УДК 004.9:61
В.М. Возний, Б. Б. Млинко канд. техн. наук, доц.
Тернопільський національний технічний університет імені І.Пулюя, Україна

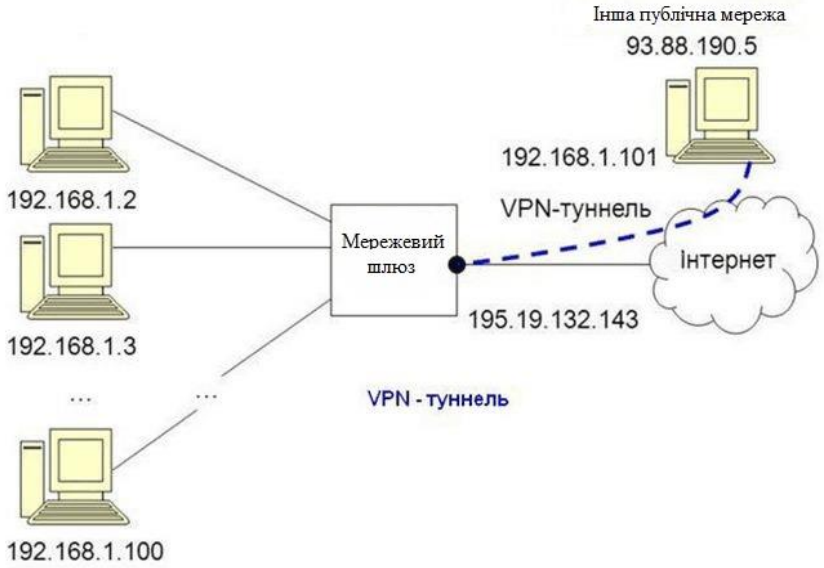
ПІДКЛЮЧЕННЯ ВІДДАЛЕНОГО ОФІСУ В ЛОКАЛЬНУ МЕРЕЖУ ЧЕРЕЗ ВИДІЛЕНИЙ ТРАНСПОРТ ПРОВАЙДЕРА

V.M. Volodymyr, B.B. Mlynko Ph.D., Assoc. Prof.

CONNECTING A REMOTE OFFICE TO A LOCAL NETWORK THROUGH DEDICATED PROVIDER TRANSPORT

Віртуальна приватна мережа (vpn) - це технологія, що забезпечує захищену (закриту від зовнішнього доступу) зв`язок логічної мережі поверх приватної або публічної при наявності високошвидкісного інтернету.Таке мережеве з`єднання комп`ютерів (географічно віддалених один від одного на пристойну відстань) використовує підключення типу «точка - точка» (іншими словами, «комп`ютер-комп`ютер»). Науково, такий спосіб з`єднання називається vpn тунель (або тунельний протокол). Підключитися до такого тунелю можна при наявності комп`ютера з будь операційною системою, в яку інтегрований VPN-клієнт, здатний робити «кидок» віртуальних портів з використанням протоколу TCP / IP в іншу мережу.

Основна перевага vpn полягає в тому, що погоджує сторонам необхідна платформа підключення, яка не тільки швидко масштабується, а й (в першу чергу) забезпечує конфіденційність даних, цілісність даних і аутентифікацію.



На схемі наочно представлено використання vpn мереж. Тут, комп`ютери з ip-адресами 192.168.1.1-100 підключаються через мережевий шлюз, який також виконує функцію VPN-сервера. Попередньо на сервері і маршрутизаторе повинні бути прописані правила для з`єднань по захищеному каналу.

Коли відбувається підключення через vpn, в заголовку повідомлення передається інформація про ip-адресу VPN-сервера і віддаленому маршруті. Інкапсульовані дані, що проходять по загальній або публічної мережі, неможливо перехопити, оскільки вся інформація зашифрована. Етап VPN шифрування реалізується на стороні відправника, а розшифровуються дані у одержувача по заголовку повідомлення (при наявності загального ключа шифрування). Після правильної розшифровки повідомлення між

двома мережами встановлюється ВПН з`єднання, яке дозволяє також працювати в публічній мережі (наприклад, обмінюватися даними з клієнтом 93.88.190.5). Що стосується інформаційної безпеки, то інтернет є вкрай незахищеною мережею, а мережа VPN з протоколами OpenVPN, L2TP / IPSec, PPTP, PPPoE - цілком захищеним і безпечним способом передачі даних. Vpn тунелювання використовується:

- всередині корпоративної мережі;
- для об`єднання віддалених офісів, а також дрібних відділень;
- для обслуговування цифрової телефонії з великим набором телекомунікаційних послуг;
- для доступу до зовнішніх IT-ресурсів;
- для побудови та реалізації відеоконференцій.

Для корпоративного зв`язку в великих організаціях або об`єднання віддалених один від одного офісів використовують апаратне обладнання, здатне підтримувати безперервну, захищену роботу в мережі. Для реалізації vpn-технологій в ролі шлюзу можуть виступати: сервера Unix, сервера Windows, мережевий маршрутизатор і мережевий шлюз на якому піднято VPN. Сервер або пристрій, що використовується для створення vpn мережі підприємства або vpn каналу між віддаленими офісами, має виконувати складні технічні завдання і забезпечувати весь спектр послуг користувачам як на робочих станціях, так і на мобільних пристроях. Будь-який роутер або vpn маршрутизатор повинен забезпечувати надійну роботу в мережі без «зависань». А вбудована функція ВПН дозволяє змінювати конфігурацію мережі для роботи вдома, в організації або віддаленому офісі.

У загальному випадку настройка VPN на роутері здійснюється за допомогою веб-інтерфейсу маршрутизатора. На «класичних» пристроях для організації vpn потрібно зайти в розділ «settings» або «network settings», де вибрати розділ VPN, вказати тип протоколу, внести налаштування адреси вашої підмережі, маски і вказати діапазон ip-адрес для користувачів. Крім того, для безпеки з`єднання потрібно вказати алгоритми кодування, методи аутентифікації, згенерувати ключі узгодження і вказати сервера DNS WINS. В параметрах «Gateway» потрібно вказати ip-адреса шлюзу (свій ip) і заповнити дані на всіх мережевих адаптерах. Якщо в мережі кілька маршрутизаторів необхідно заповнити таблицю vpn маршрутизації для всіх пристроїв в VPN тунелі. Список апаратного обладнанні, що використовується при побудові VPN-мереж:

- Маршрутизатор компанії Dlink: DIR-320, DIR-620, DSR-1000 с новими прошивками або Роутер D-Link DI808HV.
- Маршрутизатор Cisco PIX 501, Cisco 871-SEC-K9
- Роутер Linksys Rv082 з підтримкою близько 50 VPN-тунелів
- Netgear маршрутизатор DG834G і роутери моделей FVS318G, FVS318N, FVS336G, SRX5308
- Маршрутизатор Mikrotik з функцією OpenVPN. Приклад RouterBoard RB / 2011L-IN Mikrotik
- vpn обладнання RVPN S-Terra або VPN Gate
- Маршрутизатор ASUS моделей RT-N66U, RT-N16 і RT N-10
- ZyXel маршрутизатори ZyWALL 5, ZyWALL P1, ZyWALL USG