УДК 528.71

Д. Е. Панков[1] *

Модуль автоматизированной установки и конфигурирования безопасного удаленного доступа к операционным системам семейства Linux

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: pankov.d.009@gmail.com

Аннотация. В работе представлен модуль автоматизированной установки и конфигурирования безопасного удаленного доступа к операционным системам Linux. Рассмотрена проблематика эффективного управления удаленным доступом в не доверенных сетевых средах и вынесен на обзор новый подход к решению этой задачи. Объектом исследования являются средства обеспечения безопасного удаленного доступа к конечным точкам. Цель работы заключается в обеспечении информационной безопасности процесса удаленного администрирования семейства ОС Linux. В статье рассмотрена важность проблемы организации безопасного удаленного доступа. В результате исследования были получены BPMN диаграмма предметной области и формализованная архитектура модуля в виде UML диаграмм. В рамках проектирования и программной реализации был определен набор компонентов, из которых состоит разрабатываемый модуль, разработаны UML диаграммы подключения к удаленному рабочему хосту, определен стек технологий. Предложенное решение предоставляет возможность обеспечения конфиденциальности и аутентичности процесса удаленного администрирования и может быть использовано как в корпоративной, так и в домашней среде для защиты удаленного доступа к системам на базе семейства ОС Linux.

Ключевые слова: безопасный удаленный доступ, VPN, автоматизированное конфигурирование, Linux

D. E. Pankov[1] *

Module for Automated Installation and Configuration of Secure Remote Access to Linux Operating Systems

[1] National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation
* e-mail: pankov.d.009@gmail.com

Abstract. The work presents a module for automated installation and configuration of secure remote access to Linux operating systems. The problems of effective remote access management in untrusted network environments are considered and a new approach to solving this problem is presented for review. The object of the study is the means of providing secure remote access to endpoints. The purpose of the work is to ensure information security of the process of remote administration of the Linux OS family. The article discusses the importance of the problem of organizing secure remote access; as a result of the study, a BPMN domain diagram and a formalized module architecture in the form of UML diagrams were obtained. As part of the design and software implementation, the set of components that made up the developed module was determined, UML diagrams for connecting to a remote working host were developed, and a technology stack was defined. The proposed solution provides the ability to ensure confidentiality and authenticity of the remote administration process

and can be used in both corporate and home environments to protect remote access to systems based on the Linux OS family.

Keywords: secure remote connection, VPN, automated configuration, Linux

Введение

В настоящее время удаленный доступ к компьютерным системам стал неотъемлемой частью работы многих организаций и предприятий. Однако при этом возникает ряд проблем, связанных с безопасностью, так как удаленный доступ может быть использован злоумышленниками для несанкционированного доступа к конфиденциальной информации [1, 2]. Существует множество научных исследований и работ, посвященных безопасности удаленного доступа к операционным системам. Одним из основных направлений в этой области является разработка методов и средств защиты от атак на протоколы удаленного доступа. В статье, опубликованной группой ученых из Технического университета г. Грац, Австрия, рассматривается создание системы безопасной удаленной конфигурации информационных кибер-физических систем [3, 4]. Авторы предлагают решение, основанное на двухсторонней аутентификации, Transport Layer Security (TLS), Authenticated Encryption (AE), технологии Secure Element (SE) для обеспечения защищенной от несанкционированного доступа и безопасной связи между объектами во внутренней и внешней сетях. Другим подходом является модель системы безопасного удаленного доступа к ресурсам университета на основе стека протоколов IPSEC [5]. Весь трафик шифруется и инкапсулируется стороне клиента. Затем он отправляется на VPN-сервер через Интернет и при получении расшифровывается и ретранслируется целевому хосту во внутренней сети, но только когда параметры безопасности между VPN-сервером и VPN-клиентом совпадают.

Помимо достоинств, которые несут в себе предлагаемые решения, есть и некоторые недостатки, в том числе проблемы с совместимостью, невозможность удаленного обновления конфигураций и ограниченная масштабируемость. Несмотря на значительные успехи в этой области, остаются нерешенными проблемы автоматизации процесса настройки безопасного удаленного доступа.

В статье предложен и обсужден модуль автоматизированной установки и конфигурирования безопасного удаленного доступа к операционным системам семейства Linux, учитывающий современные требования к безопасности и управляемости. Будут рассмотрены технологические аспекты, примеры использования и потенциальные преимущества такого подхода. Таким образом, цель данной статьи – решение проблем обеспечения конфиденциальности и аутентичности процессов системного и сетевого администрирования.

