ПОРІВНЯННЯ ПРОТОКОЛІВ VPN ДЛЯ ОРГАНІЗАЦІЇ КОРПОРАТИВНОЇ ПРИВАТНОЇ МЕРЕЖІ

Рябко М.С.
Науковий керівник – доц. Костромицький А.І.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Інформаційно-мережної інженерії
тел. (057) 702-14-29)

This paper considers a comparison of the VPN protocols that are most commonly used when deploying a corporate virtual private network. An Internet-based enterprise VPN is required for the exchange of private information between physically remote equipment and employees. Building a VPN requires knowledge of the protocol features that will be used to transport and encrypt personal data. An understanding of the principles of working via the Internet and the equipment features of network participants is also required. The comparison was based on protocol characteristics such as data transfer rate, security, availability, complexity of blocking and implementation.

Дані, що передаються корпоративною мережею, представляють собою приватну інформацію, яка повинна залишатись конфіденційною під час її транспортування. Оскільки майже всі підприємства, що використовують корпоративну мережу фізично розташовані за межами однієї локальної мережі, є необхідність об’єднати віддалені офіси або окремих співробітників в єдину мережу, використовуючи мережу загального доступу Інтернет. Для об’єднання декількох локальних мереж створюють VPN, що забезпечує шифрування даних і їх наскрізну передачу між користувачами мережі.

Вірний вибір протоколів є основою для VPN , так як всі протоколи мають певні характеристики та вимоги, що до налаштування і реалізації. Тому існує необхідність перед вибором протоколів, виявити, який трафік буде маршрутизуватися, тип та характеристики обладнання користувачів мережі, сумісність протоколів і обладнання, що плануються для використання.

Найчастіше використовують такі протоколи:

- PPTP;
- L2TP/IPsec;
- OpenVPN.

Серед інших протоколів, їх перевагами є сумісність з багатьма операційними системами та доступність.

PPTP це протокол тунельного зв'язку, який працює на канальному рівні. Він створює тунель через мережу Інтернет до сервера-одержувача і передає PPP-пакети віддаленого клієнта, використовуючи інкапсуляцію IP-пакетів. Для автентифікації використовує протокол MS-CHAPv2.

Шифрування – MPPE-128 біт[1]. Середня швидкість 70 Мбіт/с при широкосмуговому з'єднанні 100 Мбіт/с.

Його перевагами являються: швидкість, простота реалізації, стабільність з'єднання, підтримка всіх операційних систем.

Недоліки: низький рівень безпеки – 128 - бітне шифрування, легкий спосіб блокування, працює лише через 1723 порт.

L2TP – це протокол тунельного зв'язку, оскільки він не забезпечує шифрування, разом з ним використовується протокол шифрування IPsec, для забезпечення конфіденційності даних. Використовує 500 UDP-порт. На даний момент IPsec вважається безпечним рішенням при використанні алгоритмів шифрування AES[1].

Переваги: простота реалізації, підтримка всіх операційних систем, високий рівень безпеки та стабільність з'єднання.

Недоліки: низька швидкість та високий рівень використання ресурсів CPU для забезпечення подвійної інкапсуляції, легкий спосіб блокування.

OpenVPN – інструмент з відкритим вихідним кодом. Працює в режимі точка-точка або клієнти-сервер. Має три режими автентифікації:

- за допомогою встановленого ключа;
- автентифікація по сертифікату;
- по логіну і паролю.

Існує підтримка з'єднання VPN з динамічними віддаленими вузлами, тунелі поверх NAT або за допомогою повноцінного брандмауера. Безпеку і шифрування забезпечено бібліотекою OpenSSL або PolarSSL і протоколом транспортного рівня Transport Layer Security. Дозволяє підключатися через UDP-порт або TCP-порт. При підключенні по UDP підвищується швидкість передачі даних, а при підключені по TCP підвищується надійність за рахунок збільшення часу затримки.

Переваги: гнучке налаштування, високий рівень безпеки, може працювати крізь брандмауери, використовує широкий спектр алгоритмів шифрування, підтримка багатьох операційних систем.

Недоліки: складність інсталяції, необхідність встановлювати додаткове програмне забезпечення, обмежена підтримка портативними пристроями.

Оскільки кожен з протоколів має певні переваги та недоліки в порівнянні з іншими, зробити однозначний висновок, який з протоколів краще використовувати, можна, тільки провівши більш детальний розбір, що буде виконано в магістерській роботі.

Перелік джерел:

1. Charlie Scott Virtual Private Networks, Second Edition / Charlie Scott, Paul Wolfe, Mike Erwin. – O'Reilly Media, Inc., 1999.