

Практический опыт внедрения NGFW в enterprise

Дмитрий Хомутов, директор Ideco



ideco

Миграция



Проработка плана
миграции



Экспертная тех.
поддержка



Скрипты (в том числе
кастомные)

CheckPoint

Fortigate

Cisco

Kerio

Mikrotik

D-Link

pfSense

и другие

Кейс: Миграция «Петербургского тракторного завода» на Ideco



АО «Петербургский тракторный завод» – производитель тракторов «Кировец», входящий в Группу ПАО «Кировский завод». Лидер в сегменте колесных тракторов



Задача

- ✓ Импортозамещение Kerio Control
- ✓ Защита **1300** пользователей
- ✓ **500** Мбит канал и необходимость расшифровки HTTPS-трафика
- ✓ Решение ограничений Kerio Control (для **>300** пользователей)

Результат

- ✓ Бесшовный переход на решение Ideco
- ✓ Наличие готовых списков интернет-ресурсов ускорили настройку
- ✓ Поддержка оперативно отвечала на возникающие вопросы

Кейс: Замена Cisco ASA в энергетической компании



Крупная энергетическая компания, входящая в многопрофильный холдинг

Задача

- ✓ Замена Cisco ASA на отечественное решение
- ✓ Автоматический перенос настроек
- ✓ Централизованный мониторинг

Результат

- ✓ Бесшовная миграция на решение Ideco с автоматическим переносом конфигурации Cisco
- ✓ Расширенный сервис и централизованное управление, позволяющее в реальном времени отслеживать параметры сети

Кейс: Внедрение в СТД «Петрович»



СТД «Петрович» — один из крупнейших ритейлеров строительных материалов в России

Федеральная сеть филиалов и логистических центров

Основной фокус бизнеса — бесперебойность торговли и обслуживания клиентов

Более **5000** сотрудников

Около **23 000** пользователей инфраструктуры

ПЕТРОВИЧ

Задача

- ✓ Контроль доступа подрядчиков
- ✓ Минимизация риска утечек данных
- ✓ Упрощение администрирования сетевой инфраструктуры
- ✓ Автоматическое реагирование на атаки
- ✓ Соответствие требованиям 152-ФЗ по защите персональных данных

Результат

- ✓ Формат: виртуальный образ
- ✓ Сроки: 1–3 месяца (с учётом миграции ЦОД и кадровых ограничений)
- ✓ Сложность: настройка кластера отказоустойчивости

Кейс: Внедрение Idesco в ГК «Атриум» (Кальдера)



ГК «Атриум» (компания «Кальдера») – предприятие в сфере ТЭК с распределенной инфраструктурой, насчитывающее **180** объектов по всей России. В рамках стратегии импортозамещения и увеличения количества объектов до **300+** к **2026–2027** годам, компании потребовалось модернизировать сеть и обеспечить надежность коммуникаций.



Задача

- ✓ Импортозамещение распределенной инфраструктуры
- ✓ Сертифицированное ФСТЭК решения с поддержкой шифрования IPsec
- ✓ Масштабирование сети и повышение надежности соединений

Результат

- ✓ Развернута и протестирована система на **180** объектах, с планами расширения до **300+**
- ✓ Существенное сокращение необходимости ручного администрирования
- ✓ Надежная и удобная инфраструктура, полностью соответствующая требованиям регуляторов

Кейс: Южно-Уральский государственный медицинский университет



Задача

- ✓ 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!»

Запись вебинара

- академик РАН, Заслуженный врач РФ, главный онколог и радиолог УрФО, и.о. ректора ФГБОУ ВО ЮУГМУ Минздрава России Андрей Владимирович Важенин

Кейс: Департамент информационных технологий и цифрового развития ХМАО



Задача

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.

Кейс: АО «ИК Банк»



Задача

Переход на новый межсетевой экран.

Главные критерии:

- ✓ использование решения отечественного производителя;
- ✓ решение сертифицировано ФСТЭК.

Результат

Осуществлен переход с Fortigate на версию Ideco UTM ФСТЭК. Используется система предотвращения вторжений (IDS/IPS), контроль приложений (DPI), контентная фильтрация веб-трафика (включая HTTPS).

