ideco

Закрытие уязвимостей и атак при помощи IPS от Ideco

Алексей Киселев
Presale-инженер

О компании Ideco

Ideco — российский разработчик решений для защиты корпоративных сетей от кибератак и фильтрации трафика.

2005 год основания

5500+ компаний-заказчиков

250+ сотрудников в команде

3 мажорных релиза каждый год

ideco

2025

Российская действительность в ИБ

Актуальные угрозы и вопросы, с которыми столкнулись организации

ideco

- Увеличение количества атак на российский сегмент
- Уязвимости нулевого дня
- Уязвимости ПО
- Российские решения не могут полностью заменить ушедшие решения по скорости обработки трафика и функциональности
- Выполнение рекомендаций регуляторов (гос организации , КИИ)

Уязвимости вендоров новые каналы подготовки и проведения атак

ideco

Вендоры не предоставляют обновлений для закрытия уязвимостей для российских организаций

«Серые» каналы обновлений могут использоваться для подготовки и проведения атак

Техподдержка прекращена

Отозвали сертификаты ФСТЭК

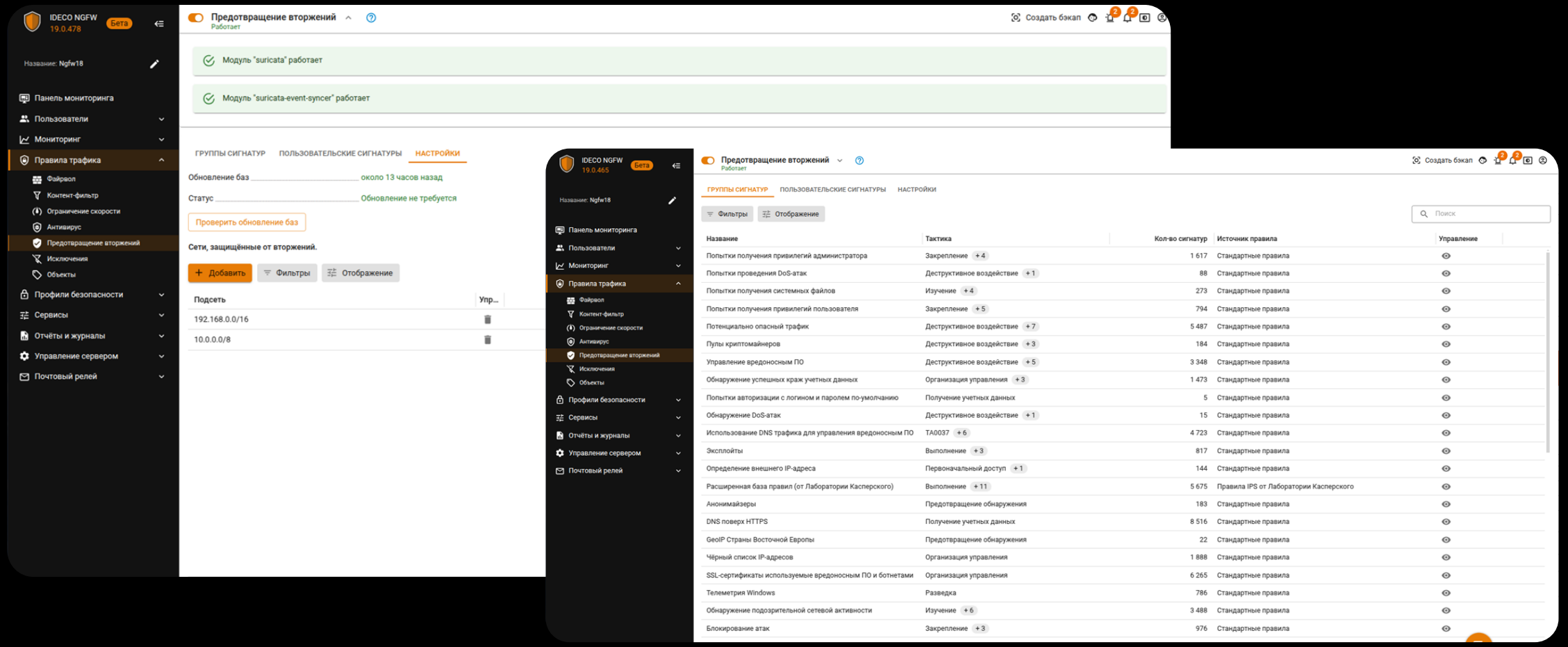
Решение Ideco NGFW

Защита нулевого дня

Быстрое развитие продукта до 3 релизов в год , минорные обновление версий постоянная проверка кода при выпуске версий, регулярные выпуски сертифицированных версий решений

