АНАЛИЗ ПРИМЕНИМЫХ ПРОТОКОЛОВ В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ

Сухотский Тимур Дмитриевич

магистрант, Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ, РФ, г. Казань

Актуальность исследования связанна с разработкой методов и средств анализа виртуальных частных сетей, построенных с применением различных технологии. В настоящее время виртуальные частные сети играть большую роль в повседневной жизни. VPN необходим для защищенной передачи данных, создания защищённого соединения которое практически невозможно прослушать. Также VPN необходим для защиты структуры организации, которая преимущественно обладает в сети Интернет.

Виртуальная частная сеть [1, с. 5] (Virtual Private Network) – это зашифрованное соединение через Интернет от устройства к сети. Зашифрованное соединение помогает обеспечить безопасную передачу конфиденциальных данных. Данное соединение предотвращает прослушивание трафика несанкционированными пользователями и позволяет пользователю выполнять работу удаленно с отображением IP-адрес указанного сервера, маскирующий личность и местоположение.

Как и любой протокол VPN, IKEv2 [2, с. 23] (Internet Key Exchange version 2) отвечает за создание безопасного туннеля между VPN-клиентом и VPN-сервером. Это происходит путем аутентификации клиента и сервера, а затем согласования того, какие методы шифрования будут использоваться. IKEv2 поддерживает последние алгоритмы шифрования IPSec наряду с IKEv2 несколькими другими типами шифрования. Протокол IKE использует UDP-пакеты и UDP-порт 500. Он поддерживает 256-битное шифрование и может использовать такие алгоритмы шифрования, как AES, 3DES, Camellia и ChaCha20. IKEv2/IPSec один из самых быстрых протоколов VPN. Это все благодаря улучшенной архитектуре и эффективному процессу обмена сообщениями между ответами и запросами. Кроме того, тот факт, что он работает на UDP-порту 500, гарантирует низкую задержку в районе 40-50 мс.

Протокол туннелирования уровня 2 (Layer 2 Networking Protocol) [4, с. 2], в отличие от других протоколов VPN, не шифрует и не защищает данные. Из-за этого часто используются дополнительные протоколы, в частности IPSec (Internet Protocol Security), с помощью которого данные шифруются еще до передачи. Все современные устройства и системы, совместимые с VPN, имеют встроенный протокол L2TP/IPSec. Установка и настройка совершатся легко и не занимают много времени, однако может возникнуть проблема с использованием порта UDP 500, который блокируется файрволлами NAT (Network Address Translation). Так что, если протокол используется с брандмауэром, может потребоваться переадресация портов. Не известно о каких-либо крупных уязвимостях IPSec, и при правильном применении, этот протокол обеспечивает полную защиту конфиденциальных данных. Но двукратное инкапсулирование данных делает протокол не столь эффективным, как, например, решения на основе SSL, но при этом он работает медленнее других протоколов.

Протокол PPTP [3, с. 5] разработан компанией Microsoft и представляет собой туннелирование «точка-точка», то есть создается виртуальная частная сеть внутри общей сети, этот протокол был, есть и остается стандартом VPN с момента создания. Это первый VPN-протокол, поддерживаемый Windows, безопасность обеспечивается различными методами аутентификации, например, самый распространенный из них MS-CHAP v2. Каждое устройство, работающее с VPN, поддерживает PPTP по умолчанию, и, поскольку его очень просто настроить, этот протокол продолжает оставаться самым популярным среди владельцев

Сухотский Т.Д. Анализ применимых протоколов в виртуальных частных сетях // Технические и математические науки. Студенческий научный форум: электр. сб. ст. по мат. XXIX междунар. студ. науч.-практ. конф. № 6(29). URL: https://nauchforum.ru/archive/SNF_tech/6(29).pdf *(дата обращения: 06.09.2025)*

компаний и VPN-провайдеров, так как для его реализации требуется меньше всего вычислений.

Однако, хотя по умолчанию используется 128-битное шифрование, присутствуют определенные уязвимости безопасности, одна из самых серьезных — неинкапсулированная аутентификация MS-CHAP v2. Из-за этого PPTP можно скомпрометировать в течение двух дней.

В заключение можно сказать, что каждый выбирает для себя параметры, которые ему обходимы.

Такие как защищенность, скорость соединения или простота настройки и использования. Сравнения скоростей при скорости канала 100Мбит/с. представлены на рисунке.

