УДК 004.7

Охріменко Д. С., магістрант
Науковий керівник: Єфіменко А. А., канд. техн. наук, доцент, зав. кафедри КІ та КБ,
Вакалюк Т. А. д-р пед. наук, професор, професор кафедри ІПЗ
Державний університет «Житомирська політехніка»

ТИПИ ТУНЕЛЬНИХ З'ЄДНАНЬ ДЛЯ ПОБУДОВИ VPN-МЕРЕЖ

Протокол PPTP (Point-to-Point Tunneling Protocol) – один з найбільш відомих тунельних протоколів клієнт-сервер, отримав поширення завдяки тому, що з Windows 95 клієнт PPTP OSR2 був включений до складу операційної системи. Технічно PPTP використовує два мережевих з'єднання: канал управління, що працює через TCP і використовує порт 1723 та GRE-тунель для передачі даних. Через це можуть виникати складнощі з використанням в мережах мобільних операторів, проблема з одночасною роботою декількох клієнтів через NAT та проблема прокидання PPTP з'єднання через NAT. Іншим істотним недоліком є низька безпека протоколу PPTP, через це не можна будувати на базі PPTP захищені віртуальні мережі [1].

Протокол L2TP (Layer 2 Tunneling Protocol) – це технологія, розроблена компаніями Cisco та Microsoft, яка використовує єдине UDP-з'єднання на порту 1701 для передачі даних і контрольних повідомлень, але не містить жодних вбудованих функцій інформаційної безпеки. Клієнт L2TP також інтегрований з усіма сучасними мережевими системами та пристроями.

Без шифрування L2TP широко використовується провайдерами для надання доступу до Інтернету, забезпечуючи таким чином розділення між безкоштовним інтранет і дорогим інтернет-трафіком. L2TP через IPsec (L2TP / IPsec) зазвичай використовується для створення VPN, де IPsec працює в транспортному режимі та виконує шифрування даних в пакетах L2TP. У цьому випадку тунель L2TP створюється всередині каналу IPsec, для його встановлення необхідно спочатку забезпечити з'єднання IPsec між вузлами. До переваг L2TP можна віднести високу поширеність і надійність, IPsec не має серйозних вразливостей, через це він вважається дуже безпечним. До недоліків можна віднести велике навантаження на обладнання та низька швидкість [2].

Протокол IP-IP (IP over IP) є одним з найпростіших тому що має найнижчі накладні витрати при тунелюванні, але на відміну від GRE, він інкапсулює лише одноадресний (unicast) трафік IPv4. Це також протокол без збереження стану та вбудованих механізмів безпеки, які зазвичай використовуються з IPsec (IP-IP over IPsec). Підтримується UNIX-подібними системами та мережевим обладнанням. Оскільки GRE не використовує порти і не проходить через NAT, номер протоколу 4.

Протокол SSTP (Secure Socket Tunneling Protocol) – безпечний протокол VPN, розроблений компанією Microsoft, відноситься до SSN VPN, поширюється переважно в середовищі Windows. Технічно SSTP – це тунельне з'єднання PPP з вашим HTTPS-сеансом через стандартний порт 443. Це дозволяє успішно працювати в мережах різного типу, оскільки HTTPS широко використовується для доступу до сайтів, усуває проблему пробудження або роботи через NAT [3].

Протокол GRE (Generic Routing Encapsulation) – тунельний протокол, розроблений Cisco, що використовується для інкапсуляції всіх протоколів мережевого рівня OSI (тобто не тільки IP), GRE працює безпосередньо через IP і не використовує порти, не проходить через NAT, номер протоколу 47. Протокол GRE через IPsec зазвичай використовується разом для створення безпечних рішень, коли тунель GRE налаштований через захищений канал IPsec [4].

Протокол EoIP (Ethernet over IP) – розроблений компанією Mikrotik тунельний протокол (L2) канального рівня, працює на основі протоколу GRE, інкапсулюючи кадри Ethernet в пакети GRE. Дана технолгія дозволяє підключати віддалені мережі на рівні канальному та забезпечує зв'язок між маршрутизаторами без необхідності налаштування маршрутизації. Слід розуміти, що таке з'єднання передбачає проходження широкомовного трафіку, це може значно погіршити продуктивність тунелю, зокрема на вузьких каналах та з відчутними затримками. Також EoIP можна використовувати для підключення промислового та комерційного обладнання, яке не може працювати на рівні мережі (L3) з використанням маршрутизації[4].

Перелік використаних джерел

1. Протоколи тунелювання VPN [Електронний ресурс]. URL: http://cmd4win.ru/windows-2008/845-protokoly-tunnelirovaniya-vpn.

2. Віртуальна приватна мережа [Електронний ресурс]. URL: https://www.sites.google.com/site/zahistlokalnoiemerezi/zahist/virtualna-privatna-mereza.

3. Як влаштований VPN через SSTP [Електронний ресурс]. URL: https://habr.com/ru/post/196134/.

4. Мережі для найменших. Частина сьома. VPN [Електронний ресурс]. URL: https://habr.com/ru/post/170895/.