



КОД ИБ

ИТОГИ

NGFW как центр безопасности экосистемы российских решений для защиты вашего бизнеса

ДМИТРИЙ ХОМУТОВ
CEO
Ideco





КОД ИБ

ИТОГИ

О нас

Idesco – продуктовая IT-компания

- + Больше 1000 серверов на Idesco NGFW 18
- + Экспертная и быстрая поддержка
- + Защищаем от кибератак
- + Сами используем Idesco NGFW и Idesco VPN

2005 год

3 мажорных релиза в год

5500 клиентов

240 сотрудников





КОД ИБ

ИТОГИ

NGFW должен работать



Интересный факт: в сериалах WeCrashed («Не сработало») и The Dropout («Выбывшая»)





КОД ИБ

ИТОГИ

Сложность выбора NGFW увеличивается



Вы когда-нибудь мечтали стать лучшей версией NGFW?





КОД ИБ

ИТОГИ

Технологические тренды 2024

Конкуренция в создании высокопроизводительного решения

Сертификация ФСТЭК по требованиям к NGFW

Создание смежных решений





КОД ИБ

ИТОГИ

Idesco — единственный NGFW с DNS Security

Основные показатели

Все запросы
181,340,567,923

→ Разрешенные запросы
885,409,098

→ Все заблокированные запросы
894

→ Предупрежденные угрозы
120

Общие сведения о логике ваших запросов и общее количество конкретных типов запросов.

- Разрешенные запросы**
Запросы, прошедшие через веб-фильтр, поскольку наши алгоритмы не обнаружили киберугроз или ограничений в категории вашей учетной записи или настройках домена.
- Все заблокированные запросы**
Запросы, которые помечены алгоритмом SafeDNS или потенциально опасные или ограничены на основании пользовательских настроек в вашей учетной записи.
- Предупрежденные угрозы**
Общее количество предупрежденных угроз выдает в себе список, идентифицированные нашими алгоритмами как вредоносные или связанные с заблокированными категориями безопасности в настройках вашей учетной записи.

Основные показатели

ТОП ЗАБЛОКИРОВАННЫХ ДОМЕНОВ	ТОП ЗАБЛОКИРОВАННЫХ УСТРОЙСТВ	ТОП ЗАБЛОКИРОВАННЫХ КАТЕГОРИЙ
youtube.com 32416	устройства215 67493	Порнография и секс 67493
facebook.com 21684	elniclub32 33483	Здоровье 62098
vk.com 20287	mltrapsa497 49883	Социальные сети 58837
linkedin.com 18045	mltclub444 34277	Чаты и мессенджеры 52765
twitter.com 16825	infocap4720 32187	Фуроры 48276
vkua.com 13825	mltclub355 21107	Туренты и P2P сети 37964
reddit.com 8825	beautifulyou101 18002	Игры 32001
medium.com 4298	luprand886 12112	Астрология 28871
instagram.com 4288	mltrabb0554 12087	Фильмы и видео онлайн 21437
gitee.com 3214	mltclub9483 8987	Жизни, история, телекоммуникации 17043

10 самых заблокированных доменов, устройств с наибольшим количеством попыток доступа и заблокированных категорий по количеству запросов.

Топ заблокированных доменов
Список из 10 доменов, к которым ваши пользователи постоянно пытаются получить доступ, подавляющее в заблокированных категориях или точно заблокированных сайтах.

Топ заблокированных устройств
Список из 10 устройств, которые чаще всего пытаются получить доступ к заблокированным сайтам доменам в категории.

Топ заблокированных категорий
Список из 10 категорий, к которым ваши пользователи постоянно пытаются получить доступ, подавляющее под настройками блокировки вашего аккаунта.

Безопасность

Общее количество вредоносных запросов
12,345 (-564 (-34%)) по сравнению с прошлым месяцем

Общее количество предупрежденных угроз
12,345 100%

Грубость, мат, непристойность: 885 / 1045

Распространение вирусов: 674 / 987

Запаркованные домены: 526 / 3801

Фишинг: 526 / 1134

Агрессия, расизм, терроризм: 987 / 4882837

Криптомайнинг: 674 / 987

Плагиат и рефераты: 674 / 987

Обновлено 3 минуты назад

Разбивка категорий безопасности по количеству запросов, предупрежденных угрозам и проценту каждой категории в общей области.

Если вы заметили несоответствие между количеством блоков и запросов, это может быть связано с:

- Домены этой категории были заблокированы в настройках вашей учетной записи не часть выбранного периода.
- Ранее домен относился к другой категории или не имел категории, но теперь демонстрирует признаки угрозы или контроля, заблокированного настройками личной учетной записи.
- Классифицированный доступ в вашей личной учетной записи или сайте со стороны внутреннего или внешнего взаимодействия.
- Администратор разрешил эту категорию в вашей учетной записи.

Если вы подозреваете, что несоответствие не связано с вашими действиями, проверьте журналы своей учетной записи или сообщите нам, что вы подозреваете сетевой атаку.

