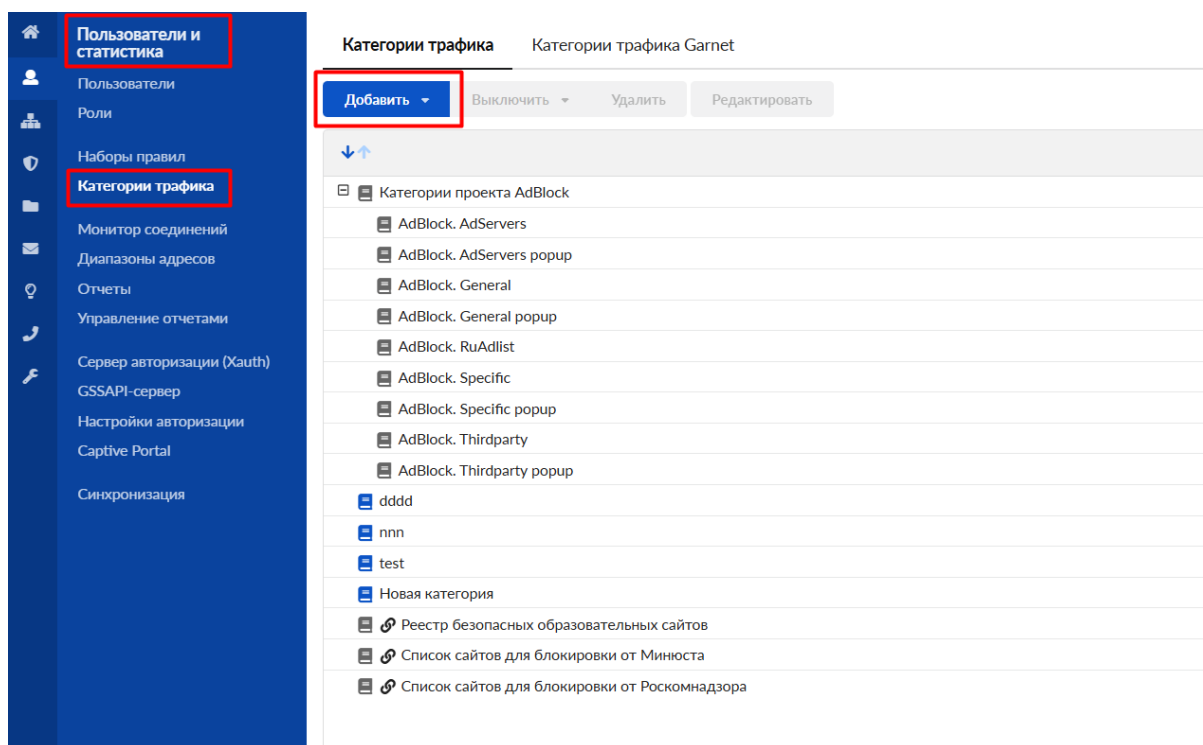


3.2 Категории трафика

Категории трафика позволяют блокировать трафик по доменам, расширениям или MIME-типам. В ИКС есть предустановленные базы для блокировки по Категориям трафика, которые можно использовать (базы Минюста, Роскомнадзора, списки для школ, AdBlock). В версии ИКС NGFW кроме этого есть возможность использовать категоризатор трафика Garnet.

Веб-фильтр **Garnet** определяет категории сайтов на основе анализа его текстового содержимого при помощи алгоритмов машинного обучения. На данный момент он содержит 36 категорий сайтов.

Для создания своих Категорий трафика, перейдите в меню «Пользователи и статистика» → «Категории трафика» → «Добавить». Можно добавлять сайты как вручную, так и через текстовый документ и в дальнейшем использовать списки для разрешающих или запрещающих правил, которые будут назначаться на пользователей или группы.



3.3 Application Firewall

В ИКС есть встроенный модуль контроля приложений. С его помощью администратор может блокировать активность установленных на пользовательские компьютеры программ. Блокировка осуществляется благодаря Application Firewall, который использует возможности библиотеки nDPI или утилиты Xauth.

Можно добавить правило Application Firewall в индивидуальном модуле пользователя или группы на вкладке «Пользователи и статистика» → «Пользователи» → «Правила и ограничения» → «Правило L7 фильтра».



В нем мы можем выбрать протоколы или приложения, запущенные на конечном устройстве (если пользователь авторизовался через утилиту Xauth) и заблокировать их.

3.4 Добавление правил пользователей

После настройки расшифровки трафика, мы можем настроить правила для пользователей. Создавать свои наборы правил, которые будут применяться к пользователям или группам, либо редактировать предустановленные. В ИКС есть набор для создания «Белых списков» или «Правила для школ», которые упрощают настройку.

Наборы правил находятся в меню «Пользователи и статистика» → «Наборы правил».

Правила можно назначить как конкретному пользователю, так и группе, в которой находится пользователь. В меню Пользователя, мы можем видеть все варианты правил, которые возможно применить для настройки.



ИКС Моя тестовая > Пользователи > уапа > Правила и ограничения

Пользователи и статистика

- Пользователи
- Роли
- Наборы правил
- Категории трафика
- Монитор соединений
- Диапазоны адресов
- Отчеты
- Управление отчетами
- Сервер авторизации (Xauth)
- GSSAPI-сервер
- Настройки авторизации
- Captive Portal
- Синхронизация

Состояние Сводный отчет IP/MAC-адреса **Правила и ограничения** Почта и телефония Перенаправление

Добавить Удалить Выключить Редактировать Подробнее

- Набор правил
- Ограничение количества соединений
- Запрещающее правило
- Ограничение скорости
- Запрещающее правило Application firewall
- Выделение полосы пропускания
- Разрешающее правило
- Маршрут
- Исключение
- Квота
- Запрещающее правило прокси
- Правило контентной фильтрации
- Разрешающее правило прокси
- Исключение прокси

При анализе трафика для пользователей в ИКС действует следующий порядок правил:

1. Личные правила пользователя.
2. Наборы правил, назначенные на пользователя. Если к пользователю прикреплено несколько наборов правил, они объединяются и проверяются как один набор.
3. Правила родительской группы.
4. Наборы правил, назначенные на родительскую группу. Если к группе прикреплено несколько наборов правил, они объединяются и проверяются как один набор.
5. Повторяются шаги 3-4 до тех пор, пока не будет достигнута корневая группа.

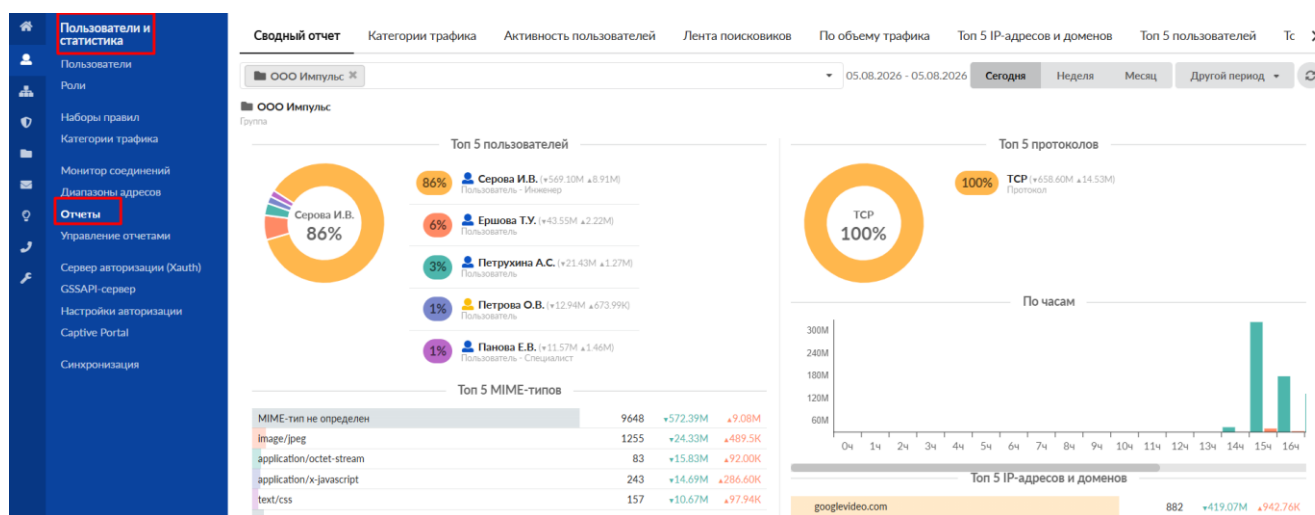
В каждом шаге правила проверяются в следующем порядке:

1. Исключения
2. Разрешающие
3. Запрещающие
4. Контент-фильтр

4. Статистика и отчеты

Систему статистики пользователей в ИКС можно настроить вручную, либо вывести с помощью нескольких стандартизированных отчетов. Каждый отчет выводится в соответствующей вкладке:

- «Сводный отчет»
- «Категории трафика»
- «Активность пользователей»
- «Лента поисковиков»
- «По объему трафика»
- «Топ 5 IP-адресов и доменов»
- «Топ 5 пользователей»



Отчеты можно смотреть как на вкладке «Пользователи и статистика» → «Отчеты», так и в индивидуальном модуле пользователя. Более детализированные отчеты можно составить через «Конструктор отчетов»: «Пользователи и статистика» → «Управление отчетами» → «Конструктор отчетов».

