Практический опыт внедрения NGFW в enterprise

Марина Подолянюк, менеджер по продажам Ideco

ideco

Ideco сегодня

20 лет на рынке, тысячи защищённых компаний и регулярные продуктовые релизы — решения Ideco создаются командой, где более половины сотрудников (150 человек) сосредоточены на разработке.

Мы растём вместе с нашими клиентами, масштабируем решения и поддерживаем безопасность сотен тысяч пользователей по всей стране.

20+
лет на рынке

5500+
компаний под защитой

2400+
участников сообщества

55%
сотрудников в R&D

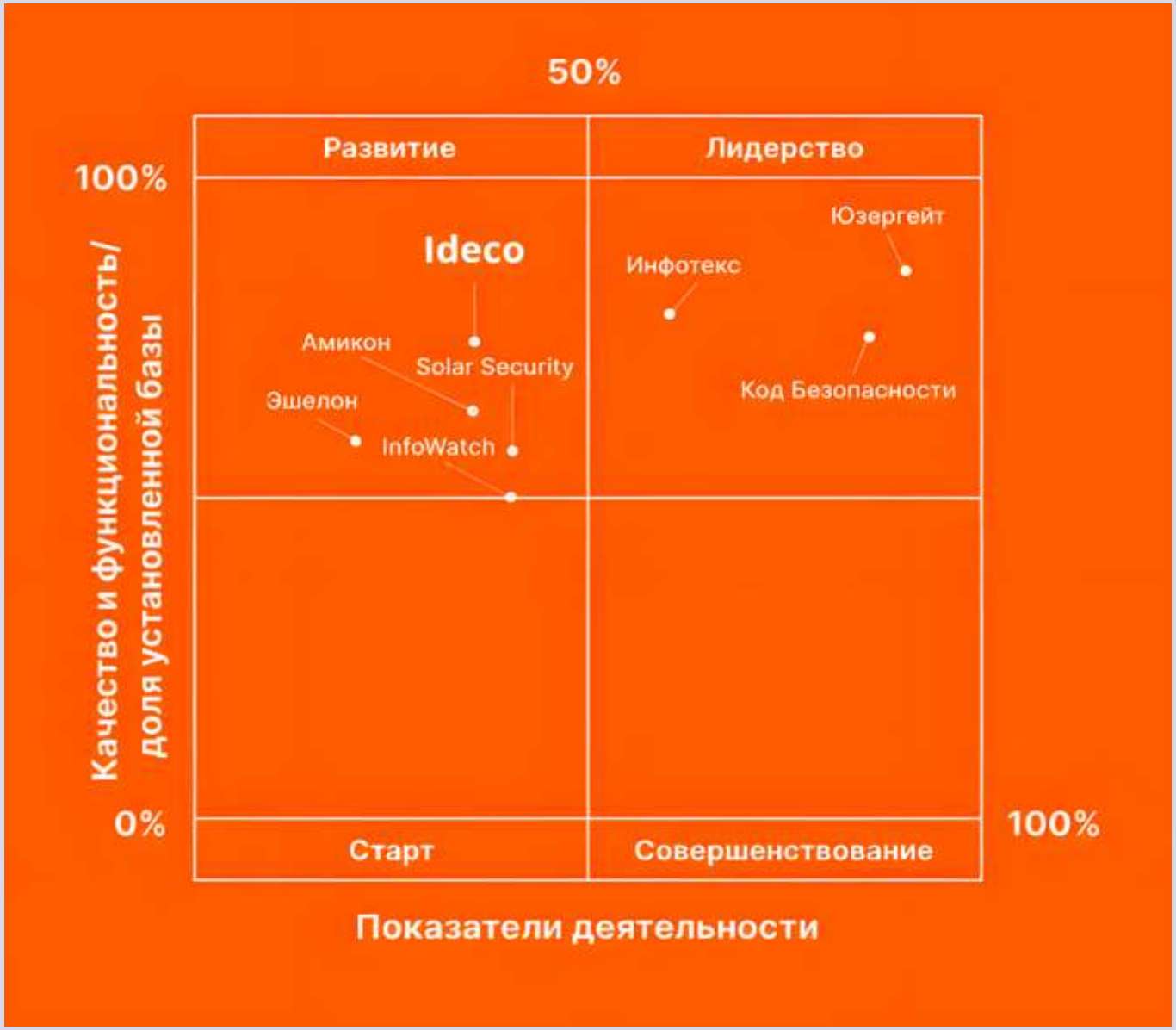
25000
атак блокируются ежедневно

4
мажорных релиза продукта в год

Ideco сегодня — лидер развития

Текущий ландшафт отечественного рынка NGFW предрекает серьезную конкуренцию между поставщиками.