Сигнатуры Касперского

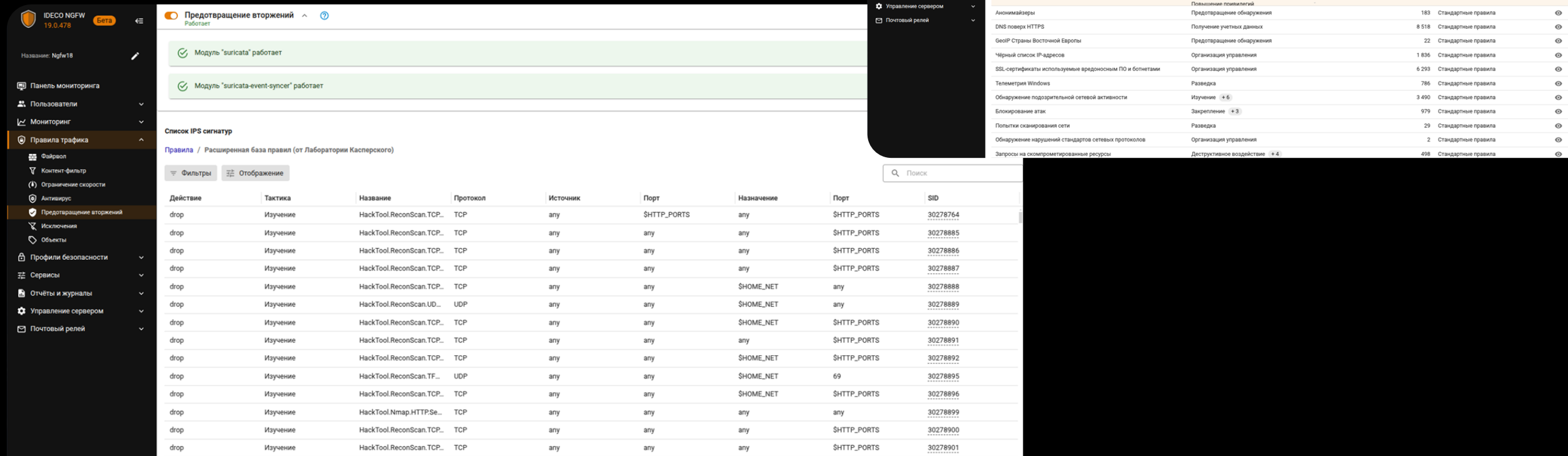
Модуль обнаружения и предотвращения атак