Управление отчетами **Конструктор отчетов** Службы Настройки Журнал

Сохранить 05.08.2026 - 05.08.2026 Сегодня Неделя Месяц Другой период Экспорт

Вид: Детализация HTTP

Группировка: По назначению

Источник: (любой)

Назначение: (любой)

Интерфейс: (любой)

IP-адрес или домен

Время	Результат	Источник	Назначение	URL	Категория трафика	MIME-тип	Трафик
30.05.2019 14:...	200 OK	192.168.17.11...	87.240.182.22...	https://vk.com/...	Социальные сети	text/html	+750 +955
30.05.2019 14:...	302 Found	192.168.17.11...	87.240.129.13...	https://login.vk...	Социальные сети	text/html	+883 +1.09K
30.05.2019 14:...	200 OK	192.168.17.11...	87.240.182.22...	https://vk.com/...	Социальные сети	text/html	+0 +194
30.05.2019 14:...	200 OK	192.168.17.11...	87.240.182.22...	https://vk.com/...	Социальные сети	text/html	+2.13K +1.13K
30.05.2019 14:...	200 OK	192.168.17.11...	87.240.182.22...	https://vk.com/...	Социальные сети	text/html	+0 +194
30.05.2019 14:...	200 OK	192.168.17.11...	87.240.182.22...	https://vk.com/...	Социальные сети	text/html	+0 +194
30.05.2019 14:...	302 Found	192.168.17.11...	87.240.182.22...	https://vk.com/...	Социальные сети	text/html	+1.30K +1.010
30.05.2019 14:...	200 OK	192.168.17.11...	87.240.182.22...	https://vk.com/...	Социальные сети	text/html	+0 +194
30.05.2019 14:...	200 OK	192.168.17.11...	87.240.129.13...	https://login.vk...	Социальные сети	text/html	+0 +206
30.05.2019 14:...	200 OK	192.168.17.11...	87.240.129.13...	https://login.vk...	Социальные сети	text/html	+0 +206



Можно выбрать разные варианты группировки и вида для этого отчета, указать домен или IP-адрес, время, либо конкретный результат, который нас интересует. Также есть возможность сохранения и выгрузки отчетов в разных форматах и версия для печати.

5. Защита сети и маршрутизация

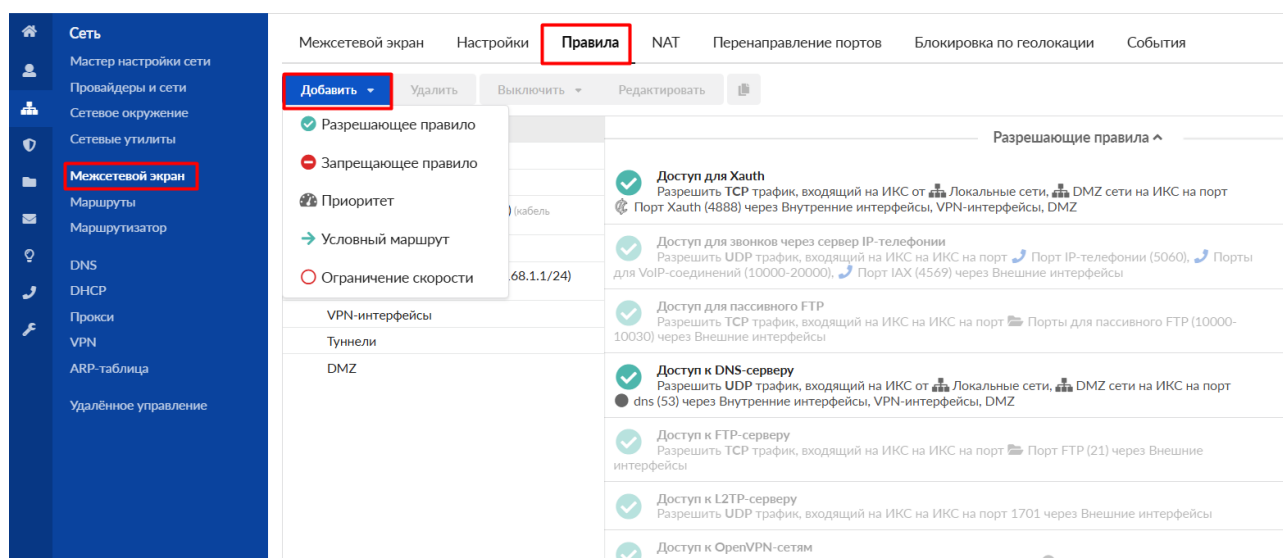
5.1 Межсетевой экран

За защиту сети на ИКС отвечает в первую очередь сам межсетевой экран. Он работает по принципу «Все, что не разрешено - запрещено». Он позволяет контролировать движение трафика на уровне IP-адресов и портов, а также поддерживает NAT. Для корректной работы ИКС, Межсетевой экран должен быть всегда запущен.

На вкладке «Сеть» → «Межсетевой экран» (или «Защита» → «Межсетевой экран») вы можете выставить количество активных соединений, которое будет поддерживаться.

На вкладке «Правила», можно создавать «Разрешающие» и «Запрещающие» правила доступа. По умолчанию в ИКС всегда есть общее запрещающее правило для всего трафика.

Разрешающие правила в ИКС всегда приоритетнее запрещающих и используются для того, чтобы открывать доступ только к определенным службам. При установке в ИКС автоматически создаются разрешающие правила для самых популярных служб. Программа предоставляет возможность управлять этими правилами на свое усмотрение (оставить, удалить, модифицировать).



На вкладке «NAT», можно создать правила, чтобы преобразовывать IP-адреса транзитных пакетов. Правила NAT применяются сверху вниз в том порядке, в котором они расположены на вкладке. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Таким образом, чем выше правило в списке, тем оно приоритетнее.

Редактирование правила NAT

Название *
Новое правило NAT

Протокол (любой) Интерфейс (любой)

Источник Новая OpenVPN-сеть (10.8.0.0/24) Порт источника (любой)

Назначение Локальная сеть (192.168.1.1/24) Порт назначения (любой)

Действие:
☒ Преобразовывать в ☐ Не преобразовывать

Адрес *
192.168.1.1

☐ Статический порт

Время действия
(всегда)

Сохранить Отмена

На вкладке «**Перенаправление портов**», вы можете настроить доступ снаружи к оборудованию внутри вашей сети. Стоит обратить внимание на то, что Перенаправление портов не является безопасным инструментом для предоставления Удаленного доступа к Локальной сети, если вы не указываете конкретный Источник. И если есть возможность, действовать через настройку безопасного удаленного подключения каким-нибудь из типов VPN (в ИКС есть 5 вариантов, которые можно настроить).