"Отличная техническая поддержка, при необходимости могут подключиться и проконсультировать по возникшему вопросу. Аппаратная платформа Ideco MX со своей задачей справляется претензий по работе и быстрдействию нет"

- Марат Калимов, директор Департамента информационных технологий

Кейс: Создание защищенной сетевой инфраструктуры для крупного российского банка

Крупному коммерческому банку, входящему в ТОП-100 банков России, предоставляющему широкий спектр банковских услуг, необходима система информационной безопасности с высоким уровнем защищенности, которая не допустит появления критических уязвимостей в защите при возникновении новых угроз.

Задача

Главные критерии:

- ✓ защита корпоративной информационной системы от современных угроз;
- ✓ фильтрация и контроль сервисов, приложений и веб-трафика;
- ✓ системы обнаружения и предотвращения вторжений;
- ✓ IPSec-туннели для объединения филиальной сети с возможностью резервирования каналов;
- ✓ удобство пользовательского интерфейса;
- ✓ +централизованное управление и мониторинг.

Результат

В рамках проекта было внедрено комплексное решение Ideco NGFW, создано единое сетевое пространство с централизованным управлением системой.

Были объединены все офисы в единый сетевой контур, в который вошли центральный офис в Москве и 17 региональных офисов. Решение Ideco NGFW позволило обеспечить:

- ✓ высокий уровень сетевой безопасности;
- ✓ оптимизацию систему централизованного управления NGFW;
- ✓ защиту от современных атак и угроз;
- ✓ организовать безопасные способы подключения к удаленным офисам и работу сотрудников с корпоративными ресурсами компании.

Кейс: Построение защищенной сети для российского банка



Российскому коммерческому банку требовалось модернизировать систему обеспечения безопасности корпоративной сети в полном соответствии с требованиями регулятора и внутренними политиками.

Задача

Главные критерии:

- ✓ обеспечение требований со стороны регулятора;
- ✓ защита конфиденциальной информации и персональных данных;
- ✓ круглосуточная техническая поддержка с выделенным каналом связи.

Результат

В результате реализации проекта заказчик получил современное решение, полностью соответствующее требованиям регулятора, обеспечивающее безопасность конфиденциальной информации и персональных данных. Компания Ideco оказывает заказчику премиальную техническую поддержку, включающую предоставление:

- ✓ выделенного инженера ОТП;
- ✓ персонального менеджера отдела продаж;
- ✓ сокращенное время эскалации обращения на вторую линию ТП и в ОРПО;
- ✓ расширенное время работы ОТП, включая 24x7x365;
- ✓ приоритетное планирование расширения функциональности продукта.

Кейс: ФГУП «ПО «Маяк»



Задача

Переход на новый межсетевой экран, новый прокси-сервер.

Главные критерии:

- ✓ удобство пользовательского интерфейса
- ✓ использование решения от одного отечественного производителя во всех филиалах организации.

Результат

Осуществлен переход всех филиалов организации на версию Ideco UTM ФСТЭК. Оперативное решение вопросов заказчика в процессе внедрения и эксплуатации. Удобный и интуитивно понятный интерфейс продукта позволяет оперативно изменять настройки и обновлять данные.

Запись вебинара

Кейс: Энергетическая компания, входящая в крупный многопрофильный холдинг



Задача

- ✓ Замена Cisco ASA на решение отечественного производителя, с возможностью переноса всех настроек
- ✓ Централизованное управление и мониторинг
- ✓ Расширенная гарантия на оборудование

Результат

Произведена бесшовная миграция на межсетевой экран Ideco. При помощи готовых скриптов в автоматическом режиме перенесены все настройки с оборудования Cisco. Заказчику предоставлена расширенная гарантия. Централизованное управление и мониторинг системы позволяют в режиме реального времени отслеживать ключевые параметры сети.

Кейс: Миграция на решение отечественного производителя для крупной нефтесервисной компании



Задача

- ✓ Замена решения зарубежного производителя на отечественное решение, сертифицированное ФСТЭК России
- ✓ Наличие системы обнаружения и предотвращения вторжений
- ✓ Возможность фильтрации и контроля веб-трафика

Результат

В рамках проекта произведена миграция на решение Ideco UTM ФСТЭК, в которое заложен базовый набор функций, включая контроль приложений, систему предотвращения вторжений с расширенными сигнатурами от «Лаборатории Касперского» и веб-фильтрацию. Решение сертифицировано ФСТЭК России, включено в реестр российского ПО (рег. номер ПО № №329 от 08.04.2016).

