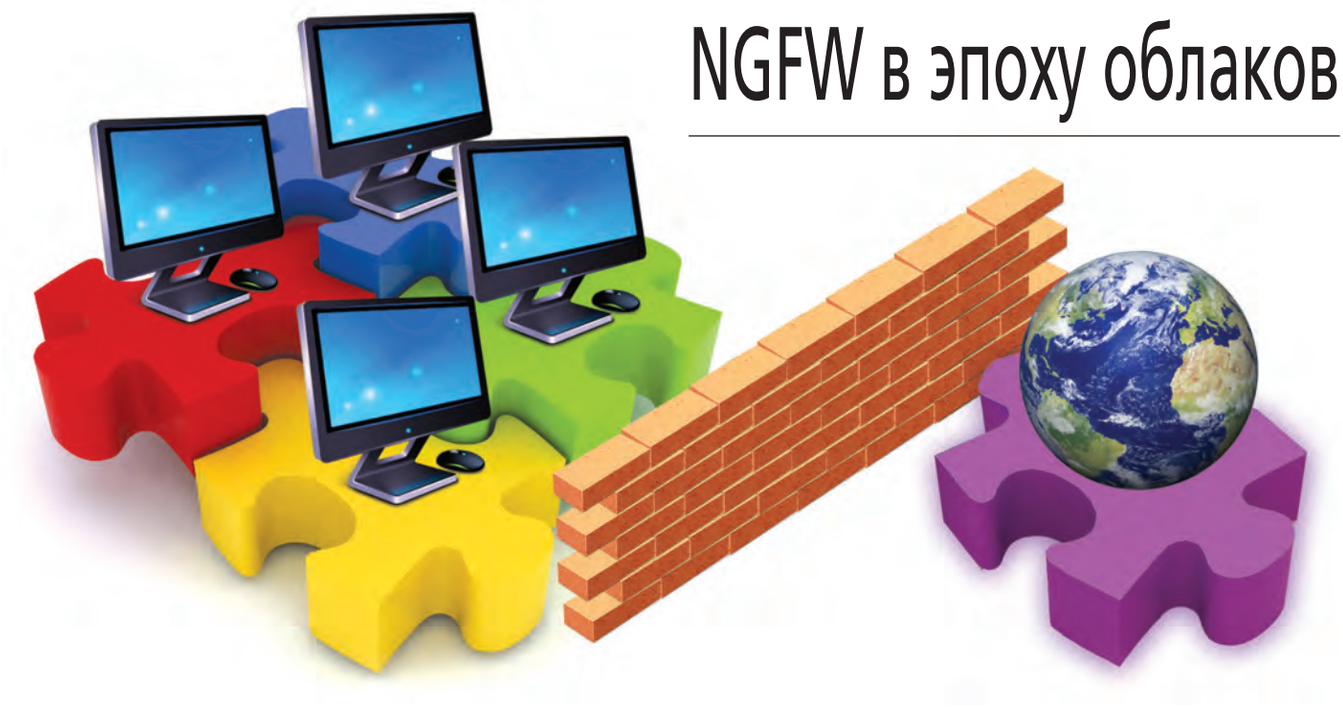
Когда рушатся стены:

NGFW в эпоху облаков



Межсетевой экран уже объявляли мертвым, но эти слухи пока не подтверждаются.

Межсетевые экраны следующего поколения (NGFW) объединяют в себе целый ряд функций защиты (антивирус, антиспам, предотвращение вторжений, веб-фильтр, проверка шифрованного трафика и т.д.). Эти устройства, в комплексе с другими системами безопасности, призваны дать бой сложным многовекторным атакам. В последнее время NGFW все чаще используются в облачной версии.

«СиБ» выяснил, как менялись технологии за последние годы, что появилось у производителей систем защиты нового поколения в 2018 году и какая продукция представлена в Украине.

Каждый межсетевой экран — это NGFW

Традиционно начнем обзор с оценок мирового рынка и международных рейтингов. Согласно отчету ***Markets&Markets***, рынок увеличится с $2,39 млрд в 2017 году до $4,27 млрд в 2022-м при среднем росте на уровне 12,3% в год. ***Gartner*** в прошлогоднем отчете о межсетевых экранах корпоративного класса приводит такие цифры: в 2018 году размер рынка оценивался на уровне $11,32 млрд, прогноз на 2022 год составлял $14,5 млрд, причем темпы роста замедляются, что свидетельствует о насыщении спроса.

