NGFW в 2016 году: что новенького

Защита ИТ-инфраструктуры становится еще более комплексной — межсетевому экрану теперь помогают другие системы.

Совершенствование методов информационных атак и вредоносного кода влечет за собой ответные меры со стороны производителей систем безопасности — извечное противостояние щита и меча не останавливается. Растет и производительность межсетевых экранов следующего поколения (Next-Generation Firewall, NGFW) в минимальной конфигурации выходя за 1 Тбит/с. Эти устройства объединяют в себе целый ряд функций защиты (антивирус, антиспам, предотвращение вторжений, веб-фильтр, проверка шифрованного трафика и т.д.) и обеспечивают контроль трафика на уровне приложений. NGFW, зачастую в комплексе с другими системами безопасности, призваны дать бой сложным атакам, в том числе с применением методов социальной инженерии, целенаправленным атакам типа APT.

Здесь мы расскажем, какие решения появились у производителей систем защиты нового поколения в 2016 году, что интересует заказчиков и как нынче выглядят взаимоотношения компаний, представляющих эту продукцию в Украине.

Мировой рынок: доли и цифры

Компания IDC в мартовском пресс-релизе сообщила, что в целом объем рынка устройств безопасности в 2016 году составил $11,6 млрд, что почти на 10% больше по сравнению с предыдущим годом, при этом всего было поставлено свыше 2,7 млн устройств (прирост 18%). Половина доходов приходится на сегмент UTM, который одновременно показывает самый высокий рост (17%), тогда как в сегменте межсетевых экранов доходы увеличились на 10,4%. Пятерку лидеров продаж составляют ***Cisco***, ***Check Point***, ***Palo Alto***, ***Fortinet*** и ***Huawei***. При этом Huawei демонстрирует наибольший рост выручки — более 70%.

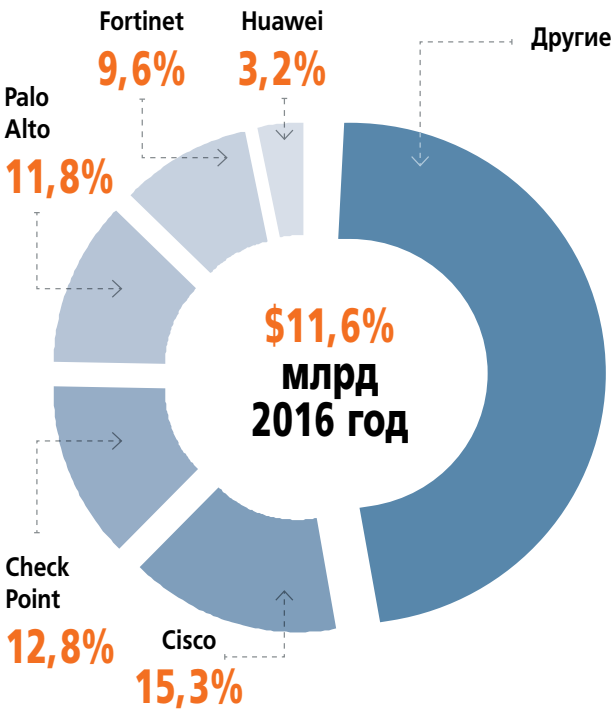
Переходя непосредственно к NGFW, для начала рассмотрим оценки Gartner, которые можно посмотреть в июньском отчете под названием Magic Quadrant for Enterprise Network Firewalls («Магический квадрант межсетевых экранов корпоративного класса»).

Агентство отмечает, что все производители внедрили в свои решения функции NGFW для обеспечения политик безопасности (контроль пользователей и приложений) и выявления новых угроз (IPS, «песочницы» и интеграция с аналитическими сервисами). Поэтому в целом термин «корпоративный межсетевой экран» теперь является синонимом NGFW.

