УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ФУНКЦИОНАЛЬНОСТИ NGFW И ТРАДИЦИОННЫХ МЕЖСЕТЕВЫХ ЭКРАНОВ НА ПЕРИМЕТРЕ КОМПЬЮТЕРНОЙ СЕТИ УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ

Романюк М.В.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Алексеев В.Ф. – канд.техн.наук, доцент, доцент кафедры ПИКС

Аннотация. Рассмотрена функциональность межсетевых экранов без отслеживания состояния и с отслеживанием состояния, а также межсетевые экраны нового поколения. Выявлены преимущества и недостатки использования различных технологий фильтрации сетевого трафика на периметре компьютерной сети. Предложены способы совершенствования методов защиты периметра компьютерной сети учреждения образования.

Ключевые слова: межсетевой экран, NGFW, защита периметра компьютерной сети

Введение. Защита периметра компьютерной сети является важным компонентом защиты данных организации. В современном мире существует большое количество методов и средств защиты информации, однако на периметре компьютерной сети чаще всего применяются брандмауэры с фильтрацией пакетов (без отслеживания состояния (*stateless firewall*), с отслеживанием состояния (*stateful firewall*) и брандмауэры нового поколения (*NGFW*). Каждый вид брандмауэра имеет свои преимущества и недостатки при эксплуатации, которые будут рассмотрены в данной статье [1–5].

Недостаточная степень защищенности периметра компьютерной сети неизбежно ведет к несанкционированному доступу к информации, ее повреждению или модификации.

В данной статье будет рассмотрена функциональность различных типов межсетевых экранов (МСЭ), выполнен сравнительный анализ, сделаны выводы и применимости данных типов межсетевых экранов для защиты периметра сети учреждения образования.

Основная часть. Для проведения сравнительного анализа функциональности различных типов межсетевых экранов необходимо рассмотреть функциональность каждого типа МСЭ и выделить их функциональные особенности, влияющие на возможность обеспечения требуемой степени защищенности компьютерной сети.

Брандмауэр с фильтрацией пакетов (*Packet filtering firewall*, *PFF*) – это самый базовый тип брандмауэра, который выполняет фильтрацию пакетов на основании проверки *IP* адреса источника и назначения, протоколов (*TCP, UDP*) и номеров портов. Пакеты маршрутизируются через брандмауэр только в том случае, если они соответствуют предопределенным правилам фильтрации; в противном случае они отклоняются.

PFF подразделяются на две категории:

– *PFF* с отслеживанием состояния;

– *PFF* без отслеживания состояния.

PFF с отслеживанием состояния – брандмауэр, работающий на 3 и 4 уровне модели *OSI*. Как следует из названия, межсетевой экран с контролем состояния всегда отслеживает состояние сетевых соединений. После того как определенный вид трафика был одобрен межсетевым экраном, он добавляется в таблицу состояний. Записи в таблице состояний создаются для потоков *TCP* или датаграмм *UDP*, которым разрешено проходить через брандмауэр в соответствии с настроенной политикой безопасности. Если в течение определенного времени (зависит от реализации) трафик отсутствует, соединение удаляется из таблицы состояний.

Под отслеживаем состоянием здесь понимается процесс контроля за состоянием процесса передачи. Например, в *TCP*-потоке клиент инициирует соединение при помощи трехстороннего рукопожатия. Флаг *SYN* при этом указывает на начало нового соединения. После

этого клиент должен получить от сервера сообщение с флагами *SYN+ACK*. После этого брандмауэр в своей таблице соединений помечает соединение как установленное (*established*) и разрешает коммуникацию в рамках данного соединения. Чтобы проверить принадлежность пакетов к разрешенной сессии брандмауэр использует контекст – метаданные соединения, которые включают в себя *IP*-адреса и номер порта источника и назначения, длину пакета, информацию 3 уровня, связанную с повторной сборкой и фрагментацией, порядковые номера пакетов *TCP*, флаги и т.д. Когда *PFF* с отслеживает состояния получает пакет с флагом *RST* или *FIN+ACK*, он помечает состояние соединения для удаления. Любые будущие пакеты для этого соединения будут отклонены [1].

К преимуществам *PFF* с отслеживанием состояния относят:

– высокая степень защиты от поддельных сообщения и несанкционированного доступа к компьютерной сети и сетевым сервисам;

– принятие решений о фильтрации сообщений принимается на основе прошлых и настоящих результатов;

К недостаткам *PFF* с отслеживанием состояния относят:

– повышенные требования к вычислительным ресурсам (оперативной памяти);

– невозможность обработки зашифрованного трафика (включая *HTTPS*), что ведет к возможности реализации атак посредством запуска веб-скриптов или передачи зараженных файлов через зашифрованные каналы связи;

– журналы содержат недостаточное количество информации для подробного анализа действий пользователей в сети;

– уязвимость атакам типа отказ в обслуживании (*DOS*).

