NGFW: МЕЖСЕТЕВЫЕ ЭКРАНЫ НОВОГО ПОКОЛЕНИЯ

СТАТИСТИКА

66%

вредоносного ПО
устанавливается из файлов,
прикрепленных к письмам

43%

атак происходит
с использованием
социальной инженерии

73%

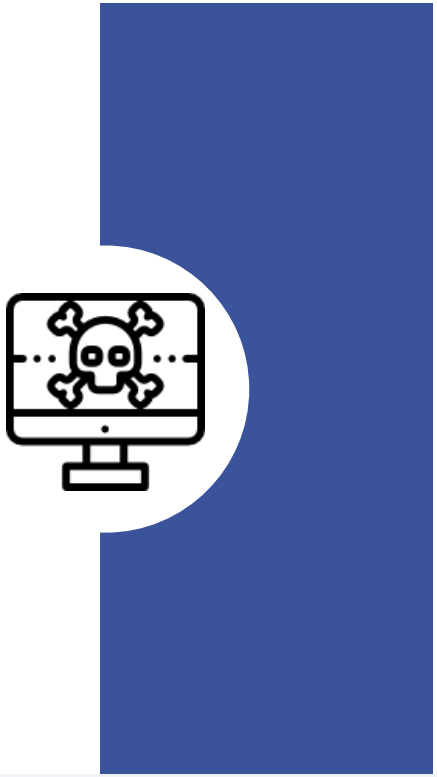
проникновений
финансово мотивированы

75%

проникновений
совершаются извне

**по данным Data Breach Investigations Report 2017*

ТЕНДЕНЦИИ КИБЕРАТАК



Изменчивость: все время появляются новые

Индивидуальный подход: вредоносы создаются «под жертву»

Человеческий фактор: использование социальной инженерии, включая фишинг

Зашифрованный трафик: не все средства ИБ могут обнаружить угрозы

Атаки через приложения, включая облачные

Как противостоять современным угрозам?

Интегрировать традиционные инструменты с другими системами, выстраивать процессы реагирования

ЦЕЛИ И РЕЗУЛЬТАТЫ NGFW

Повысить уровень защищенности по сравнению с классическим МСЭ

Получить больший контроль над сетевым трафиком на уровне приложений

Снижение рисков безопасности и комплаенс-рисков

Операционная эффективность отдела ИБ

Упрощенное управление МСЭ

Высокая отказоустойчивость МСЭ за счёт кластеризации

Точное понимание потоков трафика

Легко расширяемый набор функций без замены оборудования

ТРАДИЦИОННЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ

TRADITIONAL FIREWALL VS NGFW

ТРАДИЦИОННЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ

Контролируют входящий и исходящий трафик на основе сконфигурированных правил

Поддерживают VPN

NGFW (NEXT GENERATION FIREWALL)

Все функции традиционных МСЭ

Интегрированная система предотвращения вторжений (IPS)

Расширенная защита от угроз (ATP)

Управление приложениями

Веб-фильтрация

Антивирус и антиспам

Песочница (опционально)

Обычные межсетевые экраны не видят угроз: большинство атак идет через разрешенные сетевые подключения (http, smtp, tcp и др.)

ПЕСОЧНИЦА: ЕЩЕ ОДИН УРОВЕНЬ ЗАЩИТЫ

К NGFW можно подключить песочницу (локально или в облаке) и проверять подозрительные файлы, чтобы защититься от целевых кибератак (APT)

ЭТАПЫ РАБОТЫ С ФАЙЛАМИ

ОТКРЫТЬ ФАЙЛ В БЕЗОПАСНОЙ СРЕДЕ

ОТСЛЕДИТЬ АКТИВНОСТЬ (ИЗМЕНЕНИЯ В РЕЕСТРЕ, ЗАПУСК СИСТЕМНЫХ ПРОЦЕССОВ И Т.Д.)

ЗАБЛОКИРОВАТЬ ИЛИ ДОПУСТИТЬ К ИСПОЛЬЗОВАНИЮ

МИФЫ И ЗАБЛУЖДЕНИЯ

У нас уже есть межсетевой экран, NGFW нам не нужен

Современная практика показывает, что блокировки на уровне протоколов и портов недостаточно. Портовые сканнеры легко обходятся, туннелирование и шифрование – за пределами действия обычного межсетевого экрана.

Антивирус нам поможет и заблокирует угрозы

Обычные антивирусы не справляются с изменчивостью вирусов и потоком свыше 10Гбит/сек. И реагируют не сразу: шифровальщики успеют зашифровать данные. Нужны и другие средства защиты, например, песочница.

Мы надежно защищаем периметр, враг не пройдет

Пользователи перемещаются, атака может идти через облачные приложения или анонимайзеры, через вложения в почте или мессенджерах, полученные даже от коллег. Трафик надо проверять в песочнице, чтобы уберечься от целевых атак.

ВАРИАНТЫ ВНЕДРЕНИЯ NGFW

ФИЗИЧЕСКОЕ УСТРОЙСТВО

Поставка сервера
от вендора
с установленным
и настроенным ПО

ВИРТУАЛЬНОЕ УСТРОЙСТВО

Установка и настройка
ПО на сервере заказчика

ПОДКЛЮЧЕНИЕ К ОБЛАЧНОМУ СЕРВИСУ

Направление данных
на NGFW-сервер
через защищенный
канал связи

ПРИМЕР ПРОЕКТА ПО ВНЕДРЕНИЮ

КОМПАНИЯ «А»

20000 сотрудников

23 устройства Palo Alto Networks

суммарная пропускная способность внешних каналов – больше 1 Гбит/сек

СРОКИ:

6 месяцев

РЕЗУЛЬТАТЫ:

миграция со старых решений без влияния на работу компании

сопровождение в период объединения компаний (включая унификацию политик)

успешная интеграция с песочницей стороннего вендора (FireEye)

встраивание в процессы центра мониторинга и реагирования на инциденты ИБ (SOC)

НАШИ ПРЕИМУЩЕСТВА

Опыт реализации проектов NGFW в крупных организациях (свыше 10000 пользователей)

Награда в престижной номинации «Проект года 2017» на саммите Palo Alto Networks

Профильные сертифицированные инженеры с многолетним опытом работы с NGFW

gk-is.ru