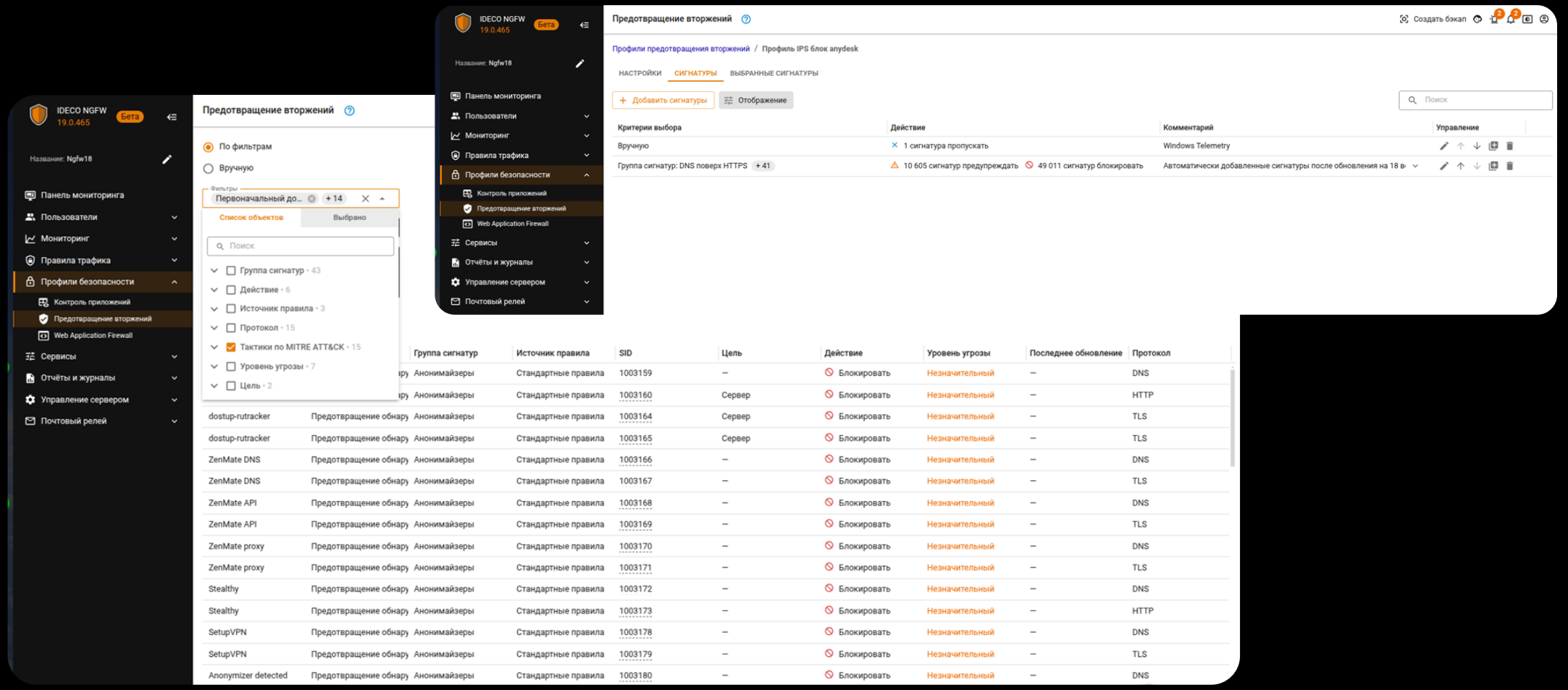


Расширенные сигнатуры IPS

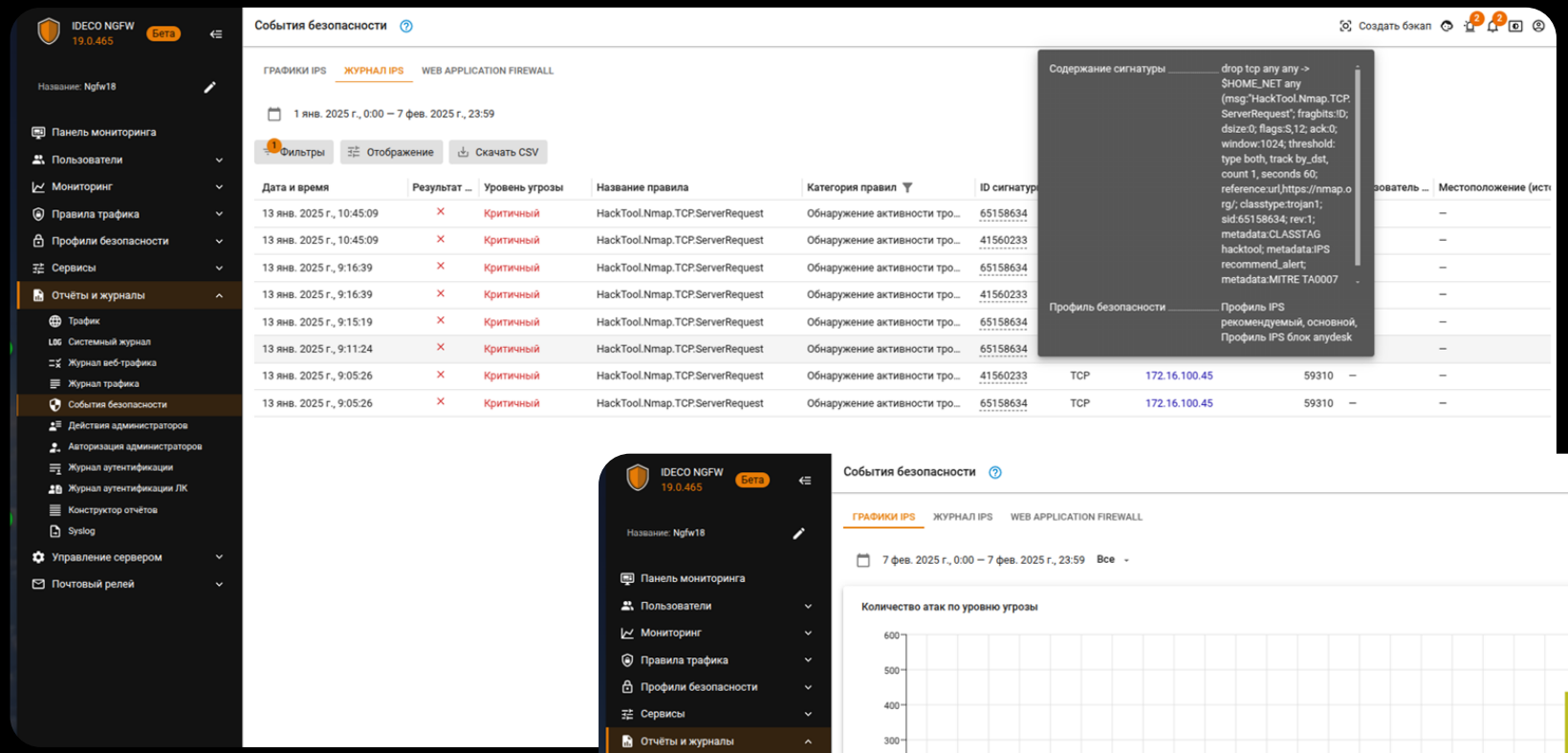
Возможность использования расширенной базы правил предотвращения вторжений от Лаборатории Касперского.