Активность

Общее количество заблокированных запросов: **12,345**

Общее количество заблокированных устройств: **885**

Общее количество предупрежденных угроз: **120**

Общее количество разрешенных запросов: **11,340**

ИИ

Категории: Все

Категория	Запросы IP
com	3758
.com	76840
	83
em	543
	6573
	1121
	1121
	1121
	1121
	1121

иет о 10 доменах, к которым пользователи пытались получить доступ чаще всего.

Разрешенный домен
Запросы, прошедшие через веб-фильтр, поскольку наши алгоритмы не обнаружили киберугроз или ограничений в категориях вашей

Заблокированный домен
Запросы включают в себя случаи, которые наши алгоритмы идентифицировали как вредоносные или которые связаны с

Смещенный домен
Домены с низким статусом в те периоды — заблокированы разрешенными или измененными, включая те



КОД ИБ

ИТОГИ

Ставка на технологии и быструю разработку

Быстрые релизы
и инвестиции в R&D

Технологическое сотрудничество
с российскими компаниями

Сертификация ФСТЭК
по требованиям NGFW

Разработка версии для
высоконагруженных сетей

Добавление новых аппаратных
платформ в сертификат ФСТЭК

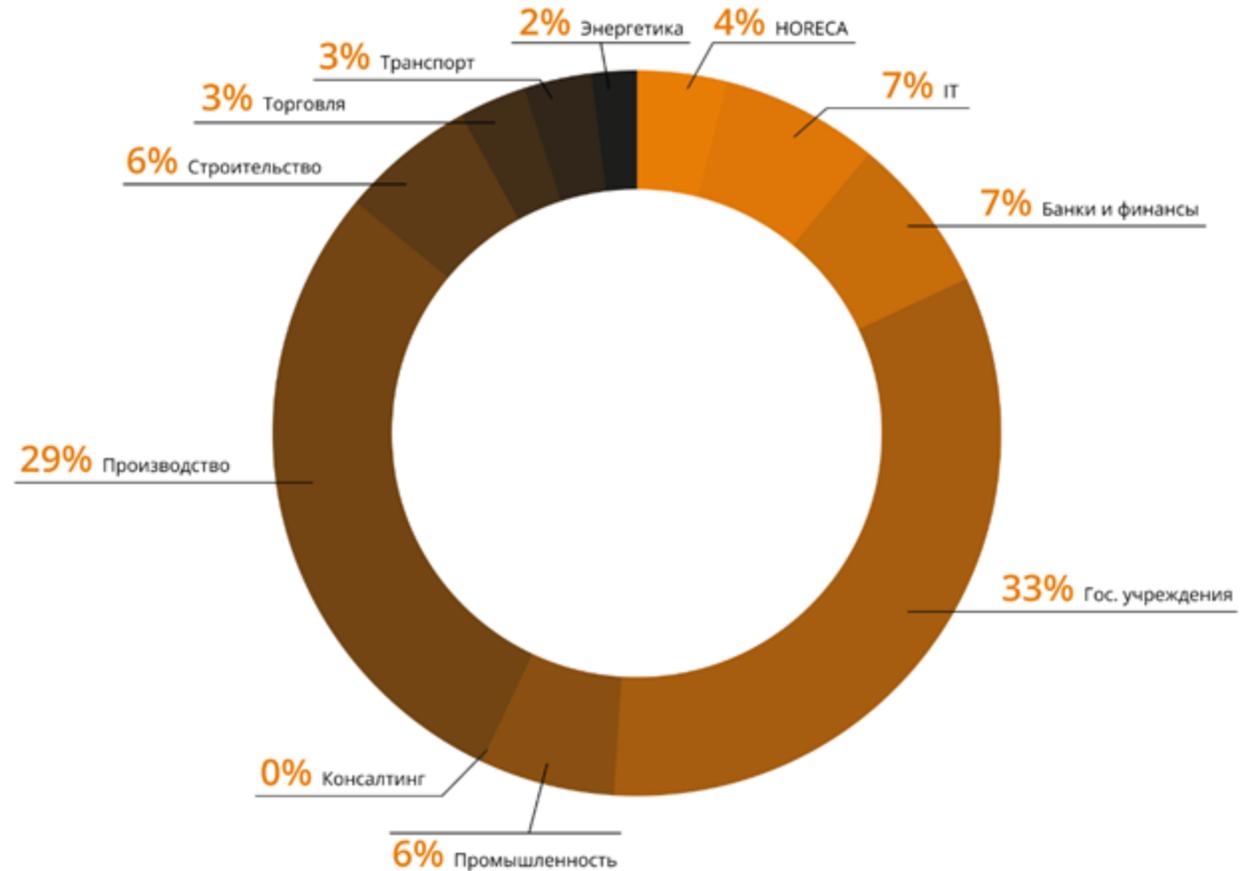




Исследование

Аудитория исследования

В рамках исследования мы получили ответы на вопросы более 100 ИТ и ИБ руководителя компаний различных сфер деятельности.





Исследование

Ключевые факторы при выборе NGFW

33% участников исследования считают функциональность ключевым фактором при выборе межсетевого экрана следующего поколения.

