ОБОСНОВАНИЕ ВЫБОРА ЭМУЛЯТОРА GNS3 ДЛЯ ИЗУЧЕНИЯ ПРИНЦИПОВ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ С МЕЖСЕТЕВЫМ ЭКРАНИРОВАНИЕМ

До М.К., ст. гр. 961402

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук

Аннотация. В статье представлены результаты сравнения и обоснования выбора среды моделирования для изучения принципов конфигурации межсетевых экранов и их внедрения в локальные сети. Показаны преимущества использования GNS3 VM и межсетевой экрана FortiGate-VM. Составлены рекомендации по использованию GNS3 в образовательном процессе.

Ключевые слова. Моделирование локальных сетей, межсетевой экран, GNS3, Fortinet, FortiGate.

GNS3 (Graphical Network Simulator 3) – это программный эмулятор сетевого оборудования, который позволяет создавать модели виртуальных сетей [1-2]. Его главным отличием от известного симулятора локальных сетей Cisco Packet Tracer является полная эмуляция сетевых устройств без ограничения их функциональности. GNS3 поддерживается различными операционными системами (Microsoft Windows, MacOS, Linux), его использование является бесплатным и требует лицензии. GNS3 включает в себя два вида программного обеспечения: GNS3-all-in-one software (GUI), GNS3 virtual machine (VM). В GNS3 есть поддержка эмуляции сетевых устройств разных производителей (Fortinet, Juniper и др.), а также серверов и оконечных устройств с разными операционными системами (Windows, Ubuntu). Работа GNS3 основана на использовании среды виртуализации, VirtualBox или VMWare.

Использование эмуляторов сетевого оборудования упрощает настройку, управление и мониторинг смоделированной виртуальной сети благодаря удобному графическому интерфейсу, который предназначен для опытных специалистов, имеющих опыт работы с технологиями виртуализации. Графические инструменты GNS3 позволят более быстро и легко осуществлять проектирование виртуальной сети.

Таким образом, можно выделить следующие основные достоинства использования программного эмулятора сетевых устройств GNS3 для изучения принципов построения локальных сетей:

− возможность полной эмуляции сетевых устройств без ограничения их функционала;

− проектирование гетерогенных сетей, которые будут включать в себя устройства разных производителей;

− внедрение в спроектированную виртуальную сеть полноценных рабочих станций и серверов под управлением разных операционных систем.

При создании топологии в GNS3 созданные устройства должно быть размещены и запущены серверным процессом. Существует несколько вариантов серверной части ПО: локальный сервер GNS3, локальная виртуальная машина Если устройство пользователя использует виртуальную машину GNS3, ее запуск осуществляется на ПК с помощью программного обеспечения для виртуализации, также возможен запуск виртуальной машины GNS3 удаленно на сервере с помощью VMWare ESXi или в облаке. Возможно использование GNS3 без виртуальной машины GNS3, но при этом функционал будет ограничен. При необходимости создания сложной топологии GNS3 с использованием таких устройств как Cisco VIRL, для которого требуется Qemu, требуется запуск виртуальной машины GNS3. Таким образом, GNS3 поддерживает как эмулированные, так и смоделированные устройства.

При установке необходимо совпадение версий программного обеспечения GNS3 и GNS3 VM, в данной работе использовалась версия 2.2.32, реализованная на платформе VMware Workstation версии 14.0. Для построения топологии сети в VMware Workstation были добавлены виртуальные машины GNS3 в качестве удаленного сервера и Window 10 в качестве клиента.

Установка GNS3 VM начинается с запуска VWware Workstation Player14, выбора пункт Open a Virtual Machine и добавления вирутальной машины, скачанной с сайта GNS3. В открывшемся окне вводится имя GNS3 VMware. Образ будет импортирован в хранилище виртуальных машин vmware.

Для настройки программного обеспечения GNS3 и его синхронизации с виртуальной машиной GNS3 VM в VMware необходимо перейти в раздел Edit → Preferences → GNS3 и активировать «Enable the GNS3 VM», выбрать имя добавленной в VMware виртуальной машиной GNS3 VM.

Межсетевые экраны являются аппаратно-программными устройствами или программами, которые регулируют поток сетевого трафика между сетями. Большинство межсетевых экранов расположено на границы сетевого периметра, и в первую очередь они предназначены для защиты внутренних устройств от внешних атак.

На рисунке 1 показан пример получения доступа и настройки IP-адреса межсетевого экрана FortiGate-VM посредством CLI (Command Line Interface), на рисунке 2 – результат подключения с помощью GUI (Graphic User Interface).

