УДК 004.7:004.715

ВЫБОР ПРОТОКОЛА МАРШРУТИЗАЦИИ ДЛЯ ОРГАНИЗАЦИИ VPN

Ковалько О.А., Кулешов И.С.

гр. 367041

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Саломатин С.Б. – кандидат технических наук, доцент кафедры ИКТ

Аннотация. В статье рассматривается вопрос выбора протокола маршрутизации для организации сетей VPN. Анализируются наиболее популярные протоколы маршрутизации, такие как MPLS, IPSec, и OpenVPN, их преимущества и недостатки в различных сценариях использования. Статья помогает инженерам и администраторам сети сделать обоснованный выбор в пользу наиболее подходящего протокола для их конкретных нужд.

Ключевые слова: VPN, протоколы маршрутизации, MPLS, IPSec, OpenVPN, сетевая безопасность.

Введение. В эпоху цифровой трансформации, когда объемы цифровых данных растут с невиданными ранее темпами, а угрозы информационной безопасности становятся всё более прогрессивными и хитрыми — защита конфиденциальности и целостности данных приобретает критическое значение.

Особенно это касается организаций, стремящихся обеспечить безопасное и надежное взаимодействие внутри своих корпоративных сетей и за их пределами. Виртуальные частные сети (VPN) — на сегодняшний день, являются одним из ключевых инструментов, обеспечивающих защиту данных в процессе их передачи через общедоступные сети [1]. Однако эффективность VPN во многом зависит от выбора подходящего протокола маршрутизации, который обеспечивает не только безопасность, но и высокую производительность, масштабируемость и экономическую эффективность.

В этом контексте, выбор протокола маршрутизации для VPN представляет собой сложную задачу, требующую учета множества факторов, от технических характеристик и требований к безопасности до стоимости внедрения и поддержки [2]. Настоящая статья посвящена обзору этих ключевых аспектов и предлагает комплексный анализ, направленный на помощь в выборе наиболее подходящего протокола маршрутизации для организации эффективных и безопасных VPN-сетей [3].

Основная часть. Обзор протоколов маршрутизации, MPLS (Multiprotocol Label Switching). MPLS представляет собой механизм в высокопроизводительных телекоммуникационных сетях, который направляет данные от одной сетевой ноды к другой на основе коротких путевых меток вместо длинных сетевых адресов, ускоряя тем самым процесс передачи данных. Он поддерживает разделение трафика и его приоритизацию, что критически важно для приложений, требующих высокой пропускной способности и низкой задержки, таких как видеоконференции и VoIP. В корпоративных сетях MPLS обеспечивает улучшенное качество обслуживания, позволяя компаниям гарантировать определенный уровень производительности сети для критически важных приложений [4].

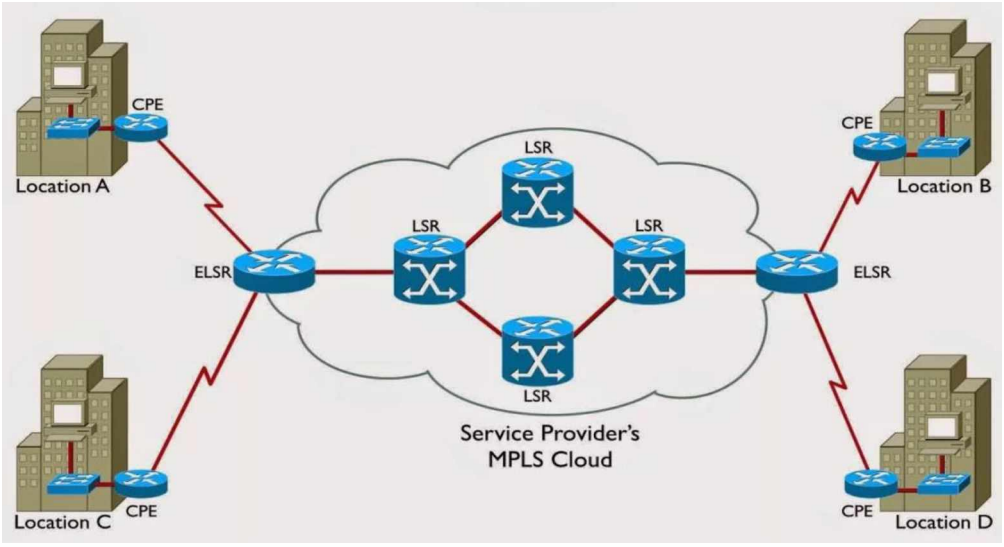

Рисунок 1 – Структура работы MPLS (Multiprotocol Label Switching)

IPSec (Internet Protocol Security). IPSec является набором протоколов для защиты данных, передаваемых через IP-сети, путем аутентификации и шифрования каждого IP-пакета в потоке коммуникации. Он широко применяется для создания защищенных соединений между сетями (сайт-сайт VPN) или между удаленным пользователем и сетью (клиент-сеть VPN). IPSec обеспечивает конфиденциальность передаваемых данных, защищая их от прослушивания, а также проверяет целостность и подлинность данных, предотвращая их подмену или несанкционированный доступ [5].

