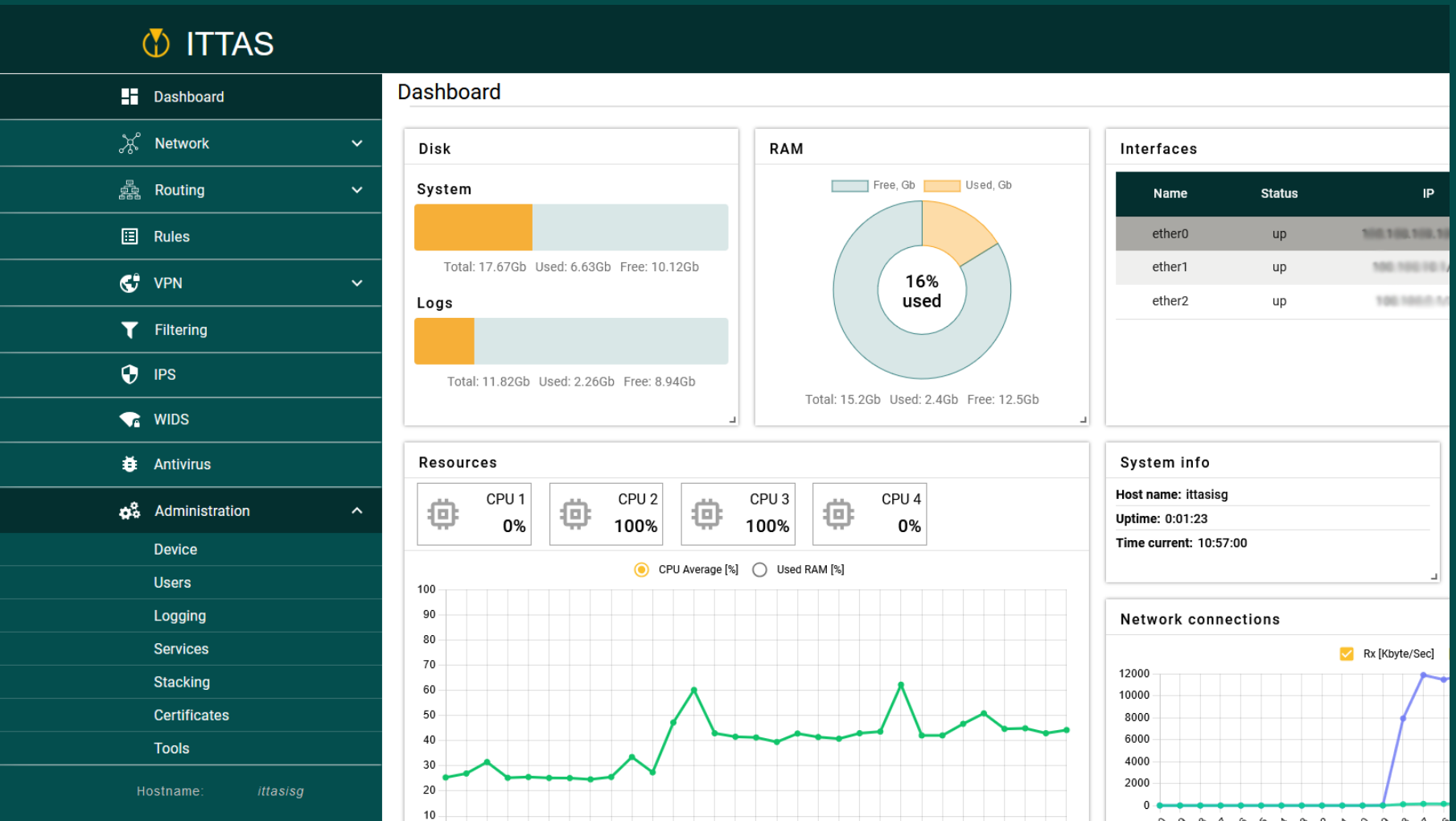
ITTAS

SECURITY GATEWAY

Межсетевой экран нового поколения, обеспечивающий комплексную защиту сетевого периметра. Сочетает в себе функции антивируса, системы обнаружения и предотвращения вторжений (IPS), системы обнаружения сетевых аномалий в беспроводных сетях (WIDS) и контроля приложений для защиты от широкого спектра угроз.

Security Gateway

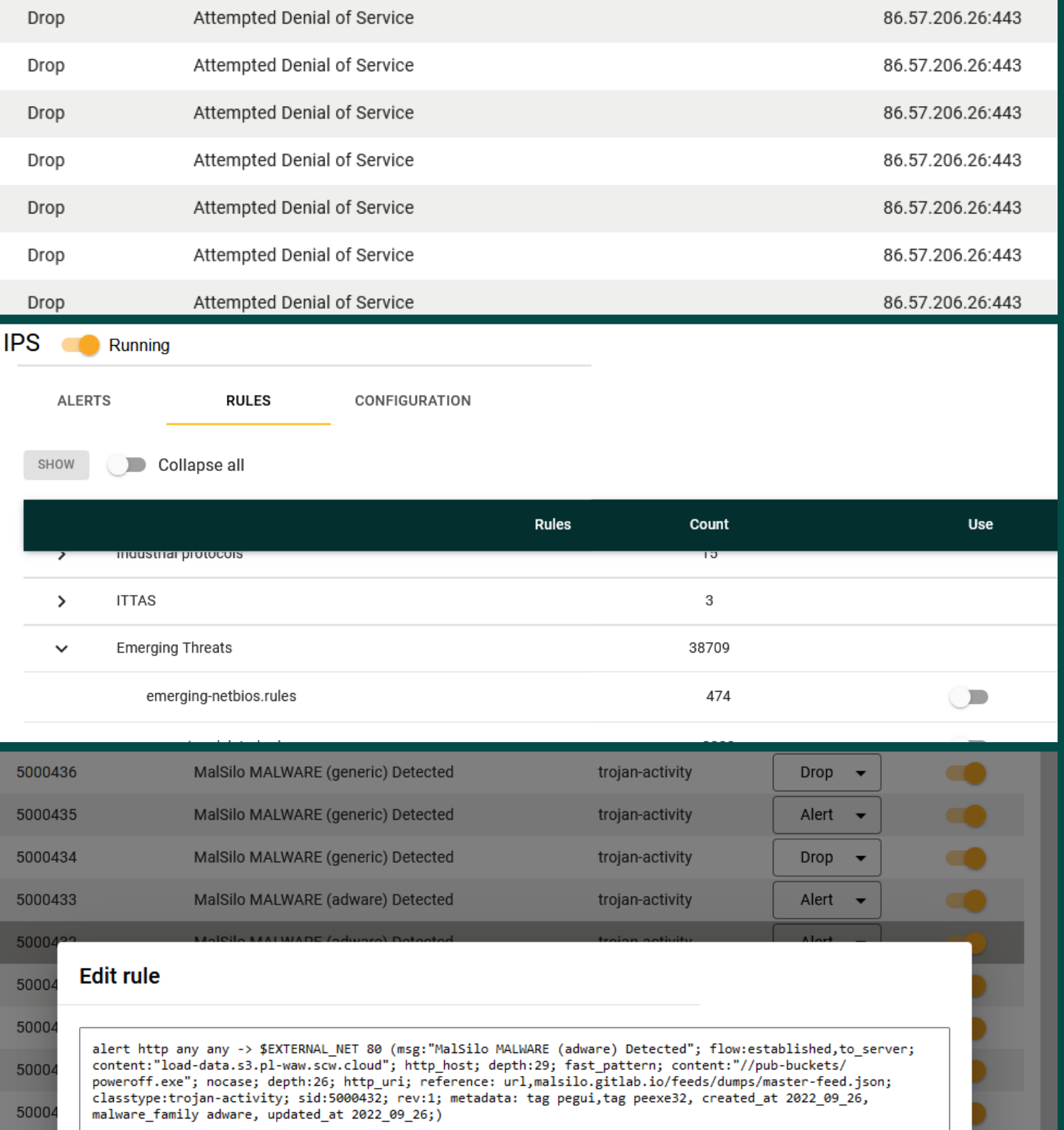
ITTAS (ISG)



