

Разработка архитектуры виртуализированной среды для тестирования одноранговых сетей

В.Д. Зюзин¹, В.Д. Красавин²

*Нижегородский государственный университет им. Н.И. Лобачевского
Высшая школа экономики – Нижний Новгород*

Аннотация: В работе описывается виртуализированная среда, позволяющая проводить комплексные эксперименты с одноранговыми сетями и алгоритмами информационной безопасности. Архитектура построена на интеграции гипервизора VMware и платформы эмуляции сетевых устройств EVE-NG, что обеспечивает гибкое распределение ресурсов и воспроизведение реалистичных топологий. Центральным узлом выступает маршрутизатор MikroTik, через который организована «звездообразная» схема взаимодействия виртуальных машин на различных ОС (Windows 7, 10, 11, Linux Debian). Продемонстрировано, как выбранная конфигурация упрощает тестирование алгоритмов множественных стартовых соединений и многоуровневой криптографии, обеспечивает устойчивую маршрутизацию и допускает дальнейшую автоматизацию установки ПО с помощью Bash- или PowerShell-скриптов.

Ключевые слова: информационная безопасность, виртуализированная среда, множественные стартовые соединения, одноранговая сеть, виртуальная частная сеть.

Введение

Одноранговые (Peer-to-Peer – P2P) сети находят широкое применение в задачах распределенного обмена данными и построения виртуальных частных сетей, требующих повышенной анонимности и отказоустойчивости [1]. В предыдущих работах предложены алгоритмы множественных стартовых соединений [2] и многоуровневой криптографической защиты [3], направленные на повышение безопасности в одноранговых виртуальных частных сетях. Однако полноценное тестирование подобных решений невозможно без корректно развернутой и управляемой виртуальной инфраструктуры, позволяющей моделировать различные сценарии маршрутизации и анализировать их устойчивость к кибератакам.

Предлагаемая архитектура виртуализированной среды базируется на интеграции технологий VMware и EVE-NG и отличается рядом нововведений по сравнению с известными решениями. В частности, уникальность разработки заключается в возможности одновременного моделирования

сценариев маршрутизации и тестирования алгоритмов безопасности с использованием виртуальных машин на различных операционных системах (ОС) Windows и Linux, а также интеграцией виртуального маршрутизатора MikroTik. Новизна предлагаемой архитектуры также заключается в ее модульности и масштабируемости, позволяющих быстро адаптировать среду под специфические задачи и увеличивать ее возможности за счет добавления новых узлов и сценариев. Данная архитектура позволяет реализовывать сложные алгоритмы, такие, как множественные стартовые соединения и многоуровневая криптографическая защита, в условиях, максимально приближенных к реальным.

Использование платформ VMware и EVE-NG оправдано их широким функционалом и развитым сообществом, что делает их востребованными как в научных исследованиях, так и в образовательных целях.

Обоснование выбора виртуальных платформ VMWare и EVE-NG

В научной литературе по вопросу выбора инструментов виртуализации уделяется особое внимание гибкости и масштабируемости создаваемых стендов, поскольку они должны удовлетворять требованиям как фундаментальных исследований, так и прикладных проектов. В данной работе для решения этих задач задействованы платформы VMware и EVE-NG, зарекомендовавшие себя на рынке не только устойчивой производительностью, но и широкими возможностями интеграции с реальным оборудованием.

Продукт VMware заслуженно считается одним из наиболее стабильных гипервизоров, успешно применяемых в учебно-научной среде. Его обширный функционал обеспечивает запуск множества виртуальных машин при растущей нагрузке, а поддержка различных систем управления дает возможность исследователям эффективно координировать работу распределенных узлов. Подобная архитектура особенно востребована в

ситуациях, когда необходимо экспериментировать с передовыми методами сетевой безопасности либо моделировать сложные вычислительные процессы.

EVE-NG, в свою очередь, ориентирована на эмуляцию реальных сетевых топологий, что дает исследователю возможность воспроизводить инфраструктуру любой сложности. Наличие в EVE-NG механизмов загрузки образов «железных» маршрутизаторов и иных устройств существенно упрощает переход от теоретических схем к практически значимой эмуляции. Благодаря этой платформе возможно детальное изучение одноранговых сетей, включая вопросы анонимности и криптографической защиты, а также анализ протоколов маршрутизации в сценариях, максимально приближенных к реальным условиям эксплуатации. Кроме того, бесплатная версия EVE-NG делает ее привлекательной для лабораторий, не обладающих крупным финансированием.

Сообщество пользователей, сформировавшееся вокруг VMware и EVE-NG, предоставляет открытый доступ к методическим материалам и обмену наработками, что облегчает процесс освоения данных технологий. Наконец, обе платформы хорошо масштабируются, позволяя вначале работать с небольшими топологиями и постепенно переходить к крупным исследовательским стендам. Именно поэтому комбинация VMware и EVE-NG часто выбирается для научных экспериментов, связанных с тестированием новых алгоритмов в сфере информационной безопасности и сетевых технологий.

Аппаратно-программная конфигурация исследовательского стенда

Для решения ресурсоемких задач виртуализации в данном исследовании была использована конфигурация, обеспечивающая высокую производительность и широкие возможности масштабирования. В ее основе лежит материнская плата MSI PRO Z690-P DDR4, изначально

предназначенная для совместной работы с процессорами семейства Intel Alder Lake. В данной системе установлен центральный процессор Intel Core i5-13400, обладающий номинальными десятью вычислительными ядрами и шестнадцатью потоками с базовой тактовой частотой 2,5 ГГц (с повышением до 4,6 ГГц в режиме Turbo). С целью улучшения совместимости с некоторыми инструментами виртуализации были отключены четыре энергоэффективных ядра, в результате чего активными остались шесть продуктивных ядер, дающих в сумме двенадцать потоков.

Для визуально-интенсивных или графически нагруженных задач в конфигурацию добавлена видеокарта Colorful iGame GeForce RTX 3060 Ultra W OC, обладающая 12 ГБ видеопамати. Наличие такого GPU позволяет эффективно решать проблемы рендеринга и поддерживать ускоренную обработку ряда вычислительных процессов. В качестве основного накопителя используется твердотельный SSD SAMSUNG PM9A1 (объем 1 ТБ, интерфейс PCIe 4.0), что существенно снижает задержки при работе с данными. Дополнительно система снабжена классическим жестким диском WD Blue Desktop на 500 ГБ, ориентированным на долгосрочное хранение резервных копий.

Объем оперативной памяти достигает 96 ГБ, набранных из модулей Patriot Viper 4 (64 ГБ) и ADATA XPG Spectrix D60G (32 ГБ). Подобная конфигурация памяти дает возможность одновременно запускать несколько виртуальных машин с достаточным запасом ресурса. Высокоскоростной сетевой адаптер Tenda 3, поддерживающий передачу данных до 2,5 Гбит/с, обеспечивает необходимую полосу пропускания при взаимодействии с удаленными или локальными узлами.

Вся инфраструктура функционирует под управлением ОС Windows 11 Pro, в которой активирована аппаратная поддержка виртуализации Intel VT-x. Данный выбор позволил использовать

усовершенствованные механизмы распределения ресурсов и обеспечил совместимость с широким спектром программных средств для построения экспериментальных стендов.

Развертывание гипервизора VMWare и конфигурация виртуальных машин

Для создания исследовательской среды, способной удовлетворить потребностям как в управлении вычислительными ресурсами, так и в эмуляции сетевых устройств, сначала был развернут гипервизор VMware. Процесс установки начинался с загрузки дистрибутива с официального сайта [4] и включал установку необходимых компонентов, обеспечивающих поддержку аппаратной виртуализации и многопоточности. На этапе конфигурации основной виртуальной машины задействовали двенадцать потоков процессора, 64 ГБ оперативной памяти и 100 ГБ дискового пространства (динамический тип хранения). Такая политика обеспечения ресурсами была выбрана с учетом перспективы параллельного запуска нескольких узлов и проведения ресурсоёмких экспериментов.

Следующим шагом стало импортирование в VMware дистрибутива EVE-NG [5], которому также выделили требуемые объемы оперативной памяти и CPU-потоков. При первом запуске EVE-NG была выполнена стандартная инициализация: настройка пароля администратора, имени хоста и сетевых параметров. Для стабильного доступа к веб-интерфейсу использовался статический IP-адрес, а в качестве DNS-серверов выбраны общедоступные узлы (8.8.8.8). Данная конфигурация позволяет в дальнейшем без сложностей добавлять новые виртуальные машины либо подключать дополнительное оборудование, необходимое для экспериментов по моделированию одноранговых сетей.

После успешной инициализации EVE-NG осуществлялось подключение к ее веб-интерфейсу, где последовательно развернули четыре

виртуальные машины с различными операционными системами: Windows 7 Pro, Windows 10 Pro, Windows 11 Pro [6] и Linux Debian 10 [7]. Каждая из этих машин получила по 4 Гб оперативной памяти, 2 потока процессора, 60 Гб дискового пространства и сетевой адаптер Intel Pro / 1000 MT (1 Гбит/с). Такой выбор характеристик соответствует требованиям к нагрузке при отладке одноранговых сетевых алгоритмов и позволяет проводить множественные тестовые запуски без снижения производительности.

Для организации маршрутизации внутри EVE-NG был дополнительно развернут виртуальный маршрутизатор MikroTik [8, 9]. Исходный образ Mikrotik Cloud Router (.img) предварительно был конвертирован в формат qcow2, после чего выделено 1 ядро CPU, 1 поток и 256 Мб оперативной памяти. Конфигурация маршрутизатора предусматривает 5 сетевых портов, один из которых используется для подключения к внешней сети, а оставшиеся четыре предназначены для взаимодействия с виртуальными машинами. С целью упростить процесс адресации и обеспечить централизованное управление был реализован двухуровневый подход: физический маршрутизатор выдает DHCP-адрес узлу MikroTik, который в свою очередь раздает IP-адреса виртуальным машинам либо использует статическую конфигурацию. Такая гибкость упрощает наращивание инфраструктуры и согласованно объединяет узлы в единую одноранговую топологию, подготавливая её к дальнейшим экспериментам по исследованию алгоритмов и протоколов информационной безопасности.

Разработка сетевой топологии в EVE-NG и дальнейшее тестирование системы

В рамках проведенного исследования была реализована «звездообразная» топология, где маршрутизатор MikroTik выступает центральным узлом (рис. 1). Основой для построения виртуальной сети

послужила интегрированная среда, сочетающая гипервизор VMware (обеспечивающий гибкое распределение ресурсов и поддержку многопоточности) и эмулятор сетевых устройств EVE-NG, позволяющий визуализировать и детально настраивать каждое соединение. Такой подход обеспечивает единый исследовательский полигон, на котором можно разворачивать сразу несколько ОС (Windows 7, 10, 11, а также Linux Debian) и моделировать сценарии, приближенные к реальным условиям эксплуатации.

Интеграция MikroTik в качестве центрального маршрутизатора позволяет тестировать схемы распределенной маршрутизации, характерные для одноранговых сетей, а также подготовить инфраструктуру для проверки алгоритмов, изложенных в [2, 3], и разработанное программное обеспечение [10]. При конфигурации узлов каждой виртуальной машины назначались статические IP-адреса, после чего проверялась корректность маршрутов. Для оценки связности использовались пинг-тесты с помощью ICMP-запросов, демонстрирующие стабильный отклик от всех узлов и подтверждающие, что виртуальная среда удовлетворяет предъявляемым требованиям по надежности и производительности.

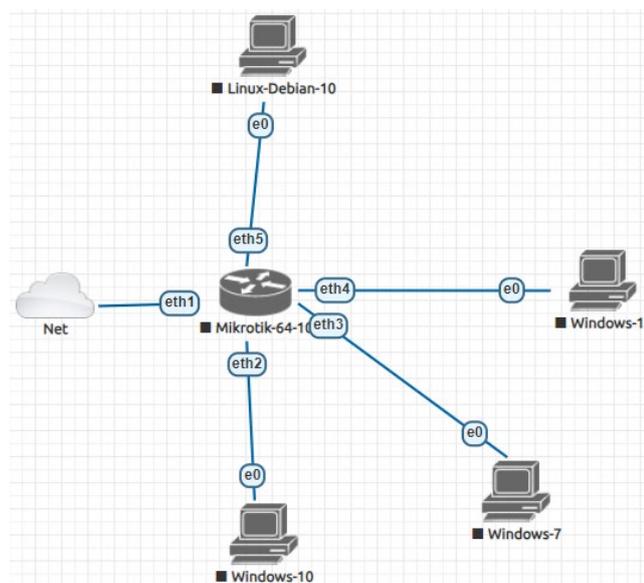


Рис. 1 – Виртуальная сетевая инфраструктура

Одним из ключевых преимуществ выбранной архитектуры является поддержка различных ОС в рамках одной топологии: это дает возможность комплексно анализировать производительность сетевых алгоритмов и поведение разработанных приложений под Windows и Linux. В последующем планируется реализация дополнительных скриптов автоматизации (в частности, Bash-скрипты для Linux и PowerShell-скрипты для Windows), что облегчит процедуру установки и настройки ПО, а также позволит проводить массовые тесты без ручного вмешательства.

Наконец, благодаря гибкой масштабируемости EVE-NG исследователи получают возможность расширять топологию за счет добавления новых виртуальных узлов и дальнейшего усложнения сценариев. Это особенно актуально при тестировании алгоритмов множественных стартовых соединений [2], многоуровневой криптографии [3] и других механизмов защиты. Дополнительно платформа EVE-NG поддерживает подключение сервисов мониторинга (Zabbix, Nagios) и анализ трафика (через встроенные средства или Wireshark), что позволит более детально отслеживать поведение сети в различных режимах и оперативно выявлять потенциальные уязвимости или некорректную конфигурацию.

Таким образом, совместное использование гипервизора VMware и среды EVE-NG в комбинации с маршрутизатором MikroTik дает высокую степень гибкости при изучении одноранговых сетей и тестировании новейших алгоритмов информационной безопасности. Успешное прохождение пинг-тестов подтвердило корректность работы предложенной конфигурации и доказало ее готовность к проведению дальнейших экспериментов по моделированию и анализу распределенных систем.

Заключение

В ходе проведенного исследования была разработана и описана виртуализированная среда, ориентированная на моделирование одноранговых сетей и тестирование методов информационной безопасности. Интеграция гипервизора VMware и платформы EVE-NG, в сочетании с маршрутизатором MikroTik, позволила добиться гибкой масштабируемости, воспроизводя топологии, максимально приближенные к реальным условиям эксплуатации. Проведенные пинг-тесты и оценка работы распределенных узлов подтвердили корректность предложенной конфигурации, ее готовность к глубокому анализу маршрутизации и эффективности криптографических алгоритмов.

Перспективы дальнейших исследований связаны с внедрением скриптов автоматизации (Bash и PowerShell) и разработкой дополнительных сценариев для тестирования алгоритмов множественных стартовых соединений, многоуровневой криптографии и других механизмов защиты данных. Такое расширение функционала позволит повышать масштаб экспериментов, вовремя выявлять уязвимости и проводить сравнительный анализ различных протоколов, что актуально как для фундаментальных изысканий, так и для прикладных проектов в области сетевой безопасности.

Литература

1. Xuemin Shen, Heather Yu, John Buford, Mursalin Akon (Eds.). Handbook of Peer-to-Peer Networking. Springer, 2010. 1421 p. ISBN 978-0-387-09750-3. DOI 10.1007/978-0-387-09751-0.
2. Зюзин В.Д., Болдыревский П.Б. Метод множественных стартовых соединений как инструмент повышения информационной безопасности в одноранговых виртуальных частных сетях // Инженерный вестник Дона, 2024, № 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9709.