Методы и материалы

В данном разделе будет рассмотрено проектирование модуля автоматизированной установки и конфигурирования безопасного удаленного доступа для операционных систем семейства Linux. Было решено спроектировать модуль на ос-

нове технологии виртуальных частных сетей (VPN) [6, 7]. В связи с этим в рамках виртуальной сетевой лаборатории был проведен экспериментальный сравнительный анализ протоколов VPN. Результаты анализа представлены в табл. 1.

Таблица 1

Сравнительный анализ VPN-протоколов

Критерий	WireGuard	OpenVPN	L2TP/IPSec	SoftEther
Пропускная способность	1009 Мб/с	248 Мб/с	812 Мб/с	784 Мб/с
Поддерживаемые платформы	Windows, mac OS, GNU/Linux, Apple iOS, Android	Windows, Linux, mac OS, iOS, Android	Windows, mac OS, Linux, iOS, Android	Windows, mac OS, Linux, iOS, Android
Устойчивость ко множественному NAT	устойчив	устойчив	неустойчив	устойчив
Прозрачность трафика	протокол виден при сканировании	протокол виден при сканировании	протокол не виден при сканировании	протокол не виден при сканировании
Поддержка транспортных протоколов	UDP	TCP, UDP	TCP, UDP	TCP, UDP

Также была разработана BPMN-диаграмма процесса удаленного подключения (рис. 1). Процесс будет заключаться в следующем:

– пользователь отправляет запрос со своего локального компьютера на подключение по VPN;

– должен быть пройден брандмауэр;

– на стороне сервера должна быть пройдена аутентификация по сертификату и проведена авторизация пользователя;

– пользователь получает удалённый доступ.

В рамках разработки модели решения и на основе анализа инструментов был выбран следующий стек технологий:

– Ansible для автоматизации конфигурирования хостов. Ansible написан на python, а также имеет безагентную архитектуру;

– Wireguard для организации VPN-подключения. Данный протокол выбран из-за простоты конфигурирования, кроссплатформенности и скорости;

– Shadowsocks для маскировки трафика под HTTPS. Shadowsocks сделает менее детектируемым VPN-протокол, используемый при удаленном администрировании;

– Port knocking для привнесения дополнительного слоя аутентификации клиентов. Данная технология поддерживает возможность использования одноразовых ключевых последовательностей;

– Vagrant + VirtualBox для создания и конфигурирования виртуальной среды разработки.