ISG — это программное решение, которое можно развернуть в среде виртуализации, а также установить на физический сервер, а затем смонтировать в серверную стойку и использовать в качестве полноценного программно-аппаратного межсетевого экрана.

КЛЮЧЕВЫЕ ФУНКЦИИ

- СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IPS)
- ПОТОКОВЫЙ HTTP(S) АНТИВИРУС
- КОНТРОЛЬ ПРИЛОЖЕНИЙ (DPI)
- HTTP/HTTPS ПРОКСИ-СЕРВЕР, ОБЕСПЕЧИВАЮЩИЙ ПРОЗРАЧНЫЙ И НЕПРОЗРАЧНЫЙ РЕЖИМЫ
- КОНТЕНТНАЯ ФИЛЬТРАЦИЯ
- ИНТЕГРАЦИЯ С ACTIVE DIRECTORY
- МОНИТОРИНГ И ПОДГОТОВКА ОТЧЕТОВ
- ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ В БЕСПРОВОДНЫХ СЕТЯХ (WIDS)
- СТЕКИРОВАНИЕ УСТРОЙСТВ
- ИНТЕГРАЦИЯ СО СРЕДСТВОМ ШИФРОВАНИЯ КАНАЛА ITVPN



СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IPS)

Высокопроизводительная система обнаружения и предотвращения вторжений предлагает обширный функционал для защиты сети от различных угроз. Она включает предустановленную базу периодически обновляемых правил фильтрации трафика, что упрощает настройку и эксплуатацию. Модуль использует гибкую систему создания и активации пользовательских правил, позволяя адаптировать защиту под специфические требования организации. Система также обеспечивает мониторинг в реальном времени, что позволяет оперативно реагировать на потенциальные угрозы и поддерживать высокий уровень безопасности.

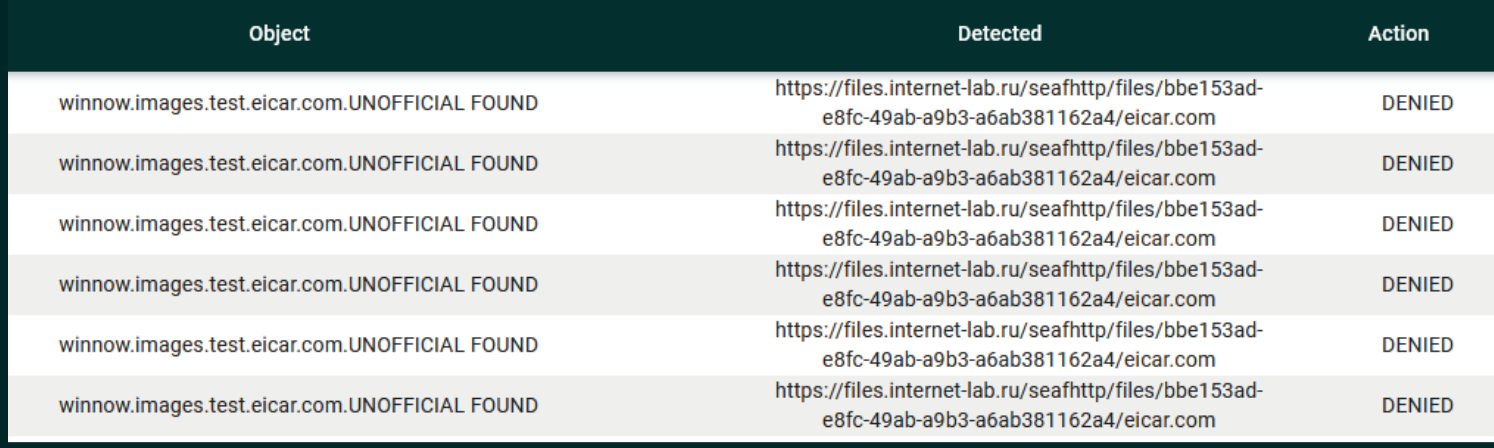
АНТИВИРУС

Функции антивирусной проверки, в том числе файлов, выполняются в рамках проверки веб-трафика, передаваемого посредством как http, так и https протоколов, что достигается за счет возможности подмены сертификата.