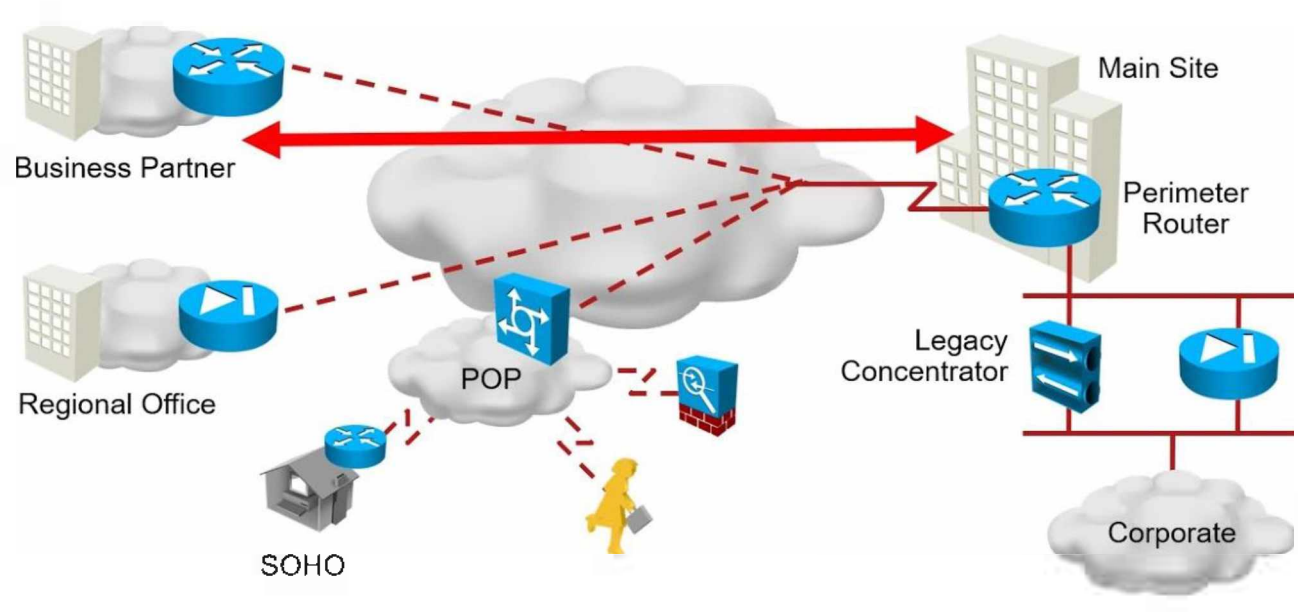

Рисунок 2 – Структура работы IPSec (Internet Protocol Security)

OpenVPN. Этот протокол представляет собой решение с открытым исходным кодом, обеспечивающее создание защищенных VPN-соединений. OpenVPN характеризуется высокой степенью гибкости и конфигурируемости, поддерживая различные типы аутентификации, включая сертификаты, ключи предварительного обмена, и двухфакторную аутентификацию. Благодаря поддержке стандартного SSL/TLS для шифрования сессий, OpenVPN предоставляет сильную защиту данных, делая его подходящим для использования в малых и средних предприятиях, которые ищут надежное, но при этом экономически эффективное решение для организации VPN [6].

Рисунок 3 – Структура работы OpenVPN

Комплексный анализ преимуществ и недостатков протоколов маршрутизации MPLS, IPSec и OpenVPN с учетом технических и экономических аспектов:

- MPLS предлагает высокую производительность и надежность для корпоративных сетей, поддерживая различные типы трафика и качество обслуживания. Однако, внедрение MPLS может быть дорогостоящим и сложным, требуя специализированных знаний и оборудования.

