А. А. Демещик, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732

ОРГАНИЗАЦИЯ УДАЛЕННОГО БЕЗОПАСНОГО ПРИСОЕДИНЕНИЯ К КОМПЬЮТЕРНОЙ СЕТИ СРЕДСТВАМИ WIREGUARD

Аннотация. В статье анализируется функционал безопасного удаленного соединения, созданного с использованием программного обеспечения WireGuard. Сравниваются современные протоколы виртуальных частных сетей и рассматриваются популярные открытые решения в области межсетевых экранов. В результате проведенного анализа построена практическая модель применения WireGuard в моделируемой сети предприятия.
Ключевые слова: VPN, WireGuard, pfSense, удаленный доступ.

Введение. В современном мире VPN (Virtual Private Network) — неотъемлемая часть корпоративных сетей [1]. Это технология, которая обеспечивает безопасную и защищенную передачу данных через интернет. VPN устанавливает защищенное соединение между компьютером и удаленным сервером, который может находиться как в другой части города, так и за пределами страны [2].

При использовании данной технологии изначальный IP-адрес устройства скрывается, а сетевой трафик перенаправляется через удаленный сервер [3]. Это означает, что при взаимодействии с сетью VPN-сервер становится источником пользовательских запросов. VPN-туннель функционирует в незащищенной сети Интернет [4], однако сетевой трафик подвергается шифрованию вследствие чего передаваемые данные будут в безопасности, даже если третья сторона перехватит трафик [5].

Проблема исследования. Учитывая растущую популярность формата работы вне офиса, можно сказать, что одной из важнейших задач в современном мире деловых коммуникаций является организация безопасного удаленного доступа к сети предприятия.

В настоящее время распространенным решением данной задачи являются VPN-протоколы, которые позволяют пользователям удаленно подключаться к сети предприятия. На рынке предоставлено большое количество различных решений, поэтому у компании может появиться трудность в выборе программного обеспечения.

Для организации безопасного удаленного соединения к сети предприятия были поставлены следующие задачи:

- изучить современные VPN-технологии и теоретические особенности WireGuard;
- проанализировать открытые решения в области межсетевых экранов и выявить особенности их применения в реальных сетях;
- смоделировать сеть предприятия, использующую pfSense и WireGuard в EVE-NG.

Материалы и методы. Методами данного исследования стали наблюдение, эксперимент, измерение и абстрагирование. Для эмуляции сети предприятия было выбрано программное обеспечение EVE-NG 5.0.1-19.

Результаты. Проведенный анализ показал, что OpenVPN — популярное решение с открытым исходным кодом, которое для криптографии использует библиотеку OpenSSL с поддержкой шифрования TLS. IKEv2 — развитие протокола IPsec VPN. Его особенность — автоматическое поддерживание VPN-соединения при изменениях в компьютерной сети. L2TP также применяется для туннелирования, его часто используют в сочетании с IPsec для обеспечения безопасности. Все перечисленные протоколы являются классическими решениями организации туннелирования и поддерживаются многими операционными системами, включая Windows, macOS, IOS и Android. Нами же был выбран новый протокол WireGuard по следующим причинам:

1. Высокая скорость работы (тесты показывают приблизительно пятикратное превосходство пропускной способности сети при использовании WireGuard, по сравнению с популярным решением OpenVPN);
2. Простота настройки конфигурации;
3. Легковесность (протокол легко анализировать на наличие уязвимостей, так как его исходный код умещается примерно в 4000 строки). Например, библиотека OpenSSL, которую использует OpenVPN, состоит примерно из 70000 строк кода, поэтому у протокола WireGuard меньшая поверхность атаки.

В решениях Open Source имеется достаточно большое количество пакетов и дистрибутивов, реализующих функционал межсетевых

экранов. Iptables — встроенный межсетевой экран большинства систем Linux. Данное решение не требует установки дополнительного программного обеспечения и имеет возможность сложной конфигурации правил фильтрации трафика, однако у него нет графического интерфейса. IPfire — дистрибутив Linux, ориентированный на безопасность, имеющий интуитивный интерфейс и простую настройку. У него также есть возможность устанавливать дополнительные пакеты. PfSense основан на FreeBSD и может расширять функционал установкой дополнительных пакетов. OPNsense является ответвлением PfSense.

Так как на рынке присутствует несколько схожих по функционалу решений, наш выбор в сторону pfSense основывается на наличии лучшей документации и высокой популярности решения.