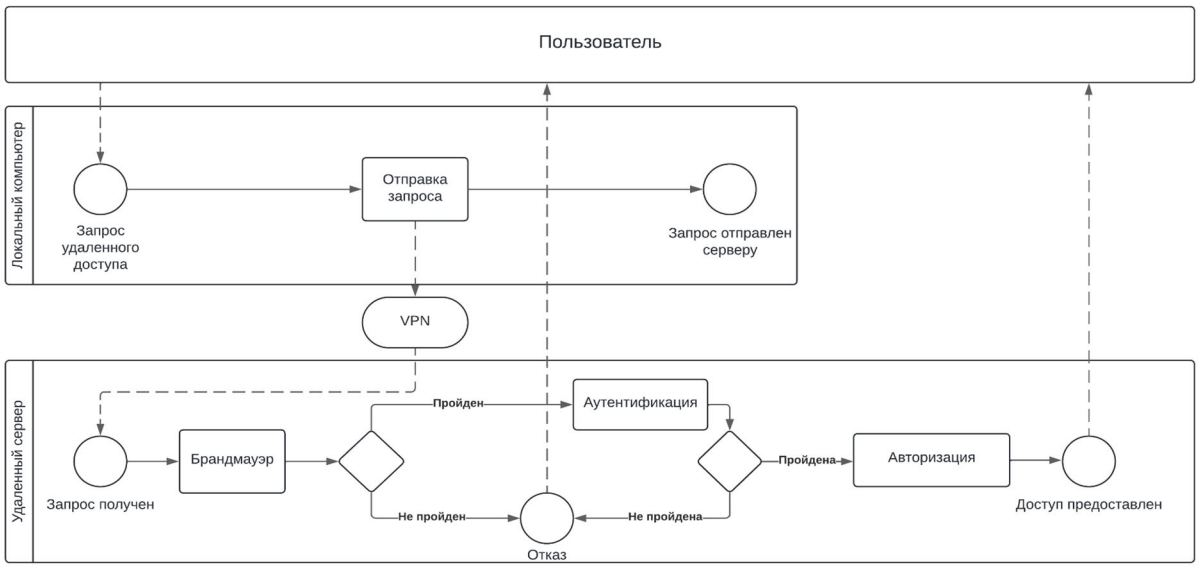

Рис. 1. BPMN-диаграмма процесса удаленного подключения

Данный стек был использован на этапе программной реализации рассматриваемого модуля [8, 9].

Результаты

В ходе программной разработки был представлен модуль автоматизированной установки и конфигурирования безопасного удаленного доступа к операционным системам семейства Linux (рис. 2). Компонент Wireguard, в автоматизированном режиме устанавливает необходимые пакеты в систему, а затем создает конфигурационные файлы на стороне клиента и на стороне пользователя. Далее модуль Wireguard автоматизированно устанавливает VPN-соединение между клиентом и сервером.

Важно отметить, что для хранения секретной информации, такой как приватный ключ сервера, использовался специальный модуль Ansible. Он позволяет не хранить секреты в открытом виде [10, 11].

Компонент Port knocking использует файл с заранее подготовленными одноразовыми последовательностями, которые клиентский узел будет использовать для соединения с сервером. При отправке данных последовательностей серверу использованная комбинация будет помечаться, и при следующем подключении будет использована идущая за ней последовательность [12]. Модуль

Shadowsocks работает следующим образом: весь идущий от клиента к серверу трафик будет замаскирован под обычные HTTP-запросы. Это позволит уменьшить видимость используемых протоколов для снифферов [13, 14, 15].

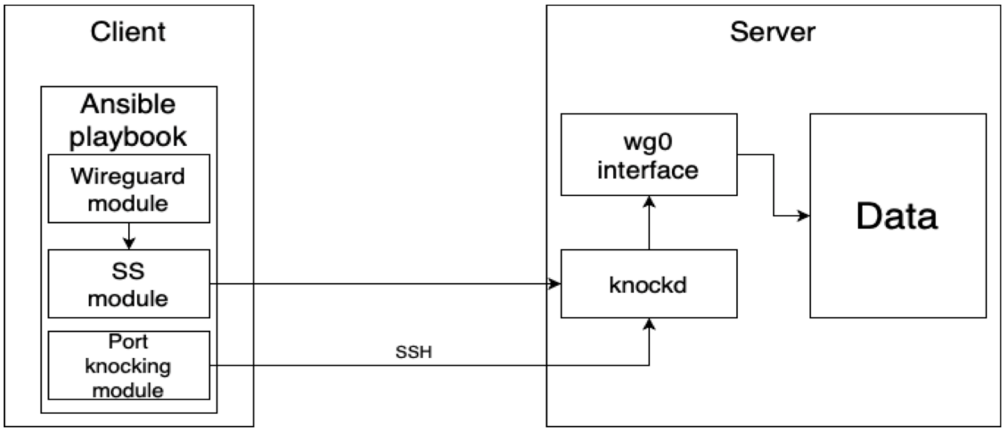

Рис. 2. UML-диаграмма разработанного модуля

Обсуждение и заключение

В данной статье был представлен модуль автоматизированной установки и конфигурирования безопасного удаленного доступа к операционным системам Linux, который предлагает новый подход к управлению безопасностью удаленного доступа на серверах.

Основной проблемой, которую решает предложенный модуль, является сложность настройки безопасного удаленного доступа на множестве серверов в сети. Существующие инструменты часто требуют ручной конфигурации или настройки каждого сервера отдельно, что может привести к ошибкам, уязвимостям и несоответствию стандартам безопасности. Предложенный модуль позволяет стандартизировать процесс установки и настройки безопасного удаленного доступа через автоматизированные процедуры, снижая риск человеческой ошибки.

Одной из ключевых особенностей данного модуля является маскировка трафика. Она позволит сделать менее детектируемым сам факт процесса удаленного подключения. Несмотря на значительные преимущества предложенного модуля, остаются некоторые нерешенные проблемы. Например, интеграция с различными типами аутентификации (например, MFA) может потребовать дальнейшей разработки.