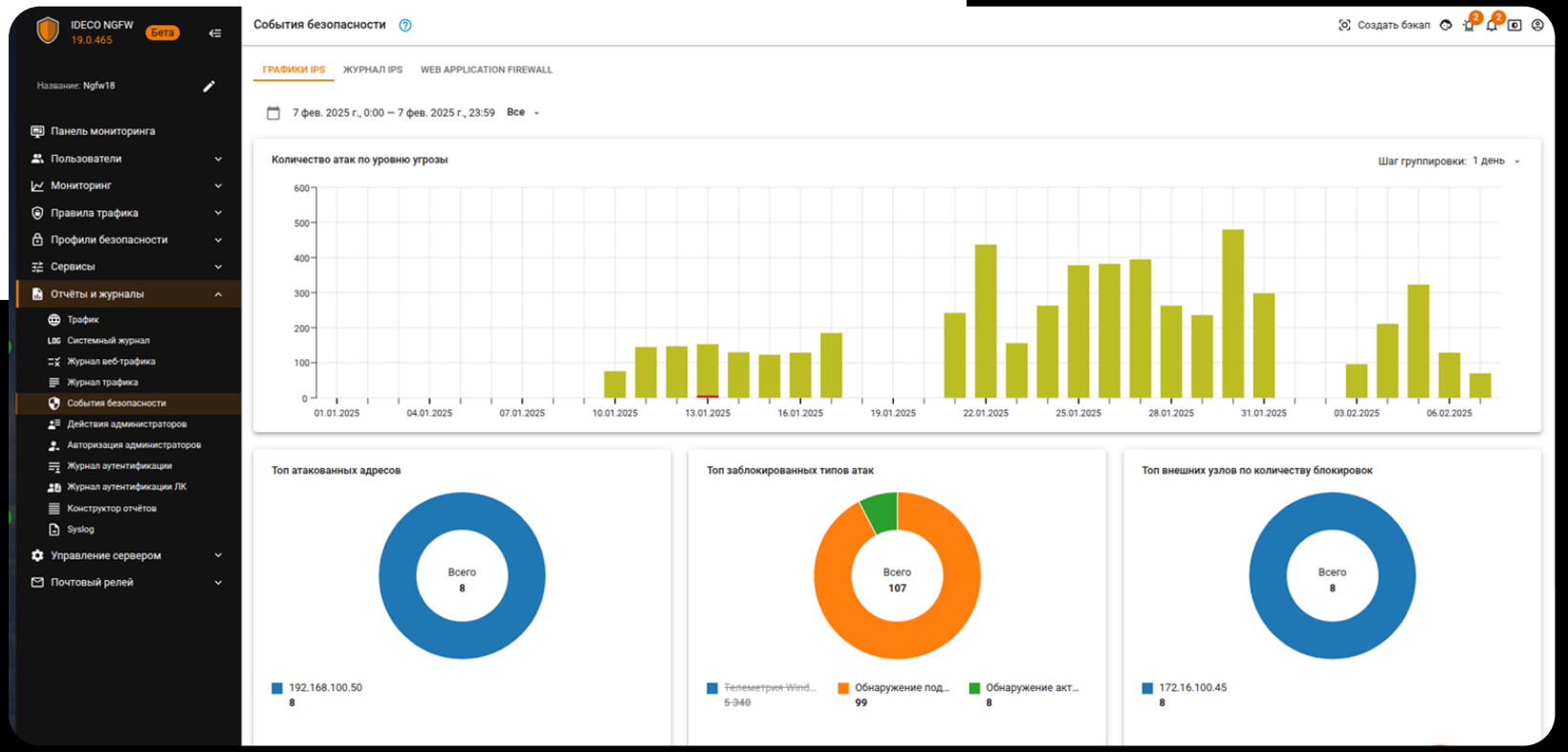
Требует дополнительного лицензирования.