Кейс: Обеспечение периметра сетевой безопасности для дочерних подразделений нефтегазовой компании



Задача

- ✓ Защита внешнего периметра организации
- ✓ Обнаружение и блокировка атак на веб-приложения и инфраструктуру
- ✓ Соответствие регуляторным требованиям

Результат

В результате проведенного тестирования заказчик выбрал программно-аппаратный комплекс Ideco UTM ФСТЭК, который полностью соответствует требованиям регулятора и обеспечивает:

- ✓ защиту сети от киберугроз;
- ✓ контроль приложений;
- ✓ веб-фильтрацию.

Решение обеспечивает соответствие требованиям регулятора, сертифицировано по требованиям к межсетевым экранам 4-го класса и системам обнаружения вторжений.

Кейс: Федеральный дистрибьютор электротехники «Русский свет»



Задача

- ✓ 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.

Кейс: Обеспечение безопасности сетевого контура для филиалов розничной продовольственной сети

Задача

- ✓ Защита распределенной инфраструктуры от современных киберугроз
- ✓ Централизованное управление и мониторинг
- ✓ Системы обнаружение и предотвращение вторжений
- ✓ Удобство пользовательского интерфейса

Результат

Решение Ideco NGFW объединило все офисы заказчика в единый сетевой контур, в который вошли 18 розничных магазинов сети.

Удобство настройки и интеграции системы позволило специалистам заказчика самостоятельно развернуть решение в кратчайшие сроки.

Решение Ideco NGFW позволило заказчику повысить уровень сетевой безопасности и оптимизировать систему централизованного управления межсетевыми экранами нового поколения, а включенные и настроенные модули безопасности позволили защититься от современных атак и угроз, организовать безопасные способы подключения к удаленным филиалам.

Кейс: Создание защищенной сетевой инфраструктуры для розничной торговой компании

Задача

- ✓ Решение для обеспечения защиты сети для распределенных филиалов
- ✓ Системы обнаружение и предотвращение вторжений
- ✓ Централизованное управление и мониторинг

Результат

По итогам тестирования заказчиком выбрано решение Ideco NGFW.

Решение включает в себя межсетевой экран с расширенными настройками, систему обнаружения и предотвращения вторжений, защиту от скачивания вредоносных программ и приложений, контентную фильтрацию.

Ideco NGFW позволяет управлять всей инфраструктурой из единой точки и имеет функцию предоставления защищенного удаленного доступа к корпоративным ресурсам.

Кейс: Сеть медицинских центров города Москвы



Задача

Замена решения иностранного производителя на отечественное решение, с возможностью переноса всех настроек

- ✓ Наличие системы обнаружения и предотвращения вторжений,
- ✓ Возможность фильтрации и контроля веб-трафика,
- ✓ Соответствие регуляторным требованиям

Один из ключевых факторов быстрая и качественная техническая поддержка.

Результат

В рамках проекта произведена миграция на решение Ideco UTM ФСТЭК, в которое заложен базовый набор функций, включая систему предотвращения вторжений с расширенными сигнатурами от «Лаборатории Касперского», контроль приложений и веб-фильтрацию. Решение сертифицировано ФСТЭК России, включено в реестр российского ПО (рег. номер ПО № №329 от 08.04.2016).

Кейс: Сеть стоматологических клиник

Задача

- ✓ Защита внешнего периметра организации
- ✓ Обнаружение и блокировка атак на веб-приложения и инфраструктуру
- ✓ Соответствие регуляторным требованиям

Результат

В результате проведенного тестирования заказчик выбрал программно-аппаратный комплекс Ideco UTM ФСТЭК, который полностью соответствует требованиям регулятора и обеспечивает:

- ✓ защиту сети от киберугроз;
- ✓ контроль приложений;
- ✓ веб-фильтрацию.

Решение обеспечивает соответствие требованиям регулятора, сертифицировано по требованиям к межсетевым экранам 4-го класса и системам обнаружения вторжений.

*«Система настолько стабильна,
что нам практически не
приходится в нее заходить.*

*Можно сказать, что забыли
пароль — все работало без
сбоев, и не было
необходимости что-то
исправлять».*