Вендоры из квадранта «Развитие» ничуть не уступают лидерам по качеству решений.



Источник: СТРИМ Консалтинг «Матрица Импортозамещения 2025: Межсетевые экраны следующего поколения (NGFW)»

https://strimconsult.com/matrix-2025-ngfw-continue

Экосистема Ideco

ideco

Для совместимости, удалённого доступа

Windows, macOS, alt linux, РЕДОС, ASTRA LINUX, fedora, ubuntu

Виртуализация / гипервизоры

vmware, Microsoft Hyper-V, KVM, CITRIX XenServer, VirtualBox, PROXMOX

Анализ трафика, правил, IDS/IPS

EFROS, SkyDNS, SURICATA, kaspersky

VPN-совместимость

MikroTik, pfsense, cisco, KerioControl, KEENETIC

Песочницы и антивирусные ядра

kaspersky

Мониторинг, SIEM и комплаенс

ZABBIX, elasticsearch, positive technologies, kaspersky, UDV DATAPK Industrial Kit, SECURITM

Аутентификация и управление доступом

MULTIFACTOR, Active Directory, SAMBA, ALD Pro

4 ключевых решения в продукте

ideco

Защита от атак

DPI, IPS, WAF, DNS Security, антивирус

Сегментация сети

Zone-based FW, OSPF, BGP, PBR, балансировка каналов

Безопасный доступ

IPsec, ZTNA, User Identity, Комплаенс-проверка устройств

Контроль и аудит

Ideco Center, мониторинг и журналирование, интеграция с SIEM

Потребности в NGFW корпоративного уровня

ideco

Сложная инфраструктура

Невозможность кардинально менять сеть: нужен бесшовный переход без переделки архитектуры, с L2-встраиванием и адаптацией под существующие процессы

Высокая нагрузка и требования к отказоустойчивости

Тысячи пользователей, филиалы, удалённые сотрудники — всё это требует производительности, устойчивости и быстрой диагностики инцидентов

Ограниченные ресурсы на администрирование

Не хватает времени и людей на рутину — нужен понятный интерфейс, централизованное управление, стабильность и возможность делегирования

Интеграция с другими системами ИБ

Имеются SIEM, DLP, DevOps-инфраструктура, политики безопасности — важно, чтобы NGFW не был «чёрным ящиком», а легко встраивался и автоматизировался

Изоляция и сегментация

Потребность разделять зоны безопасности, развёртывать пилоты, проводить тесты без влияния на основную сеть — важна поддержка виртуальных контекстов

Причины выбрать **Ideco NGFW Novum**

ideco

Производительность уровня ядра сети

До 200 Гбит/с, 25 млн сессий,
1 млн новых TCP-сессий/сек

Встраивание в инфраструктуру Заказчика

L2-мост позволяет интегрировать NGFW без перестройки сети.
Быстрый старт для пилотов и действующих систем

Виртуальные контексты

Реализация высокопроизводительных сценариев NGFW - мониторинг трафика, VPN, кластеризация, контентная фильтрация

Готовность к нагрузкам корпоративного уровня

Поддержка работы с сотнями тысяч пользователей и групп Active Directory

100 000 правил Firewall

Устойчивость при высоком количестве политик

Возможности Ideco NGFW Novum

ideco

Сетевые службы

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

Фильтрация трафика L7

МЭ, СОВ, Контроль приложений, Контент-фильтр

Мониторинг и отчёты

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

Управление

Веб-интерфейс, SSH, центральная консоль

Маршрутизация

Статическая, динамическая OSPF, BGP

Отказоустойчивость

Кластеризация Active/Passive, резервное копирование, программный Watchdog

Удаленный доступ

Site-to-Site IPsec, IKEv2, SSTP, WireGuard (клиент), L2TP/IPsec

Пользователи

Интеграция с LDAP, авторизация (IP, MAC, Kerberos, Web, Агент, подсеть)

Клиентский путь

1

Знакомство с компанией и продуктом

- Первичный контакт.
- Знакомство с Ideco, вводная информация о компании.
- Демонстрация Ideco NGFW Novum, ключевых сценариев и преимуществ.
- Ответы на организационные и технические вопросы.