PFF без отслеживания состояния также известен как список контроля доступа (*ACL*). Такой брандмауэр не хранит информацию о состоянии соединения и принимает решение о разрешении или запрете прохождения отдельного пакета только на основании предопределенных правил на основе адресов источника и получателя или других статических значений [2].

К преимуществам *PFF* без отслеживания состояния относят:

– высокая скорость обработки пакетов ввиду отсутствия необходимости контроля контекста сетевого трафика;

– высокая устойчивость к атакам типа отказ в обслуживании (*DOS*).

К недостаткам PFF без отслеживания состояния относят:

– невозможность идентификации типа трафика, что ведет к снижению безопасности в сравнении с PFF с отслеживанием состояния;

– журналы содержат недостаточное количество информации для подробного анализа действий пользователей в сети;

– необходимость глубоких знаний и понимания типа трафика в защищаемой компьютерной сети.

Таким образом, можно сделать вывод, что использование данных межсетевых экранов целесообразно только для защиты сети малого и среднего бизнеса.

Для защиты крупных корпоративных сетей в настоящее время существуют межсетевые экраны, которые позволяют выполнять глубокий анализ сетевого трафика и выявлять большее количество сетевых и вирусных атак.

Брандмауэр нового поколения (*Next Generation firewall*, NGFW) – межсетевой экран для глубокой фильтрации трафика с отслеживанием состояния, интегрированный с *IDS* (Intrusion *Detection System*, система обнаружения вторжений), *IPS* (*Intrusion Prevention System*, система предотвращения вторжений), *DLP* (*Data Leak Protection*) и обладающий возможностью контролировать и блокировать трафик на уровне приложений [3].

Такие межсетевые экраны относят к межсетевым экранам уровня приложений (7 уровень модели *OSI*) так как они выполняют фильтрацию не только на основе соединений, но и на основе содержимого пакетов, сигнатур приложений и файлов, репутации сайтов и приложений и т.д.

Современные *NGFW* имеют в своем арсенале большой набор программных компонентов для различных целей. Так, например, производитель межсетевых комплексов *Check Point* выделяет следующие компоненты *NGFW* [4]:

– *Firewall* – функционал традиционного межсетевого экрана;

– *IPSec VPN* – функционал для построения частных виртуальных сетей;

– *Mobile Access* – функционал организации удаленного доступа с мобильных устройств и ПК во внутреннюю сеть организации;

– *IPS* – система предотвращения вторжений;

– *Anti-Bot* – защита от ботнет сетей;

– *AntiVirus* – потоковый антивирус;

– *AntiSpam & Email Security* – функционал для защиты корпоративной почты;

– *Identity Awareness* – интеграция со службой Active Directory для аутентификации и авторизации пользователей;

– *Application Control* – межсетевой экран уровня приложений;

– *URL* Filtering – обеспечение безопасности доступа к веб-ресурсам с возможностью инспекции HTTPS трафика;

– *Data Loss* Prevention – функционал защиты от утечек информации (DLP);

– *Threat Emulation* – технология песочниц (*SandBox*);

– *Threat Extraction* – технология очистки файлов от вирусного функционала;

– *QoS* – приоритезация трафика.

К преимуществам *NGFW* относят:

– высокая степень защищенности;

– возможность контроля зашифрованного трафика (*HTTPS*);

– интеграция с различными вспомогательными системами (потоковый антивирус, *IPS*, *IDS, AntiBot* и т.д.)

– журналы содержат достаточное количество информации для глубокого ретроспективного анализа действий пользователей;

– возможность фильтрации трафика на основе поведения отдельных пользователей.

К недостаткам *NGFW* относят:

– высокая требовательность к вычислительным ресурсам (процессор и оперативная память), а также к объему дискового пространства;

– зависимость пропускной способности от количества анализируемой информации и характера трафика;

– высокая стоимость;

– высокие требования к квалификации администраторов.

В таблице 1 представлено сравнение описанных ранее типов МСЭ по различным критериям.

Таблица 1 – Сравнение основных характеристик МСЭ

Критерий оценки	**Характеристика Stateless PFF**	**Характеристика Stateful PFF**	**Характеристика NGFW**
1	**2**	**3**	**4**
Контроль за состоянием соединения	Нет	Контроль за состоянием соединения на основе флагов TCP-сессии	Контроль за состоянием соединения на основе флагов TCP-сессии

Продолжение таблицы 1

1	2	3	4
Критерий проверки попадания трафика под правила МСЭ	IP-адрес и порт источника или пункта назначения	IP-адрес и порт источника или пункта назначения, флаги TCP-сессии, номер пакета в TCP-сессии, размер пакета	IP-адрес и порт источника или пункта назначения, флаги TCP-сессии, номер пакета в TCP-сессии, размер пакета, сигнатуры приложений и файлов, службы репутации и идентификации личности пользователя
Контроль зашифрованных соединений	Нет	Нет	Возможна SSL-инспекция
Требовательность к вычислительным ресурсам	Низкая	Средняя, повышенные требования к оперативной памяти	Высокая, повышенные требования к оперативной памяти и процессору
Защита от вирусных атак	Очень низкая	Низкая	Высокая при использовании функционала потокового антивируса
Производительность и пропускная способность	Высокая	Ниже, чем у stateless PFF ввиду большего количества критериев оценки	Равна или ниже, чем у stateful PFF, значительно изменяется в зависимости от количества анализируемой информации и характера трафика
Логирование	Статистика по количеству отброшенных пакетов с определенным адресом источника или пункта назначения	Статистика по количеству отброшенных пакетов с определенным адресом источника или пункта назначения	Статистика по количеству отброшенных пакетов с определенным адресом источника или пункта назначения, используемого приложения или сервиса с указанием пользователя и других критериев, по которым производится фильтрация
Сложность настройки и администрирования	Средняя сложность, необходимы глубокие знания и понимание типа трафика в защищаемой сети	Средняя сложность	Высокая сложность, необходимо специализированное обучение персонала для организации высокой степени защищенности компьютерной сети
Стоимость	Бесплатные решения или низкая стоимость	Бесплатные решения с ограничением по производительности или функциональности или средняя стоимость	Высокая стоимость
Целевая аудитория	Малый бизнес	Средний бизнес	Крупный бизнес,ЦОД, государственные органы и службы

Учебные заведения в большинстве случаев можно отнести к представителям крупного бизнеса. Это обусловлено большим количеством сотрудников и обучающихся с совокупности с необходимостью контроля за их действиями в компьютерной сети.

Одной из ключевых особенностей доступа к компьютерной сети в учреждениях образования является возможность подключения к компьютерной сети с личных устройств, которые не контролируются администраторами сети, не имеют антивирусного ПО и корпоратив-

ных утилит и, следовательно, на данных устройствах не может быть гарантировано отсутствие вредоносного ПО. Это потенциально расширяет поверхность атак на сеть и корпоративные сервера и сервисы.

Исходя из вышесказанного можно сделать вывод о том, что для жесткого контроля за безопасностью сети учебного заведения целесообразно использование межсетевых экранов нового поколения.

Заключение. Выполнен анализ *PFF* и *NGFW*-решений для защиты периметра компьютерной сети. Выявлено, что для защиты периметра сети учреждения образования, как представителя крупного бизнеса, целесообразнее всего использовать *NGFW*, который позволяет гибко контролировать набор правил, согласно которым происходит фильтрация входящего и исходящего трафика. *NGFW*, благодаря подсистемам глубокой фильтрации трафика, позволяет заблокировать вредоносный трафик и предотвратить различные типы вторжений на периметре компьютерной сети.

Для более полной защиты компьютерной сети необходимо введение ограничений на загрузку исполняемых файлов, ограничение доступа к потенциально вредоносным и опасным сайтам различных категорий, а также введение расширенного логирования для всех правил с описанием всех установленных и отклоненных сетевых сессий.

Список литературы

1. *Stateless vs Stateful Packet Filtering Firewalls [Electronic resource]. – Web-portal Geeks for geeks, 2021. – Mode of access : https://www.geeksforgeeks.org/stateless-vs-stateful-packet-filtering-firewalls/. – Date of access : 18.03.2023.*

2. *Understanding Stateful vs Stateless Firewalls for Stateful Protocol Inspection [Electronic resource] / ed. Rupesh Mishra. – Illumio Cybersecurity Company, 2019. – Mode of access : https://www.illumio.com/blog/firewall-stateful-inspection. – Date of access : 19.03.2023.*

3. Next Generation Firewall (NGFW) [Электронный ресурс] / Энциклопедия лаборатории Касперского. – Режим доступа : https://encyclopedia.kaspersky.ru/glossary/next-generation-firewall-ngfw/. – Дата доступа : 20.03.2023.

4. Integrated *security architecture [Electronic resource]. – Check Point Software Technologies Ltd, 2021. – Mode of access : https://www.checkpoint.com/downloads/product-related/brochure/Software-Blades-Architecture.pdf. – Date of access : 17.03.2023.*

5. Оценка качества передачи информации в системе диспетчеризации на базе MQTT-архитектуры / В. Ф. Алексеев [и др.] // BIG DATA and Advanced Analytics = BIG DATA и анализ высокого уровня : сборник научный статей VIII Международной научно-практической конференции, Минск, 11-12 мая 2022 года / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: В. А. Богуш [и др.]. – Минск, 2022. – С. 483–488.

UDC 004.056.53

COMPARATIVE ANALYSIS OF NGFW FUNCTIONALITY AND TRADITIONAL FIREWALLS ON THE PERIMETER OF AN EDUCATIONAL INSTITUTION'S COMPUTER NETWORK

Romaniuk M.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Alekseev V.F. – PhD, associate professor, associate professor of the Department of ICSD

Annotation. The functionality of stateless and stateful firewalls, as well as new generation firewalls, is considered. The advantages and disadvantages of using various technologies for filtering network traffic at the perimeter of a computer network are revealed. Methods for improving the methods of protecting the perimeter of the computer network of an educational institution are proposed.

Keywords: firewall, NGFW, computer network perimeter protection