- IPSec обеспечивает сильную защиту на сетевом уровне, шифрует весь трафик между точками. Он подходит для создания безопасных соединений через общедоступные сети, но может быть сложен в настройке и управлении, особенно в крупных сетях.

- OpenVPN предлагает высокую гибкость и конфигурируемость, подходят для малых и средних предприятий благодаря открытому исходному коду и поддержке различных методов аутентификации и шифрования. Его недостатком может быть необходимость в дополнительной настройке и потенциально более низкая скорость передачи данных по сравнению с MPLS в некоторых случаях.

Важно учитывать специфику организации и ее требования к безопасности, производительности и стоимости при выборе между этими протоколами.

При выборе протокола маршрутизации для VPN следует учитывать следующие критерии, адаптированные к специфике организации:

- Требования к безопасности. Если высокий уровень безопасности является приоритетом, IPSec может быть предпочтительным выбором за счет его способности шифровать весь трафик на сетевом уровне. OpenVPN также предлагает сильную защиту с гибкостью настройки.

- Производительность и масштабируемость. Для крупных корпоративных сетей, где важны высокая производительность и масштабируемость, MPLS может быть лучшим выбором благодаря его способности управлять различными типами трафика и обеспечивать качество обслуживания.

- Сложность настройки и стоимость. Если ресурсы ограничены, и требуется более экономичный вариант с простотой настройки, OpenVPN может быть наиболее подходящим из-за его открытого исходного кода и поддержки широкого спектра операционных систем.

- Объем и характер передаваемых данных. Рассмотрите характер вашего трафика и какие данные передаются. Для чувствительных данных, где требуется гарантия целостности и конфиденциальности, IPSec или OpenVPN могут предложить более надежные решения.

Выбор должен базироваться на комплексном анализе текущих и будущих потребностей организации в области безопасности, производительности и стоимости владения.

Заключение. Анализ выбора протокола маршрутизации для VPN показал, что эффективное обеспечение безопасности корпоративной сети требует тщательного подхода к выбору протокола. Отсутствие универсального решения подчеркивает необходимость взвешенного анализа сильных и слабых сторон каждого протокола, в зависимости от специфических потребностей и условий использования. Ключевые аспекты, такие как технические характеристики, экономическая эффективность, и требования к безопасности, должны быть тщательно оценены для достижения оптимального баланса между стоимостью внедрения и уровнем защиты данных. Этот комплексный подход позволит организациям эффективно защитить свои сети, обеспечив при этом соответствие их бизнес-целям и требованиям.

Список литературы

1. *Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Учебник / В. Олифер, Н. Олифер. — СПб.: Питер, 2016. — 318 с.*
2. *Рыленков, Д. А. Анализ механизмов безопасности в протоколах динамической маршрутизации / Д. А. Рыленков. — Текст : непосредственный // Молодой ученый. — 2021. — № 45 (385). — С. 15-16. — URL: https://www.elibrary.ru/item.asp?edn=ebphix (дата обращения: 15.02.2024).*
3. *Таненбаум, Э. С. Компьютерные сети / Э. С. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2018. — 512 с.*
4. *Гольдштейн, А. Б. Транспортные сети IP/MPLS. Технология и протоколы : учебное пособие / А. Б. Гольдштейн, А. В. Никитин, А. А. Шкрыль. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2016. — 78 с. — ISBN 978-5-89160-129-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180159 (дата обращения: 15.02.2024). — Режим доступа: для авториз. пользователей.*
5. *Dayananda M.S., Kumar A. Architecture for Intercloud Services Using IPsec VPN // Second International Conference on Advanced Computing & Communication Technologies. Rohtak, Haryana, 2012. Pp. 463-467.*
6. *OpenVPN Cookbook - Second Edition - Keyser, J.J. SN - 9781786463128 UR - https://books.google.kz/books?id=MgNvgAACAAJ - 2017. Packt Publishing*

UDC УДК 004.7:004.715

THE CHOICE OF THE ROUTING PROTOCOL FOR THE VPN ORGANIZATION

Kovalko O.A, Kuleshov I.S.

gr.367041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Salomatin S.B. – Candidate of Technical Sciences, Associate Professor of the Department of ICT

Annotation. The article discusses the issue of choosing a routing protocol for organizing VPN networks. The most popular routing protocols, such as MPLS, IPsec and OpenVPN, are analyzed, their advantages and disadvantages in various use cases. The article helps engineers and network administrators to make an informed choice in favor of the most appropriate protocol for their specific needs.

Keywords: VPN, routing protocols, MPLS, IPsec, OpenVPN, network security.