- настройка профилей для организации защиты
- отчеты о выявленных и заблокированных угрозах


IDECO NGFW
19.0.465
Бета
Название: Ngfw18
Панель мониторинга
Пользователи
Мониторинг
Правила трафика
Профили безопасности
Сервисы
Отчёты и журналы
Трафик
Системный журнал
Журнал веб-трафика
Журнал трафика
События безопасности
Действия администраторов
Авторизация администраторов
Журнал аутентификации
Журнал аутентификации ЛК
Конструктор отчётов
Syslog
Управление сервером
Почтовый релей
События безопасности
Создать бэкап
ГРАФИКИ IPS
ЖУРНАЛ IPS
WEB APPLICATION FIREWALL
1 янв. 2025 г., 0:00 — 7 фев. 2025 г., 23:59
Фильтры
Отображение
Скачать CSV
Дата и время
Результат ...
Уровень угрозы
Название правила
Категория правил
ID сигнатур
13 янв. 2025 г., 10:45:09
Критичный
HackTool.Nmap.TCP.ServerRequest
Обнаружение активности тро...
65158634
41560233
13 янв. 2025 г., 9:16:39
13 янв. 2025 г., 9:15:19
13 янв. 2025 г., 9:11:24
13 янв. 2025 г., 9:05:26
TCP
172.16.100.45
59310
Содержание сигнатуры
drop tcp any any -> $HOME_NET any (msg:"HackTool.Nmap.TCP.ServerRequest"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:1024; threshold: type both, track by_dst, count 1, seconds 60; reference:url,https://nmap.org/; classtype:trojan1; sid:65158634; rev:1; metadata:CLASSTAG hacktool; metadata:IPS recommend_alert; metadata:MITRE TA0007
Профиль безопасности
Профиль IPS рекомендуемый, основной, Профиль IPS блок anydesk


IDECO NGFW
19.0.465
Бета
Название: Ngfw18
Панель мониторинга
Пользователи
Мониторинг
Правила трафика
Профили безопасности
Сервисы
Отчёты и журналы
Трафик
Системный журнал
Журнал веб-трафика
Журнал трафика
События безопасности
Действия администраторов
Авторизация администраторов
Журнал аутентификации
Журнал аутентификации ЛК
Конструктор отчётов
Syslog
Управление сервером
Почтовый релей
События безопасности
Создать бэкап
ГРАФИКИ IPS
ЖУРНАЛ IPS
WEB APPLICATION FIREWALL
7 фев. 2025 г., 0:00 — 7 фев. 2025 г., 23:59
Все
Количество атак по уровню угрозы
Шаг группировки: 1 день
600
500
400
300
200
100
0
01.01.2025
04.01.2025
07.01.2025
10.01.2025
13.01.2025
16.01.2025
19.01.2025
22.01.2025
25.01.2025
28.01.2025
31.01.2025
03.02.2025
06.02.2025
Топ атакованных адресов
Всего
8
192.168.100.50
8
Топ заблокированных типов атак
Всего
107
Телеметрия Wind...
5 340
Обнаружение под...
99
Обнаружение акт...
8
Топ внешних узлов по количеству блокировок
Всего
8
172.16.100.45
8

А что же по скорости..?

