ideco

Роль NGFW в промышленности

Дмитрий Хомутов
директор Ideco

Вызовы и риски

Атаки, направленные на подрыв процесса производства, могут нанести не только финансовый и материальный, но и экологический ущерб

Риски кибербезопасности

- Риск компрометации конфиденциальных данных, в том числе технологических процессов, чертежей, персональных данных сотрудников.
- Необходимость разграничения прав доступа пользователей к определенным ресурсам.
- Кибератаки, направленные на дестабилизацию инфраструктуры, подрыв процесса производства.
- Кибершпионаж

52% промышленных предприятий в 2024 году столкнулись с утечкой информации (в 2023 г.—60%)*

40% Субъектов КИИ остаются незащищенными**

* Отчет Отчет ГК Солар, 2025
** Отчет СерчИнформ, 2025

ИБ-инциденты в промышленности. Кейс №1

Атака шифровальщиков на промышленное предприятие в России (2024)

Последствия

- Простой производственных мощностей на 48 часов.
- Ущерб оценивается в миллионы рублей.
- Репутационные потери, необходимость дополнительных инвестиций в киберзащиту.

Крупное российское металлургическое предприятие подверглось атаке шифровальщиков, что привело к остановке конвейеров и значительным финансовым потерям. Вредоносное ПО проникло через уязвимость в удалённом доступе сотрудников.

Источник: Коммерсант

Разбор случаев и меры NGFW для предотвращения инцидентов. Кейс №1

ideco

Ответ NGFW на атаку шифровальщика:

Контроль и ограничение удалённого доступа

NGFW позволяет блокировать подозрительные соединения и применять строгую аутентификацию (MFA, VPN).

Анализ трафика и предотвращение атак (IPS)

NGFW способен выявлять и блокировать попытки эксплуатации уязвимостей, через которые распространяются шифровальщики.

Фильтрация вредоносного контента

Защита от вредоносных вложений в почте и скачиваемых файлов через контентную фильтрацию.

ИБ-инциденты в промышленности. Кейс №2

Утечка данных на заводе электроники в Казахстане (2023)

Последствия

- Продажа данных конкурентам.
- Риск компрометации технологий и интеллектуальной собственности.
- Финансовые и регуляторные штрафы.

На одном из ведущих заводов по производству электроники в Казахстане произошла утечка конфиденциальных данных. Причина – незащищённые API-интерфейсы, через которые злоумышленники получили доступ к чертежам и технологической документации.

Источник: Tengrinews

Разбор случаев и меры NGFW для предотвращения инцидентов. Кейс №2

ideco

Ответ NGFW на риск утечки данных через уязвимость API:

Межсетевая сегментация

Разграничение доступа к внутренним ресурсам, предотвращение несанкционированного обращения к API.

Контроль трафика на уровне приложений (L7)

NGFW позволяет отслеживать аномальные запросы к API, блокировать попытки утечек данных.

SSL-инспекция

Анализ зашифрованного трафика на предмет подозрительных запросов и атак.

ИБ-инциденты в промышленности. Кейс №3

DDoS-атака на системы управления нефтеперерабатывающего завода в Беларуси (2023)

Последствия

- Временный выход из строя SCADA-систем, управляющих оборудованием.
- Замедление производственных процессов.
- Потенциальные угрозы для безопасности сотрудников и экологии.

Массированная DDoS-атака на системы управления технологическими процессами нефтеперерабатывающего завода вызвала перебои в работе автоматизированных систем.

Источник: Tut.by

Разбор случаев и меры NGFW для предотвращения инцидентов. Кейс №3

ideco

Ответ NGFW на атаку:

Фильтрация и ограничение вредоносного трафика

Защита от DoS-атак с помощью ограничений по количеству соединений с одного источника.

Контроль доступа на уровне приложений (L7)

Возможность блокировки подозрительных IP-адресов и ограничение доступа к критически важным сервисам.

Мониторинг аномальной активности

Выявление резкого роста количества запросов и их автоматическая блокировка на уровне брандмауэра.

Интеграция с SIEM-системами

Передача логов активности для оперативного анализа угроз и корреляции событий.

Задачи и решения

Обнаружение и реагирование

- **Задача:** Мониторинг аномальной активности → **Решение:** Сканер выявляет подозрительные действия в сети.
- **Задача:** Предотвращение атак → **Решение:** IPS блокирует вторжения и эксплуатацию уязвимостей.
- **Задача:** Блокировка подозрительных соединений → **Решение:** Контроль приложений анализирует трафик и отключает вредоносные сессии.

Продвинутая защита от угроз

- **Задача:** Фишинг и вредоносные сайты → **Решение:** Контентная фильтрация блокирует угрозы и анонимайзеры.
- **Задача:** Скрытые атаки в HTTPS-трафике → **Решение:** Инспекция SSL выявляет угрозы в зашифрованных соединениях.
- **Задача:** Ботнеты и зараженные устройства → **Решение:** Автоблокировка сетей ботнетов предотвращает атаки.