Gartner оценивает производителей по отзывам их клиентов и, в частности, по по-

Система управления и предупреждения об угрозах

Рынок устройств безопасности 2016 года, по данным IDC



ДОЛИ Fortinet и Huawei ВЫРОСЛИ на 1% по сравнению с 2015 годом, а Palo Alto — на 2%

Cisco — ЛИДЕР НА РЫНКЕ, но за последний год доля компании снизилась на 1%

паданию в списки потенциальных поставщиков. К квадранту лидеров Gartner отнес трех производителей: Check Point, Fortinet и Palo Alto. Компании Cisco и Huawei названы претендентами. Квадрант «визионеров» занят компаниями Forcepoint и Sophos, первая образовалась недавно и еще не успела отметиться большим количеством заказов, а вторая специализируется нарешениях для небольших предприятий и территориально-распределенных организаций.

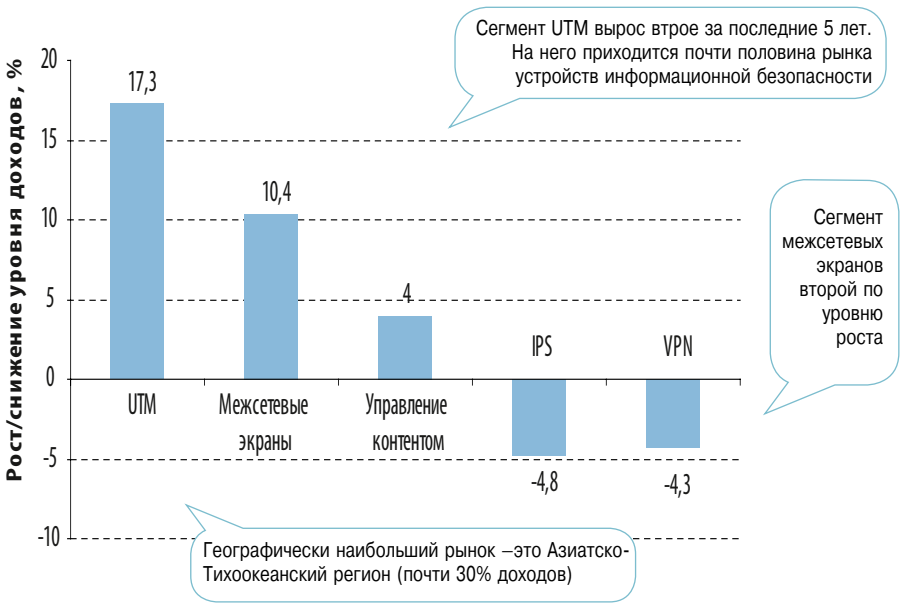
Проверка на прочность

Техническое сравнение предложений разных производителей традиционно можно увидеть в отчете NSS Labs — Security Value Map («Карта ценности защиты»), который вышел также в июне. Компания протестировала одиннадцать решений от десяти поставщиков (включая два от Fortinet), сопоставив их по двум обобщенным показателям: эффективности защиты и совокупной стоимости владения, которая приходится на защищаемый 1 Мбит/с. Схема испытаний оборудования каждого из производителей включала пять единиц NGFW и один центральный блок управления.

Первое место занял межсетевой экран ***Forcepoint*** 3301, заблокировавший все атаки и закрывший 99,89% уязвимостей, а также обеспечивший на 100% блокирование техник обхода защиты. По последнему показателю стопроцентный результат показало и решение Cisco Firepower 4110, хотя в других категориях оценки оказались несколько ниже. Все остальные производители не прошли тест по блокированию техник обхода защиты — как минимум одной (***Check Point*** по результатам испытаний выпустила обновление, заблокировавшее пропущенный метод обхода, но NSS Labs не оценивала влияние этого патча на работу устройства). Самая низкая стоимость владения оказалась у решения ***Fortinet*** 600D. Также к рекомендованным продуктам NSS Labs отнесла Fortinet 3200D и ***Watchguard*** Firebox M4600. Межсетевые экраны ***Barracuda*** F600.E20, ***Juniper*** SRX 4200, ***SonicWall*** NSA 6600 и ***Palo Alto*** PA-5250 оказались в сегменте «ниже среднего», показав эффективность защиты в пределах 20–40% и довольно высокую стоимость владения (только у Palo Alto она оказалась на уровне Cisco). В целом средняя эффективность защиты составила 67,3%, средняя совокупная стоимость владения — $25,2 на защищаемый 1 Мбит/с.