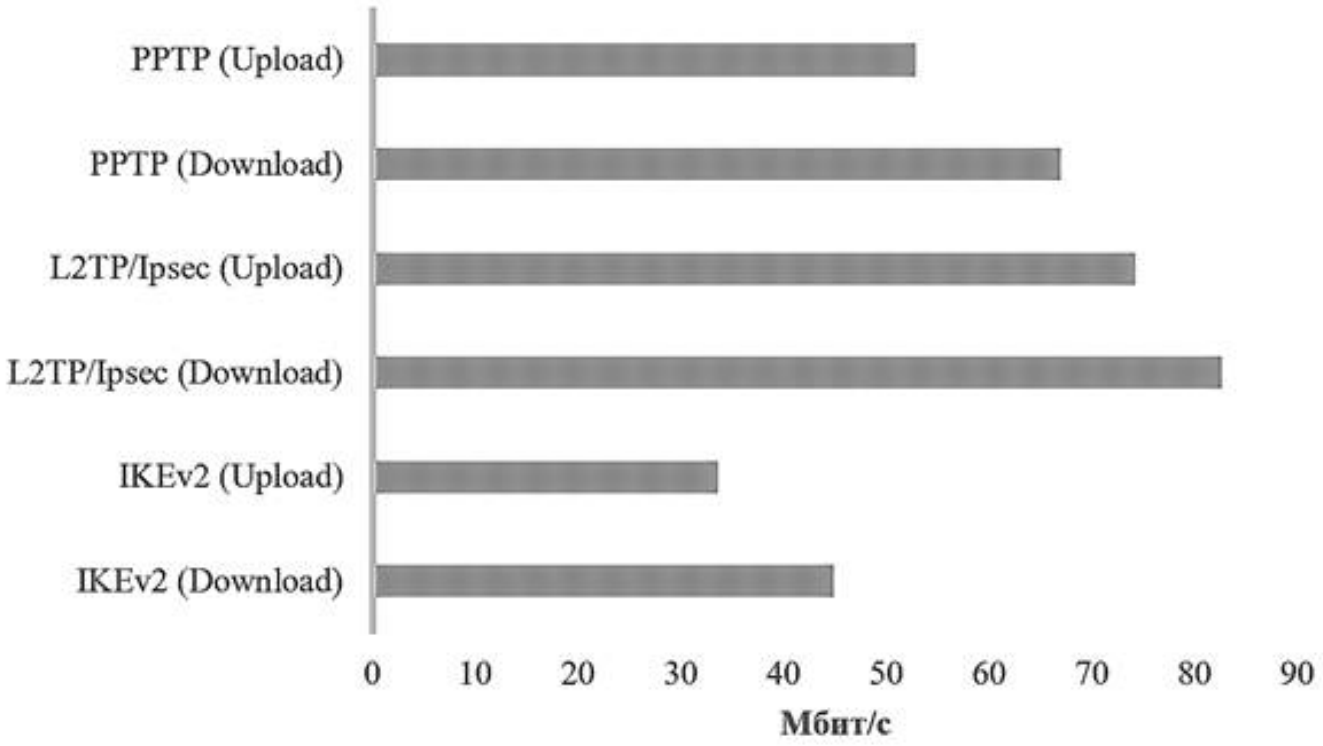

Рисунок. Сравнение скоростей анализируемых протоколов

Список литературы:

1. Andersson L., Madsen T. Provider Provisioned Virtual Private Network (VPN) Terminology. – [Электронный ресурс] – Режим доступа. –URL: https://tools.ietf.org/html/rfc4026 (Дата обращения: 16.05.2020).

2. Bartlett G., Inamdar A. IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS (Networking Technology: Security) 1st Edition. Индианаполис: Cisco Press, 2017. 607 с.

3. Hamzeh K., Pall G., Verthein W. Point-to-Point Tunneling Protocol (PPTP). – [Электронный ресурс] – Режим доступа. –URL: https://tools.ietf.org/html/rfc2637 (Дата обращения: 13.05.2020).

4. T'Joens Y., Sales B., Crivellari P. Layer Two Tunnelling Protocol (L2TP) . – [Электронный ресурс] – Режим доступа. –URL: https://tools.ietf.org/html/rfc3301 (Дата обращения: 12.05.2020).