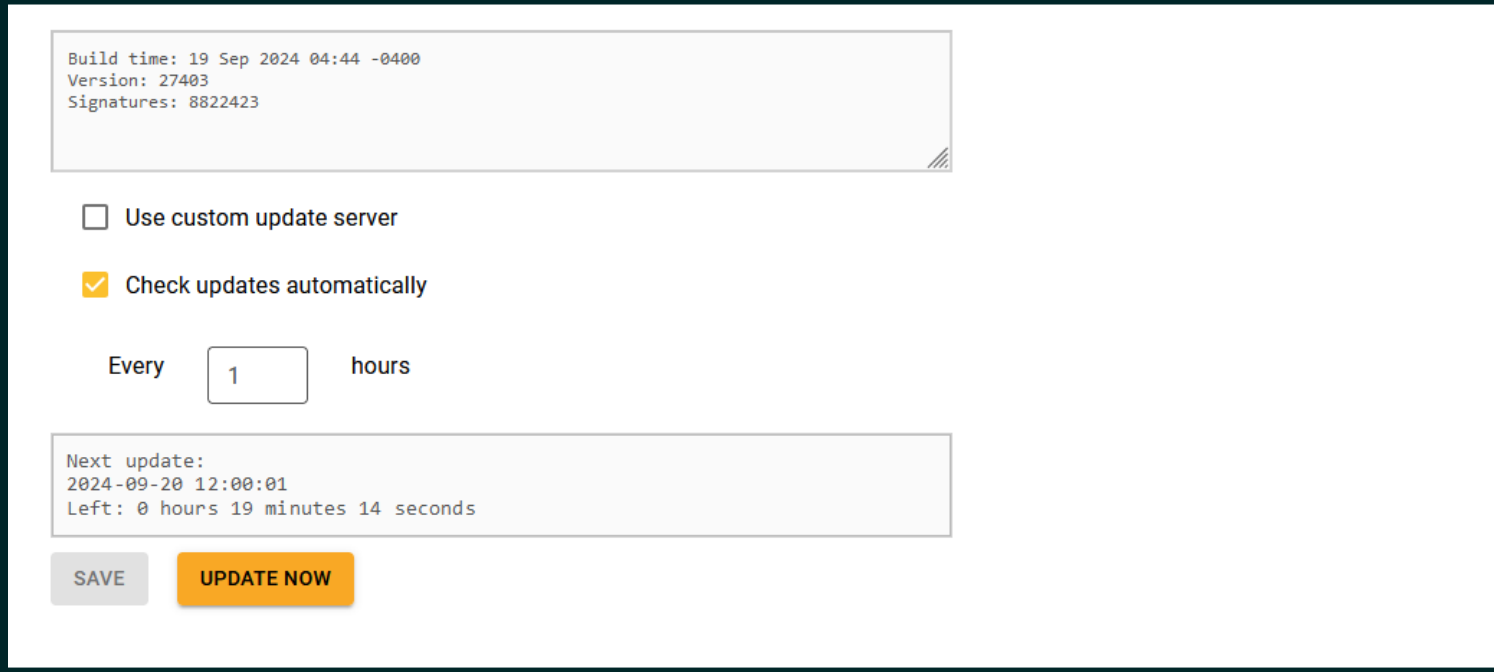
Нами обеспечиваются ежедневные обновления расширенных баз сигнатур.

Более того, ISG реализует возможность подключения собственного сервера обновлений сигнатурных баз антивируса.

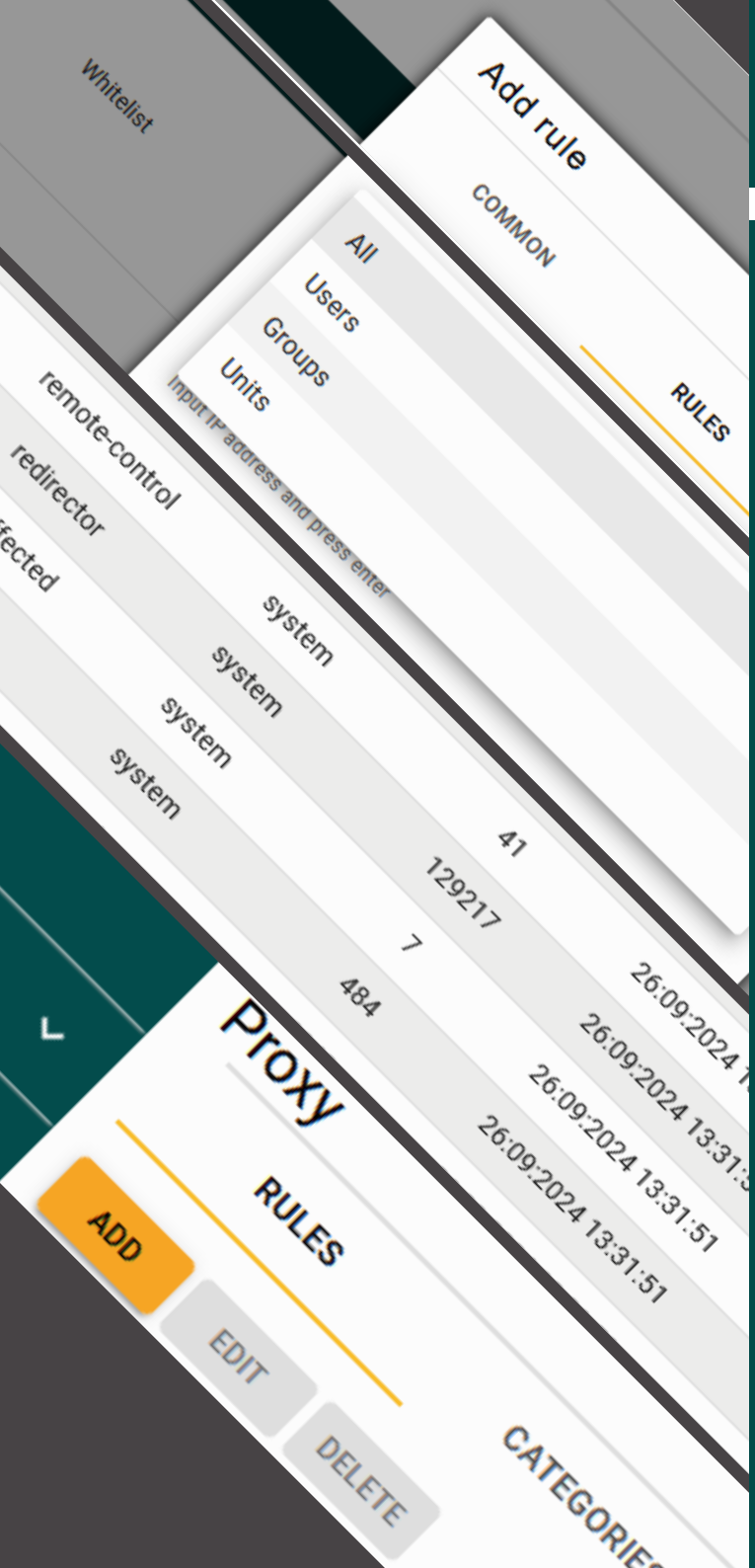
Также наше решение поддерживает интеграцию со сторонними антивирусными ядрами, что расширяет функциональность системы. Это делает нашу платформу универсальным инструментом для обеспечения безопасности вашей сети и защиты данных пользователей.