2

Пилотное тестирование

- Совместная установочная сессия (ВКС):
  - Анализ текущей инфраструктуры,
  - Выбор формата поставки (ПАК, виртуальный образ),
  - Постановка целей и ПМИ пилота.
- Установка образа или оборудования, базовая настройка политик.
- Поддержка пресейл-инженеров на старте.

3

Анализ результатов пилота

- Клиент оценивает результаты тестирования.
- Сравнение Ideco с другими вендорами.
- Подведение итогов: качество фильтрации, выявленные угрозы, удобство управления.
- Проверка соответствия целям и ПМИ.
- Подготовка сводного заключения.

4

Внедрение и эксплуатация

- Знакомство с выделенным менеджером сопровождения и регистрация на портале технической поддержки.
- Перенос конфигурации из тестовой среды в действующую инфраструктуру.
- Активация коммерческой лицензии.

СБЕР
РЕШЕНИЯ

Комплексные решения по информационной безопасности

СБЕР РЕШЕНИЯ

Лидер в области аутсорсинга бизнес-процессов и ИТ-поддержки*

ideco

СберРешения – высокий уровень развития безопасности ИТ-инфраструктуры и комплексные решения по ИТ и ИБ для вашего бизнеса

№1
* В рейтинге RAEX

30+
Лет на рынке

2020
Старт продаж Комплексных решений по ИТ и ИБ

100+
Реализованных проектов ИТ и ИБ

2
ЦОДа

700+
Виртуальных серверов (uptime)

1000+
АРМ

99,9
Доступность ИТ-сервисов

130
АС

43
АС Business & Mission critical

3500+
Клиентских баз данных

150+
Экспертов ИТ и ИБ

СберРешения:

- Аккредитованная ИТ-компания
- Лицензиат ФСТЭК России
- Лицензиат ФСБ России
- Оператор персональных данных
- Сертифицированы по ISO 27001
- Сертифицированы по ISO 9001

Что мы искали?

- All inclusive из коробки
- Планируемое внедрение
- Российская техподдержка
- Перспективный продукт
- Интеграции в систему эшелонированной защиты

Критерий выбора – эшелонированная защита

Эшелонированная защита (defense in depth)* — наличие множественной защиты, в частности в виде уровней, с целью предотвращения или хотя бы сдерживания атаки

Преимущества

- Снизить риски незаметного прохождения злоумышленником в сеть компании
- Недостаток СЗИ на внешнем уровне может быть компенсирован на более глубоком уровне сети
- Модель безопасности системы сводится к набору уровней, которые определяют также общую защищённость сети

Трудности

- Много различных СЗИ – сложность в администрировании
- Увеличение стоимости владения СЗИ
- Модель безопасности системы сводится к набору уровней, которые определяют также общую защищённость сети

NGFW – эшелон в 1 устройстве: FW + WAF => L7 DPI => Контент Фильтр => AntiVirus for Traffic

* ГОСТ Р 56205-2014 IEC/TS 6244HLP-563353-1-1:2009

Наш путь внедрения

2022

Выбор NGFW

Формирование требований и доработок

Первый пилот IDECO UTM 15

2023

Второй пилот IDECO NGFW 16 с доработкам:

- интеграция с AD
- определение места NGFW в сети

2024

Установка кластера NGFW 16 на наше железо в ЦОД №1

Ввод за NGFW филиалов компании 6 этапов

Первый крупный сбой и формирование новых доработок

2025

Пилот + Продуктив виртуального NGFW 19 кластера в ЦОД №2

Приведение всех NGFW компании к версии 19.5

Пилот IDECO NGFW NOVUM в тестовом контуре

Метрики

Сбор метрик осуществляется в системах SOC и SGRC

SOC

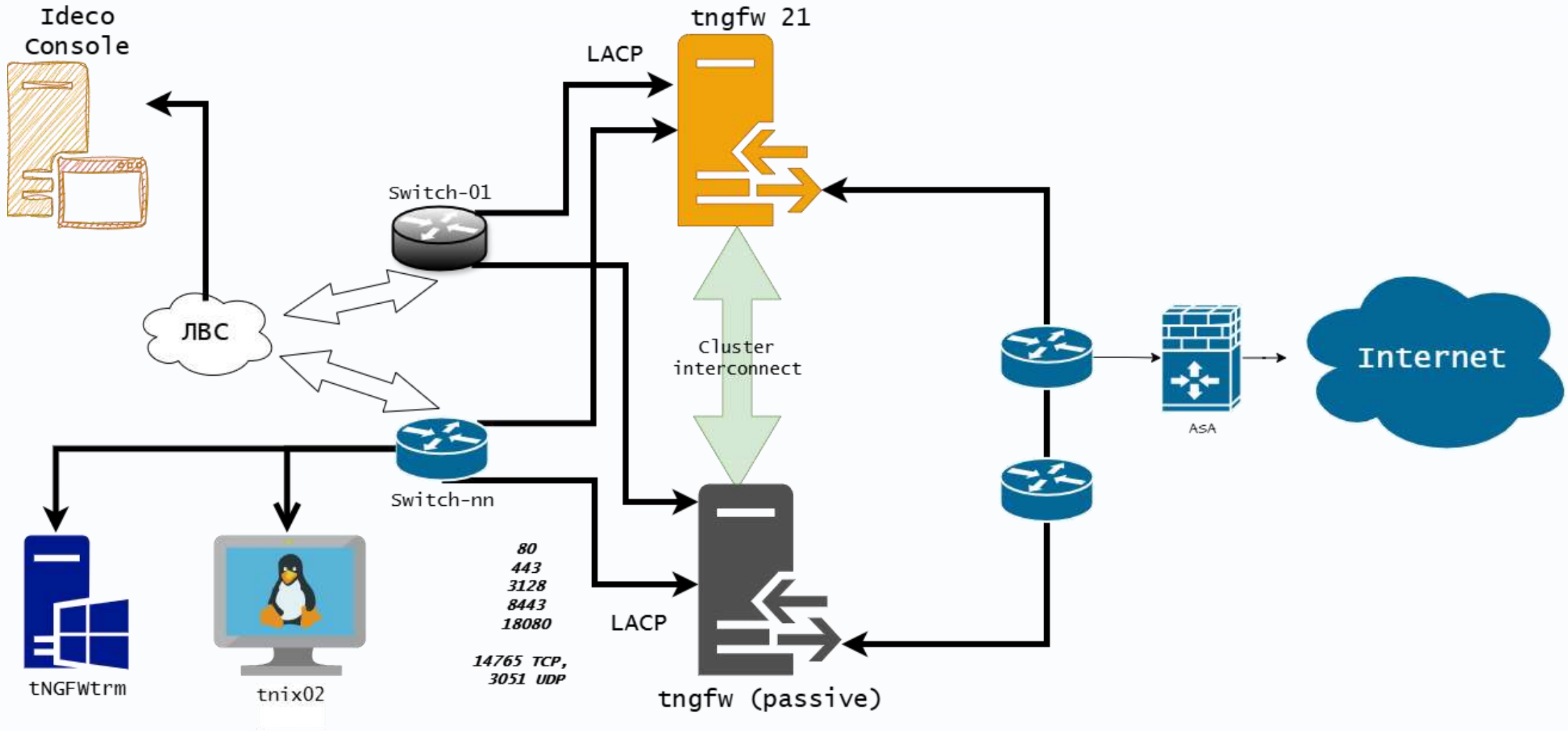
Непрерывный аудит событий СЗИ

- АВПО
- SDM
- DLP
- SCM
- SGRC
- Mail GW
- DCAP
- PAM
- NGFW
- MDM

Результат

- Обогащение данных в инцидентах ИБ в контексте сетевых соединений
- Повышение точности результатов расследования
- Выявление регулярных сетевых инцидентов ИБ
- **Фактический простой за 3 года из-за NGFW - 4 дня**

Схема тестовый контур



К чему пришли?

Done

- Интеграция с AD
- Пул категорийных правил IDS
- L7 DPI
- Shaper
- Кластеризация
- Администраторы из AD

Backlog

- Работа с терминальными серверами на Windows 2022*
- Центральная консоль*
- Распределённый пул узлов
- Георезерв
- LACP на кластерных интерфейсах

Future

- Центральная консоль работающая с разными версиями IDECO
- CLI с функционалом первичной настройки:
  - маршрутизации и сетей
  - интеграции с AD

* В процессе внедрения

СБЕР РЕШЕНИЯ

Благодарю за внимание!
Вопросы?

ДМИТРИЙ ЮЮКИН
Ведущий специалист
Департамента безопасности

dvyuyukin@sber-solutions.ru
+7 99 55 100-179

+7 (495) 660 13 77
sber-solutions.ru