Инженерный вестник Дона, №12 (2024)
ivdon.ru/ru/magazine/archive/n12y2024/9714

Разработка алгоритма установления защищенного соединения для одноранговых виртуальных частных сетей с использованием многоуровневой криптографической защиты

В.Д. Зюзин, П.Б. Болдыревский

Нижегородский государственный университет им. Н.И. Лобачевского

Аннотация: В статье представлен алгоритм установления защищенного соединения для одноранговых виртуальных частных сетей, направленный на повышение информационной безопасности. Алгоритм использует современные криптографические протоколы IKEv2, RSA и DH, обеспечивая многоуровневую защиту данных. Разработанная структура алгоритма включает динамическое формирование и уничтожение временных ключей, что снижает риски компрометации. Предложенное решение предназначено для применения в системах защиты корпоративных сетей, Интернета вещей и распределенных систем.
Ключевые слова: виртуальная частная сеть, одноранговая сеть, криптографические протоколы, RSA, Diffie-Hellman, IKEv2, защищенное соединение, многослойная защита, информационная безопасность, распределенные системы.

Введение

Современные информационные технологии предоставляют широкие возможности для реализации защищенного обмена данными посредством виртуальных частных сетей (ВЧС). На фоне цифровой трансформации экономики ВЧС становятся ключевым инструментом для обеспечения конфиденциальности и целостности передаваемой информации, что особенно важно в условиях растущего числа кибератак [1, 2].

Среди различных архитектур ВЧС особое внимание привлекают сети одноранговой архитектуры, отличающиеся высокой гибкостью и отсутствием необходимости в централизованном сервере для управления соединениями [3–5]. Эта децентрализованная модель позволяет не только минимизировать затраты на инфраструктуру, но и обеспечивает устойчивость к сбоям, что делает одноранговые ВЧС востребованными в распределенных системах, критически зависящих от высокой доступности и надежности данных.

Однако эксплуатация одноранговых ВЧС сопряжена с рядом проблем, главная из которых – обеспечение информационной безопасности. Отсутствие централизованного контроля создает дополнительные риски, связанные с возможной компрометацией узлов и перехватом сетевого трафика [6]. С учетом глобальной тенденции к усложнению методов атак злоумышленников, включая использование уязвимостей промежуточных узлов, требуется разработка более надежных механизмов защиты.

Особую актуальность приобретает реализация многоуровневых подходов к обеспечению безопасности, интегрирующих передовые криптографические методы и адаптивные алгоритмы управления соединениями [7, 8]. Настоящее исследование направлено на разработку и анализ алгоритма, который использует современные криптографические протоколы и технологии для повышения устойчивости одноранговых ВЧС к угрозам информационной безопасности.

Алгоритм установления защищенного соединения в одноранговой виртуальной частной сети

Базовая концепция алгоритма установления защищенного соединения была впервые предложена в работе «Подход к установлению соединений в распределенной VPN». В последующих исследованиях, включая публикацию [9], озаглавленную «Модифицированная процедура установления соединения в виртуальной частной сети» [10], предложенная концепция была существенно доработана. Эти исследования заложили основу для разработки усовершенствованного алгоритма, представленного в настоящей статье.

Разработанный нами алгоритм представляет собой эволюционное развитие указанных подходов и включает ряд нововведений, направленных на повышение безопасности и эффективности установления соединений в одноранговых виртуальных частных сетях. Алгоритм реализует последовательный процесс взаимодействия узлов, где каждый этап

обеспечивается использованием современных криптографических протоколов, таких как протокол обмена ключами в интернете 2-ой версии (Internet Key Exchange version 2 – IKEv2), протокол Ривеста-Шамира-Адлемана (Rivest-Shamir-Adleman – RSA) и протокол Диффи-Хеллмана (Diffie-Hellman – DH). Кроме того, алгоритм предусматривает многоуровневую защиту данных посредством временных ключей и контекстуального шифрования.

