ИнфоТеКС: в разработке NGFW у нас свой путь

Алексей Данилов, *руководитель продуктового направления компании "ИнфоТеКС"*

Фото: ИнфоТеКС

Ожидание от импортозамещения NGFW — час-два на перенос настроек и готово. При этом замена иностранного оборудования на российское не прерывает технологические процессы в ИТ-инфраструктуре, а после замены все продолжает работать как прежде, а единственным изменением становится новый логотип на оборудовании и в интерфейсе консоли управления.

Такая иллюзия становится причиной глубокого разочарования, когда реальность вступает в противоречие с ожиданиями. Многие заказчики не могут найти достойной замены используемым решениям на российском рынке.

Возьмем FortiGate NGFW. На сегодняшний день ни одно российское и ни одно зарубежное решение не способны воспроизвести его главную конкурентную характеристику – высокую скорость обработки сетевого трафика. Секрет кроется в специально разработанных микросхемах, поэтому если заказчик выбрал для решения своих задач FortiGate, то подобрать идентичное по производительности решение даже среди зарубежных будет крайне сложно.

Ожидания заказчиков понятны: хочется, чтобы решение работало сразу – без проволочек и сложных компромиссов. В приоритете зачастую стабильность и предсказуемость работы NGFW при выполнении основных функций сетевой безопасности, то есть непосредственно защиты. Это основная задача при создании межсетевого экрана следующего поколения в ИнфоТеКС. Наличие дополнительных функциональных характеристик важно, но не первостепенно, при отсутствии стабильности в работе базовых модулей использование такого NGFW становится проблемой для ИБ-служб.

Процесс создания продуктов класса NGFW в ИнфоТеКС включает в себя лучшие практики разработки, которые накопились в активе компании за долгие годы работы с сетевыми фильтрами, VPN-шлюзами, системами обнаружения и предотвращения вторжений. Однако мы не ограничились простым объединением этих технологий – каждая из них была переосмыслена, переработана и включена в единую, логически целостную платформу.

Принципиальный подход заключается в том, чтобы изначально проектировать полнофункциональный продукт нового поколения, а не просто собирать набор существующих сервисов под одной оболочкой. Ведь технически объединить модули не представляет особой сложности – такой прототип можно собрать за несколько недель. Истинная ценность решения проявляется тогда, когда его компоненты взаимодействуют между собой слаженно, усиливая друг друга и создавая надежную и гибкую защиту.

Два ответа на разные вызовы

В ИнфоТеКС параллельно развиваются две самостоятельные продуктовые линейки межсетевых экранов следующего поколения: ViPNet Coordinator HW[1] и ViPNet xFirewall[2]. Каждая из них создается с учетом специфических задач и требований различных заказчиков, а не как вариация единой универсальной платформы.

ViPNet xFirewall 5 – это классический межсетевой экран следующего поколения, созданный для сценариев, где нет необходимости использования VPN с отечественными криптографическими алгоритмами. Он включает в себя весь необходимый функционал для защиты инфраструктуры на современном уровне, обеспечивая высокую производительность, гибкость настройки и интеграцию с внешними системами.

В этом году мы готовим выпуск шестого поколения ViPNet xFirewall, развивающего данный подход в том числе автономными сценариями использования отдельных NGFW.

ViPNet Coordinator HW 5, напротив, с самого начала разрабатывался как специализированное решение для построения защищенных сетей на базе ГОСТ-криптографии. В 2024 г. пятое поколение платформы прошло сертификацию ФСБ России и при наличии действующего сертификата ФСТЭК России стало единственным предложением на рынке, сочетающим статус сертифицированного межсетевого экрана с полноценной криптографической защитой по национальным стандартам.