Сеть

Мастер настройки сети

Провайдеры и сети

Сетевое окружение

Сетевые утилиты

Межсетевой экран

Маршруты

Маршрутизатор

DNS

DHCP

Межсетевой экран

Настройки

Правила

NAT

Перенаправление портов

Блокировка по геолокации

Добавить

Удалить

Выключить

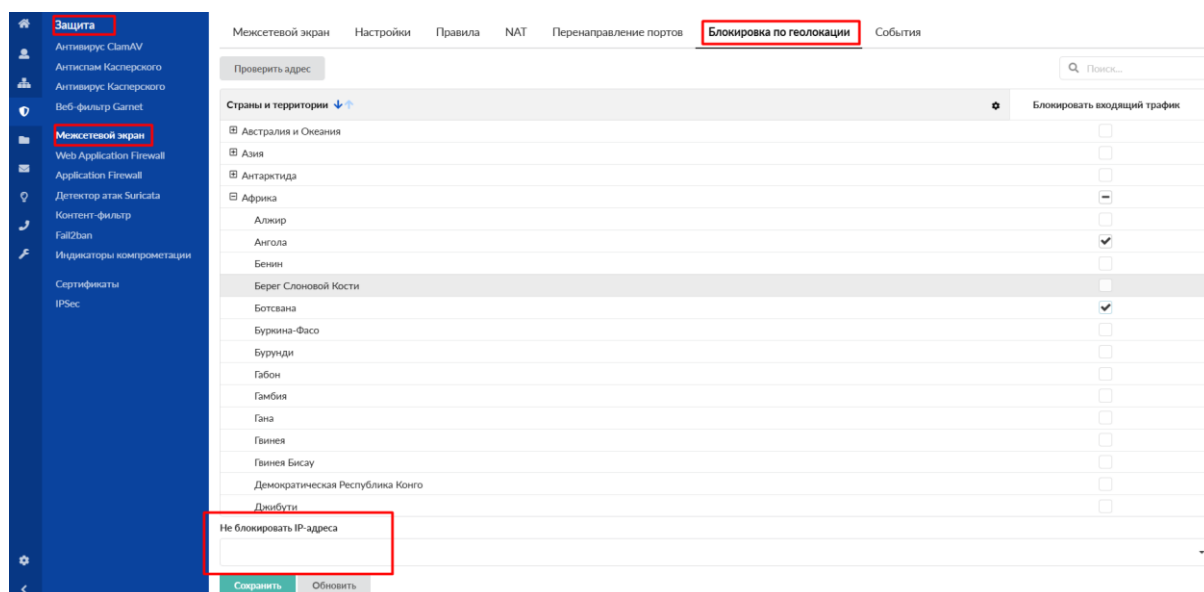
Редактировать

Новое перенаправление

Перенаправить TCP трафик, идущий на порт Порт SMTP (25), на адрес 192.168.1.5 на порт 505

Связано с разрешающими правилами: ☒ Разрешающее правило для перенаправления портов Новое перенаправление 1 ☒ Разрешающее правило для перенаправления портов Новое перенаправление 2

В ИКС есть возможность использовать блокировку по геолокации (вкладка «Блокировка по геолокации». Если мы хотим заблокировать весь входящий трафик от какой-либо страны, достаточно поставить напротив нее флаг в соответствующем меню. Если какие-то адреса нам требуется исключить из блокировки, мы можем это сделать, добавив их в исключения.

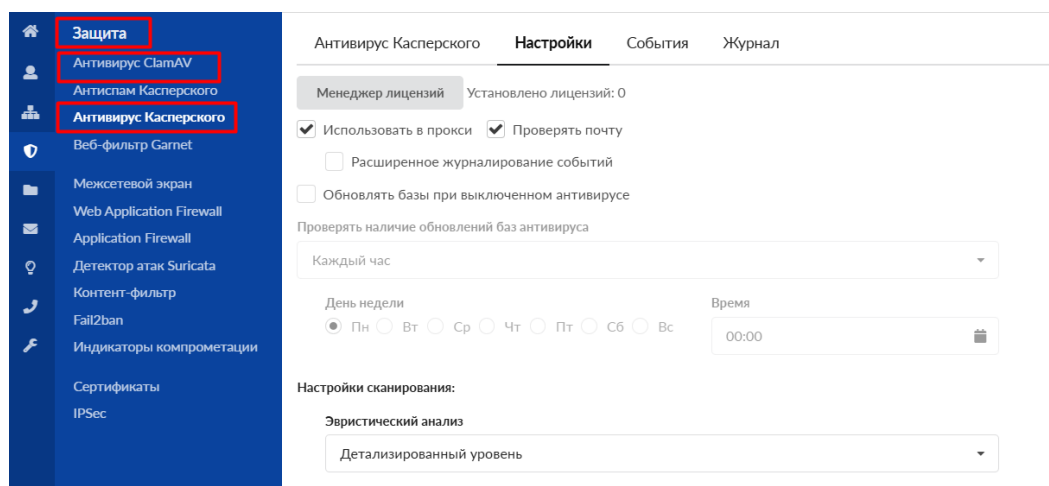


5.2 Поточные антивирусы ClamAV и Касперский

В ИКС версии NGFW есть возможность использовать потоковые антивирусы. Поточный антивирус проверяет трафик, проходящий через прокси-сервер ИКС, а также может проверить почту, если она расположена на ИКС, либо если настроен Почтовый домен с перенаправлением.

Для того, чтобы антивирус проверял трафик, на ИКС должна быть настроена **полная** расшифровка трафика с подменой сертификата.

В ИКС версии NGFW представлено 2 варианта потоковых антивирусов. Бесплатное решение - антивирус ClamAV и платное решение Антивирус Касперского. Антивирус Касперского можно протестировать в течение 30 дней, запросив ключ через менеджера.



5.3 Детектор атак Suricata

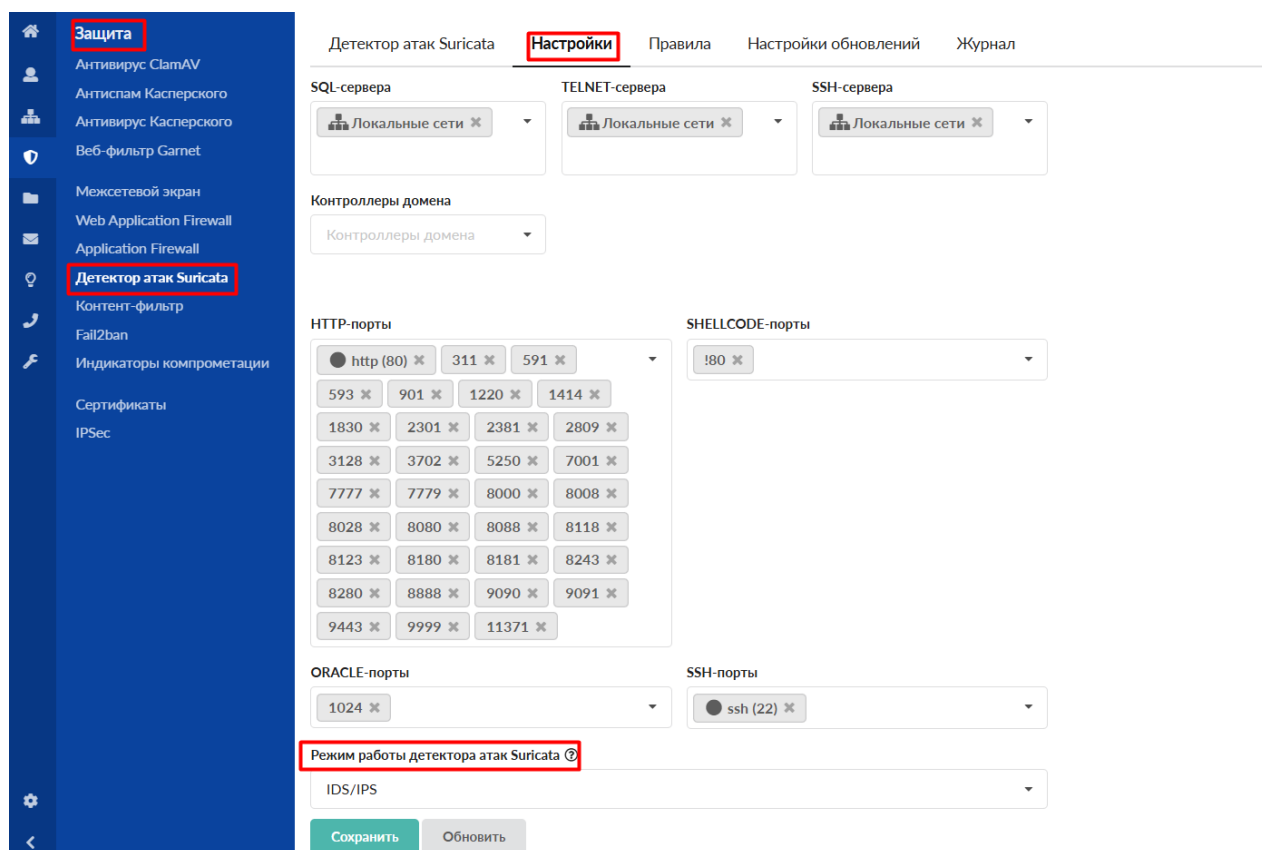
Детектор атак Suricata - это система обнаружения (IDS) и предотвращения (IPS) вторжений. Занимается анализом и блокировкой сетевого трафика.