Летом прошлого года ***NSS Labs*** опубликовала результаты исследования, в ходе которого продукты десяти компаний оценивались по критериям эффективности защиты, производительности и совокупной стоимости владения. Из них шесть продемонстрировали устойчивость к распространенным технологиям маскировки атак (evasion), остальные четыре не смогли распознать как минимум одну технологию маскировки. По эффективности защиты первое место занял ***Forcepoint NGFW 2105 Appliance***, лишь немного ему уступил ***Fortinet FortiGate 500E***, у которого оказалась самая низкая стоимость владения. Также в категорию NGFW со стопроцентным распознаванием замаскированных атак отнесены продукты ***Palo Alto***, ***SonicWall***, ***Barracuda*** и ***Versa Networks***.

Дополнительно в этот раз проверялась устойчивость защиты от модифицированных эксплойтов (вредоносного кода, использующего уязвимости в ПО). Под устойчивостью понимается способность NGFW обнаруживать и блокировать различные варианты атаки. Из исследуемых продуктов ни один не продемонстрировал полной устойчивости. Также в программу были включены атаки, использующие JavaScript и технологии обфускации, или запутывания кода. NGFW не смогли декодировать JavaScript, вместо этого все они пытались детектировать распространенные средства запутывания, используя сигнатурный анализ. Исследование показало, что обфускация сокращает эффективность детектирования злонамеренной деятельности на 34%, причем некоторые продукты пропустили вплоть до 60% атак, запутанных при помощи средств JavaScript. Кроме того,

Таблица 1. Основные производители систем NGFW и их украинские партнеры в 2018 году

Производитель	Штаб-квартира	Представительство в Украине	Дистрибьюторы	Партнеры	
				Название компании	Статус
Check Point	Израиль	+	МУК, RRC	Infosafe, Svit IT, ИТ Платформа	Check Point Star Partner *** (наивысший)
				14 компаний	Check Point Star Partner **
Cisco	США	+	ERC, Мегатрейд, МУК	S&T Ukraine, AM-BITS, ИТ-Интегратор	Gold
				SI BIS	Premier
				11 компаний	Select
Forcepoint	США	-	RRC Украина, Softprom	Data Expert, ISSP, Интрасистемс	Gold
Fortinet	США	+	МУК, ERC	Смарт Нет	Platinum
				Лан Системс, Netwave, PF Service, Смарт Нет	Gold
				Амрита Комплексные Решения, Belintech, iIT-Trading, Silvery	Silver
Palo Alto Networks	США	-	БАКОТЕК	16 компаний	Innovator
Watchguard	США	-	БАКОТЕК	-	-

преобразование безвредного контента с помощью средств JavaScript может у некоторых продуктов более чем вдвое увеличить число ложных срабатываний, а это чревато дополнительной нагрузкой на персонал безопасности, поскольку те же средства используются при обычном просмотре веб-страниц.

Gartner в отчете Magic Quadrant for Enterprise Network Firewalls, который вышел осенью прошлого года, отмечает, что все производители уже предлагают в своих решениях функции NGFW, такие как контроль пользователей и приложений, IPS, «песочницы», сторонняя аналитика угроз, поэтому термины «межсетевой экран корпоративного класса» и «NGFW» стали синонимами. По сути, сам термин «межсетевой экран следующего поколения», когда-то и родившийся в отчетах Gartner, уже не актуален. Компания ожидает, что с учетом циклов обновления оборудования длительностью в 4–5 лет замещение традиционных экранов новыми завершится в ближайшие два года.

К квадранту лидеров Gartner в прошлом году отнес ***Palo Alto Networks***, ***Fortinet***, ***Check Point*** и ***Cisco***. ***Huawei*** получил статус претендента, тогда как ***Forcepoint*** разместился в квадранте нишевых игроков. Напомним, Gartner оценивает производителей по отзывам их клиентов и, в частности, по попаданию в списки потенциальных поставщиков. При этом используются две группы критериев: ***полнота видения*** (сюда включены такие маркеры, как понимание потребностей рынка, стратегия продаж, развития продукции и территориальный охват) и ***потенциал реализации*** (собственно, возможности и качество продукции, финансовое состояние компании, ценообразование, программы взаимодействия с клиентами и т.д.).