Вкратце расскажем о лидере рейтинга. Компания ***Forcepoint*** возникла в 2015 году в результате слияния ***Raytheon*** и ***Websense***. В 2016-м она выкупила у Intel Security оба подразделения, которые специализировались на межсетевых экранах (McAfee Next Generation Firewall и McAfee Firewall Enterprise). Вместе с этой покупкой в Forcepoint перешла бывшая компания ***Stonesoft***, которую McAfee купила в 2013 году. Среди прочего, Forcepoint выпускает несколько серий NGFW разного применения с пропускной способностью в режиме межсетевого экрана от 1,5 до 240 Гбит/с. С ноября прошлого года существует возможность развертывания виртуальных NGFW в облаках AWS при сохранении централизованного управления как аппаратными, так и виртуальными межсетевыми экранами. В новой версии ПО, которая вышла в апреле этого года, добавлена поддержка облачной службы

Динамика доходов на мировом рынке устройств информационной безопасности в 2016 году (по данным IDC)



обнаружения и фильтрации вредоносных программ Advanced Malware Protection.

В Украине у Forcepoint нет дистрибьютора, но Data Expert, ISSP и «Техносерв Украина» являются партнерами этого производителя.

Украинский рынок: основные игроки

Круг производителей NGFW, чьи решения можно встретить в Украине, довольно невелик и уменьшился еще больше с тех пор, как HPE продала направление безопасности компании Trend Micro. Ведущие производители NGFW и их украинские партнеры перечислены в таблице.

Обзор решений начнем с ***Cisco***. Семейство Firepower является результатом слияния приобретенной в 2013 году платформы Firepower с межсетевыми экранами Cisco ASA. В прошлом году компания представила «среднюю» серию Firepower 4100, в которую входят четыре модели с пропускной способностью от 12 до 30 Гбит/с — они предназначены для использования в ЦОД. Более производительная серия 9300 (30–135 Гбит/с) рассчитана на потребности крупных ЦОД и операторов связи; она обеспечивает задержку менее 5 мкс, также есть возможность кластеризации с достижением суммарной пропускной способности свыше 1 Тбит/с. Уже в этом году была представлена новая серия 2100 в составе четырех моделей производительностью от 2 до 8,5 Гбит/с, пришедшая на смену устройствам ASA-5500. Предлагает Cisco и виртуализированные версии NGFW, которые могут работать в различных средах и типах облаков.

Производители внедряют в свои решения функции выявления

новых угроз

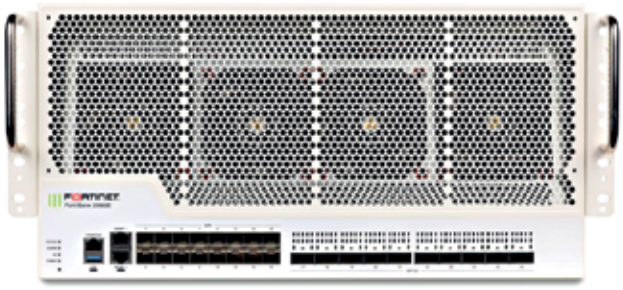
Устройства Firepower поддерживают технологию ретроспективного анализа угроз Advanced Malware Protection, которая позволяет выявлять сложный вредоносный код, проникший сквозь защиту. Также в NGFW интегрированы «песочница» для анализа вредоносного кода и функции защиты от DDoS-атак с использованием технологий Radware. Cisco предлагает три варианта управления защитой: Device Management (локальное на устройстве), Firepower Management Center (централизованное) и Cloud Defense Orchestrator (облачное).