В ИКС есть 5 наборов правил, которые можно настроить и использовать для защиты сети:

- правила с сайта snort.org;
- правила Kaspersky Suricata Rules Feed;
- правила НКЦКИ;
- правила Positive Technologies Open Ruleset;
- правила Emerging Threats.

Набор правил Kaspersky Suricata Rules Feed лицензируется отдельно. Доступен с первого дня тестирования.

Для настройки Детектора атак Suricata, откройте «Защита» → «Детектор атак Suricata» → «Настройки».



На этой вкладке можно указать внутренние и внешние сети, диапазоны адресов различных серверов, а также используемые порты. Всем этим переменным присвоены значения по умолчанию, с которыми детектор атак может корректно запускаться.

Для ячеек в блоках «сети» и «сервера» допустимыми являются следующие значения: доменное имя (host.ru); IP-адрес (192.168.1.1); IP-адрес/префикс (192.168.1.1/24); IP-адрес: маска (192.168.1.1:255.255.255.0); диапазон IP-адресов (192.168.1.1 - 192.168.1.254);

пользователь; группа; локальная, внутренняя сеть, VPN, OpenVPN, Wi-Fi-сети; другие объекты, которыми оперирует ИКС.

Для ячеек в блоке «**порты**» допустимыми являются следующие значения: номер порта (25, 110); диапазон портов (1000-2000); порты, заведенные на ИКС. Для ячейки «**SHELLCODE-порты**» также допустимо исключение портов (например, !80).

Выбор режима работы детектора атак Suricata:

- Для работы детектора атак в режиме **IPS** используется фреймворк Netmap. Он позволяет работать с сетевыми картами в двух **режимах**:
 - Режим эмулирования.
 - Нативный режим.
- Нативный режим является предпочтительным и возможен при условии поддержки его сетевыми адаптерами. Данный режим позволяет обрабатывать трафик с минимальными потерями в скорости. Он включается автоматически, если в поле «Интерфейсы» в настройках детектора атак указаны исключительно адаптеры из следующего списка: cxgbe, em, igb, lem, ixgbe, ixl, re, vtnet.
- Если в поле «Интерфейсы» указан хотя бы один интерфейс не из этого списка, Netmap будет работать в режиме эмулирования, основным недостатком которого является потеря скорости обработки пакетов и вероятное значительное уменьшение скорости интернет-канала.
- При использовании режима **IDS** Детектор атак также может обрабатывать трафик с высокой скоростью на сетевых картах, которые не поддерживают нативный режим Netmap. Однако при использовании данного режима отсутствует возможность блокировки трафика Детектором атак.

Чтобы изменения вступили в силу, нажмите «**Сохранить**».

Внимание! Suricata работает с PPPoE-провайдерами только в режиме IDS.

Настройка правил

Во вкладке Правила напротив каждого файла показано, какое количество правил в нем содержится.

Для **просмотра правил** и выбора действия нажмите на имя файла — откроется новое диалоговое окно с таблицей. В таблице расположены следующие поля:

- ID правила — номер правила;
- приоритет — значение угрозы;
- предупреждение — описание производимой атаки;
- классификация — класс атаки;
- действие — определяет, что необходимо сделать при обнаружении данной атаки (alert — записать в собственный лог обнаружение и пропустить, drop — уничтожить пакет,

pass — пропустить, reject — уничтожить пакет и уведомить отправителя о данном событии);

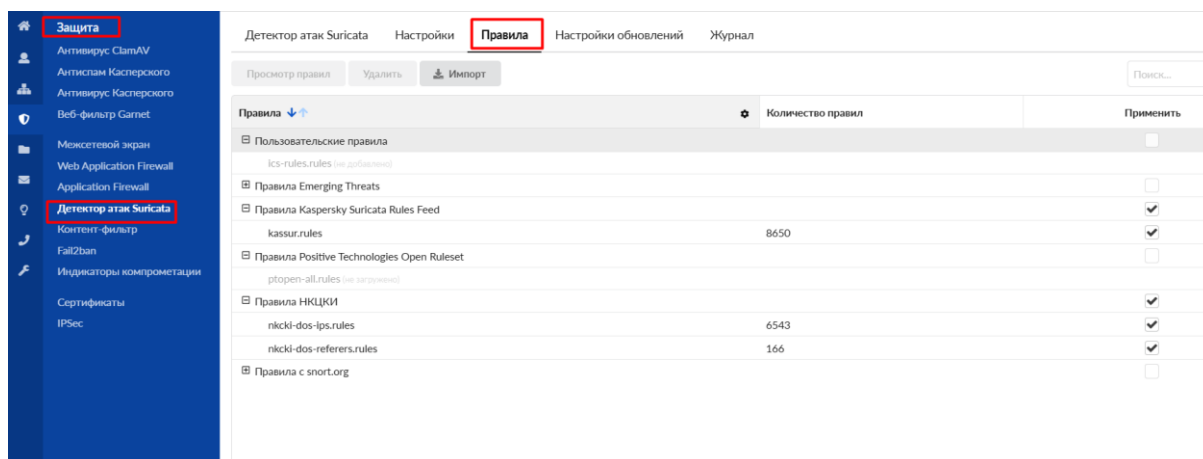
- направление — определяет источник и назначение действия правила;
- включение/выключение соответствующего правила.

На вкладке предусмотрена возможность **импортировать правила** работы Детектора атак Suricata. Выберите нужный набор правил и нажмите кнопку **«Импорт»**.

Правила для импорта можно предварительно создать и настроить в соответствии с вашими запросами.

В журнале можно отслеживать события и формировать по ним разные отчеты. Действия имеют следующие значения:

- **Pass** — Suricata прекратит сканирование пакета и разрешит его, не создавая предупреждения.
- **Drop** — при работе в режиме IPS Suricata немедленно прекратит обработку пакета и сгенерирует предупреждение. Если соединение, сгенерировавшее пакет, использует TCP, время ожидания истечет.
- **Reject** — когда Suricata работает в режиме IPS, будет отправлен пакет сброса TCP, и Suricata отбросит соответствующий пакет.
- **Alert** — Suricata создаст предупреждение и зарегистрирует его для дальнейшего анализа.



5.4 Fail2ban

Fail2ban - это защита от брутфорс атак сервисов, расположенных на ИКС. Он сканирует лог-файлы и блокирует IP-адреса, которые ведут себя подозрительно (совершают множественные попытки авторизации).

Его можно настроить на вкладке «Защита» → «Fail2ban». Не рекомендуется ставить менее трех неудачных попыток для авторизации.

Флаги **«Защитить почтовый сервер»**, **«Защитить веб-почту»**, **«Защитить сервер**

телефонии», «Защитить VPN-сервер», «SSH», «FTP», «GUI» позволяют Fail2ban анализировать логи авторизации в соответствующих модулях.

Если Fail2ban заблокирует IP-адрес по одному из сервисов, то доступ с IP-адреса к другим сервисам также будет заблокирован.

На вкладке «Белые списки» можно указать IP-адрес, который не будет блокироваться независимо от неудачных попыток авторизации.

Fail2ban **Настройки** Белый список Заблокированные IP-адреса Журнал

Защищать

☒ Почтовый сервер ☒ Web-почту ☒ Сервер телефонии ☒ VPN-сервер

☐ SSH ☒ FTP ☐ GUI

Количество неудачных попыток авторизаций* 3

Интервал неудачных попыток авторизаций* 10 мин.