Украинский рынок в гигабитах

Основные производители NGFW и их украинские партнеры представлены в **табл. 1**. Местный рынок NGFW фактически разделен между четырьмя торговыми марками: Check Point, Fortinet, Cisco и Palo Alto. Насколько

Таблица 2. Параметры некоторых межсетевых экранов Check Point, Cisco, Fortinet и Palo Alto

Модель	Производительность в режиме межсетевого экрана	Производительность в режиме NGFW (межсетевой экран, контроль приложений и IPS)	Производительность в режиме защиты от угроз (Threat Protection)	Кол-во одновременных сеансов, млн	Кол-во новых сеансов в секунду, тыс.
Check Point 4200	3 Гбит/с	165 Мбит/с (без App-ID)	н/д	1,2	25
Check Point 15600	76 Гбит/с	17 Гбит/с	13,1 Гбит/с	25,6	300
Check Point 64000	800 Гбит/с	408 Гбит/с	180 Гбит/с	110,4	4920
Cisco ASA 5506-FTD-X	250 Мбит/с (с App-ID)	125 Мбит/с	н/д	0,02	3
Cisco Firepower 4120	20 Гбит/с (с App-ID)	15 Гбит/с (с App-ID)	н/д	15	120
Cisco Firepower 9300 с 3 модулями SM-44	118 Гбит/с (с App-ID)	117 Гбит/с (с App-ID)	н/д	60	900
Fortinet FortiGate/ FortiWiFi 30E	950 Мбит/с	200 Мбит/с	150 Мбит/с	0,9	15
Fortinet FortiGate 500E	36 Гбит/с	5 Гбит/с	4,7 Гбит/с	8	300
Fortinet FortiGate 6500F	239 Гбит/с	150 Гбит/с	100 Гбит/с	200	3000
Palo Alto Networks PA-220	560 Мбит/с (с App-ID)	н/д	260 Мбит/с	0,064	4,2
Palo Alto Networks PA-5220	20 Гбит/с (с App-ID)	н/д	9 Гбит/с	4	150
Palo Alto Networks PA-7080	720 Гбит/с (с App-ID)	н/д	350 Гбит/с	430	4800

известно, межсетевые экраны Forcepoint у нас не продаются, хотя партнеры у компании есть.

В **табл. 2** приведены основные параметры некоторых межсетевых экранов четырех производителей: самой простой и самой мощной моделей, а также устройства, которое тестировала NSS Labs. В таблице указаны величины производительности в трех режимах: обычного межсетевого экрана (некоторые указывают значение при включенной функции распознавания приложений), NGFW (межсетевой экран, контроль приложений и IPS) и полного предотвращения угроз, куда также входят дополнительные функции, такие как расширенный анализ вредоносного ПО, противодействие шпионским программам и т.д. В цифрах, которые приводят компании, трафик измеряется по-разному. Например, Palo Alto дает два значения производительности: для 64K http и для смешанного трафика разных приложений.

Далее расскажем, что, собственно, производители предлагают и как изменилась их продукция за последний год.

Гипермасштабируемые кластеры Check Point

Портфель решений для сетевой безопасности израильской компании Check Point носит название Check Point Infinity Architecture. Она объединяет как межсетевые экраны (аппаратные и виртуализированные), так и другие решения, в том числе группу средств защиты от атак нулевого дня SandBlast. Последняя, в свою очередь, включает решения для защиты сети, конечных точек и мобильных устройств. Представленная в прошлом году технология CADET (Context-Aware Detection and Elimination of Threats — контекстно-ориентированное обнаружение и устранение угроз) сокращает уровень ложной тревоги при анализе входящих файлов.

В семейство межсетевых экранов Check Point Software Technologies входит больше десятка серий разного назначения, от филиалов и небольших предприятий до крупных ЦОД и операторов связи. Наиболее производительные модели — 44000 и 66000. В последней обеспечено резервирование на уровне шасси, также в обеих платформах продублированы модули коммутации и управления, возможна установка двух устройств в высокодоступном режиме.

В прошлом году серия 23000 (тоже уровня больших предприятий и ЦОД) пополнилась моделью 23900 (**рис. 1**). Это устройство в форм-факторе 2U имеет производительность 128 Гбит/с в режиме обычного межсетевого экрана, 24 Гбит/с как NGFW и 22,7 Гбит/с при полном предотвращении угроз (в том числе с использованием технологии SandBlast Zero-Day). Устройство имеет порты 1, 10, 25, 40 и 100 Гбит/с, количество сетевых интерфейсов может быть доведено до 42.