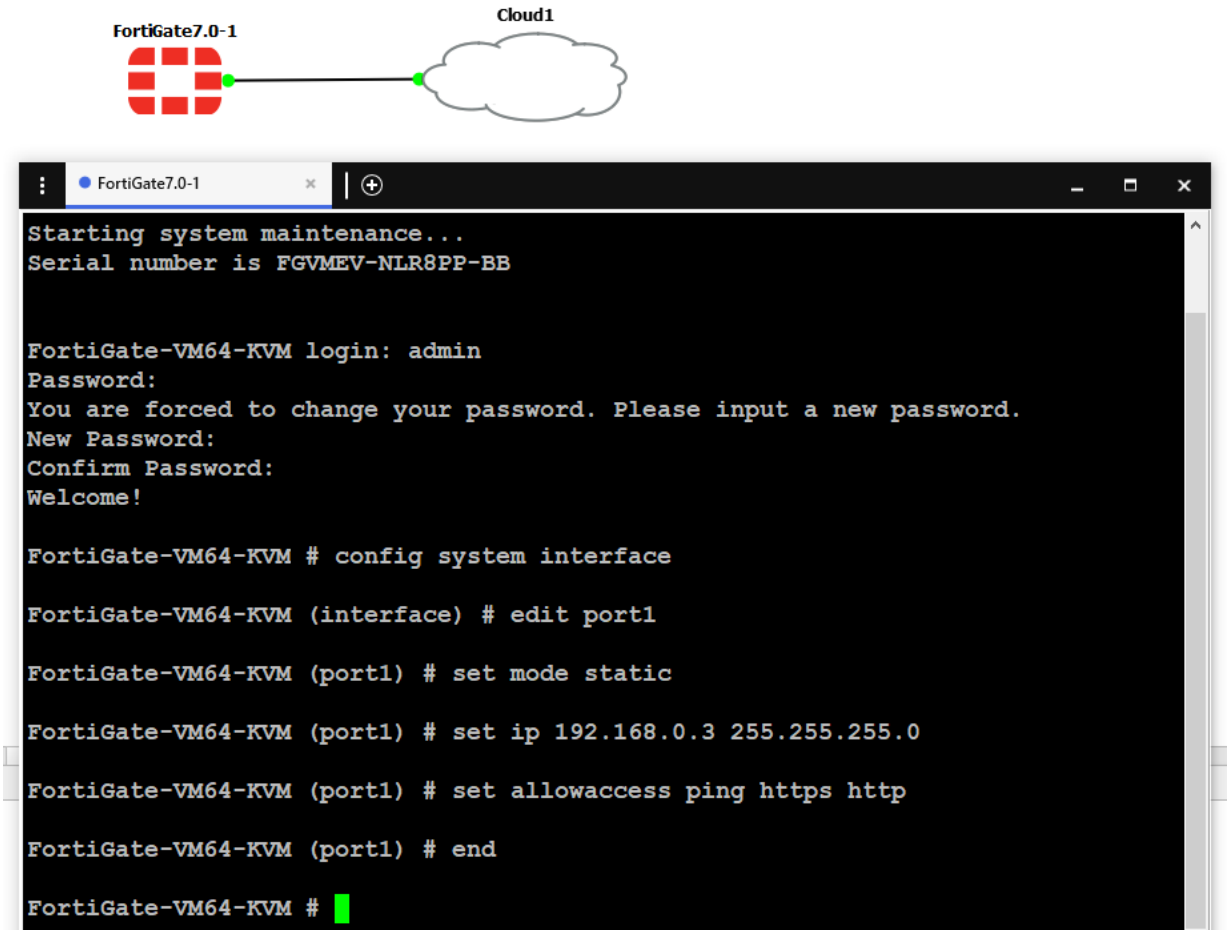

Рисунок 1 – Результат добавления FortiGate-VM в рабочую область GNS3 и получения доступа по CLI

