ИНСТРУКЦИЯ ПО ПОДБОРУ NGFW

Next Generation Firewall (NGFW) представляют собой интегрированные платформы сетевой безопасности, в которых традиционные брандмауэры сочетаются с другими сетевыми решениями для фильтрации трафика, такими как системы глубокого анализа трафика Deep Packet Inspection (DPI), система предотвращения вторжений (IPS) и др.

Разберем механизмы защиты NGFW и категории выбора межсетевых экранов.

Функции безопасности одинаковые во всех NGFW:

- **DPI** – функция глубокой проверки пакетов на уровне приложений, а не только в рамках инспекции портов и протоколов.
- **IDS / IPS** – функция блокирует вредоносный трафик в режиме реального времени на основе сигнатур. Информация о новых угрозах обновляется в базе и поступает на устройства NGFW за 10–60 минут. IPS работает по принципу «запрещено все, что не разрешено», то есть если приложение не идентифицировано или выполняет нетипичные для него действия, оно будет заблокировано.
- **Антивирусные сигнатуры для NGFW** обновляются в онлайн-режиме. Трафик проверяется на наличие вирусов, шпионского ПО, троянов и червей.
- **DLP** – средство для предотвращение утечек данных в NGFW отслеживает все потоки данных, которые выходят за пределы локальной сети. При обнаружении в потоке конфиденциальной информации, передача автоматически блокируется. Иностранный регламент по защите персональных данных (General Data Protection Regulation, GDPR) ограничивает возможности вендоров в создании решений. Поэтому, в отличии от российских разработок, функции DLP сильно обрезаны.
- **Фильтрация по URL** позволяет автоматически блокировать скомпрометированные сайты, не загружая с них данные на основе репутационных данных.
- **VPN** – распространенная функция среди NGFW, обеспечивающая защиту почтовых сервисов, обмена данных, удаленной работы.
- **Инспектирование SSL** позволяет проверять SSL-трафик.
- **Антиспам**.
- **Application Control** отслеживает метки приложений, используемые в сети. Если пользователь попытается запустить неизвестную программу, NGFW заблокирует запуск и уведомит администратора.
- **Web Application Firewall** – схожий механизм что и Application Firewall для веб-приложений.
- **Аутентификация пользователей** – контроль прав доступа пользователей.
- **Sandboxing** – безопасная среда для тестирования, использующаяся для проверки подозрительных приложений и файлов.

Критерии для выбора:

1. **Работа компании в России**. Техподдержка, склады, представительства и сеть дистрибьюторов.
2. **Особенности NGFW**. Например, выбор количества оперативной памяти при покупке или уникальные процессоры.
3. **Собственные разработки компании**. Экосистема или исследовательские лаборатории.
4. **Количество моделей и удобство масштабирования**.

ОСНОВНЫЕ ПРОИЗВОДИТЕЛИ NGFW НА МИРОВОМ РЫНКЕ

Check Point Software Technologies LTD:

В России есть представительство Check Point в Москве. Для русскоязычных пользователей доступна поддержка на английском языке.

Отправить неисправное устройство можно на адрес представительства в Москве, а вот ждать его придётся со складов в Европе. В документах Check Point указано, что условия обмена устройств за сутки по специальной программе RMA доступны только в США и ЕС. Для остальных стран условия обговариваются индивидуально с клиентом.

Особенности покупки модели Check Point Quantum (как выбрать объем памяти и возможность гипермасштабирования файрволлов с помощью Master Hyperscale) представлены по ссылке.

> Например, компания занимается анализом больших данных и хочет поставить новое сетевое оборудование. На данный момент есть 2 заказа с известным трафиком, но непонятно, какие мощности понадобятся потом.
>
> Устанавливается аппаратный NGFW Check Point под текущий трафик, а если понадобится увеличить мощность — компания установит виртуальную версию NGFW в облаке или на своих серверах и соединит ее с устройством на предприятии.
>
> Пропускная способность файрволла увеличивается в 3–4 раза с помощью гипермасштабирования. В итоге компания платит только за реально необходимые мощности, и ей не нужно думать о создании «запаса на будущее». Ведь расширить схему можно в любой момент.
>
> Собственной разработкой компании является система защиты от угроз нулевого дня SandBlast Zero-Day Protection. Система основана на искусственном интеллекте и продвинутых алгоритмах эмуляции рабочий среды. Подробнее читайте в документе Check Point.