Object	Detected	Action
winnow.images.test.eicar.com.UNOFFICIAL FOUND	https://files.internet-lab.ru/seafhttp/files/bbe153ad-e8fc-49ab-a9b3-a6ab381162a4/eicar.com	DENIED
winnow.images.test.eicar.com.UNOFFICIAL FOUND	https://files.internet-lab.ru/seafhttp/files/bbe153ad-e8fc-49ab-a9b3-a6ab381162a4/eicar.com	DENIED
winnow.images.test.eicar.com.UNOFFICIAL FOUND	https://files.internet-lab.ru/seafhttp/files/bbe153ad-e8fc-49ab-a9b3-a6ab381162a4/eicar.com	DENIED
winnow.images.test.eicar.com.UNOFFICIAL FOUND	https://files.internet-lab.ru/seafhttp/files/bbe153ad-e8fc-49ab-a9b3-a6ab381162a4/eicar.com	DENIED
winnow.images.test.eicar.com.UNOFFICIAL FOUND	https://files.internet-lab.ru/seafhttp/files/bbe153ad-e8fc-49ab-a9b3-a6ab381162a4/eicar.com	DENIED
winnow.images.test.eicar.com.UNOFFICIAL FOUND	https://files.internet-lab.ru/seafhttp/files/bbe153ad-e8fc-49ab-a9b3-a6ab381162a4/eicar.com	DENIED



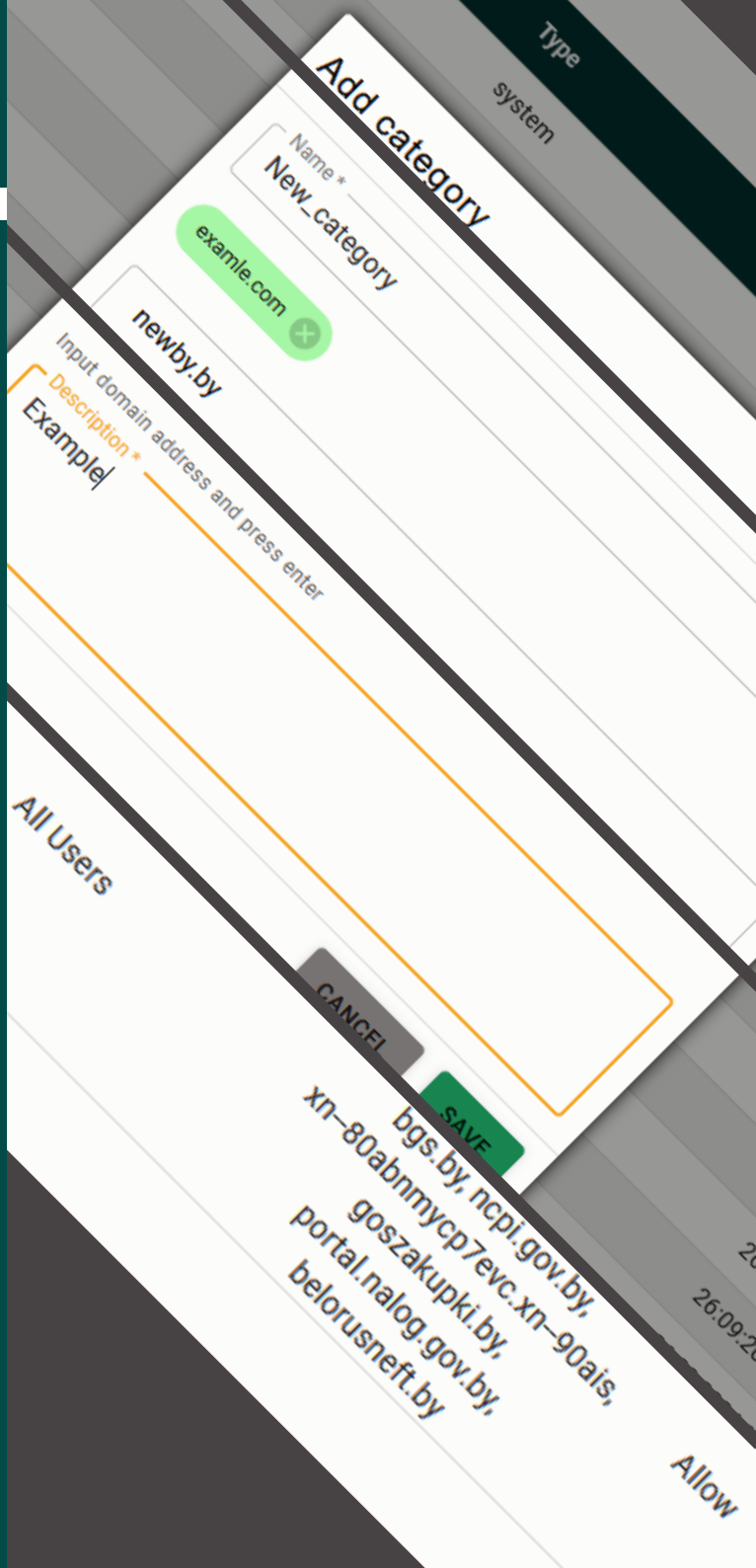
КОНТЕНТНАЯ ФИЛЬТРАЦИЯ



Компонент может ограничивать доступ к более чем 2 645 000 сущностям почти в 59 категориях*, а также позволяет:

- категорировать ресурсы сети Интернет и обеспечивать фильтрацию доступа пользователей на основе данных категорий;
- переопределять категории ресурсов, фильтровать доступ пользователей к ресурсам сети на основе фильтрации содержимого;
- автоматически обновлять базу данных ресурсов сети Интернет, предназначенных для блокировки;
- фильтровать передаваемый контент и блокировать определенные типы файлов, в том числе в SSL-трафике;
- гибко настраивать правила ограничения пользователей