Производительность Ideco NGFW VPP

Передовые технологии

Собственный сетевой стек технологий на базе DPDK/VPP, обеспечивающий высочайшую скорость фильтрации трафика

Результаты нагрузочных тестов*

Пропускная способность EMIX:

Firewall - до 100 Гбит/с
Firewall и "Инспекция приложений" - до 75 Гбит/с
IPS и "Инспекция приложений" - до 25 Гбит/с

Пропускная способность HTTP 250 Kb:

Firewall - до 200 Гбит/с
Макс. кол-во парал. сессий TCP -до 25 000 000
Макс. кол-во сессий в секунду TCP -1 000 000

*Результаты получены на Ideco EX

Выполнение требований регуляторов

Высокопроизводительные платформы для бизнеса любого масштаба

Ideco SX+ ФСТЭК

до 100 активных пользователей интернет

Ideco LX ФСТЭК

от 300 до 1000 активных пользователей интернет

Ideco EX ФСТЭК

для крупных компаний, дата-центров и высоконагруженных сетей

Дополнительные модули в Ideco для обеспечения безопасности периметра организации

ideco

Сетевые службы

DNS, DHCP, NTP, балансировка и резервирование канала, квоты, шейпер трафика

Фильтрация трафика L7

МЭ, СОВ, Контроль приложений, Контент-фильтр

Мониторинг и отчётность

Telegram-бот, Zabbix Агент, Syslog, SNMP, SIEM, отчётность по пользователям

Управление

Веб-интерфейс, ssh, центральная консоль

IDECO NGFW

Маршрутизация

Статическая
динамическая OSPF, BGP

Отказоустойчивость

Кластеризация Active/Passive, резервное копирование, программный Watchdog

VPN

Site-To-Site IPsec, IKEv2, SSTP, Wireguard (клиент), L2TP/IPsec

Пользователи

Интеграция с LDAP, локальная база пользователей, авторизация (IP, MAC, Kerberos, Web, Агент, подсеть), пользователи и группы как объекты в политиках фильтрации