На сегодня есть 18 моделей, не считая линейки устройств для производств. Подобрать решение получится как для малого офиса, так и в дата-центр провайдера.

Описание моделей Check Point: 1590, 6400, 7000, 28000, 64000.

Fortinet:

Компания выпускает NGFW Fortigate в аппаратной и виртуальной версиях. В России у Fortinet свое представительство в Москве. Склады с оборудованием в Москве и Санкт-Петербурге.

Устройства на замену доставляют за 1–2 дня по этим городам, за несколько дней в другие регионы России (курьерской службой). Если бы склад находился в Европе, одна таможня могла задержать устройства на несколько недель.

Собственные разработки компании:

- Экосистема фабрики безопасности. Fortinet создает устройства для любых задач – от создания защищенного Wi-Fi подключения до управления сетью в 2000–3000 устройств.
- Процессоры ASIC.
- Лаборатория безопасности FortiGuard Labs, в которой разрабатываются алгоритмы искусственного интеллекта для обнаружения вторжений и анализируются данные об атаках и вирусах со всех устройств Fortinet в мире.
- Технология виртуальных доменов VDOMs. На одном Fortigate можно обрабатывать трафик с разных компаний, и он будет изолирован и защищен.

Моделей Fortigate больше 30, есть влаго- и пылезащищенные устройства для производств из серии Rudged. Легко найти устройство под любой размер компании и объем трафика.

Подробно о моделях можно прочитать в статье «Модельный ряд Fortigate» или в спецификациях на сайте Fortinet.

Описание моделей Fortinet: 60F, 200F, 1800F, 4200F, 7060E.

Cisco:

В России компания представлена лучше всех остальных. Маршрутизаторы Catalyst и модули для них, Wi-Fi точки доступа Aironet и другие товары производятся на заводе в Твери.

NGFW от Cisco не совсем NGFW. Это сервисы сетевой безопасности Firepower и ПО ASA, которые могут устанавливаться на обычные фаерволы, а не только специально спроектированную серию. Это значит, что можно расширить возможность оборудования в компании лишь купив лицензию, без физической замены.

Собственные разработки компании:

- Сервисы Firepower начали активно продвигаться на российском рынке в 2016–2017 годах.
- Кроме ориентации на софт, никаких прорывных технологий или новых решений в этом сегменте рынка нет.
- Академия сетевой безопасности Cisco и широкая сеть центров обучения. При дополнении сети новыми устройствами всегда можно пройти обучение в крупных городах.

Моделей на рынке 17 с 1U-место в стойке, независимо от производительности устройств. Check Point, Fortinet и Palo Alto последовательно увеличивают размер своих устройств с 1 до 4U.

Описание моделей Cisco: 1010, 2120–2140, 4145, 9300.

Palo Alto:

Именно Palo Alto придумали термин NGFW и закрепили его на рынке. Компания имеет представительство в Москве. Однако оно нигде не указывается. Материалов на русском нет, информации о техподдержке и складах оборудования — тоже.

Palo Alto считает особенностью своих межсетевых экранов технологию обработки трафика Single Pass. Каждая операция для пакета выполняется только один раз:

- установление соединения,
- загрузка пакета в память,
- дешифровка,
- применения правил происходит одновременно для каждой функции безопасности.

Подробнее о технологии и параллельной обработке трафика можно прочитать в методичке Palo Alto от 2011 года «The PA-5000 Series Architecture».

Собственные разработки компании:

- Система идентификации приложений App-ID
- Система идентификации пользователей User-ID
- Система идентификации данных Content-ID

13 моделей. Притом два флагмана задуманы для ЦОДов и для большинства компаний не нужны. Подобрать модель под себя может быть сложно — остается всего 11 в среднем и топ-сегменте. Полную спецификацию файрволлов Palo Alto можно найти по ссылке.

Описание моделей Palo Alto: 820, 3250, 5220-5280, 7080.