** Примечание: в целях улучшения продукта, состав и количество категорий может меняться.*



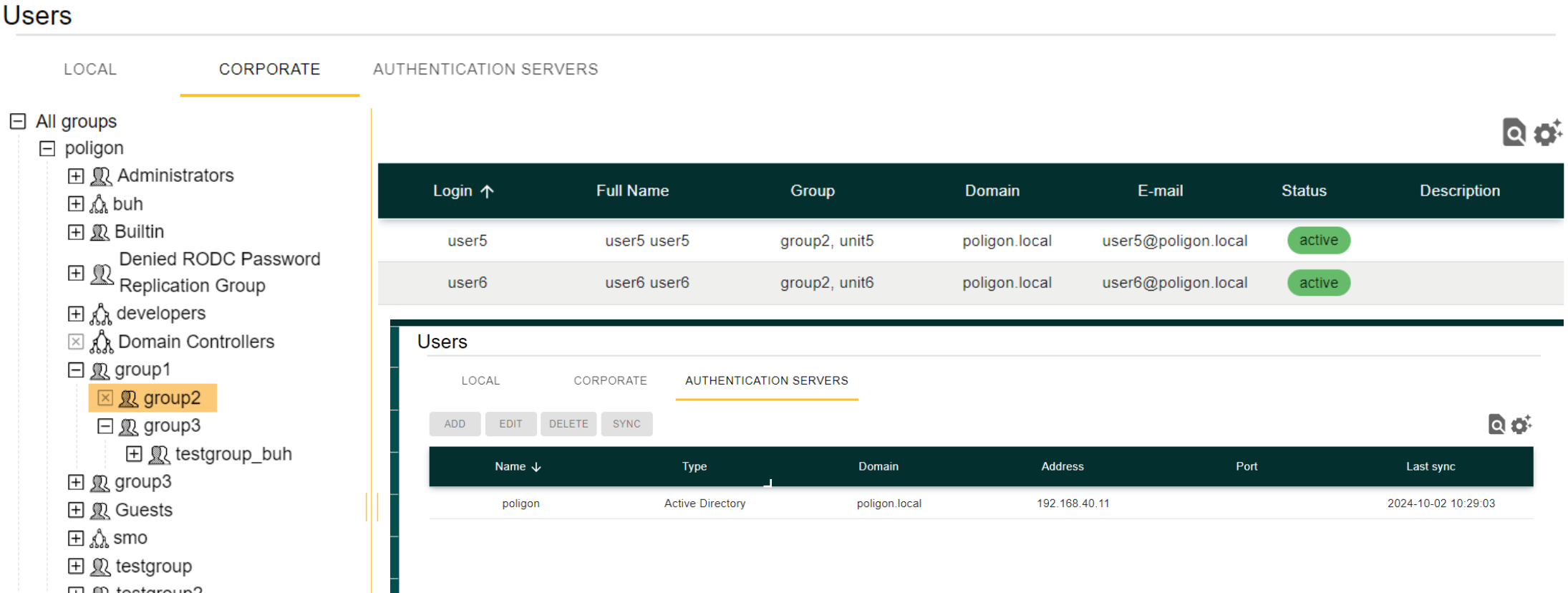
ПРОКСИ-СЕРВЕР

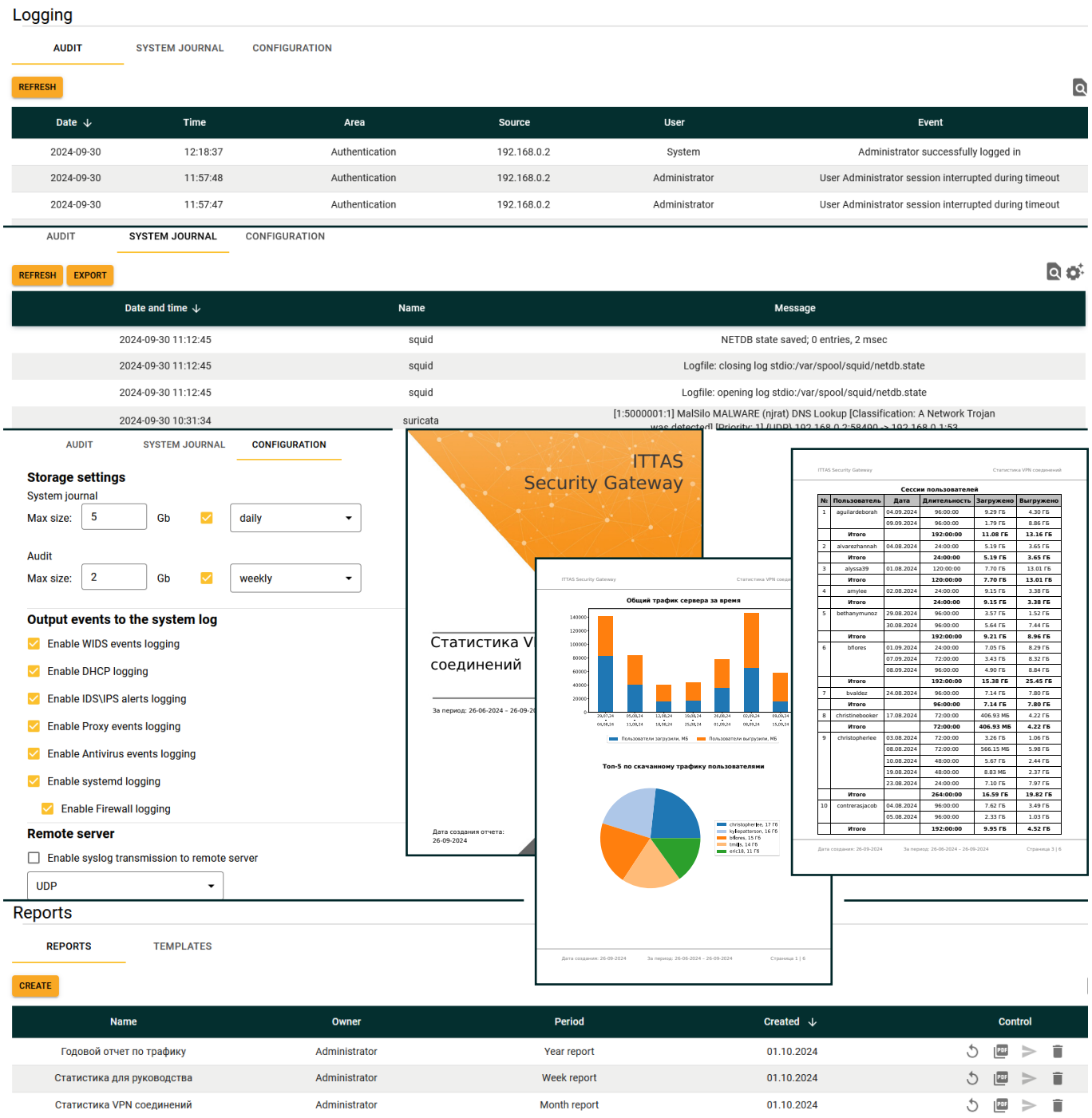
Реализует прозрачное и непрозрачное проксирование http/https трафика, обеспечивая безопасный доступ к ресурсам сети, которые используют как зашифрованные, так и незашифрованные каналы связи. Возможно указать ресурсы сети, траффик которых не будет обрабатываться.

ИНТЕГРАЦИЯ С ACTIVE DIRECTORY

Интеграция со службой каталогов Active Directory обеспечивает единую точку управления для всех пользователей, возможность применять групповые политики для настройки доступа, обеспечивая единую точку управления для всех пользователей. Интеграция позволяет вести учет доступа пользователей, что помогает в анализе трафика и выявлении злоупотреблений.

Возможность подключения нескольких серверов Active Directory позволяет полноценно использовать функции прокси-сервера даже в распределенных и сегментированных информационных системах





МОНИТОРИНГ И ПОДГОТОВКА ОТЧЕТОВ

Наше решение предлагает широкие возможности для генерации отчетов и отображения событий. Пользователи могут создавать отчеты под конкретные задачи с возможностью выбора временных периодов. Гибкие настройки обеспечивают управление логами и отчетами, позволяя пользователям адаптировать систему под свои нужды и оптимизировать процессы мониторинга и аудита.

Интуитивно понятный интерфейс обеспечивает легкость в навигации, что делает работу с данными удобной и эффективной.

Благодаря этим функциям, системные администраторы без труда могут анализировать информацию, принимать обоснованные решения на основе актуальных данных и формировать отчеты для руководства.