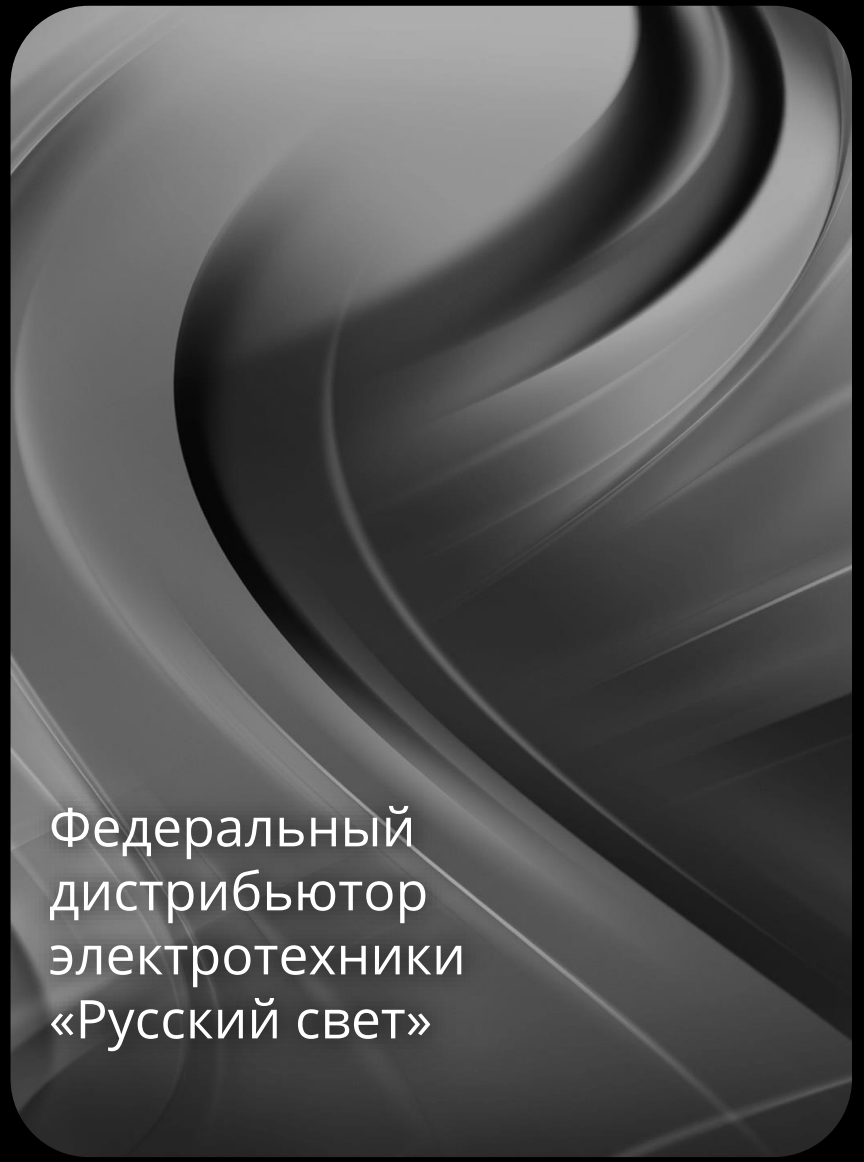
Поддержка заказчиков

1. Зарегистрироваться на my.ideco.ru
2. Скачать Ideco NGFW
3. Установить Ideco NGFW

my.ideco.ru

+ 42 дня тестовая лицензия
+ Помощь в тестировании
+ Обратная связь

Проектный опыт



Федеральный дистрибьютор электротехники «Русский свет»

Задачи

+ Решение на 4 000 пользователей для замены Cisco и open source
+ Круглосуточная техническая поддержка с выделенным каналом связи
+ Централизованное управление и мониторинг

Результат

Осуществлен переход на решение Ideco NGFW. Оперативное решение вопросов заказчика в процессе внедрения и эксплуатации.

«Функционал продукта отвечает всем нашим требованиям! Используем Ideco NGFW в нашей компании с июля 2022 года. Все работает без нареканий, рады продолжать наше плодотворное сотрудничество», - Алексей Савченко, начальник управления по инфраструктуре ИТ.

Южно-Уральский государственный медицинский университет

Задачи

+ Замена решения по защите сети
+ Фильтрация трафика
+ Организация удаленного доступа
+ Контроль выхода в интернет пользователей
+ Отчетность по веб-трафику, публикации сайта

Результат

Внедрена аппаратная платформа Ideco UTM MX, обеспечивающая безопасность сети университета.

20 июня 2022 года модуль Web Application Firewall помог избежать тяжелых последствий DDoS-атаки, при которой в течение нескольких часов происходило более 20 тысяч запросов к сайту университета.

«Мы используем аппаратную платформу Ideco UTM MX с сентября 2019 года. В очередной раз убедились, что сделали правильный выбор!», - академик РАН, Заслуженный врач РФ, главный онколог и радиолог УрФО, и.о. ректора ФГБОУ ВО ЮУГМУ Минздрава России Андрей Владимирович Важенин.

Департамент информационных технологий и цифрового развития ХМАО

Задачи

Обеспечить безопасность сети
для 2500 пользователей:

+ удобство настройки,
+ интеграция с Active Directory,
+ фильтрация трафика.

Один из ключевых факторов - быстрая
и качественная техническая поддержка.

Результат

Произведена интеграция межсетевого экрана Ideco, закрывающая все потребности заказчика: фильтрация трафика L7, контроль приложений, интеграция с Active Directory. Решение полностью соответствует требованиям заказчика по удобству настройки и интеграции в существующую инфраструктуру. Техническая поддержка по 5 каналам связи. Ответ в веб-интерфейсе продукта в течение 30 секунд.

ideco СОЗДАЕМ ВМЕСТЕ

Алексей Киселев
presale-инженер

e-mail: a.kiselev@ideco.ru
tg: @kiselev_au