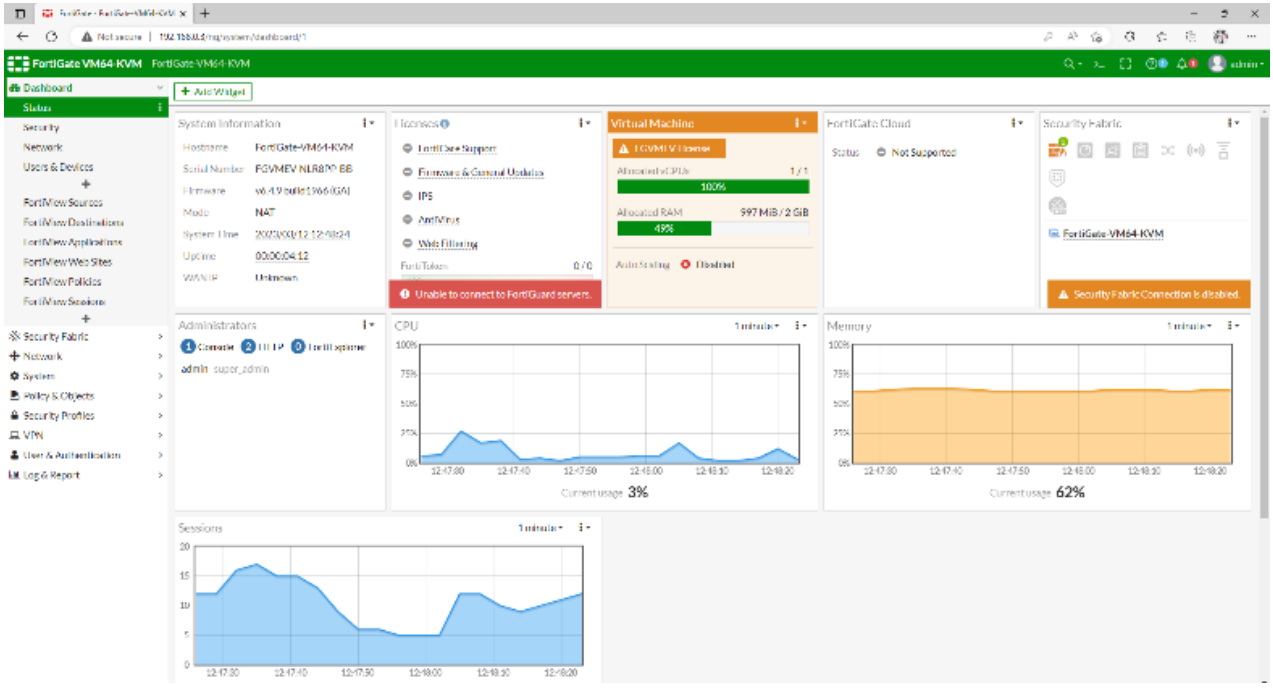

Рисунок 2 – Результат подключения к FortiGate-VM посредством GUI

FortiGate-VM – это полнофункциональный межсетевой экран FortiGate в виде виртуального устройства [3], которое подходит для мониторинга и управления виртуальным трафиком на платформах виртуализации, облаках и SDN, включая VMware vSphere, Hyper-V, Xen, KVM и AWS. FortiGate-VM можно организовать в программно-определяемой среде для предоставления гибких и эластичных услуг сетевой безопасности для виртуальных рабочих нагрузок.

Для скачивания FortiGate-VM на сайте Fortinet [4] необходимо в разделе Support → VM images выбрать платформу KVM. Далее в консоли GNS3 после подключения к виртуальной машине GNS3 необходимо добавить FortiGate в разделе Browse all appliances → New template → Install an appliance from the GNS3 server → Next → Firewalls → FortiGate → Install → Install the appliance on the GNS3 → Next.

Как только образ FortiGate-VM будет установлен на виртуальной машине GNS3, его можно добавить на рабочую область и осуществить конфигурацию (рисунок 1).

Таким образом, GNS3 – это одна из самых популярных программ эмуляции сети, которая позволяет не только изучать взаимодействие сетевых устройств в различных топологиях сетей, но и осуществлять их конфигурацию. В GNS3 эмулируются все основные компоненты устройств, в том числе процессор, память, устройства ввода/вывода, имитируется поведение системы и ее интерфейсов. Описанные достоинства и удобства использования GNS3 на примере добавления и конфигурации FortiGate-VM позволяют рекомендовать его для изучения принципов построения локальных сетей с межсетевым экранированием.

Список использованных источников:

1 Getting Started with GNS3 [Электронный ресурс]. – Режим доступа: https://docs.gns3.com/docs/.

2. Основы GNS3. Обзор [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/266503/.

3. Fortinet FortiGate VM Series [Электронный ресурс] – Режим доступа: https://www.avfirewalls.com/Fortigate-VM-Series.asp.

4. How to add a FortiGate VM into the GNS3 [Электронный ресурс] – Режим доступа: https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-add-a-FortiGate-VM-into-the-GNS3/ta-p/242132