Еще из интересных новинок можно отметить решение Maestro Hyperscale Orchestrator, значительно упрощающее процессы масштабирования межсетевых экранов — согласно пресс-релизу, можно за несколько минут создать кластер из 52 устройств. Кроме того, технология HyperSynch позволяет при этом сохранять максимальную производительность за счет использования всех ресурсов межсетевых экранов.

Cisco: аналитика и защита от DDoS

Cisco в декабре 2018 года сообщила, что серии межсетевых экранов Firepower 7000 и 8000 снимаются с продажи после 10 июня 2019-го. Устранение аппаратных неисправностей будет возможно еще в течение года после этого; расширенная поддержка продлится до 5 сентября 2023-го, а дата 5 июня 2024-го указана как конечный срок получения сервисного обслуживания и техподдержки. На смену этим сериям несколько лет назад были введены новые.

Сейчас семейство межсетевых экранов Cisco Firepower состоит из трех серий. Модельный ряд 2100, представленный в 2017 году, включает в себя 4 устройства средней производительности (2–8,5 Гбит/с в режиме NGFW). Предназначены они для применения на границе сети интернет-провайдера и ЦОД. Серия 4100 также включает 4 модели производительностью 10–24 Гбит/с. Наиболее мощной является 9300 (**рис. 2**) — модульная платформа, производительность которой благодаря кластеризации может достигать 1 Тбит/с.

Это решение предназначено для операторов связи, больших вычислительных центров, кампусных сетей, торговых площадок и других объектов, где нужна большая пропускная способность при малой задержке (до 5 мкс). Эти же серии могут работать с программным образом Adaptive Security Appliance (ASA). С другой стороны, аппаратные устройства ASA работают и с образом Firepower Threat Defence, данная серия носит название ASA 5500-FTD-X и включает в себя 8 моделей производительностью от 125 до 1250 Мбит/с, сфера их применения — от СМБ и филиалов компаний до границы сети провайдера. Наконец, есть у Cisco и виртуальные версии шлюзов Firepower.

Для конвертации платформы ASA в Firepower Cisco выпустила специальный инструмент — Firepower Migration Tool.

Устройства Firepower поддерживают технологию ретроспективного анализа угроз Advanced Malware Protection (AMP), которая позволяет выявлять сложный вредоносный код, проникший сквозь защиту, а также обеспечивают

Рис. 1. Check Point 23900

распознавание приложений и фильтрацию трафика по URL для ограничения доступа к интернет-ресурсам. Устройства 4100 и 9300 обеспечивают защиту от DDoS-атак с использованием платформы Radware Virtual DefencePro — как отмечает Gartner, это единственные межсетевые экраны, которые имеют встроенную DDoS-защиту корпоративного уровня. Cisco предлагает несколько вариантов управления защитой: централизованное, локальное на устройствах и облачное (для ASA).

Также большим достоинством Cisco является наличие группы аналитики угроз Talos, результаты работы которой используются в разных системах безопасности и автоматически загружаются при обновлениях NGFW. Кроме того, Cisco имеет партнерские соглашения с другими аналитическими службами и сообществами.

В начале прошлого года Cisco заключила соглашение с IBM, результатом которого стала интеграция Firepower и SIEM-системы IBM QRadar. Специализированное приложение позволяет пользователям Firepower видеть на сводном экране информацию о зафиксированных попытках проникновения и другой подозрительной активности, данные о частоте появления того или иного вредоносного кода и о том, какие машины могут быть заражены. Все это должно обеспечить лучшую видимость всей инфраструктуры и сократить время реагирования.

В 2018 году Cisco сообщила об уязвимости, обнаруженной в ПО межсетевых экранов ASA и Firepower. Злоумышленники использовали ее, посылая большие объемы SIP-запросов, что приводило к зависанию или перезагрузке устройств. Другая брешь, найденная в ПО ASA, позволяла пользователям без привилегий удаленно выполнять операции на межсетевом экране через веб-панель управления. Уязвимости были закрыты в февральских обновлениях.