Для наглядного представления предложенного решения в статье приведена схема последовательности операций алгоритма. Такая визуализация не только упрощает понимание процесса, но и способствует практическому внедрению алгоритма в одноранговые сети. Интеграция предложенного алгоритма позволяет существенно снизить вероятность компрометации промежуточных узлов, обеспечить надежную защиту трафика и повысить устойчивость системы к киберугрозам.

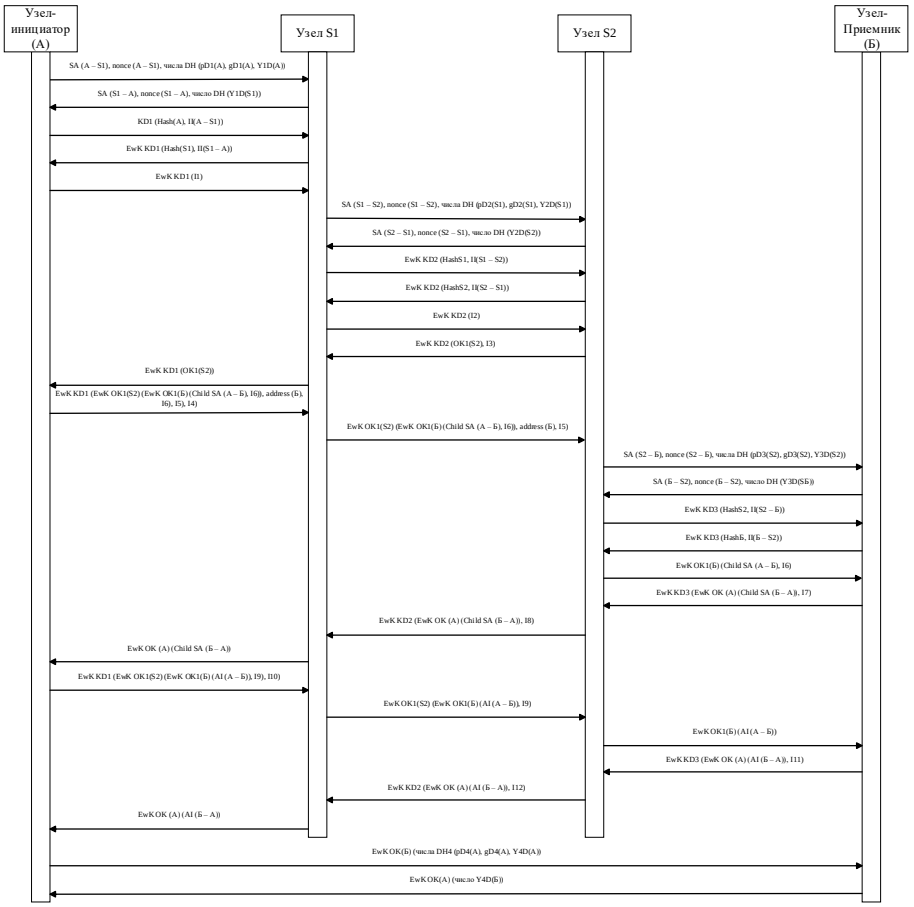

Рис. 1. – Общая схема установления защищенного соединения в одноранговой виртуальной частной сети

На рис. 1 представлена схематическая диаграмма, иллюстрирующая процесс установления защищенного соединения между узлом-инициатором и узлом-получателем в одноранговой виртуальной частной сети. Алгоритм взаимодействия узлов разработан с учетом современных криптографических стандартов и обеспечивает высокую степень защиты данных при передаче через промежуточные узлы, минимизируя риски компрометации и несанкционированного доступа.