В заключение можно отметить, что разработка модуля автоматизированной установки и конфигурации безопасного удаленного подключения для ОС Linux является актуальной и важной задачей в современном мире информационных технологий.

В ходе исследования был проведен обзор некоторых научных работ в рассматриваемой предметной области. В рамках моделирования предметной области был определен набор компонентов, из которых будет состоять разрабатыва-

емый модуль, разработаны UML-диаграммы подключения к удаленному рабочему хосту.

На основе полученных результатов был спроектирован модуль, который позволяет автоматизировать процесс установки и конфигурации безопасного удаленного подключения на базе протокола WireGuard. Модуль включает в себя следующие компоненты:

- клиентское и серверное ПО для VPN;
- конфигурационные файлы VPN;
- ПО Ansible;
- плэйбук Ansible.

Далее была осуществлена программная реализация модуля автоматизированной установки и конфигурирования безопасного удаленного доступа для операционных систем семейства Linux. Помимо Wireguard использовались также технологии Shadowsocks для маскировки трафика и модифицированная Port knocking для дополнительного уровня аутентификации.

Таким образом, разработка модуля автоматизированной установки и конфигурации безопасного удаленного подключения для ОС Linux является важным шагом в обеспечении всех аспектов безопасности информации в современном мире информационных технологий. Этот модуль в дальнейшем может быть использован как в корпоративной, так и в домашней средах для защиты удаленного доступа к системам на базе ОС Linux.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Top cybersecurity threats on enterprise networks. [Электронный ресурс] // Positive Technologies. – Доступ к ресурсу URL: https://www.ptsecurity.com/ww-en/analytics/network-traffic-analysis-2020/#id10.

2. Атаки на RDP и способы защиты от них // Positive Technologies. – URL: https://www.securitylab.ru/blog/company/USSC/352646.php?ysclid=lh2kauyfmj726922710.

3. T. Ulz, T. Pieber, C. Steger, S. Haas and R. Matischek, "Secured remote configuration approach for industrial cyber-physical systems," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 2018, pp. 812-817, doi: 10.1109/ICPHYS.2018.8390811.

4. Samuel Ndichu и др. A Remote Access Security Model based on Vulnerability Management. // I.J. Information Technology and Computer Science. – 2020. – 5. – С. 38-51.

5. Secure Remote Access IPSEC Virtual Private Network to University Network System [Электронный ресурс] // Journal of Computer Science Research. – Доступ к ресурсу URL: https://www.researchgate.net/publication/349099714_Secure_Remote_Access_IPSEC_Virtual_Private_Network_to_University_Network_System.

6. Луценко М. Н., Князев А. А., Дубровский Н. С. Сравнительный анализ программных продуктов удаленного подключения к локальной сети с использованием виртуальных каналов // Поколение будущего: Взгляд молодых ученых-2022. – 2022. – С. 226-228.

7. Документация по Wireguard // Официальный сайт Wireguard. – URL: https://www.wireguard.com.

8. Документация по Ansible // Официальный сайт Ansible. – URL: https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_variables.html.

9. Басыня Е.А. Сетевая информационная безопасность: Учебник. – Москва : НИЯУ МИФИ, 2023. – 72 с.

10. Басыня, Е. А. Самоорганизующаяся система управления трафиком вычислительной сети / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 1(31). – С. 179-184.

11. Павлов А. Н., Гладков А. Н. Разработка методики организации удаленного управления АРМ в соединении // Современная наука: актуальные проблемы теории и практики. Серия: естественные и технические науки Учредители: ООО Научные технологии. – С. 29-35.

12. Анзина А. В., Медведева А. Д., Лапина М. А. Исследование аутентификации в протоколе SSH // Студенческая наука для развития информационного общества. – 2019. – С. 224-232.

13. Настройка Port knocking на Linux (Ubuntu) // Сайт interface31. – URL: https://interface31.ru/tech_it/2021/02/nastraivaem-port-knocking-v-linux-debian-ubuntu.html.

14. Настройка Shadowsocks // Losst. – URL: https://losst.pro/nastrojka-shadowsocks.

15. Басыня, Е. А. Автоматизированная установка и конфигурирование серверных решений / Е. А. Басыня, М. С. Лукина // Современные материалы, техника и технологии. – 2016. – № 2(5). – С. 21-26.