По сообщению Cisco, новыми заказчиками межсетевых экранов в прошлом году стали более 100 клиентов, к том числе были несколько украинских банков, го-

Одна из моделей Cisco Firepower 2100

Таблица. Основные производители систем NGFW и их украинские партнеры 2016 года

ПРОИЗВОДИТЕЛЬ	ШТАБ-КВАРТИРА	ПРЕДСТАВИТЕЛЬСТВО В УКРАИНЕ	ДИСТРИБЬЮТОРЫ	ПАРТНЕРЫ	
				СТАТУС	НАЗВАНИЕ КОМПАНИИ
Check Point	Израиль	+	МУК, RRC	✪✪✪	БМС Консалтинг, Svit IT
				✪✪	23 компании
Cisco	США	+	ERC, Мегатрейд, МУК	Gold	БМС Консалтинг, ИТ-Интегратор, Ситроникс, Техносерв Украина, S&T Ukraine, Green Networks, Winncom
				Premier	5 компаний
Forcepoint	США	–	-	Gold	Data Expert, ISSP, Техносерв Украина
Fortinet	США	–	МУК, ERC	Platinum	Смарт Нет
				Gold	Лан Системс, Netwave, PF Service
				Silver	Инфотел, Спецвузавтоматика, Тирей Украина, Netbox
Palo Alto	США	–	БАКОТЕК		ITBiz
Watchguard	США	–	БАКОТЕК		



Терабитный межсетевой экран FortiGate 3980E

сударственные и промышленные предприятия, сейчас реализуется проект в одном из крупных операторов связи. Как нам сообщили в представительстве, до 90% проектов с использованием межсетевых экранов выполняются на основе NGFW. Компании большого и среднего размеров применяют новые устройства серии Firepower, тогда как в сегменте SMB по-прежнему используются младшие модели ASA. При этом производитель предлагает возможность модернизации ASA до уровня NGFW путем обновления прошивки.

Особенностью украинского рынка является большое количество инцидентов на фоне устаревшей инфраструктуры и ограниченности бюджетов на информационную безопасность. Если в 2015–2016 годах атаки были более точечными и в основном направленными на большие госструктуры, объекты энергетики, то недавние инциденты поразили тысячи организаций на всей территории страны. Компании начали больше вкладывать в инфраструктуру безопасности. С другой стороны, приходится объяснять клиентам, что NGFW не является панацеей, особенно в условиях направленных атак. Для эффективной защиты недостаточно купить устройство: нужно комплексное решение, которое включает и межсетевые экраны, и сегментацию сети, и мониторинг трафика, и настройки безопасности операционных систем, и защиту на уровне рабочих станций.

С точки зрения технологий сейчас востребована интеграция NGFW и сетевых устройств. Можно использовать гибридный подход, когда для выявления и блокировки атак используются не только специализированные межсетевые экраны на периметре, но и сами устройства общего назначения по всей сети. Это позволяет эффективнее использовать уже существующие ресурсы сети и реагировать на атаки быстрее и точнее. Еще одна особенность украинского рынка состоит в том, что большое количество клиентов используют виртуальные межсетевые экраны, как для тестирования, так и для промышленного внедрения.

Владимир Илибман,
специалист Cisco по информационной безопасности

Устройство защиты Check Point 44000

Fortinet предлагает несколько серий межсетевых экранов, от начального уровня (класса UTM) до высокопроизводительных решений для больших ЦОД и операторов связи. В 2016 году компания представила свое видение стратегии построения защиты предприятий — Fortinet Security Fabric, составляющей которой являются и решения класса NGFW. Уже в 2017 году в рамках новой стратегии производитель выпустил очередную версию операционной системы для межсетевых экранов — FortiOS 5.6, которая позволяет видеть все, что происходит в сети — от рабочих станций до облачной инфраструктуры. В начале 2017 года Fortinet пополнил семейство FortiGate 3000 высокопроизводительной моделью 3980E, обеспечивающей пропускную способность 1,12 Тбит/с (при включенном VPN — 470 Гбит/с).