Процесс установления соединения включает следующие ключевые этапы:

1. Узел-инициатор (А) устанавливает соединение с промежуточным узлом (S1) по протоколу IKEv2 (1 фаза).
2. Узел-инициатор (А) отправляет инструкцию ($I1$) промежуточному узлу (S1).
3. Промежуточный узел (S1) устанавливает соединение с промежуточным узлом (S2) по протоколу IKEv2 (1 фаза).
4. Промежуточный узел (S1) отправляет инструкцию ($I2$) промежуточному узлу (S2) и получает в ответ его открытый ключ RSA – ($OK1(S2)$).
5. Промежуточный узел (S1) отправляет узлу-инициатору (А) открытый ключ промежуточного узла (S2), полученный в пункте 4.
6. Узел-инициатор (А) отправляет промежуточному узлу (S2) адрес узла-получателя (Б) ($address$ (Б)) и зашифрованные открытым ключом RSA узла-получателя (Б) (OK(Б)) параметры безопасности ($Child\ SA$ (А – Б)) и инструкцию ($I6$) через промежуточный узел (S1).
7. Промежуточный узел (S2) устанавливает соединение с узлом-получателем (Б) протоколу IKEv2 (1 фаза).

8. Промежуточный узел (S2) отправляет узлу-получателю (Б) зашифрованные открытым ключом RSA узла-получателя (Б) (OK(Б)) параметры безопасности ($Child\ SA$ (А – Б)) и инструкцию ($I6$), полученные в пункте 7.
9. Узел-получатель (Б) отправляет в ответ узлу-инициатору (А) зашифрованные открытым ключом RSA узла-получателя (А) (OK(А)) параметры безопасности ($Child\ SA$ (Б – А)) через промежуточный узел (S2) и промежуточный узел (S1).
10. Узел-инициатор (А) отправляет узлу-получателю (Б) зашифрованные открытым ключом RSA узла-получателя (Б) (OK(Б)) аутентификационные данные (AI (А – Б)) через промежуточный узел (S1) и промежуточный узел (S2).
11. Узел-получатель (Б) отправляет в ответ узлу-инициатору (А) зашифрованные открытым ключом RSA узла-инициатора (А) (OK(А)) аутентификационные данные (AI (Б – А)) через промежуточный узел (S2) и промежуточный узел (S1).
12. Узел-инициатор (А) обменивается с узлом-получателем (Б) (напрямую) зашифрованные открытыми ключами RSA (OK(А), OK(Б)) открытыми числами DH с целью вычисления секретного ключа DH.

Заключение

В данной статье представлен разработанный нами алгоритм установления защищенного соединения в одноранговых виртуальных частных сетях. Основное внимание уделено реализации многоуровневой защиты данных, достигаемой за счет использования современных криптографических протоколов IKEv2, RSA и DH. Особенностью алгоритма является динамическое формирование и уничтожение временных ключей, что существенно снижает риски компрометации данных и делает

предложенный подход устойчивым к угрозам информационной безопасности.

Разработанный нами алгоритм обеспечивает:

- Устойчивость сети к компрометации промежуточных узлов;
- Надежное шифрование данных на каждом этапе соединения;
- Гибкость в использовании промежуточных узлов для маршрутизации трафика.

Алгоритм планируется реализовать в виде программного обеспечения с целью его дальнейшей интеграции в системы информационной безопасности. Для реализации будет использован современный язык программирования, такой, как Python, что обеспечит совместимость с платформами Windows (версии 7 и выше) и Linux.

Литература

1. Организация защищенного обмена данными с помощью виртуальных частных сетей (VPN) // IBM. URL: ibm.com/docs/ru/i/7.1?topic=options-virtual-private-network-secure-private-communications (дата обращения: 20.09.2024).
2. Основы построения защищенных компьютерных сетей // vec.etu.ru URL: vec.etu.ru/moodle/pluginfile.php/294002/mod_resource/content/1/Виртуальные%20частные%20сети%20презентация.pdf (дата обращения: 25.09.2024). — С. 1–25.
3. Architecture architecturale (P2P) // geeksforgeeks.org. URL: geeksforgeeks.org/peer-to-peer-p2p-architecture/ (дата обращения: 13.10.2024).