Важная особенность ViPNet Coordinator HW 5 – в его способности сочетать основные функции NGFW с поддержкой ресурсоемких криптографических алгоритмов. ГОСТ-криптография предъявляет серьезные требования к вычислительным мощностям, а зарубежная микроэлектроника, к сожалению, не оптимизирована под подобные операции. Мы поэтапно внедряем собственные

Рис. 1. Внешний вид ViPNet xFirewall 5

[1] *https://infotecs.ru/products/vipnet-coordinator-hw-5/*
[2] *https://infotecs.ru/products/vipnet-xfirewall-5/*

решения для сохранения оптимального баланса между производительностью, функциональностью и соответствием требованиям безопасности.

С точки зрения позиционирования на рынке ViPNet Coordinator HW 5 и ViPNet xFirewall 5 не конкурируют друг с другом, а органично дополняют портфель решений. У каждого продукта свой потребитель.

В основе цикла развития наших NGFW – револьверная модель, предполагающая постепенное развитие функциональности продуктов небольшими итерациями. В ViPNet xFirewall отсутствует VPN-блок с ГОСТ-криптографией, поэтому инновации здесь внедряются и обкатываются быстрее, а полученные наработки затем адаптируются для ViPNet Coordinator HW 5, с учетом дополнительных требований – от аппаратной поддержки до прохождения сложных процедур сертификации. При этом нельзя сказать, что какой-либо из продуктов является донором для другого, развитие происходит параллельно и непрерывно.

Ловушка экосистемности

Рынок информационной безопасности движется в сторону экосистемности. У многих вендоров уже выстроена целая линейка взаимодополняющих продуктов, хотя чрезмерная завязанность на экосистему одного вендора может стать ловушкой. Достаточно взглянуть на пример с популярными зарубежными ИБ-брендами, чьи российские пользователи в 2022 г. оказались в затруднительном положении, – необходимо было поменять не просто один продукт, а целую систему. Это выглядит как парадокс: стремление к унификации оборачивается новой зависимостью.

Как найти баланс между парком инструментов и глубоким погружением в моновендорную экосистему?

Баланса как такового нет. Есть конкретный заказчик со своей инфраструктурой, бюджетом, штатом и приоритетами.

Кто-то, как представители крупных организаций, прямо говорят: нашей службе эксплуатации важна стабильность. Если продукт удобен и надежен, нам не важно, чей он. У таких заказчиков решения выстраиваются вокруг одного продукта: централизованное управление, развитые механизмы корреляции, SIEM, ретроспектива, инцидент-менеджмент. Это полноценная экосистема, которую, при необходимости, можно дополнить внешними компонентами.

В другом лагере те, кто принципиально не готов быть заложником одного вендора. Часто они опираются на собственные системы оркестрации, в которые легко подключаются новые решения – через коннекторы, без переучивания персонала и смены логики. Это путь гибкости, но он требует достаточно высокого уровня зрелости и вовлеченности со стороны заказчика.