Устройство имеет 32 процессора, оснащено двумя портами GbE, 16 интерфейсами 1/10 SFP/SFP+ и десятью портами 100 GbE. Решение может использоваться для защиты ЦОД, обеспечения безопасности соединений между дата-центрами или для внутренней сегментации сети. Одновременно был выведен на рынок межсетевой экран FortiGate 7060E, который со всеми включенными функциями NGFW обеспечивает производительность на уровне 100 Гбит/с, с функцией управления приложениями — 160 Гбит/с, в режиме IPS — 120 Гбит/с. Эта модель может иметь до восьми портов 100 GbE, до шестнадцати портов 40 GbE или до сорока шести интерфейсов 10 GbE. Сценарии применения — от периметра сети до ядра ЦОД и внутрисетевой сегментации.

Широкий ассортимент межсетевых экранов предлагает и ***Check Point —*** от межсетевых экранов для SMB (пропускная способность до 350 Мбит/с) до многоюнитовых NGFW уровня больших предприятий, ЦОД и телеком-операторов. Есть в линейке Check Point и решения для виртуальных платформ (VMware, AWS, OpenStack и MS Azure). Новинки 2016 года — устройства защиты корпоративного класса серии 15000, в которую входят две модели, обеспечивающие в тестовых условиях максимальную скорость 58 и 76 Гбит/с (в реальных условиях заявлены 30 Гбит/с). Для ЦОД разработана серия 23000 также в составе двух моделей, которые в идеальных условиях обеспечивают соответственно 116 и 128 Гбит/с (в реальных — 34 и 43 Гбит/с). Кроме того, для удовлетворения потребностей крупных ЦОД и телеком-операторов производитель вывел на рынок системы защиты 44000 и 66000 (до 377 и 880 Гбит/с в тестовых условиях, до 230 и 539 Гбит/с в реальных). Отметим, что в режимах NGFW и предотвращения угроз пропускная способность заметно снижается. Есть у Check Point и системы защиты в облаке (vSEC), в прошлом году к поддерживаемым платформам добавилась Google Cloud. Наконец, в прошлом году была представлена платформа управления безопасностью сети Check Point SecuritB Украине CheckPoint работает как через дистрибьюторов («МУК» и RRC), так и через партнеров-риселлеров.

Palo Alto может предложить несколько серий межсетевых экранов — как физических, так и виртуализированных, производитель-

ностью от 100 Мбит/с до 200 Гбит/с. Эти устройства основаны на архитектуре Single Pass, которая обеспечивает проверку трафика на разные виды угроз в один проход. Как сообщили в компании ***«БАКОТЕК»***, которая является дистрибьютором Palo Alto Networks в Украине, развитие решений в 2016 году было направлено на улучшение защиты от APT и атак через уязвимости «нулевого дня», а также от атак с использованием похищенных идентификационных данных (credential-based attacks). Кроме того, производитель работал над улучшением инструментов видимости инцидентов и автоматизации реагирования, над защитой трафика облачных приложений (Google, MS Office365 и т.д.).

«БАКОТЕК» является дистрибьютором еще одного производителя систем безопасности — ***WatchGuard***. Эта американская компания выпускает несколько серий устройств защиты под маркой Firebox, куда входят как системы UTM в настольном исполнении (в частности, одна из моделей обеспечивает пропускную способность до 1 Гбит/с со всеми включенными функциями), так и большие межсетевые экраны корпоративного класса; есть и виртуализированные версии. В тестировании NSS Labs принимала участие одна из наиболее производительных моделей — M4600 (до 40 Гбит/с). Еще более мощное устройство M5600 обеспечивает пропускную способность до 60 Гбит/с в режиме межсетевого экрана, имеет восемь портов GE и четыре интерфейса 10GE.

