УДК 004.056

Е.А. БАСЫНЯ, В.Ю. САПЕГИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ВИРТУАЛЬНАЯ СЕТЕВАЯ ЛАБОРАТОРИЯ МОДЕЛИРОВАНИЯ, МОНИТОРИНГА И АНАЛИЗА СКРЫТЫХ КАНАЛОВ СВЯЗИ

В работе представлена разработка виртуальной сетевой лаборатории, предназначенной для моделирования, мониторинга и анализа скрытых каналов связи с применением децентрализованной системы обработки и хранения сетевых данных. Целью исследования являлось создание воспроизводимой, доверенной и масштабируемой среды, обеспечивающей проведение экспериментов в области построения и исследования виртуальных защищенных каналов связи, функционирующих на базе стека протоколов TCP/IP версии 4 и 6.

Обеспечение достоверности и воспроизводимости результатов научно-исследовательской деятельности является приоритетной задачей. Для ее достижения в прикладных научных изысканиях и программной инженерии следует разрабатывать и внедрять виртуальные сетевые лаборатории, которые смогут обеспечить автоматизацию процесса развертывания и управления всеми инфраструктурными объектами.

В данной работе разработана архитектура виртуальной сетевой лаборатории с применением открытых средств виртуализации и управления инфраструктурой, что обеспечило ее гибкость, переносимость и возможность горизонтального и вертикального масштабирования.

Основной платформой виртуализации было выбрано решение Proxmox Virtual Environment. Использование Proxmox VE позволяет развертывать виртуальные машины с различными конфигурациями сетевых интерфейсов, моделировать сложные топологии VPN-соединений и управлять ресурсами вычислительного кластера через API.

Автоматизация инфраструктурного уровня реализована с помощью Terraform, который обеспечивает декларативное описание конфигурации вычислительных узлов, сетевых параметров и виртуальных сред. Ansible-применяется для автоматической установки и настройки компонентов VPN-инфраструктуры (например, WireGuard, OpenVPN, StrongSwan, Trojan, Xray), а также сервисов сбора и обработки телеметрических данных.

Особенностью разработанной виртуальной лаборатории является возможность эмуляции сетевых состояний, характерных для реальных распределенных систем. На уровне сетевых модулей виртуальных машин

моделируются параметры деградации каналов связи – задержки, джиттер, потери пакетов и ограничение пропускной способности. Для этого используются встроенные механизмы tc (Traffic Control) и netem, позволяющие вносить управляемые и воспроизводимые искажения в трафик между узлами.

Ключевой особенностью предлагаемого решения является применение децентрализованной системы обработки и хранения сетевых событий, реализованной на основе принципов, изложенных в [1]. Каждое сетевое событие, зафиксированное в процессе эксперимента, проходит процедуру хеширования и записи метаданных в децентрализованный реестр, что обеспечивает неизменность данных, прозрачность аудита и возможность независимой верификации результатов. Такая архитектура позволяет достичь доверенной фиксации результатов мониторинга VPN-трафика и повысить достоверность научно-практических исследований.

Для моделирования VPN-коммуникаций использовался метод построения самоорганизующихся защищенных каналов связи, основанный на стохастическом многоуровневом шифровании и оверлейных технологиях, описанных в [2]. Виртуальная сетевая лаборатория обеспечивает возможность воссоздания различных топологий взаимодействия узлов, что делает данный стенд эффективным инструментом для проверки эффективности методов защиты информации. Кроме того, в рамках данной лаборатории проводится исследование и апробация современных методов детекции VPN-трафика на основе машинного обучения (ML), реализуемых в режиме реального времени, включая алгоритмы анализа сетевых потоков и классификации зашифрованных соединений, основанные на принципах, представленных в [3].

Результаты разработки могут быть использованы для проведения научно-практических экспериментов, направленных на повышение доверенности и устойчивости VPN-инфраструктур, а также для тестирования новых методов защиты информации и протоколов безопасной передачи данных.

Список литературы

1. Басыня Е.А., Сафронов А.В. Метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия //Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 4 (34). – С. 35–44.

2. Basinya E.A. et al. System of a self-organizing virtual secure communication channel based on stochastic multi-layer encryption and overlay technologies. – 2022.

3. Wu H. et al. Real-time identification of VPN traffic based on counting Bloom filter and chained hash table from sampled data in high-speed networks // ICC 2022-IEEE International Conference on Communications. – IEEE, 2022. – P. 5070–5075.