УДК 004.056.52
DOI: 10.33764/2618-981X-2021-6-67-69

РАЗРАБОТКА ПРОЕКТА ПО СОЗДАНИЮ ЗАЩИЩЕННОЙ КОРПОРАТИВНОЙ СЕТИ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ VPN

Ольга Андреевна Дворникова
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности, тел. (999)451-98-14, e-mail: dvornikovaOlga21@gmail.com

Глеб Владимирович Попков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (913)478-91-30, e-mail: glebpopkov@inbox.ru

На текущий момент использование VPN соединения является популярным среди пользователей сети Интернет. 2020 год показал необходимость создания корпоративной удаленной сети для организаций всех сфер. Технология VPN позволяет с помощью специальных программ объединть отдельные компьютеры и локальные сети для защиты передаваемой информации. При соединении с сервером, находящимся в сети общего доступа, VPN технология формирует канал, защищающий информацию с помощью алгоритмов шифрования.

Ключевые слова: VPN, корпоративная сеть, информационная безопасность, шифрование, защищенный канал

DEVELOPMENT OF A PROJECT TO CREATE A PROTECTED CORPORATE NETWORK USING VPN TECHNOLOGIES

Olga A. Dvornikova
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Information Security, phone: (999)451-98-14, e-mail: dvornikovaOlga21@gmail.com

Gleb V. Popkov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Information Security, phone: (913)478-91-30, e-mail: glebpopkov@inbox.ru

At the moment, using a VPN connection is popular among Internet users. 2020 showed the need to create a corporate remote network for organizations of all spheres. VPN technology allows using special programs to unite individual computers and local networks to protect the transmitted information. When connecting to a server located in the VPN public access network, the technology forms a channel that is protected by information using encryption algorithms.

Keywords: VPN, corporate network, information security, encryption, secure channel

Введение

Рост пандемии COVID-19 вызвал множество проблем, которые даже эксперты не ожидали увидеть, а скорость, с которой компании почти мгновенно перешли на цифровую платформу, выдвинула на первый план множество техноло-

гических потребностей, которые ранее игнорировались [1]. Перед пандемией корпоративный VPN был роскошью, предоставляемой удаленным работникам и руководству высшего звена, которое составляло лишь небольшую часть персонала [2]. Согласно исследованию OpenVPN, проведенному в 2019 году, 24 % компаний не обновляли свою политику безопасности удаленной работы более года, а 44 % говорят, что их ИТ-отдел не руководил планом политики безопасности удаленной работы [3]. На текущий момент VPN предоставляет сотрудникам возможность работать удаленно, защищая при этом их личную информацию, включая их физическое местоположении и IP-адрес. Стоит отметить, что мир удаленной работы никуда не денется после пандемии. Организациям необходимо оценить текущую инфраструктуру безопасности на предмет слабых мест, которые остались без внимания во время внезапного перехода к удаленному доступу и начать планировать долгосрочную стратегию удаленной безопасности.

Если раньше VPN были новаторскими технологическими решениями, то теперь они стали необходимыми инструментами [4]. На базовом уровне VPN защищают вашу конфиденциальность в Интернете, поэтому вас нельзя преследовать или дискриминировать в зависимости от местоположения. VPN работают на уровне операционной системы, поэтому они перенаправляют весь трафик через другие серверы.

Материалы

VPN позволяет удаленным устройствам, например, ноутбукам, работать так, как будто они находятся в одной локальной сети [5]. Многие устройства VPN-маршрутизатора могут поддерживать десятки туннелей одновременно с использованием простых инструментов настройки, гарантируя всем сотрудникам доступ к данным компании, независимо от того, где они находятся [6].

Для настройки корпоративной сети понадобится VPN-клиент, VPN-сервер, VPN-маршрутизатор. Многие маршрутизаторы поставляются со встроенными клиентами VPN. Маршрутизатор должен подходить к требованиям безопасности. Двумя наиболее важными областями являются: шифрование и защита паролем. Необходимо выбрать наиболее безопасное шифрование, которое поддерживает маршрутизатор. После чего изменить пароль маршрутизатора. Несмотря на то, что смена пароля является банальным и обязательным во всех сферах IT, многие пренебрегают этим способом защиты. Далее из программного обеспечения роутера предоставляется доступ пользователям [7].

Результаты

Виртуальные частные сети защищают предприятия и пользователей, а также их конфиденциальные данные. Вот другие причины, по которым ваш бизнес может получить выгоду от VPN: удобство, лучшая безопасность, легкое администрирование.

VPN – это удобный способ предоставить сотрудникам, в том числе удаленным, легкий доступ к вашей бизнес-сети без необходимости физического присутствия при сохранении безопасности частных сетей и бизнес-ресурсов [8].

Связь с VPN-соединением обеспечивает более высокий уровень безопасности по сравнению с другими методами удаленной связи, закрывая частные сети для людей, не имеющих авторизованного доступа. Фактические географические местоположения пользователей защищены и не доступны для публичных или общих сетей, таких как Интернет [9].

С помощью гибких программных инструментов VPN легко добавлять новых пользователей или группы пользователей. Это хорошо для предприятий, которые растут быстрее, чем их бюджеты, поскольку это означает, что вы можете часто расширять сетевую площадь без добавления новых компонентов или создания сложных сетевых конфигураций [10].

Заключение

VPN создает «туннель», в котором вы можете отправить данные надежно с помощью шифрования и аутентификации инструментов. Компании часто используют VPN-соединения, потому что это более безопасный способ помочь сотрудникам удаленно получить доступ к частным сетям компании, даже если они работают вне офиса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Портал социологических данных РАНХиГС [Электронный ресурс]. URL: https://social.ranepa.ru/novosti/item/issledovanie-sociologov-ranhigs-vyyavilo-otnoshenie-rossiyan-k-rabote-v-udalennom-rezhime/ (дата обращения: 08.04.2021).
2. Запечников С.В. Основы построения виртуальных частных сетей / С.В. Запечников, Н.Г.Милославская, А.И. Толстой. – М: Горячая Линия, Телеком, 211. – 248 с.
3. Как организована удаленная работа в России и страна СНГ [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/remote-work-in-russia-and-the-cis-2020/ (дата обращения: 01.05.2021).
4. Обеспечиваем кибербезопасность удалённой работы сотрудников во время пандемии COVID-19 - Anti-Malware [Электронный ресурс]. URL: https://www.anti-malware.ru/practice/methods/Employee-Remote-Work-Cybersecurity/ (дата обращения: 05.04.2021).
5. Организация корпоративных сетей на основе VPN: построение, управление, безопасность [Электронный ресурс]. URL: https://www.kp.ru/guide/korporativnaja-set.html (дата обращения: 10.04.2021).
6. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие для студ. высш. учеб. заведений/ В.В. Платонов. — М. : Издательский центр «Академия», 2006. — 240 с.
7. Настройка VPN – CISCO [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html (дата обращения: 10.04.2021).
8. Сайт компании Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/ (дата обращения: 14.04.2021).
9. Что такое обработка естественного языка - NeuroHive [Электронный ресурс]. URL: https://neurohive.io/ru/osnovy-data-science/5-metodov-v-nlp-kotorye-izmenjat-obshhenie-v-budushhem// (дата обращения: 10.03.2021).
10. Гома Х. Проектирование систем реального времени, параллельных и распределенных приложений: Пер. с англ., – М. : ДМК, 2011. – 704с.