4. Одноранговые сети (сети без централизованного управления) // studfile.net. URL: studfile.net/preview/2802302/page:6/ (дата обращения: 16.10.2024).
5. 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.
6. Наталья Васильевна Михайленко, Светлана Владимировна Мурадян, Александр Александрович Вихляев Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях // Аудиторские ведомости. 2022. №1. — С. 140–145.
7. Васильев Алексей Викторович. Причины роста количества кибератак: анализ технических и нетехнических факторов // Системный анализ и прикладная информатика. 2023. №3. — С. 48–54.
8. Экспертно-Аналитический центр InfoWatch. Тенденции развития киберинцидентов АСУ ТП за 2023 год: аналитический отчет. — М.: InfoWatch, 2024. — 21 с.
9. Рябов, А. А., Тетеркин М.А. Подход к установлению соединений в распределенной VPN // Труды XXIII научной конференции по радиофизике, посвященной 100-летию со дня рождения Н.А. Железцова, Нижний Новгород, 13–21 мая 2019 года / Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2019. – С. 531-532.
10. Зюзин, В. Д., Рябов А.А. Модифицированная процедура установления соединения в виртуальной частной сети / Труды XXVII научной конференции по радиофизике, Нижний Новгород,

15–25 мая 2023 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2023. – С. 537.

References

1. Organizatsiya zashchishchennogo obmena dannymi s pomoshchyu virtualnykh chastnykh setey (VPN) [Organization of Secure Data Exchange Using Virtual Private Networks (VPN)]. IBM. URL: ibm.com/docs/ru/i/7.1?topic=options-virtual-private-network-secure-private-communications (accessed: 20.09.2024).
2. Osnovy postroeniya zashchishchennykh komp'yuternykh setey [Fundamentals of Secured Computer Networks]. URL: vec.etu.ru/moodle/pluginfile.php/294002/mod_resource/content/1/Virtualnye%20chastnye%20seti%20prezentatsiya.pdf (accessed: 25.09.2024). P. 1–25.
3. Architecture architecturale (P2P). GeeksforGeeks. URL: geeksforgeeks.org/peer-to-peer-p2p-architecture/ (accessed: 13.10.2024).
4. Peer-to-peer networks (networks without centralized management). studfile.net. URL: studfile.net/preview/2802302/page:6/ (accessed: 16.10.2024).
5. Shen, X., Yu, H., Buford, J., Akon, M. (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.
6. Mikhaylenko N.V., Muradyan S.V., Vikhlyaev A.A. Auditorskie vedomosti. 2022. No. 1. pp. 140–145.
7. Vasil'ev A. V. Sistemnyi analiz i prikladnaya informatika. 2023. №3. pp. 48–54.
8. Ekspertno-Analiticheskiy tsentr InfoWatch. Tendentsii razvitiya kiberintsidentov ASU TP za 2023 god: analiticheskiy otchet [Trends in

the Development of Cyber Incidents in ICS for 2023: Analytical Report]. M.: InfoWatch, 2024. 21 p.

9. 9.Ryabov, A. A., Teterkin M.A. Trudy XXIII nauchnoj konferencii po radiofizike, posvyashchennoj 100-letiyu so dnya rozhdeniya N.A. Zhelezcova, Nizhnij Novgorod, 13–21 maya 2019 goda. Nacional'nyj issledovatel'skij Nizhegorodskij gosudarstvennyj universitet im. N.I. Lobachevskogo. Nizhnij Novgorod: Nacional'nyj issledovatel'skij Nizhegorodskij gosudarstvennyj universitet im. N.I. Lobachevskogo, 2019. pp. 531-532.
10. 10.Zyuzin, V. D., Ryabov A.A. Modificirovannaya procedura ustanovleniya soedineniya v virtual'noj chastnoj seti. Trudy XXVII nauchnoj konferencii po radiofizike, Nizhnij Novgorod, 15–25 maya 2023 goda. Nizhnij Novgorod: Nacional'nyj issledovatel'skij Nizhegorodskij gosudarstvennyj universitet im. N.I. Lobachevskogo, 2023. p. 537.

Дата поступления: 6.11.2024

Дата публикации: 15.12.2024