21% респондентов наряду с функциональностью выделяют стоимость в качестве ключевого фактора.

12% участников опроса считают, что при выборе NGFW важны все факторы.

Есть к чему стремиться

29% респондентов недовольны стоимостью отечественных NGFW.

17% участников исследования считают, что функциональность российских NGFW пока еще сильно уступает зарубежным.

34% респондентов довольны качеством межсетевых экранов отечественного производства.





КОД ИБ

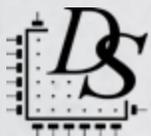
ИТОГИ

Ideco open ecosystem



MULTIFACTOR

SKYDNS



ЦИФРОВЫЕ
РЕШЕНИЯ



РЕДСОФТ

ASTRA LINUX®

kaspersky





КОД ИБ

ИТОГИ

Ideco Client (ZTNA/NAC/VPN)

СОВМЕСТИМОСТЬ

- Windows 10 и старше
- MacOS
- Linux (Ubuntu, Debian, Fedora)
- Астра, Альт ОС, Ред ОС





Следование отраслевым стандартам

IPSec site-to-site

ICAP

SYSLOG

RADIUS

синтаксис snort/suricata

SNMP/Zabbix

Интересный факт: Ideco NGFW может создавать VPN с Fortigate, Checkpoint, Cisco, Mikrotik.





КОД ИБ

ИТОГИ

Открытое и документированное API

docs.ideco.dev/api





КОД ИБ

ИТОГИ

Что нового в 2024 для миграции с западных NGFW

- Zone Based Firewall;
- профили DPI и IPS в Firewall;
- ZTNA/NAC Client;
- Virtual Context Engine;
- профили WAF и защита от DoS;
- интеграция с ALD Pro;
- GRE, SPAN, loopback.





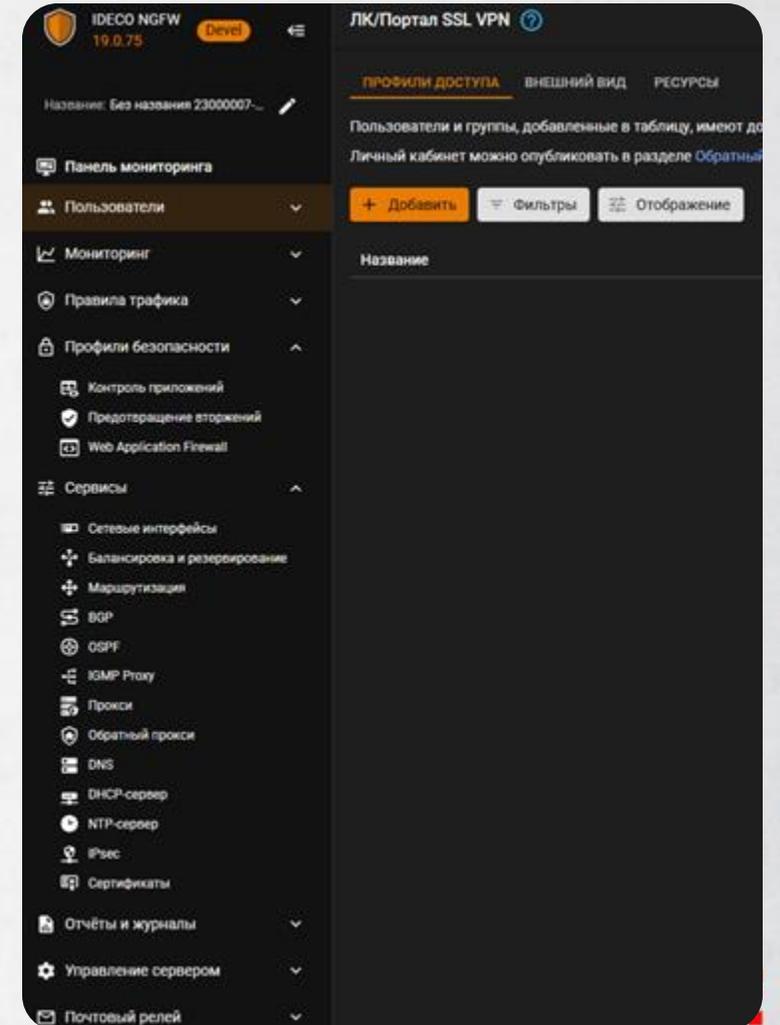
КОД ИБ

ИТОГИ

В 2024 выйдет и IdecO NGFW 19

- Новейшая платформа
- Портал SSL VPN
- Netflow сенсор
- Профили Split tunneling для VPN
- Ускорение синхронизации групп безопасности с Active Directory
- Улучшенная отчетность по трафику
- Ввод кода 2FA в IdecO Client
- Active-Active балансировка VPN соединений IdecO Client

Интересный факт: релиз IdecO UTM ФСТЭК 18 выйдет в декабре этого года.





КОД ИБ

ИТОГИ

2025





КОД ИБ

ИТОГИ

СПАСИБО ЗА ВНИМАНИЕ!



8 800 555 33 40

sales@ideco.ru

ideco.ru

