Из истории одного проекта по замене NGFW

Алексей Хмыров, *руководитель отдела по развитию бизнеса АО "ЭЛВИС-ПЛЮС"*

Фото: Сергей Кураев

Комплексный проект по созданию системы защиты объекта КИИ, о котором пойдет рассказ, стартовал до ввода в действие нормативно-правовой базы о технологической независимости, но к завершающей стадии проекта мы все же столкнулись с этими изменениями в законодательстве. Рассмотрим, каким образом удалось перестроить проект и преодолеть возникшие сложности в части использования решений класса NGFW.

План реализации системы безопасности КИИ включал в себя разработку типового технического проекта для нескольких видов бизнеса заказчика с последующей адаптацией проекта на разные площадки. На момент разработки типовых технических решений еще не было требований по импортозамещению, поэтому выбор СЗИ проводился с учетом всего спектра рынка ИБ, доступного на тот момент. Мы выбирали лучшие средства по техническим и ценовым показателям. Например, в качестве СЗИ в составе подсистемы сетевой безопасности был выбран NGFW FortiGate от американской компании Fortinet. NGFW FortiGate был запроектирован как типовое средство межсетевого экранирования и успешно внедрен нами на пилотных площадках. Его функционал закрывал не только классический для такого класса решений набор мер приказа ФСТЭК России № 239 (защита периметра, сегментирование информационной системы, организация демилитаризованной зоны, управление сетевыми потоками), но и меры по предотвращению вторжений и антивирусной защите за счет наличия сертифицированных модулей IDS/IPS и потокового антивируса.

С точки зрения удобства наладки и эксплуатации нареканий к средству защиты также не возникло. Испытания и продолжительные пилоты доказали эффективность и надежность выбранного решения.

К середине 2022 г. средство было выбрано и согласовано с заказчиком, успешно завершено пилотирование, – NGFW FortiGate был принят в постоянную эксплуатацию на двух площадках.

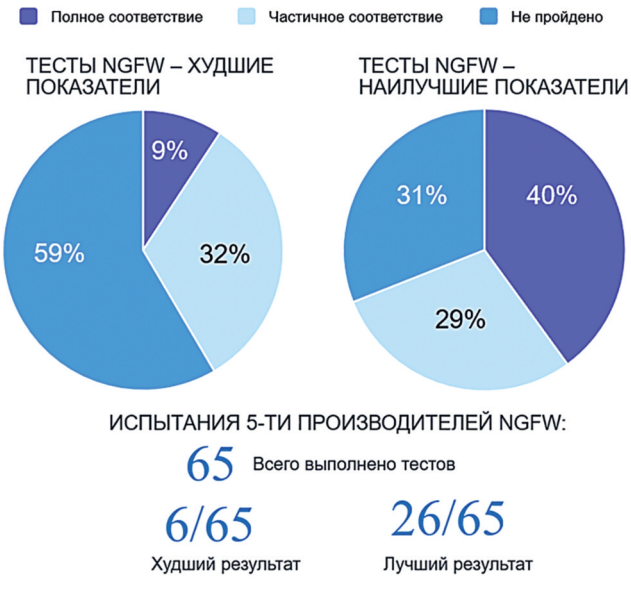

Рис. 1. Самые низкие и самые высокие результаты испытаний

И грянул гром!

Во время адаптации типового проекта на остальные площадки вступают в силу требования по импортозамещению! И сразу возникает вопрос выбора решений на замену. А готов ли российский рынок ИБ предложить аналоги? Очевидны также стали последствия: перепроектирование, повторное сравнение и выбор, проведение испытаний.

Но обстоятельства не оставляли вариантов для маневра, и мы начали процесс пересмотра технических решений с анализа российского рынка NGFW. Были приглашены на испытания все пятнадцать российских производителей межсетевых экранов, существующих на тот момент времени.

Откликнулись не все. Показательно, что после получения методики тестирования четыре производителя отказались принимать участие, еще двое отказались от продолжения испытаний уже в процессе. В итоге участие в тестировании приняли пять вендоров, что говорит об ограниченности выбора на российском рынке и о незрелости продуктов. Причем, только два решения из пяти смогли пройти испытания без критичных сбоев и показать приемлемый результат.

На рис. 1 приведены данные по двум решениям, показавшим самые низкие и самые высокие результаты. Видно, что в целом показатели неудовлетворительные, никто не прошел порог в 50% успешно выполненных тестов. По ряду тестов было выявлено лишь частичное соответствие – испытания пройдены с замечаниями и требуется доработка решения. Впрочем, не все производители заявили о готовности доработать свои продукты и принять участие в повторных тестах.

По итогам можно сделать вывод, что ни одно из представленных средств не имело такого же функционала как у NGFW FortiGate. Например, сертифицированного модуля потокового антивируса не оказалось ни у одного из российских производителей. Помимо этого, из пяти тестируемых решений импортонезависимыми были только два. По результатам оценки экономической составляющей получилось, что заказчик может получить более дорогостоящие NGFW с меньшим функционалом, чем у FortiGate.