3. Зюзин В.Д., Болдыревский П.Б. Разработка алгоритма установления защищенного соединения для одноранговых виртуальных частных сетей с использованием многоуровневой криптографической защиты // Инженерный вестник Дона, 2024, № 12. URL: ivdon.ru/ru/magazine/archive/n12y2024/9714.
4. Desktop Hypervisor // vmware.com URL: vmware.com/products/desktop-hypervisor/workstation-and-fusion (дата обращения: 25.11.2024).
5. Download Links and info for EVE-NG // eve-ng.net URL: eve-ng.net/index.php/download/ (дата обращения: 25.11.2024).
6. How to create own custom MS Windows host for EVE: // eve-ng.net URL: eve-ng.net/index.php/documentation/howtos/howto-create-own-windows-host-on-the-eve/ (дата обращения: 25.11.2024).
7. Ready to go Linux image pack for EVE // URL: eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image/ (дата обращения: 25.11.2024).
8. Versions this guide is based on: // URL: eve-ng.net/index.php/documentation/howtos/howto-add-mikrotik-cloud-router/ (дата обращения: 25.11.2024).
9. Upgrading RouterOS // mikrotik.com URL: mikrotik.com/download#chr (дата обращения: 25.11.2024).
10. Зюзин В.Д. Программный комплекс организации виртуальной частной сети на основе технологии одноранговых сетей (версия 1.0). Свидетельство о регистрации № 2024610455. Дата регистрации: 11.02.2025. Заявка № 2024692699. Опубликовано: 11.02.2025. Бил. № 1. URL: elibrary.ru/item.asp?id=59916237.

References

1. Xuemin Shen, Heather Yu, John Buford, Mursalin Akon (Eds.). 2010. 1421 p. ISBN 978-0-387-09750-3. DOI 10.1007/978-0-387-09751-0.

2. Zyuzin V.D., Boldyrevsky P.B. Inzhenernyi vestnik Dona, 2024, № 12.
URL: ivdon.ru/ru/magazine/archive/n12y2024/9709.
3. Zyuzin V.D., Boldyrevsky P.B. Inzhenernyi vestnik Dona, 2024, № 12.
URL: ivdon.ru/ru/magazine/archive/n12y2024/9714.
4. Desktop Hypervisor [Desktop Hypervisor]. vmware.com. URL:
vmware.com/products/desktop-hypervisor/workstation-and-fusion
(accessed: 25.11.2024).
5. Download Links and info for EVE-NG [How to create own custom MS
Windows host for EVE]. URL: eve-ng.net/index.php/download/ (accessed:
25.11.2024).
6. How to create own custom MS Windows host for EVE [How to create own
custom MS Windows host for EVE]. URL: eve-ng.net/index.php/documentation/howtos/howto-create-own-windows-host-on-the-eve/ (accessed: 25.11.2024).
7. Ready to go Linux image pack for EVE [Ready to go Linux image pack for
EVE]. URL: eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image/ (accessed: 25.11.2024).
8. Versions this guide is based on [Versions this guide is based on]. eve-ng.net.
URL: eve-ng.net/index.php/documentation/howtos/howto-add-mikrotik-cloud-router/ (accessed: 25.11.2024).
9. Upgrading RouterOS [Upgrading RouterOS]. URL:
mikrotik.com/download#chr (accessed: 25.11.2024).
10. Zyuzin V.D. Programmnyy kompleks organizatsii virtual'noy chastnoy seti
na osnove tekhnologii odnorangovykh setey (versiya 1.0). [Software
complex of virtual private network organization on the basis of peer-to-peer
network technology (version 1.0)]. Svidetel'stvo o registratsii No
2024610455. Data registratsii: 11.02.2025. Zayavka No 2024692699.



Опубликована: 11.02.2025. Bil. No 1. URL:
elibrary.ru/item.asp?id=59916237.

Дата поступления: 3.03.2025

Дата публикации: 25.04.2025