В 2016 году WatchGuard выпустила новую версию операционной системы Fireware 11.11 с новой функцией мониторинга Network Discovery, которая сканирует сеть и составляет карту всех подключенных устройств, выявляя открытые порты и идентифицируя работающие протоколы. Также среди новых функций — выявление и блокирование бот-сетей и контроль подключенных мобильных устройств. По информации «БАКОТЕК», в 2016 году WatchGuard также занималась повышением производительности обработки трафика (особенно шифрованного). Появились и дополнительные функции безопасности — кроме улучшенной защиты от APT и уязвимостей нулевого дня, пользователи получили новую службу обнаружения и защиты Threat Detection and Response, которая анализирует и визуализирует сетевые события, а также защищает компьютеры от новых угроз, таких как программы-вымогатели. Кроме того, в 2016 году была концептуально улучшена защита корпоративных беспроводных сетей.

NGFW уже недостаточно

В упомянутом выше отчете Gartner даны некоторые тенденции мирового рынка корпоративных межсетевых экранов. Среди них — рост популярности виртуализированных решений, прежде всего на платформах VMWare и AWS, хотя на долю таких облачных экранов приходится менее 5% всего рынка. Еще одной тенденцией является использование наряду с NGFW передовых систем обнаружения угроз (Advanced Threat Detection), которые чаще всего представляют собой облачные «песочницы», чьи услуги предлагаются по фиксированной цене независимо от объема трафика. Что касается самих межсетевых экранов, то отсутствие значимых технологических инноваций приводит к сокращению технологического отставания претендентов от лидеров.

Украинских заказчиков интересует возможность выявлять и быстро блокировать сложные атаки, в том числе целевые (APT), видимость сетевого трафика на уровне приложений и производительная обработка шифрованного трафика. Также важны борьба с DDoS-атаками (обнаружение бот-сетей), функции защиты промышленных и IoT-систем.

Межсетевые экраны Watchguard M4600/M5600

На сегодняшний день технологии NGFW разных производителей по функциональности уже достаточно близки друг к другу. Поэтому компании делают ставку на платформенный подход: в линейку добавляются новые решения, осуществляется интеграция между ними, появляются инструменты автоматизации и т.д. В целом такой сценарий развития конкуренции между игроками полностью соответствует потребностям рынка, поскольку лишь комплексный подход может эффективно защищать от современных киберугроз.

Мирослав Бондарь, *менеджер по развитию бизнеса группы компаний «БАКОТЕК»*

Сегодня рынок межсетевых экранов готовится к новому этапу, который подразумевает, что компании все больше станут задумываться о безопасности инфраструктуры в момент ее построения и начнут использовать автоматизацию для улучшения возможностей защиты и управления ею. Производители межсетевых экранов должны развиваться в пяти ключевых областях: обнаружение, предотвращение, интеграция, производительность и более низкая стоимость.

Мирослав Мищенко, *менеджер по работе с ключевыми клиентами в Украине и Беларуси компании Fortinet*

Участникам рынка был задан вопрос о том, как NGFW мог бы защитить сеть предприятия от программ-вымогателей вроде нашумевших WannaCry и Petya.A. Как и следовало ожидать, единого рецепта не существует: поможет только сбалансированный подход к обеспечению информационной безопасности в организации. Подобные атаки используют методы социальной инженерии, проникают по доверенным каналам и заражают компьютеры изнутри корпоративной среды. Здесь может помочь сегментация сети с использованием межсетевых экранов — для этой цели у некоторых производителей есть специализированные устройства, но с тем же успехом применяются и NGFW. В целом для противостояния вымогателям не обойтись без комплексной защиты, включающей в себя не только межсетевые экраны, но и защиту рабочих станций, электронной почты и других служб, а также систему мониторинга и анализа угроз. Поставщики осторожно надеются, что недавние атаки заставили бизнес задуматься об этом.

Василий ТКАЧЕНКО, СиБ