Fortinet: сегментация на основе намерений

Fortinet тоже может предложить межсетевые экраны разного назначения — от систем начального уровня до высокопроизводительных комплексных решений. Нижний сегмент включает в себя модели в компактном корпусе без вентилятора, предназначенные для филиалов офисов и предприятий СМБ; через порт USB можно подключить модем 3G/4G. На другом конце спектра находятся устройства серии 6000, производительность которых измеряется сотнями Гбит/с, они рассчитаны на операторов связи, крупные предприятия и ЦОД. Есть и виртуальные версии NGFW (серия FortiGate VM), которые обеспечивают пропускную способность в режиме защиты от угроз до 2 Гбит/с.

Рис. 2. Cisco Firepower 9300

Архитектура безопасности Fortinet называется Security Fabric. Она объединяет различные устройства Fortinet (решения для защиты конечных точек, контроля доступа, «песочница» и т.д.), а также продукты сторонних производителей. Вся система обеспечивает обмен данными между разными устройствами и выводит сводную аналитику на единый экран. Интеграцию с партнерскими и облачными платформами обеспечивают программные интерфейсы Fabric Connectors, реализованные в операционной системе FortiOS.

В прошлом году Fortinet представила новую версию операционной системы для своих устройств — FortiOS 6.0. Среди ее ключевых возможностей — автоматизация реагирования на инциденты, расширение возможностей настройки NGFW и функциональность защиты программно-определяемых распределенных сетей (SD-WAN) — это нововведение рассчитано на компании с филиалами. Также была улучшена интеграция с продукцией других производителей в рамках программы Fabric Ready, что

NGFW — ЭТО ФУНДАМЕНТ ЗАЩИТЫ

Мирослав МИЩЕНКО,
представитель Fortinet в Украине

Межсетевой экран сейчас необходимо рассматривать как минимально необходимую защиту. Это своего рода фундамент, на котором строится обеспечение безопасности инфраструктуры предприятий. В ближайшем будущем NGFW скорее дополнится смежными решениями (возможно, часть функций будет реализована на базе самого экрана), чем будет заменен другими технологиями.

Нельзя забывать, что безопасность — это процесс, который необходимо строить, развивать и поддерживать. А многие новые угрозы — это хорошо забытые старые. В прошлом году в Украине участились атаки на технологические сети, есть уверенность в том, что данный тренд наверняка сохранится и в 2019-м. Также стоит обратить внимание на развитие IoT и учитывать это в стратегии защиты каждой инфраструктуры.

В Украине, с моей точки зрения, 2018 год прошел все еще под «впечатлением» от Petya и ему подобных атак. Многие заказчики реализовывали проекты с оглядкой на события лета 2017 года. Это обеспечило довольно значительный рост рынка NGFW в 2018 году.

К сожалению, большое влияние в целом оказывает политическая ситуация в стране и грядущие выборы. Эти факторы могут привести к тому, что часть проектов либо будет отложена, либо станет продвигаться более медленно. Если же вынести данный фактор за скобки, то рынок ИБ в нашей стране продолжит свой рост. Многие заказчики имеют стратегию защиты своей инфраструктуры и продолжат ее реализовывать.

дало возможность расширить круг партнеров (сейчас он включает AWS, Cisco, Google, Microsoft Azure, Nuage Networks, Oracle, ServiceNow и VMware).

В феврале нынешнего года Fortinet вывела на рынок несколько новых моделей, которые дополнили существующие серии NGFW. FortiGate 3600E (**рис. 3**) характеризуется производительностью 30 Гбит/с в режиме защиты от угроз и 34 Гбит/с при проверке SSL-трафика, FortiGate 3400E — соответственно 23 и 30 Гбит/с. Обе модели имеют интерфейсы 10G, 40G и 100G. FortiGate 600E с портами 1G и 10G обеспечивает 7 Гбит/с в режиме защиты и 8 Гбит/с при расшифровке трафика, тогда как модель 400E, предназначенная для филиалов компаний, имеет порты 1G, обеспечивая соответственно 5 и 4,8 Гбит/с. Все устройства поддерживают т.н. сегментацию на основе намерений (Intent-based segmentation), которая позволяет делить защищаемую сеть на зоны, независимо от расположения инфраструктуры (на территории предприятия или в облаке) и с учетом индивидуальных особенностей компании (политики доступа, цели защиты, уровни контроля и т.д.).