Радикальное решение проблемы

С учетом проведенного тестирования было принято решение выполнить повторный анализ всех подсистем в составе комплексной системы информационной безопасности и пересмотреть цели и задачи, возлагаемые на средство межсетевого экранирования. Дополнительно мы провели переоценку логических связей "Актуальные угрозы" – "Меры 239-го приказа" – "Функция NGFW", и в результате были выявлены угрозы и меры, которые помимо NGFW также закрываются и иными средствами. Другими словами, межсетевой экран не является единственным средством и способом для нейтрализации угроз и реализации мер. Вот несколько примеров:

- Изоляция АСУ ТП была выполнена через диоды данных – таким образом реализованы меры по защите периметра, контролю доступа из внешних систем и др.
- Обнаружение вторжений в технологическом сегменте реализовано с помощью NTA (Network Traffic Analysis) как основного решения, заменяющего функционал модуля обнаружения вторжений на NGFW.
- Отсутствие потокового антивируса на NGFW компенсировали наличием антивирусных средств на конечных точках, дополнительной проверкой файлов через песочницу и комплексом компенсирующих мероприятий.

По итогам проведенного анализа мы пересмотрели требования к межсетевому экрану и его роли в составе комплексной системы безопасности. Ну а с фильтрацией трафика вполне справится простое и недорогое решение, по сути, уже не являющееся NGFW.

Тестирование NGFW

С точки зрения анализа развития российских решений считаю важным рассказать еще про один проект с более поздними сроками реализации, также включавший выбор и сравнение NGFW.

Для максимальной честности и прозрачности испытаний было принято решение проводить тестирование в нашей лаборатории на единой инфраструктуре и в одинаковых условиях для всех участников. Стенд и программа испытаний создавались с учетом специфики объектов защиты заказчика, были выбраны разные модели NGFW, каждый под свои задачи (уровень предприятия, уровень АСУ ТП).

Мы пригласили представителей всех участников к нам в лабораторию. Показательные испытания проводились в открытом, прозрачном формате с участием представителей заказчика и всех вендоров NGFW. Такой подход позволил участникам увидеть сильные стороны конкурентов, отметить свои слабые места, провести работу над ошибками и после исправления замечаний пройти испытания повторно.

По результатам можно сделать вывод, что по сравнению с ранее описанным тестированием участвовавшие NGFW показали более сильные результаты. Стоит отметить, что одни решения показали себя лучше при работе с промышленными протоколами, другие удачнее прошли тесты для работы в корпоративном сегменте сети.

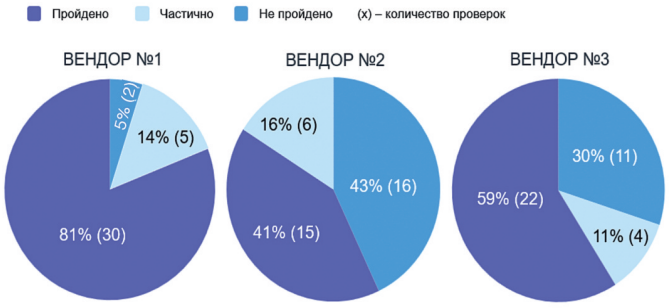

Рис. 2. Результаты тестирования NGFW

Итоги проекта

На момент выхода новелл законодательства по технической независимости российский рынок ИБ не был готов полностью заместить иностранные решения. В такой ситуации важно правильно оценить требования проекта и подобрать оптимальный набор технических, организационных и компенсирующих мер. Средства должны быть выбраны с учетом архитектурных особенностей объектов защиты и исходя из целей и задач, возлагаемых на это средство защиты в составе комплексной системы безопасности.

Таблица 1. Российские NGFW, основные проблемы и пути решения

Проблема	Решения
Трудоемкий перенос конфигураций с существующих иностранных NGFW	Разработка инструментов для автоматического переноса конфигурации и правил с популярных зарубежных продуктов. Пока мало у кого из российских вендоров есть такие решения
Просадка производительности при попадании трафика в N-ное правило	Применение аппаратных ЦУС Проведение оценки корректности конфигураций с целью оптимизации политик безопасности Пилотирование, тестирование NGFW
Ограничение функционала и снижение качества	Применение мультивендорных сборок, в зависимости от места установки и решаемых задач Оптимизация процессов разработки Повышения контроля качества, развитие здоровой конкуренции
Зависимость от зарубежных поставщиков	Развитие производства собственных комплектующих Переход на отечественное ПО для администрирования СЗИ
Отсутствие технологий	Реверс-инжиниринг зарубежных решений
Отсутствие компетенций, проблемы при настройке и эксплуатации NGFW	Развитие базы знаний, форумов и обучающих центров Подготовка партнерских программ обучения Развитие гибких программ технической поддержки с учетом потребностей малого, среднего и крупного бизнеса
Сертификация	Подготовительная работа производителей с регулятором Внедрение и развитие процессов безопасной разработки

Выводы

На основании приведенного примера изучения рынка российских NGFW можно выделить следующие проблемы и пути их решения (см. табл. 1).

Процесс импортозамещения для многих субъектов ЗОКИИ пока является сложной и затратной задачей, мало кто сейчас может заявить о полном соответствии требованиям о технологической независимости и безопасности критической информационной инфраструктуры. Но российский рынок развивается, и с первой половины 2022 г., когда вступили в силу указы № 166 и № 250, количество российских вендоров NGFW к концу 2024 г. выросло в два раза (по нашим оценкам, до тридцати). Заметна также тенденция на ужесточение требований со стороны законодательства, что в свою очередь является драйвером для развития рынка. ●

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