WIDS - ОБНАРУЖЕНИЕ АНОМАЛИЙ (ВТОРЖЕНИЙ) В БЕСПРОВОДНЫХ СЕТЯХ

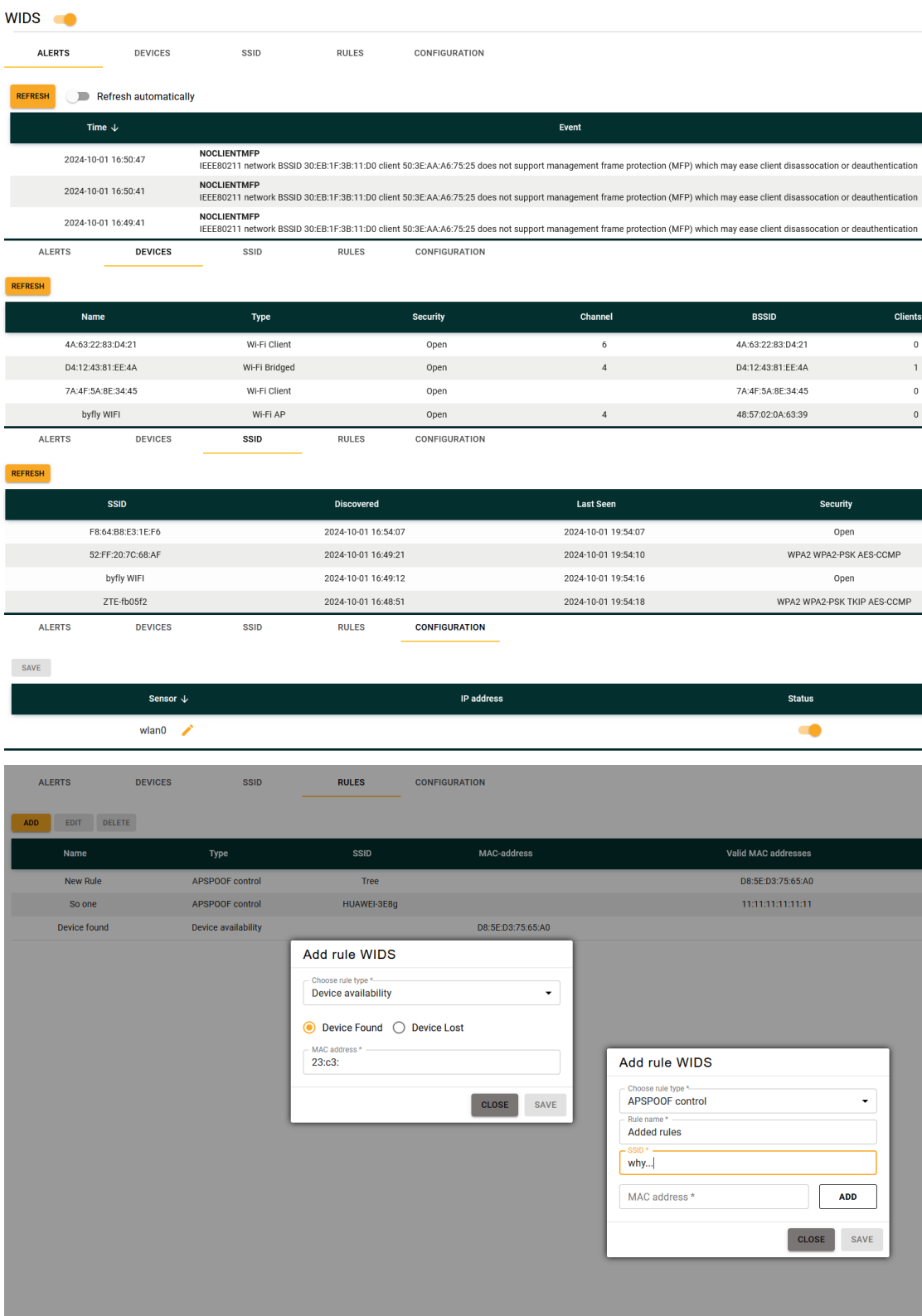
Модуль WIDS (Wireless Intrusion Detection System) предназначен для обнаружения аномальных событий в беспроводных сетях. Он интегрирован в общую архитектуру ISG и работает в реальном времени и позволяет своевременно обнаружить потенциальные попытки внешних атак.

WIDS обеспечивает непрерывный анализ беспроводного трафика для выявления подозрительных паттернов и аномалий, идентификацию различных типов атак, уведомления в случае выявления аномалий, что позволяет быстро реагировать на угрозы, интеграцию с другими системами безопасности, совместимость с SIEM-системами и другими модулями защиты для создания единого центра управления безопасностью.

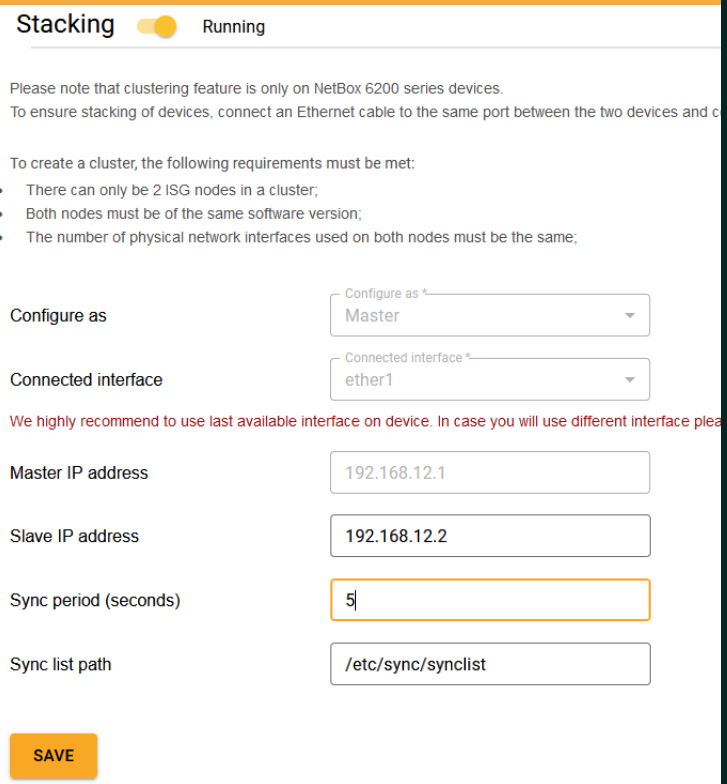
Гибкая настройка позволяет кастомизировать правила обнаружения в зависимости от специфики сети и требований бизнеса.

Удобная панель управления для мониторинга и управления системой.

В качестве сенсоров беспроводной сети могут использоваться устройства маршрутизации линейки WAP (разработанных ООО ИТТАС).