В качестве примера применения WireGuard нами была спроектирована модель простой компьютерной сети предприятия и удаленной домашней сети (рис. 1). Узел EDGE1 является пограничным маршрутизатором предприятия, на котором установлен сервер WireGuard на базе PfSense, EDGE2 — пограничный маршрутизатор домашней сети.

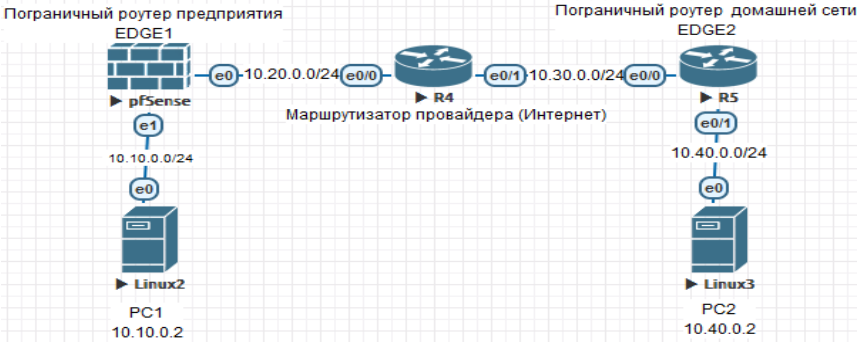

Рис. 1. Топология сети предприятия и домашней сети

Для демонстрации настройки рассмотрим базовый алгоритм конфигурации сервера и клиента:

1. Установка WireGuard на сервер и на клиентское устройство.

2. Генерация публичного и приватного ключа для каждого устройства.

3. Настройка конфигурационного файла на сервере (рис. 2).

4. Настройка клиентского конфигурационного файла (рис. 3).

5. Запуск WireGuard на стороне сервера и клиента с помощью универсальной команды wg-quick <наименование конфигурационного файла>.

```
[Interface]
PrivateKey = <приватный ключ сервера>
Address = 10.0.0.1/24
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
ListenPort = 51820

[Peer]
PublicKey = <публичный ключ клиента>
AllowedIPs = 10.0.0.2/32
```

Рис. 2. Пример конфигурационного файла на сервере

После установки и конфигурации рассматриваемого протокола на виртуальном стенде было успешно создано VPN-соединение для доступа к внутренней сети предприятия. Таким образом, при использовании WireGuard, хост PC2 имеет доступ к внутренней сети предприятия.

```
[Interface]
Address = 10.0.0.2/32
PrivateKey = <приватный ключ клиента>
DNS = 1.1.1.1

[Peer]
PublicKey = <публичный ключ сервера>
Endpoint = <публичный адрес сервера>:51820
AllowedIPs = 0.0.0.0/0, ::/0
```

Рис. 3. Пример конфигурационного файла на стороне клиента

Заключение. Использование комбинации открытого программного обеспечения pfSense и WireGuard является надежным и простым способом настройки защищенного удаленного доступа к сети малого предприятия. В результате проведенной работы был создан виртуальный стенд с настроенным безопасным VPN-каналом к

внутренней сети предприятия средствами открытого протокола WireGuard, развернутого на базе маршрутизатора PfSense.

СПИСОК ЛИТЕРАТУРЫ

1. Поротиков А. А. Корпоративные VPN сети. Виды реализации для различных организаций / А. А. Поротиков // Аллея науки. — 2020. — Т. 1, № 7(46). — С. 897-899.
2. An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN / Zhensheng Zhang, Ya-Qin Zhang, Xiaowen Chu, Bo Li // Photonic Network Communications. — 2004. — № 7. С. 213-225.
3. The Blended Methodology of Learning Computer Networks: Cloud-based Approach / Oleg Spirin, Vasyl Oleksiuk, Nadiia Balyk [и др.] // CEUR Workshop Proceedings. — 2019. — № 2393. С. 68-80.
4. Малин М. В. Использование VPN туннелей для безопасной передачи данных между офисами организации на примере Check Point / М. В. Малин // Аллея науки. — 2018. — Т. 2, № 4(20). — С. 935-938. — EDN XOHRIT.
5. Использование технологии vpn для обеспечения информационной безопасности / Д. В. Авласевич, Н. А. Дмитриев, А. А. Кириллов, А. Г. Бачинский // Форум молодых ученых. — 2020. — № 3(43). — С. 12-18.