Рис. 3. Fortinet FortiGate 3600E

Как нам сообщили в Fortinet, будет продолжена работа в направлении SD-WAN. Также в прошлом году были куплены две компании: Broadford Networks (решения для контроля доступа) и ZoneFox (сбор данных о поведении пользователей), что усилило компетенции Fortinet в этих направлениях.

Palo Alto Networks: от NGFW к «кортексу»

Межсетевые экраны ***Palo Alto Networks*** (PANW) основаны на архитектуре Single Pass, которая обеспечивает проверку трафика на разные виды угроз в один проход. Компания предлагает несколько серий NGFW разной производительности, начиная с PA-220 для территориально распределенных офисов и заканчивая двумя устройствами PA-7000, предназначенными для крупных предприятий, операторов связи и ЦОД. В серии PA-7000 используется более 1500 специализированных процессоров, сгруппированных в карты обработки сетевого трафика, управления коммутацией и журналирования.

Также производитель предлагает виртуализированные версии межсетевых экранов (серия VM).

В 2018 году Palo Alto продолжала обновлять и развивать семейство NGFW. В частности, в начале прошлого года вышла версия операционной системы PAN-OS 8.1, в которой появилось более 60 новых функций, в том числе расширенные возможности расшифровки SSL-трафика.

Тогда же были выпущены несколько аппаратных решений, в том числе новая серия 3200, которая включает три устройства производительностью от 2,6 до 4,7 Гбит/с в режиме предотвращения угроз. Они предназначены для использования на границе сети интернет-провайдера и содержат раздельные вычислительные мощности для разных задач защиты. По сравнению с предыдущими моделями PA-3200 отличаются более высокой производительностью расшифровки интернет-трафика (в 20 раз и выше). Улучшенной пропускной способностью обладает и новая модель PA-5280 (64 млн одновременных сеансов по сравнению с 32 млн у предыдущей PA-5260), сфера ее применения — крупные ЦОД и сети операторов связи. Также был представлен межсетевой экран усиленной конструкции PA-220R (**рис. 4**) в безвентиляторном корпусе, без движущихся частей и с твердотельной памятью.

Рис. 4. Межсетевой экран усиленной конструкции Palo Alto PA-220R

В феврале уже нынешнего года была анонсирована новая версия ОС — PAN-OS 9.0, также добавляющая около 60 новых возможностей. Среди них — служба защиты DNS-трафика, функциональность оптимизации управления политиками безопасности (Policy Optimizer) и поддержка дополнительных облачных сред для серии VM. Одновременно были модернизированы процессорные карты устройств PA-7000 и введена новая серия межсетевых экранов K2, разработанная для мобильных операторов с прицелом на защиту сетей 5G и IoT. Фактически серия включает в себя модели 5200, 7000 и VM, но с девятой версией ОС (аппаратные устройства также комплектуются новыми процессорными картами, в том числе 100G NPC). Представленные экраны обеспечивают улучшенную видимость сети и автоматизацию реагирования на угрозы на основе искусственного интеллекта и машинного обучения.

Для обеспечения комплексной защиты межсетевые экраны PANW могут взаимодействовать с другими продуктами компании. Среди них можно выделить облачный сервис WildFire, детектирующий и автоматически блокирующий неизвестные угрозы, и систему защиты конечных точек Traps, которая борется с различными видами вредоносного ПО, в том числе используя WildFire.

В феврале нынешнего года Palo Alto запустила также систему Cortex, которая является развитием единой системы Application Framework и состоит из облачного хранилища Cortex Data Lake и приложения Cortex XDR, с помощью средств ИИ анализирующего данные

об угрозах. Trapps и межсетевые экраны передают информацию о выявленных инцидентах и вредоносном ПО в Cortex, и защитный код автоматически загружается на все NGFW и рабочие станции.

В 2018 году PANW купила израильскую компанию Secdo, которая специализировалась на технологиях обнаружения угроз рабочим станциям и реагирования на них. Разработки Secdo были интегрированы в Traps.

Как нам сообщили в группе компаний БАКОТЕК, которая является эксклюзивным дистрибьютором Palo Alto на территории Украины и Азербайджана, продажи данной продукции в последние годы растут очень быстро (буквально в разы), что, впрочем, связано с относительно недавним появлением торговой марки на украинском рынке. Около половины поставок приходится на устройства производительностью от 1 до 20 Гбит/с, при этом среди заказчиков преобладают телекоммуникационные и ИТ-компании, а также банковский сектор.