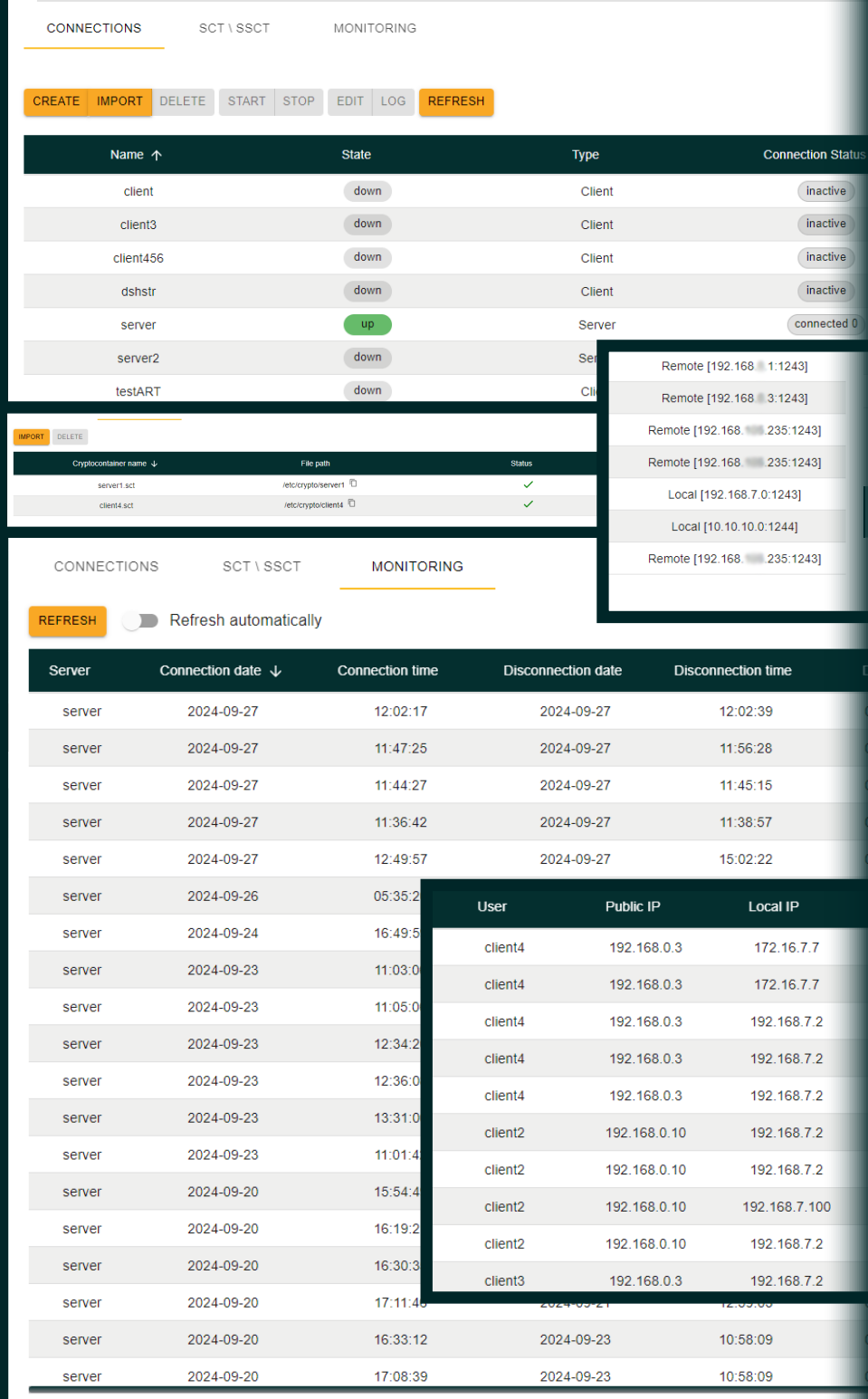
СТЕКИРОВАНИЕ УСТРОЙСТВ



ОБЕСПЕЧИВАЕТ ОТКАЗОУСТОЙЧИВОСТЬ С ПОМОЩЬЮ РЕЗЕРВИРОВАНИЯ УСТРОЙСТВ

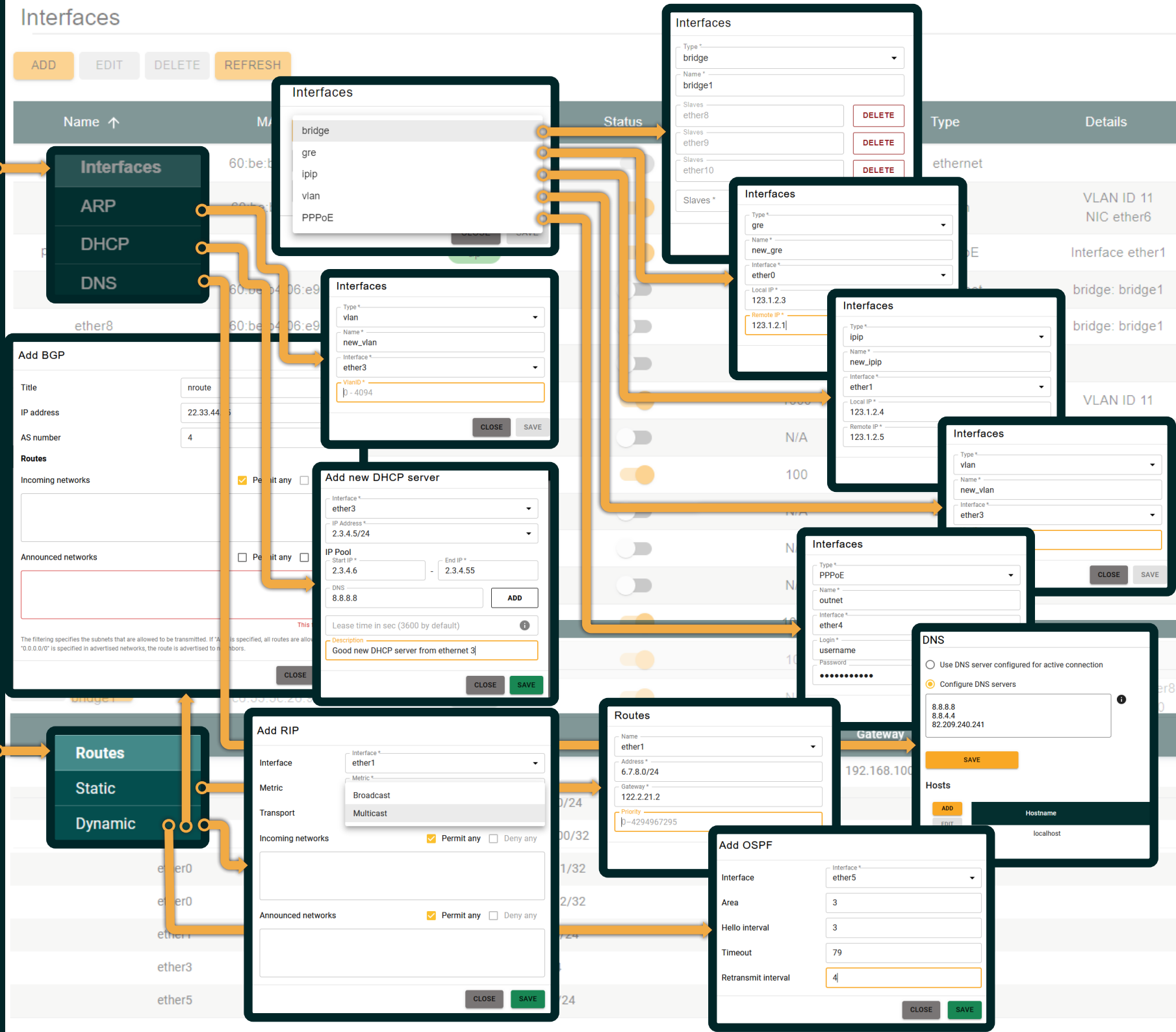
ITVPN

Средство канального шифрования ITVPN, разработанное с использованием национальных алгоритмов шифрования, представляет собой мощный инструмент для организации защищенных каналов связи. Оно интегрировано в ISG и управляется через удобный графический интерфейс, что делает его использование простым и доступным. ITVPN позволяет объединить все филиалы организации в одну частную сеть с возможностью разрешения доступа удаленным сотрудникам по закрытым каналам связи, что способствует выполнению рабочих задач без угрозы безопасности информации. Также обеспечивается контроль и предоставление отчетности действий пользователей, подключенных по защищенным каналам ITVPN.



ГИБКОЕ УПРАВЛЕНИЕ СЕТЯМИ

Наше решение обеспечивает гибкое управление сетевыми интерфейсами и инфраструктурой с использованием различных протоколов и технологий, таких как Bridge, GRE, IPIP, VLAN и PPPoE, для динамического конфигурирования и оптимизации работы сети. Также предусмотрены возможности настройки DHCP сервера, ARP, DNS и различных протоколов маршрутизации для управления маршрутами в сетях.



ВЫЧИСЛИТЕЛЬНАЯ ПЛАТФОРМА

Для реализации ISG в виде программно-аппаратного решения мы предлагаем использовать платформу NetBox.

Это позволяет предоставить Заказчику готовое решение «под ключ» , что позволяет существенно сокращать время на внедрение.

СРАВНЕНИЕ ПЛАТФОРМ NETBOX

	Идеален в качестве шлюза для филиальной сети	1U размер для монтажа в серверную стойку	
	NetBox 270	**NetBox 6200**	**NetBox 6200M**
Габаритные размеры (ДхШхВ)	125x114x43 мм	440x255x47 мм	440x255x47 мм
Варианты монтажа	настольное исполнение, крепление на стену/монитор при помощи дополнительного кронштейна	установка в стандартную стойку 19 дюймов или телекоммуникационный шкаф	
Центральный процессор	Intel Celeron N5105, FCBGA1338 (4 ядра/4 потока, кэш-память 4 Мб, частота 2,0 ГГц)	Intel Celeron N5105, FCBGA1338 (4 ядра/4 потока, кэш-память 4 Мб, частота 2,0 ГГц)	Intel i3-13100, LGA1700 (4 ядра/8 потоков, кэш-память 5 Мб, частота 3,4 ГГц)
Память	8 Гб/16 Гб DDR4	16 Гб DDR4	16 Гб DDR5
Сетевые интерфейсы	2x1000BASE-T (RJ-45)	6x2.5GBASE-T (RJ-45)	8x2.5GBASE-T (RJ-45), 2x10G SFP+
Вспомогательный (управляющий) порт	–	1xRJ45	1xRJ45
Твердотельный накопитель	256 Гб	128 Гб	256 Гб
Подключение дополнительных накопителей	поддерживается, SATA		
Электропитание	110-230 В, 50-60 Гц, не более 36 Вт	110-230 В, 50-60 Гц, не более 50 Вт	
Интерфейсы для подключения дополнительных устройств	4*USB 3.0, 1*Type-C, 2*HDMI, 1*mini-jack (3,5mm)	2*USB 3.0, 1*VGA	4*USB 3.0, 1*VGA
Рейтинг защиты	IP 20		
Модули расширения	–	–	*4x1 Гб RJ45 или 4x1Gb SFP*