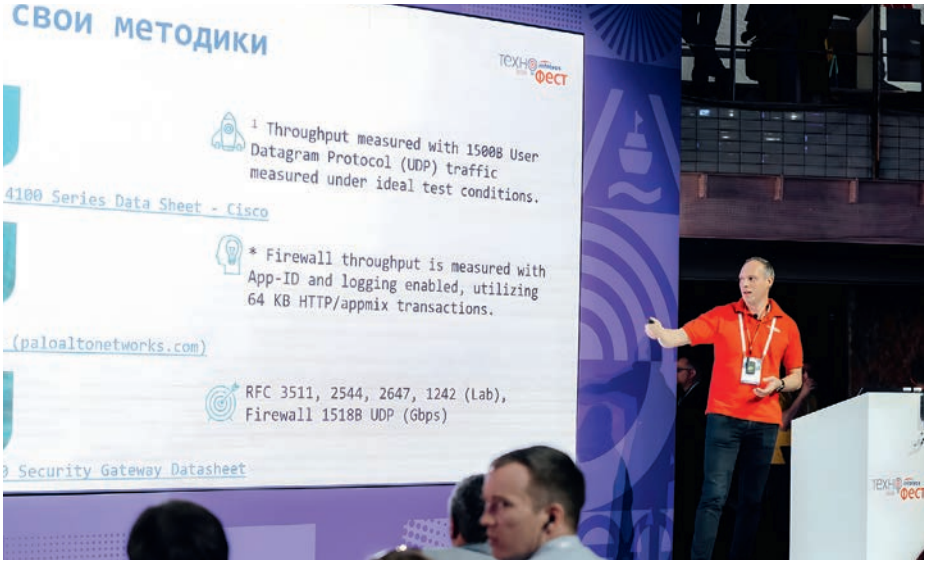

Рис. 2. Выступление на "ИнфоТеКС ТехноФест"

Каждый выбирает свою стратегию: кто-то – экосистему, кто-то – независимость. А задача производителей – быть готовыми ко всем этим сценариям. Именно поэтому сегодня все чаще звучит не просто "у нас есть своя экосистема", а "мы готовы быть частью вашей экосистемы".

Вектор развития NGFW в России

Когда компания "ИнфоТеКС" начала разработку собственных NGFW, мы решили не изобретать заново то, что уже хорошо сделано другими. Мы с самого начала старались выстраивать взаимодействие с внешними поставщиками и партнерскими компаниями. Например, в сфере антивирусной защиты в нашей стране есть достойные решения, и было логично интегрировать именно их, не создавая собственный антивирус с нуля. Отсутствующие в России технологии подбирались из числа иностранных.

Наша компания уже в 2017–2018 гг. ощутила влияние санкций и научилась в этих условиях расти и развиваться, а события 2022 г. глобально изменили правила игры для всей отрасли ИТ и ИБ. Многие международные коллеги прекратили сотрудничество, что вынудило нас, как и других российских разработчиков, пересмотреть список технологических партнеров и свои дорожные карты. Теперь мы собственными модулями закрываем те участки, где раньше полагались на западные технологии, и усилили взаимодействие с другими российскими вендорами: DPI, антивирусы, аппаратные компоненты, включая процессоры и специализированные сетевые карты.

Интероперабельность предполагает совместимость с внешними SIEM- и SOAR-системами, с аналитическими платформами и т.д. Мы учим наши решения "разговаривать" с популярными у заказчиков продуктами других производителей и быть с ними по-настоящему совместимыми.

Планируя развитие нашего NGFW на ближайшие 5 лет, мы не стремимся слепо копировать нынешние возможности глобальных вендоров. Мы выстраиваем развитие не по чужим лекалам, а исходя из собственного понимания – куда должен прийти продукт, чтобы оставаться актуальным и нужным. Это требует визионерского взгляда: нужно не просто закрывать тикеты из бэклога, а видеть, каким должно быть решение в будущем, и осмысленно к нему идти.

Путь компании "ИнфоТеКС" – это развитие NGFW как части широкой, гибкой и разноплановой адаптивной системы информационной безопасности. Мы будем усиливать собственные функциональные модули, искать и интегрировать лучшие внешние решения. Продукты сетевой безопасности, VPN-клиенты, системы обнаружения вторжений, защита конечных точек, искусственный интеллект, работающий с телеметрией и инцидентами, – все это уже сегодня формирует сквозную архитектуру. Заказчик может использовать весь комплекс или выбрать отдельные компоненты. Наш NGFW прямо сейчас становится более умным, быстрым, гибким и открытым ко всему, что помогает лучше защищать. И мы продолжим двигаться в этом направлении.

Компания "ИнфоТеКС" продолжает развивать NGFW, используя достижения современной микроэлектроники. Мы стремимся к росту производительности и надежности выполнения базовых функций безопасности, потому что именно эти качества, а не номинальное обилие функций являются решающими для заказчиков, принимающих решения по обеспечению информационной безопасности в своей ИТ-инфраструктуре.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru