Е. А. Степанов, Н. С. Шутылев, А. А. Оленников
Тюменский государственный университет, г. Тюмень
УДК 004.057

РАЗРАБОТКА БЛОКА МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ И БАЛАНСИРОВКИ НАГРУЗКИ ДЛЯ ВИРТУАЛЬНЫХ ЛАБОРАТОРНЫХ СРЕД

Аннотация. В статье предложена концепция блока межсетевого экранирования и балансировки нагрузки для виртуальных лабораторных сред. Авторами описаны функции данного блока и алгоритм его работы. Также были изучены основные функции межсетевого экранирования и балансировки нагрузки в D-link DFL 860E и описан возможный способ сопряжения блока с виртуальным стендами.

Ключевые слова: информационная безопасность, киберполигон, балансировка нагрузки, межсетевой экран, виртуальная среда, виртуальные стенды.

Введение. В связи с активной разработкой на кафедре информационной безопасности Тюменского государственного университета виртуальных лабораторных работ и Киберполигона [1, 2], возникла необходимость в виртуальном блоке межсетевого экранирования, который предоставлял бы пользователям широкие возможности по обеспечению безопасности различных сетевых инфраструктур.

Виртуальные лабораторные работы представляют из себя эмуляции информационных инфраструктур, приближенных к реальным (рис. 1). Их задачей является моделирование реальных производственных процессов. Для обеспечения информационной безопасности, в этих инфраструктурах могут использоваться межсетевые экраны, функционал которых в виртуальной среде должен быть реализован программно.

Киберполигон, как платформа для виртуального моделирования ИТ-ландшафтов различных сегментов бизнеса, необходим для практической отработки навыков кибероборонs сетей предприятий. На его базе планируется реализовать несколько сценариев использования, два из которых — это Защита информационной инфраструктуры и Нападение на нее (пентест). Для их проведения планируется смоде-

лировать серию систем, в которых используется различное телекоммуникационное оборудование. Межсетевые экраны, являясь разновидностью такого оборудования [3], также как и в виртуальных лабораторных работах, должны быть представлены программно.

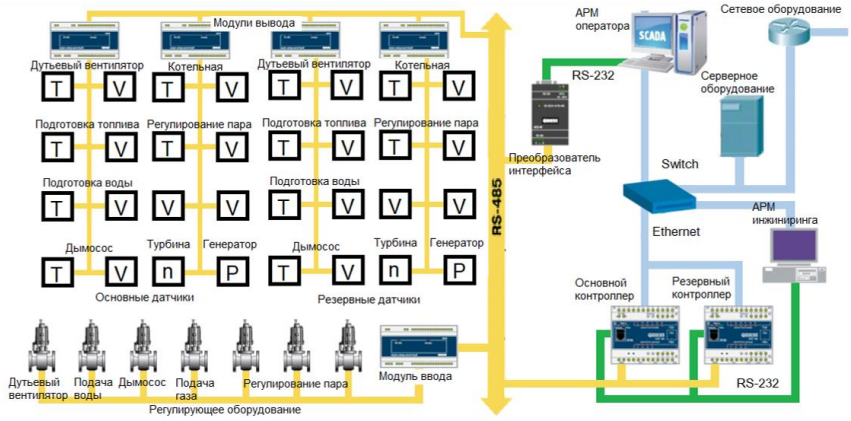

Рис. 1. Виртуальный стенд, моделирующий автоматизированную систему управления блочного модуля ТЭЦ

На сегодняшний день на рынке существует большое количество межсетевых экранов от различных производителей, каждый из которых обладает своим набором технологий, определяющим применимость устройства в той или иной ситуации [4]. Так как в различных виртуальных лабораторных работах от файрволлов может требоваться разный функционал, блок межсетевого экранирования должен быть универсальным. Его универсальность будет заключаться в возможности конфигурирования набора технологий, необходимых в конкретном проекте.

Несмотря на широкий спектр существующих устройств, все они обладают базовым функционалом межсетевого экранирования, а именно фильтрации трафика и аудита событий [5]. Этот факт и поставленное условие универсальности ставят определенные требования при выборе способа проектирования [6] программного продукта. На данный момент, наиболее подходящим под поставленные

задачи видится шаблонный метод. При его использовании блок будет обладать базовым функционалом межсетевого экранирования и работать по определенному алгоритму. С помощью шаблонов, реализующих технологии работы реальных межсетевых экранов, функционал блока может быть расширен, а поведение алгоритма переопределено в некоторых частях без изменения его структуры.

Также было решено добавить в базовый блок основные функции балансировки нагрузки [7, 8] и строить алгоритм работы устройства, принимая их во внимание. Это увеличит применимость блока без наложенных шаблонов в различных виртуальных лабораторных работах, что, в частности, расширит спектр предоставляемых студентам топологий и задач на базе Киберполигона (рис. 2, 3).

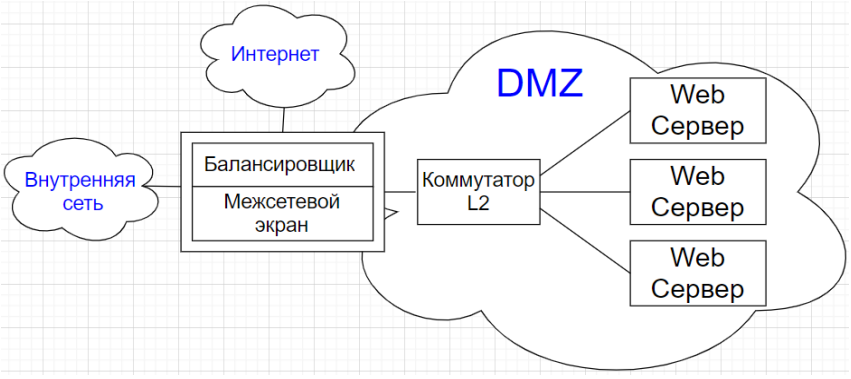

Рис. 2. Пример применения блока в офисной инфраструктуре

Например, в случае отработки сценария защиты, можно потребовать от обучающихся подготовить информационную инфраструктуру к DoS-атаке, или, в случае сценария нападения, вычислить пул серверов, между которыми распределяется трафик.

Проблема. Необходимо разработать программный блок, имеющий базовый функционал межсетевого экранирования и балансировки нагрузки, а также механизм наложения технологий работы различных вендоров при помощи шаблонов. При этом, в дальнейшем, блок будет сопрягаться с виртуальными лабораторными стендами.

Рис. 3. Пример применения блока в промышленной инфраструктуре

Материалы и методы. При проведении исследования мы поставили себе следующие задачи:

- Изучить технологию работы некоторых межсетевых экранов.
- Проанализировать работоспособность межсетевых экранов в конкретной инфраструктуре.
- Разработать алгоритм работы блока межсетевого экранирования с балансировкой нагрузки.
- Спроецировать функционал межсетевого экрана D-link на разрабатываемый блок.

– Найти способ сопряжения блока межсетевого экранирования и балансировки нагрузки с виртуальными лабораторными стендами.

В рамках проведенного анализа технологии работы межсетевых экранов в различных инфраструктурах, следующие функции были выделены как основные и необходимые для работы виртуального блока в качестве межсетевого экрана с балансировкой нагрузки:

Функции межсетевого экранирования:

- формирование адресной книги;
- формирование базы портов и сервисов;
- формирование базы сетевых правил;
- аудит событий, вызванных блокировкой трафика.

Функции балансировки нагрузки:

- обнаружение службы (получение адресов устройств, среди которых нужно распределять трафик);
- балансировка нагрузки по выбранной технологии;
- проверка работоспособности устройств.
- Общие функции:
- формирование набора виртуальных интерфейсов Ethernet;
- маршрутизация/коммутация;
- обработка трафика (NAT, GRE и прочее).

Также был сформирован общий алгоритм обработки сетевого пакета после его попадания на виртуальный интерфейс блока (рис. 4).

Чтобы лучше понять то, как должны выглядеть основные функции нашего виртуального блока, стоит посмотреть на их реализацию в реальных межсетевых экранах. В нашем случае был выбран D-link DFL 860E. Это устройство имеет адресную книгу, содержащую записи об IP-адресах сетей и хостов, которые используются при составлении сетевых правил. Также у него есть база портов и сервисов, записи которой описывают группы портов и протоколов и также используются в сетевых правилах. Сама база сетевых правил, называемая Main IP Rules, помимо правил фильтрации трафика, содержит записи о трансляции адресов и балансировке нагрузки. О последних стоит сказать подробнее.

При создании правил балансировки нагрузки, указывают параметры трафика, который нужно распределять по разным серверам. Затем выбираем адреса этих серверов из адресной книги и выделяем метод балансировки нагрузки (Round-robin, Connection-rate или Resource-usage). Также можно включить и настроить проверку работоспособности серверов с помощью периодической отправки icmp, tcp или http запросов.

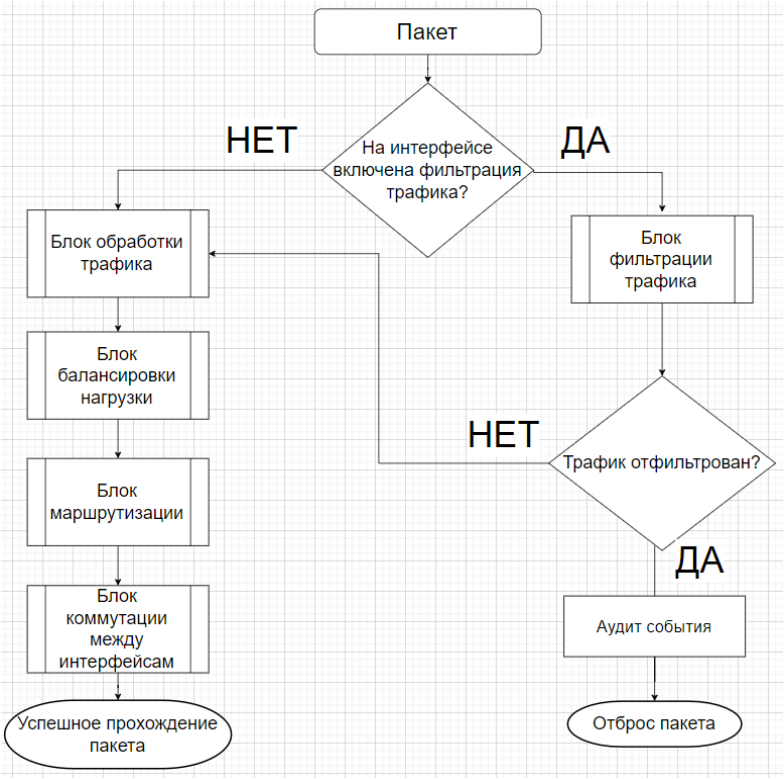

Рис. 4. Общий алгоритм обработки сетевого пакета

Аудит в D-link DFL 860E реализован в виде функций ведения журнала и анализа функционирования системы NetDefendOS, несколько сотен событий, после которых генерируются сообщения для записи в журнал. Генерацию таких сообщений можно гибко настроить через политики безопасности.

Также стоит упомянуть, что D-link DFL 860E поддерживает как статическую, так и динамическую маршрутизацию через OSPF.

Вопрос сопряжения блока межсетевого экранирования и балансировки нагрузки с виртуальными средами должен быть решен перед началом его создания, так как от этого зависит выбор набора

инструментов разработки. Мы изучили работу популярных сред виртуализации, а именно GNS3 и EVE-NG, и пришли к выводу, что наиболее оптимальным вариантом будет разработка блока на базе системы виртуализации QEMU, так как она используется во многих виртуальных средах и имеет широкие возможности по настройке. У самой виртуальной машины планируется сформировать набор виртуальных сетевых интерфейсов Ethernet и использовать ее под управлением операционной системы на базе ядра Linux. На основе nftables, подсистемы ядра Linux, будут реализованы функции межсетевого экранирования и балансировки нагрузки, описанные выше. Для предоставления возможности конфигурирования виртуального блока извне, должен быть разработан интерфейс командной строки.

Результаты. Авторами была продемонстрирована концепция блока межсетевого экранирования и балансировки нагрузки для виртуальных лабораторных работ и Киберполигона, а также его необходимость в этих средах. Выделены основные функции блока и исследована их реализация в D-link DFL 860E. Показан алгоритм его работы и предложен способ реализации с возможностью использования в виртуальных лабораторных средах.

Заключение. Проведенное исследование представляет из себя подготовительный этап перед началом разработки виртуального блока межсетевого экранирования и балансировки нагрузки. В результате была сформирована общая концепция программного продукта и выявлены направления дальнейших исследований, которые предстоит провести перед его реализацией. Необходимо подробнее изучить следующие проблемы:

- проектирование программного блока с возможностью наложения технологии работы реальных устройств, используя шаблонный метод;
- степень упрощения в работе блока по сравнению с реальными межсетевыми экранами;
- способы взаимодействия блока с виртуальными лабораторными стендами.

СПИСОК ЛИТЕРАТУРЫ

1. Толстогузов В. С. Разработка виртуального тренажера автоматизированного теплового пункта / В. С. Толстогузов, А. А. Оленников. — Текст : непосредственный // Математическое и информационное моделирование: всерос. конф. молодых ученых 17-21 мая 2021 г. — Тюмень, 2021. — С. 345-350.
2. Оленников А. А. Автоматизированный низкотемпературный стенд струйно-эмульсионного металлургического агрегата для моделирования штатной и аварийной работы / А. А. Оленников, В. А. Долгушин. — Текст : непосредственный // Математическое и информационное моделирование : всерос. конф. молодых ученых 18-23 мая 2022 г. — Тюмень, 2022. — С. 265-275.
3. Синадский Н. И. Методология синтеза интерактивной сетевой среды для компьютерных полигонов в сфере информационной безопасности : 2.3.6 : дис. … д-р техн. наук / Н. И. Синадский ; УрФУ. — Екатеринбург, 2022. — 304 с. — Текст : непосредственный.
4. Трещев И. А. Анализ межсетевых экранов для защиты периметра локально-вычислительной сети / И. А. Трещев, А. С. Ватолина. — Текст: непосредственный // Производственные технологии будущего: от создания к внедрению : междунар. науч.-практ. конф. 14 июня 2019 г. — Комсомольск-на-Амуре, 2019. — С. 304-308.
5. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание / В. Г. Олифер, Н. А. Олифер. — Санкт-Петербург: Питер, 2020. — 1008 с. — Текст: непосредственный.
6. Куликова Н. Н. Паттерны проектирования: обзор и решаемые задачи / Н. Н. Куликова, А. Д. Соломыков, О. А. Маширов, И. В. Арсеньев. — Текст : непосредственный // Наука и инновации в XXI веке: актуальные вопросы, открытия и достижения : XXVIII междунар. науч.-практ. конф. 20 дек. 2021 г. — Пенза, 2021. — С. 78-80.
7. Klein M. Introduction to modern network load balancing and proxying / M. Klein. — URL: https://blog.envoyproxy.io/introduction-to-modern-network-load-balancing-and-proxying-a57f6ff80236 (date of the application 21.05.2023). — Text : electronic.
8. Kopparapu C. Load Balancing Servers, Firewalls, and Caches / C. Kopparapu. — New York : John Wiley & Sons, 2002. — 224 p. — Direct text.