☐ Блокировать навсегда

☒ Блокировать на

Время* 10 мин.

☐ Увеличивать время бана

Прибавить к времени бана случайное время из диапазона от 0 до 1 мин.

Фактор роста 1

Список множителей 1 2 4 8 16 32 64

☐ Не разделять попытки авторизации по службам

5.5 Web Application Firewall

Модуль **Web Application Firewall** (WAF) отслеживает и блокирует весь HTTP/HTTPS-трафик, входящий и исходящий от установленных веб-приложений на ИКС или в локальной сети.

При помощи анализа HTTP/HTTPS-трафика WAF может предотвращать атаки, которые основаны на недостатках защиты веб-приложений (SQL-инъекции, межсайтовый скриптинг (XSS), включение файлов, неправильная настройка безопасности).

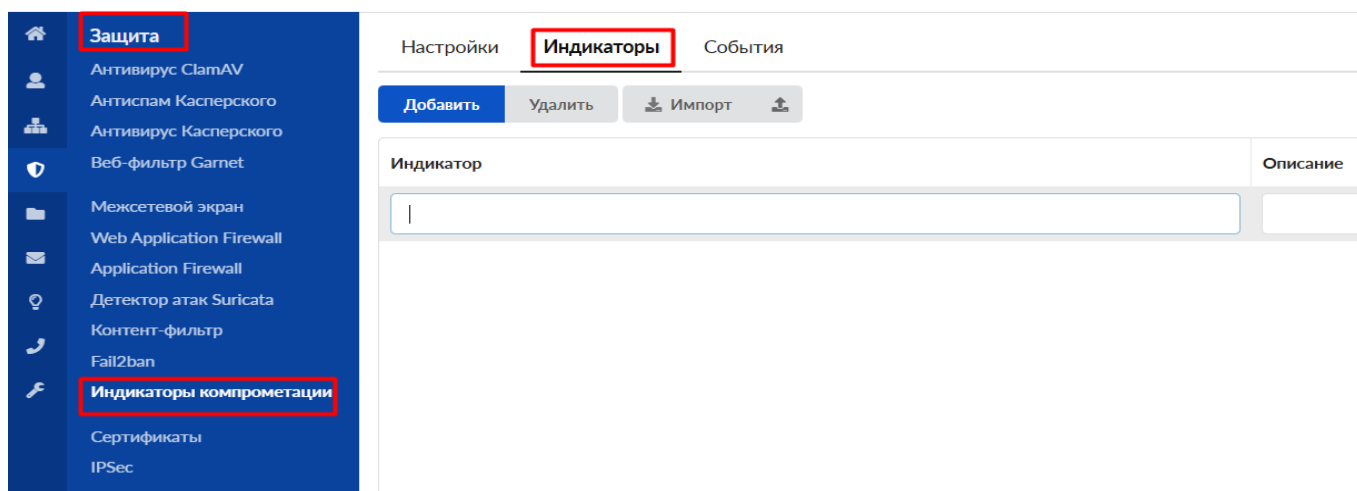
Данный модуль есть в версии **ИКС NGFW**. При создании веб-ресурса или виртуального хоста с перенаправлением, можно установить флаг «Использовать Web Application Firewall».

5.6 Индикаторы компрометации

Индикаторы компрометации предназначены для защиты от загрузки вредоносных программ через прокси-сервер.

Можно их добавить на вкладке «Защита» → «Индикаторы компрометации» → «Индикаторы».

Если файл скачивается с ресурса HTTPS, то необходимо настроить в прокси расшифровку трафика HTTPS.



The screenshot shows the 'Защита' (Protection) menu on the left, with 'Индикаторы компрометации' (Compromise Indicators) highlighted. The main panel displays the 'Индикаторы' (Indicators) tab, which includes a table with columns 'Индикатор' (Indicator) and 'Описание' (Description). The table is currently empty.

Индикатор	Описание
-----------	----------

6. Настройка удаленных подключений

В ИКС есть возможность настроить разные типы удаленных подключений. Можно настроить как site-to-site, так и client-to-site.

Для подключения пользователей предусмотрены: PPTP/L2TP, L2TP IPSec, SSTP, OpenVPN и Wireguard.

Для всех, кроме Wireguard предусмотрена двухфакторная аутентификация. Проверка логина и пароля и подтверждение в Telegram- бот или Max-бот.

Для OpenVPN также возможна настройка TOTP, как второй фактор.

Если требуется объединить офисы, есть возможность настроить IPsec, GRE, IPsec, OpenVPN и Wireguard туннели. С другой стороны может находиться как ИКС, так и любой маршрутизатор. Главное, чтобы шифрование совпадало.

Далее рассмотрим самые популярные виды удаленных подключения пользователей.

6.1 OpenVPN

Для добавления сети OpenVPN необходимо создать сертификаты для сети. Для этого на вкладке «Защита» → «Сертификаты» создаем Корневой и Конечный сертификаты:

Данные сертификата VPN корневой

Общее
Название: VPN корневой
Код страны: RU - Russian Federation
Имя или адрес хоста: test.ru

Настройки
Тип сертификата: CA
Алгоритм: SHA 256
Тип шифрования: RSA
Создан: 16.07.2020
Действует до: 16.07.2021
Длина ключа: 2048 бит

Использование ключа
Использование ключа: Certificate Sign
CRL Sign

Добавить в доверенные сертификаты

Ок

При создании конечного сертификата на вкладке «Использование ключа» в поле «Шаблон» выберите значение «VPN-сервер».

Добавление сертификата

Общее Настройки **Использование ключа** Netscape расширение

Шаблон
VPN-сервер

Использование ключа

- ☐ CRL sign
- ☐ Certificate Sign
- ☐ Non Repudiation
- ☒ Digital Signature
- ☒ Key Encipherment

Расширенное использование ключа

- ☐ E-mail Protection
- ☐ TLS Web Client Authentication
- ☐ Code Signing
- ☒ TLS Web Server Authentication
- ☐ Time Stamping

Добавить Отмена

Переходим в меню «Сеть» → «Провайдеры и сети» → «Добавить» → «OpenVPN-сеть».

Выбираем в настройках созданные сертификаты

Добавление OpenVPN-сети

Основные настройки **Шифрование и сертификаты**

Алгоритм шифрования
AES-256-GCM

Алгоритм хеширования
SHA256

☒ Проверять CN сервера ?

☐ Включить сжатие LZO

☒ Использовать дополнительную защиту TLS

☒ TLS Auth ☐ TLS Crypt v2

Корневой сертификат *
Open

Сертификат сервера *
Open_end

Добавить Отмена

Если хотим использовать дополнительные факторы, то включаем их в настройках и прописываем сети, маршруты до которых будут передаваться.

- ☒ Включить проверку логина и пароля клиента
- ☒ Использовать двухфакторную аутентификацию
 - ☒ Использовать Telegram-бот
 - ☐ Использовать MAX-бот
 - ☐ Использовать TOTP

- ☒ Разрешить трафик между клиентами
- ☐ Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей

LAN (192.168.17.234/24) ✕

Передать клиентам DNS сервера

Передать клиентам DNS сервера

Для использования ботов или TOTP их необходимо дополнительно настроить.

На вкладке «Сеть» → «VPN» → «Пользователи» мы можем выбрать пользователей, которые смогут удаленно подключаться. После проставления флагов, необходимо выгрузить сертификат для подключения. Сделать это можно либо в индивидуальном модуле пользователя, либо через «Выгрузку сертификатов», выбрав опцию у сети OpenVPN.

Сеть

Мастер настройки сети

Провайдеры и сети

Сетевое окружение

Сетевые утилиты

Межсетевой экран

Маршруты

Маршрутизатор

DNS

DHCP

Прокси

VPN

ARP-таблица

Удаленное управление

Провайдеры и сети

Логические интерфейсы

Внешние устройства

Балансировка трафика

Монитор провайдеров

Добавить

Удалить

Выключить

Редактировать

Мастер настройки сети

Новый провайдер (192.168.1.1/24)
Провайдер

LAN (192.168.17.234/24)
Локальная сеть

OpenVPN-сеть (10.8.0.0/24)
OpenVPN-сеть

IP-адрес/префикс: 10.8.0.0/24

Протокол: udp

Порт сервера: 1194

Корневой сертификат: Open

Сертификат сервера: Open_end

Проверка логина и пароля клиента: включена

Двухфакторная аутентификация: включена

Подробнее...

Управление доступом

Выгрузить сертификаты

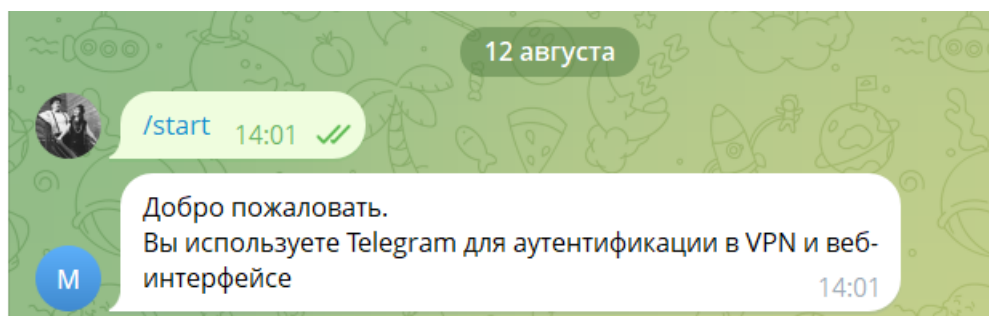
Настройка двухфакторной авторизации через Telegram

В первую очередь необходимо создать бота. Найдите в мессенджере пользователя @BotFather, нажмите «Start» и действуйте далее согласно инструкции.

На ИКС переходим на вкладку: «Обслуживание» → «Журнал и уведомления» → «Telegram-бот» и указываем Токен, полученный в результате создания бота.

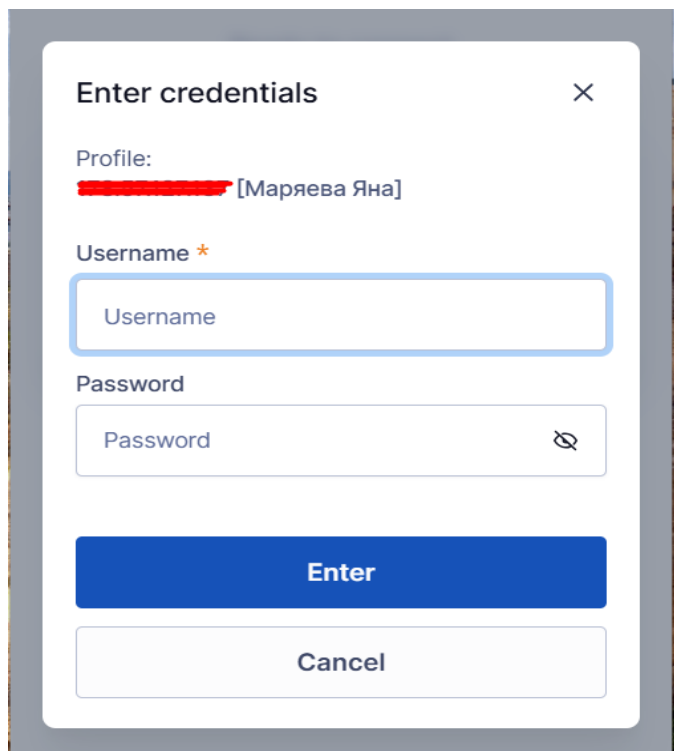
На вкладке «Сеть» → «VPN» → «Пользователи» выделяем строку с нужным пользователем и нажимаем кнопку «Двухфакторная аутентификация» → «Скопировать ссылку».

Пользователь должен перейти по ссылке, запустить бота и нажать Start.



Из индивидуального модуля пользователя выгрузите конфигурационный файл и добавьте его для подключения по **OpenVPN** в папку **config** на конечном хосте.

При подключении у пользователя сначала будет запрошен **Логин** и **Пароль**, а после подтверждения, будет приходить оповещение в Telegram. Для подключения нажмите «Да».



Enter credentials

Profile:
[Маряева Яна]

Username *

Username

Password

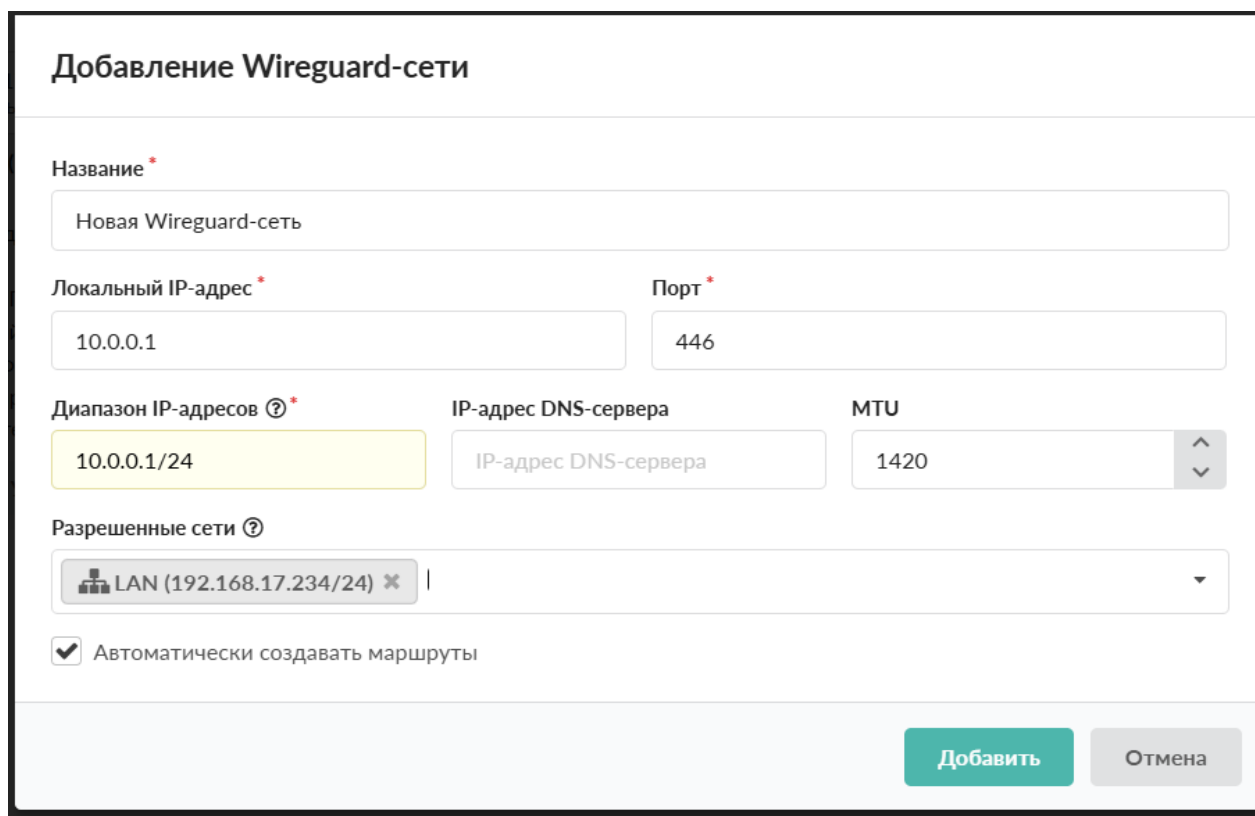
Password

Enter

Cancel

6.2 Wireguard

Добавить Wireguard можно на вкладке «Сеть» → «Провайдеры и сети» → «Добавить Wireguard».



Добавление Wireguard-сети

Название *

Новая Wireguard-сеть

Локальный IP-адрес *

10.0.0.1

Порт *

446

Диапазон IP-адресов ? *

10.0.0.1/24

IP-адрес DNS-сервера

IP-адрес DNS-сервера

MTU

1420

Разрешенные сети ?

LAN (192.168.17.234/24) x

☒ Автоматически создавать маршруты

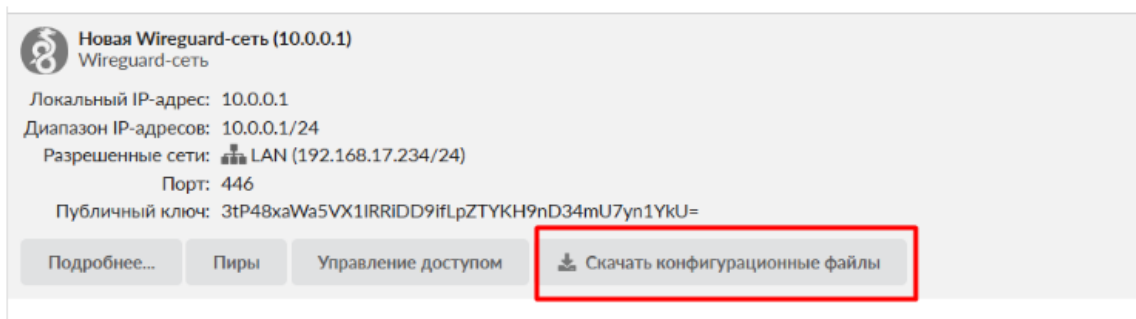
Добавить

Отмена



Указываем разрешенные сети, если требуется DNS-сервера.

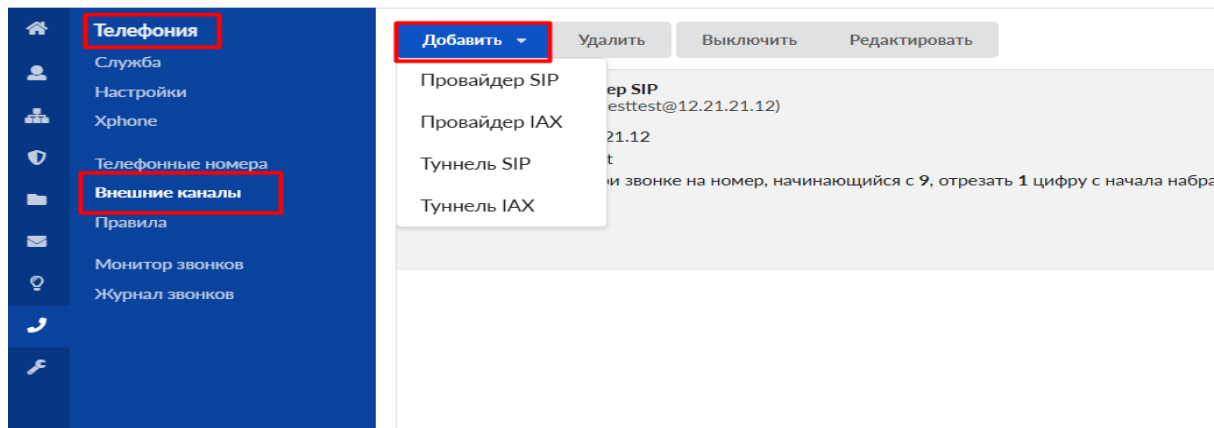
После этого выставляем права на подключения пользователям на вкладке «Сеть» → «VPN» → «Пользователи». Скачиваем конфигурационный файл для подключения.



7. Модуль «Телефония»

В ИКС версии NGFW можно настроить модуль IP-телефонии.

На вкладке «Телефония» → «Внешние каналы» можно добавить SIP-провайдеров двух типов.



Добавляем провайдера и указываем данные, которые нам предоставили для подключения.

Редактирование провайдера SIP

Название *

Новый провайдер SIP

Максимальное число каналов

100

Адрес сервера *

12.21.21.12

Порт *

5060

Номер

Логин

testtest

Пароль

.....

☒ Автоматически создавать правило, используя префикс:

9

Режим DTMF

auto

Опция insecure

invite

Опция canreinvite

yes

Опция direct_media

no

Тип подключения

Без шифрования (UDP)

Для добавления Телефонного номера, перейдите на вкладку «Телефонные номера» → «Добавить». Указываем номер, который хотим назначить пользователю, создаем надежный пароль, выбираем пользователя и если требуется, разрешение на подключение извне.

Номер

111

Пароль

(без пароля)

Описание (CallerID Name)

Время ожидания

(по умолчанию)

сек.

Максимальное число каналов

10

Пользователь

Администратор

☒ Разрешать подключаться извне

Доступ

☐ Разрешить протокол IAX

☒ SIP-клиент

☐ Xphone

Тип подключения

Без шифрования (UDP)

☐ Поддерживать подключение

При создании правил для звонков, обращаем внимание на то, что все правила отрабатываются сверху вниз. Можно добавить голосовое меню, переадресации, выбрать провайдера, через которого будет совершаться вызов, настроить разные варианты перенаправления и целые наборы правил.

На ИКС есть возможность записи телефонных звонков и их скачивания, если это требуется.

Правила

Перенаправления

Очереди

Добавить

Удалить

Выключить

Редактировать

▶ Воспроизвести

🔍 Поиск...

Наборы правил

Входящие звонки

При звонке с 79806634974, повесить трубку

→ При звонке с провайдера Новый провайдер SIP , перенаправить на набор правил Техподдержка

⌚ Ждать набора номера 15 сек.

→ При звонке на 1 , перенаправить на набор правил Менеджеры

→ Позвонить на номер Телефонные номера

📞 При звонке на все известные номера принять вызов (автоматическое)

Исходящие и внутренние звонки

📞 При звонке на все известные номера принять вызов (автоматическое)

🌐 При звонке на номер, начинающийся с 9, направить звонок через внешний канал Новый провайдер SIP , отрезать 1 цифру с начала набранного номера (автоматическое)

bnbvn

Менеджеры

→ При звонке с номера, начинающегося с 8 , позвонить на номер 222

Техподдержка

→ Позвонить на номера 123, 111, 234

8. Почтовый сервер

На ИКС версии NGFW можно настроить полноценный почтовый сервер.

На вкладке «Почта» → «Настройки» можно выбрать максимальный размер письма, какое количество писем может отправлять с одного IP-адреса в минуту, диск для хранения почты, настроить отправку через внешний SMTP, настроить ЧБ списки и 3 варианта Антиспама.

Есть возможность использовать встроенные антиспамы: Антиспам **SpamAssassin** и Антиспам **Rspamd**.

Через менеджера можно заказать тестовый ключ для Антиспама Касперского. Он лицензируется отдельно.

Для настройки почтового сервера необходимо создать некоторые записи на хостинге. Ниже пример того, что требуется создать:

A-запись : mail.domain.com 1.1.1.1

MX-запись: 10 mail.domain.com (10 приоритет)

SPF: TXT domain.com v=spf1 mx a ~all

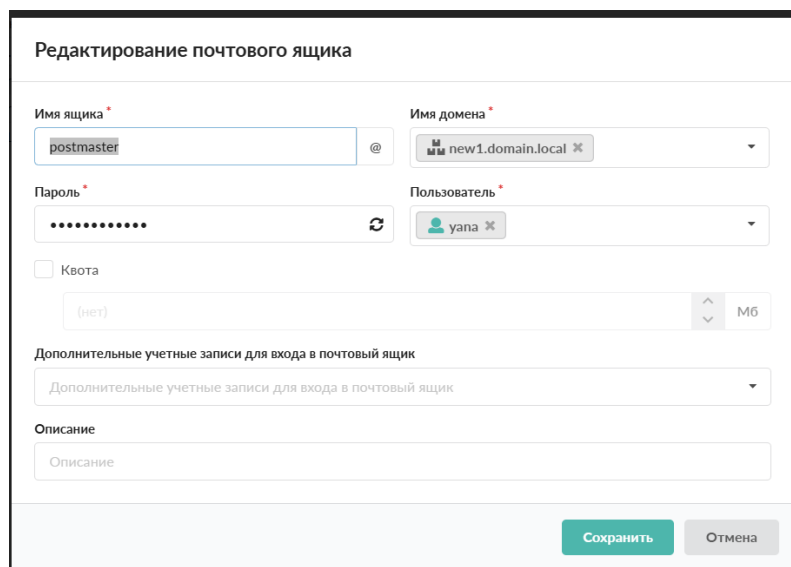
DKIM: default._domainkey. domain.com v=DKIM1; k=rsa; p=ваш ключ. (На ИКС его можно взять при редактировании домена)

PTR: 1.1.1.1 mail.domain.com (Создается у хостинга)

После добавления записей, почта сможет приходить на ИКС.

8.1 Создание почтового домена и почтовых ящиков

На вкладке «Почта» → «Домены и ящики» мы можем добавить почтовый домен и далее в нем создавать Почтовые ящики. При создании Почтового ящика, можно выбрать пользователя, которому он будет принадлежать, пароль, выставить квоту и Дополнительную учетную запись для входа в почтовый ящик, если это требуется.



Редктирование почтового ящика

Имя ящика * @

Пароль *

Пользователь *

☐ Квота МБ

Дополнительные учетные записи для входа в почтовый ящик

Описание



8.2 Остальные настройки

На ИКС можно настроить различные почтовые фильтры, рассылки и сборщик почты. Все движение писем отслеживается на вкладке «Статистика и очередь».

Почтовые фильтры позволяют создавать различные правила для пересылки писем, которые приходят на сервер. Это может быть отправка копии, удаление, перемещение письма.

Сборщик почты позволяет забирать письма со стороннего почтового сервера. Он также может определить автоматически получателя и разложить по ящикам.

8.3 Настройка DNS-записей на ИКС

Если NS-сервером будет прописан белый адрес ИКС, то DNS-зону можно настроить на нем. Для этого выполните следующие действия: в меню «Сеть» → «DNS» → «Зоны» создайте новую зону, соответствующую имени вашего домена.

Добавление DNS-зоны

Настройки

Доступ

Имя зоны *

my.zone.

Область *

Default_view x |

DNS-сервер *

127.0.0.1.

.my.zone.

E-mail администратора *

admin@host.ru

TTL *

38400

сек.

Обновление

10800

сек.

Повторение попытки *

3600

сек.

Устаревание *

604800

сек.

Отрицательное TTL *

3600

сек.

Добавить

Отмена

В созданной зоне автоматически создается NS-запись для имени хоста, которое указано в поле «DNS-сервер».

Чтобы указать зоне IP-адрес хоста ns1.myzone.loc, добавьте A-запись для данного хоста. В данном случае 192.168.25.186 — это внешний адрес ИКС, поскольку он сам является DNS-сервером.



Добавление А-записи

Имя хоста *

ns1

.my.zone.

IP-адрес *

192.168.25.186

Добавить

Отмена

Для указания почтового сервера добавьте MX-запись.

Добавление MX-записи

Почтовый сервер

@

.my.zone.

Имя хоста *

postserver

.my.zone.

Приоритет *

10

Добавить

Отмена

Создайте А-запись для связанного с MX-записью имени хоста. В качестве адреса хоста снова выступает внешний адрес ИКС.

Добавление А-записи

Имя хоста *

mail

.my.zone.

IP-адрес *

192.168.25.186

Добавить

Отмена

Для соответствия имени хоста и его IP-адреса также желательно добавить **обратную DNS-зону**. После создания зоны обратные А-записи для созданных хостов прямой зоны добавятся автоматически.



Добавление обратной DNS-зоны

Настройки

Доступ

Адрес зоны *

25.168.192.

in-addr.arpa.

Область *

Default_view ✕

DNS-сервер *

127.0.0.1.

E-mail администратора *

admin@host.ru

TTL *

38400



сек.

Обновление

10800



сек.

Повторение попытки *

3600



сек.

Устаревание *

604800



сек.

Отрицательное TTL *

3600



сек.

☐ Автоматически создавать PTR-записи для A-записей

Добавить

Отмена

Отправьте запрос вашему интернет-провайдеру для создания **PTR-записи**, связанной с внешним адресом ИКС. Укажите в качестве первичного DNS-сервера для домена **myzone.com** в настройках DNS-сервера хостера вашего домена.



9. Обслуживание, мониторинг, журнал и уведомления

На вкладке «Обслуживание» находится множество полезных опций, например, Резервные копии. Их можно создавать по расписанию в разных вариантах: Настройки, Статистика, Почтовые ящики, Базы данных веб-ресурсов.

Обслуживание

Система

Все службы

Резервные копии

Управление питанием

Жесткие диски

Время и дата

Настройки интерфейса

Мониторинг

Кластер

Планировщик

Журнал и уведомления

Техподдержка

Обновления

О программе 13.3.0.260729

Резервные копии Шаблоны Настройки

Добавить Удалить Загрузить Загрузить из хранилища файлов

my.gate.com-2024.12.11-11.06.47-s-11.4.0.2409241628-backup
Резервная копия (настройки)

my.gate.com-2024.12.16-19.18.29-s-11.4.1.2410171349-backup
Резервная копия (настройки)

my.gate.com-2024.12.23-21.34.37-s-12.0.0.2412161125-backup
Резервная копия (настройки)

my.gate.com-2024.12.24-09.53.39-stm-12.0.1.2412231632-backup
Резервная копия (настройки, статистика, почта)

my.gate.com-2025.12.10-15.06.01-s-12.0.1.2412231632-backup
Резервная копия (настройки)

my.gate.com-2026.03.04-17.35.19-s-13.0.0.2512081417-backup
Резервная копия (настройки)

my.gate.com-2026.04.02-13.01.41-s-13.1.0.2603031813-backup
Резервная копия (настройки)

my.gate.com-2026.05.25-11.07.47-s-13.1.0.2603031813-backup
Резервная копия (настройки)

my.gate.com-2026.07.28-16.21.04-s-13.2.1.2605151506-backup
Резервная копия (настройки)

my.gate.com-2026.07.28-16.21.32-s-13.2.1.2605151506-backup
Резервная копия (настройки)

my.gate.com-2026.07.28-16.22.04-s-13.2.1.2605151506-backup
Резервная копия (настройки)

На вкладке «Мониторинг», можно увидеть состояние системы и основные параметры.

Также здесь находится Zabbix-агент. Можно добавить свой сервер.

Обслуживание

Система

Все службы

Резервные копии

Управление питанием

Жесткие диски

Время и дата

Настройки интерфейса

Мониторинг

Кластер

Планировщик

Журнал и уведомления

Техподдержка

Обновления

О программе 13.3.0.260729

Графики Мониторинг состояния системы Настройки службы Аудит Настройки Zabbix-агента Журнал

Добавить Удалить Редактировать Очистить

Виртуальная память

Загрузка диска ada0

Загрузка дисков

Загрузка процессора

Загрузка системы

Запущенные процессы

Межсетевой экран

Обработанные письма

Оперативная память

Открытые файлы

Пинг до ya.ru (ya.ru)

Температура дисков

Температура системы

Трафик на интерфейсе LAN (vtnet0)

Трафик на интерфейсе Новый провайдер (em0)

Файловые системы

Загрузка процессора за последний час

Проценты

System 5% макс: 8% сред: 4% мин: 3% User 2% макс: 6% сред: 2% мин: 1%

Загрузка процессора за последние 6 часов

Проценты



Обслуживание

- Система
- Все службы
- Резервные копии
- Управление питанием
- Жесткие диски
- Время и дата
- Настройки интерфейса
- Мониторинг
- Кластер
- Планировщик
- Журнал и уведомления**
- Техподдержка
- Обновления
- О программе 13.3.0.240729

Системный журнал **Настройки уведомлений** Уведомления на почту Уведомления на Jabber Telegram-бот MAX-бот

☒ Отправлять уведомления

Посылать уведомление

сразу

Типы уведомлений

☒ Уведомлять о всех событиях

☐ Уведомлять о следующих событиях:

- ☒ События системы
- ☒ События сервисов
- ☒ Ошибки
- ☒ Другие события

Отправить тестовое сообщение

Дублировать syslog сообщения:

Добавить Удалить

Сервер syslog	Порт	Тип логов	Формат
---------------	------	-----------	--------

Здесь находится и модуль «Техподдержка», для удаленного подключения и консультации технических специалистов.

Обслуживание

- Система
- Все службы
- Резервные копии
- Управление питанием
- Жесткие диски
- Время и дата
- Настройки интерфейса
- Мониторинг
- Кластер
- Планировщик
- Журнал и уведомления
- Техподдержка**
- Обновления
- О программе 13.3.0.240729

Техподдержка Журнал

Техподдержка

Подключается к техподдержке по ssh

Подключен к dev-a-real.ru:20103

Выключить

Журнал

Connected 10:36:16

Connecting to dev-a-real.ru:20103...