Стабильность сети

- **Задача:** Перегрузка трафика внутри сети → **Решение:** Балансировка и резервирование каналов обеспечивают бесперебойную связь.
- **Задача:** Надежный удаленный доступ → **Решение:** VPN (IKEv2/IPsec, SSTP, L2TP/IPSec) защищает соединения.
- **Задача:** Отказ сети из-за сбоев → **Решение:** Работа с кластером отказоустойчивости предотвращает простои.

Контроль и управление

- **Задача:** Сложность мониторинга угроз → **Решение:** Интеграция с SIEM передает логи в единый центр безопасности.
- **Задача:** Неавторизованный доступ → **Решение:** Active Directory ограничивает доступ по корпоративным политикам.
- **Задача:** Оперативное сопровождение → **Решение:** 3 уровня технической поддержки, 5 каналов связи, 2 уровня SLA.

Кейс: Миграция «Петербургского тракторного завода» на Ideco UTM

О клиенте

АО «Петербургский тракторный завод» – производитель тракторов «Кировец», входящий в Группу ПАО «Кировский завод». Лидер в сегменте колесных тракторов мощностью от 250 л.с., производит 8 моделей К-7М и 17 видов спецтехники.

Задача

Миграция с Kerio Control на российское решение Ideco UTM. Учитывались 1300 пользователей, 500 Мбит канал и необходимость расшифровки HTTPS-трафика (проблема у Kerio Control начиналась с 300 пользователей).

Результат

Бесшовный переход на Ideco UTM, обеспечен импортозамещение. Решение отличилось готовыми списками интернет-ресурсов, ускоряющими настройку. Поддержка оперативно решала возникающие вопросы.

Кейс: Внедрение Ideco UTM в ФГУП «ПО Маяк»

О клиенте

ФГУП «ПО Маяк» – стратегическое предприятие атомной промышленности России.

Задачи

- Переход на новый межсетевой экран и прокси-сервер
- Удобный интерфейс для администрирования
- Унифицированное решение для всех филиалов

Результат

Все филиалы переведены на Ideco UTM ФСТЭК. Продукт обеспечивает централизованное управление, интуитивно понятный интерфейс и оперативное решение вопросов.

Кейс: Замена Cisco ASA в энергетической компании

О клиенте

Крупная энергетическая компания, входящая в многопрофильный холдинг.

Задачи

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

Результат

Бесшовная миграция на Ideco UTM
с автоматическим переносом конфигурации Cisco.
Обеспечен расширенный сервис
и централизованное управление, позволяющее
в реальном времени отслеживать параметры сети.

Кейс: Миграция нефтесервисной компании на отечественное решение

О клиенте

Крупная нефтесервисная компания.

Задачи

- Замена иностранного решения на сертифицированное ФСТЭК
- Обнаружение и предотвращение вторжений
- Фильтрация и контроль веб-трафика

Результат

Миграция на Ideco UTM ФСТЭК с интегрированной системой предотвращения вторжений от «Лаборатории Касперского» и веб-фильтрацией. Решение включено в реестр российского ПО.

Кейс: Обеспечение безопасности дочерних подразделений нефтегазовой компании

О клиенте

Дочерние подразделения нефтегазовой компании.

Задачи

- Защита внешнего периметра
- Блокировка атак на веб-приложения
- Соответствие регуляторным требованиям

Результат

Выбрано решение Ideco UTM ФСТЭК, обеспечивающее защиту от киберугроз, контроль приложений и веб-фильтрацию. Решение сертифицировано по требованиям к межсетевым экранам 4-го класса и системам обнаружения вторжений.

Компания Ideco повышает уровень кибербезопасности

Защищаем ваш бизнес от современных угроз с помощью
высокопроизводительного и функционального продукта Ideco NGFW*

20+
лет на рынке

5 500+
компаний под защитой

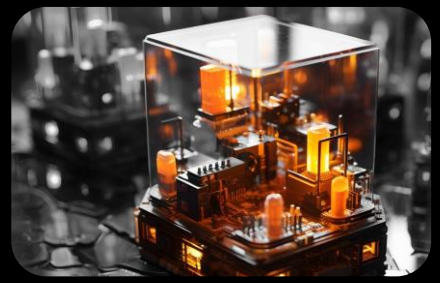
25 000+
атак блокируем ежедневно

* Межсетевой экран нового поколения

Оперативный цикл разработки и дополнения функциональности продукта

Высокий уровень сервиса от первой коммуникации и на всем протяжении взаимодействия

Приоритет на задачах заказчика для максимального соответствия запросам рынка



Выстраивание экосистемы через увеличение количества технологических интеграций с российскими производителями ИБ решений

Защищаем крупные компании

ideco

Газпром Межрегионгаз Вологда

Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Станкин Московский Государственный Технологический Университет

ВятГУ

Ростелеком

Энергия

РЖД

ЕСЛИ ОБУВЬ, ТО kari

SCAT AIRLINES

Русский Свет®

ideco СОЗДАЕМ ВМЕСТЕ

8 800 555 33 40
sales@ideco.ru
ideco.ru