Не спешите хоронить

В Интернете можно встретить мнение, что более чем десятилетней эпохе NGFW фактически приходит конец. Основной причиной называют размывание периметра корпоративной сети: данные все больше уходят в облака, сотрудники работают удаленно или вообще где придется, используя мобильные устройства. С другой стороны, облачные сервисы имеют более эффективные собственные («нативные») механизмы управления доступом и нативные же приложения с функциональностью NGFW, делающие специализированный межсетевой экран ненужным.

Gartner с такой постановкой вопроса не согласен и обращает внимание, что подобные масштабные трансформации обычно происходят крайне медленно. Кроме того, устройства управления, позволяющие администрировать как аппаратные, так и облачные системы, будут и дальше занимать важное место в инфраструктуре безопасности предприятий. Конечно, со временем рост продаж межсетевых экранов будет замедляться, но пока что, как отмечалось выше, он продолжается. Опрошенные нами эксперты тоже не верят в «смерть» NGFW, считая, что скорее они будут дополнены новыми решениями, чем заменены вовсе, и что в любом случае инфраструктура предприятий продолжит оставаться гибридной, а следовательно, потребность в каких-то решениях для защиты «наземной» части останется.

Дополнение NGFW другими средствами — это и есть стратегия производителей, каждый из которых развивает некую «архитектуру» и «платформу» безопасности, включающую в себя защиту как сети, так и мобильных устройств, рабочих станций и облака, специализированные средства для борьбы с угрозами «нулевого дня», системы мониторинга и анализа, все они должны обмениваться между собой данными об инцидентах, а искусственный интеллект — вырабатывать меры нейтрализации обнаруженного вредоносного кода. Межсетевой экран в этих условиях становится ключевым средством сбора данных. Например, NGFW играют роль сенсоров, откуда информация стекается в SIEM для обработки. В то же время, как показывает опыт последних лет, NGFW отнюдь не является панацеей, отсюда увеличенное внимание производителей к системам защиты конечных точек и решениям наподобие Palo Alto Aperture, обеспечивающим контроль доступа к облачным сервисам хранения данных.

Что касается облачных версий NGFW, то, как нам сообщили в БАКОТЕК, их доля уже составляет до 30% всех продаж и продолжает расти. Уже отмечалось, что свои версии межсетевых экранов есть у поставщиков платформ виртуализации, таких как AWS и VMware, но насколько они смогут составить конкуренцию существующим производителям, пока никто не знает.

Василий ТКАЧЕНКО, СиБ

РЫНОК ИБ СФОРМИРОВАЛСЯ В ПОСЛЕДНИЕ ГОДЫ

Мирослав БОНДАРЬ,
директор департамента
группы компаний БАКОТЕК

Украинский рынок информационной безопасности, безусловно, растет. По сути, с 2014-го по 2016-й годы не то что отдельные компании, а целые сегменты экономики – в первую очередь государственный, энергетический, нефтегазовый и производственный – начали понимать необходимость построения комплексной системы информационной безопасности. Раньше они рассматривали ее как второстепенную задачу, но после событий 2014–2016 годов, атак на критическую инфраструктуру, ИБ получила приоритет. Это привело к тому, что 2017–2018 годы показали очень серьезный рост продаж ИБ в различных сегментах – не только NGFW, но и систем защиты конечных точек, DLP, SIEM и других. По сути, за эти годы украинский рынок в целом сформировался.

Злоумышленники уже понимают, что уровень сознательности ИТ-пользователей пускай очень медленно, но все-таки растет, поэтому количество «умных» атак продолжит увеличиваться, а их интеллектуальность будет повышаться. Сейчас, например, мы наблюдаем всплеск т.н. бесфайловых атак, когда уже не нужно открывать на рабочей станции пользователя какой-то документ, который содержит, например, макрос и инициирует цепочку действий, приводящую к разрушительному результату.

Чтобы противостоять подобным угрозам, необходимо полностью контролировать ситуацию на уровне конечных точек, иметь полную видимость сети, уметь осуществлять корреляцию событий, происходящих на уровне сети и рабочих станций, постоянно работать над сокращением времени реакции на инциденты. Именно эта комбинация действий будет оставаться критерием успешности работы службы ИБ.