ITTAS Security Gateway — это высокоэффективное решение для защиты сетевой инфраструктуры и белорусская разработка. Это позволяет нам обеспечить надежное сопровождение и точечную доработку под специфические требования заказчика. Выбирая ISG вы получаете мощный инструмент для организации защиты сети и управления доступом пользователей к сетевым ресурсам. Возможность интеграции со сторонними сервисами и ведение статистики позволяют получить четкую картину состояния сети организации.
ISG повышает безопасность и продуктивность, минимизируя риски. Продукт постоянно развивается, регулярно добавляя новый функционал, что позволяет оставаться на шаг впереди.

БЛИЖАЙШИЕ ПЛАНЫ ПО РЕАЛИЗАЦИИ:

управление событиями безопасности;
политики безопасности;
интеграция антивирусных движков сторонних производителей;
реализация объектной модели управления;
повышение отказоустойчивости в процессе работы;
пассивное обнаружение узлов сети.

ДОПОЛНИТЕЛЬНЫЕ РЕШЕНИЯ ООО ITTAS

КОМПЛЕКС ЗАЩИТЫ ТРАНСПОРТНОГО УРОВНЯ **ITTLS**

уникальное программное средство, реализующее протокол защиты транспортного уровня с использованием криптографических стандартов, принятых в Республике Беларусь;

реализует одностороннюю аутентификацию;

обеспечивает защищённую передачу данных между узлами в сети Интернет;

предназначен для защиты информации приложений, работающих с сетью Интернет (веб-браузеры, электронная почта, обмен мгновенными сообщениями, IP-телефония (VoIP));

не требуются клиентские лицензии.

ШЛЮЗ ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ **OWG**

аппаратное исполнение обеспечивает защиту от взломов и утечек передаваемых данных;

защищает персональные данные, финансовые транзакции, медицинские данные, также обеспечивает контроль доступа к конфиденциальной, клиентской информациии, данным пациентов;

осуществляет одностороннюю передачу управляющих сигналов и данных в АСУ, аудио и видео систем наблюдения.

ДЛЯ ВАШЕЙ БЕЗОПАСНОСТИ

компактный защищенный корпус

высокая скорость до 10 Гбит/с

предлагается в исполнении с RJ45

либо SFP/SFP+ интерфейсами

ПРОГРАММНОЕ СРЕДСТВО КАНАЛЬНОГО ШИФРОВАНИЯ ITVPN

позволяет использовать как технологию виртуальной частной сети(Layer3), так и туннельные соединения вида точка-точка по протоколам TCP или UDP(Layer2);

возможность соединения через любой порт, что существенно затрудняет обнаружение и блокировку туннеля;

есть мониторинг соединений, пользователей и предоставление статистики, а также контроль использования сетевого трафика;

реализовано шифрование и контроль целостности сетевого трафика в соответствии с СТБ 34.101.31;

реализована аутентификация сторон и выработка общего сеансового ключа в соответствии с СТБ 34.101.65;

интегрировано с Internet Security Gateway.

+375 17 318 08 50
+375 29 315 08 50
+375 33 315 08 50

info@ittas.by

ittas.by