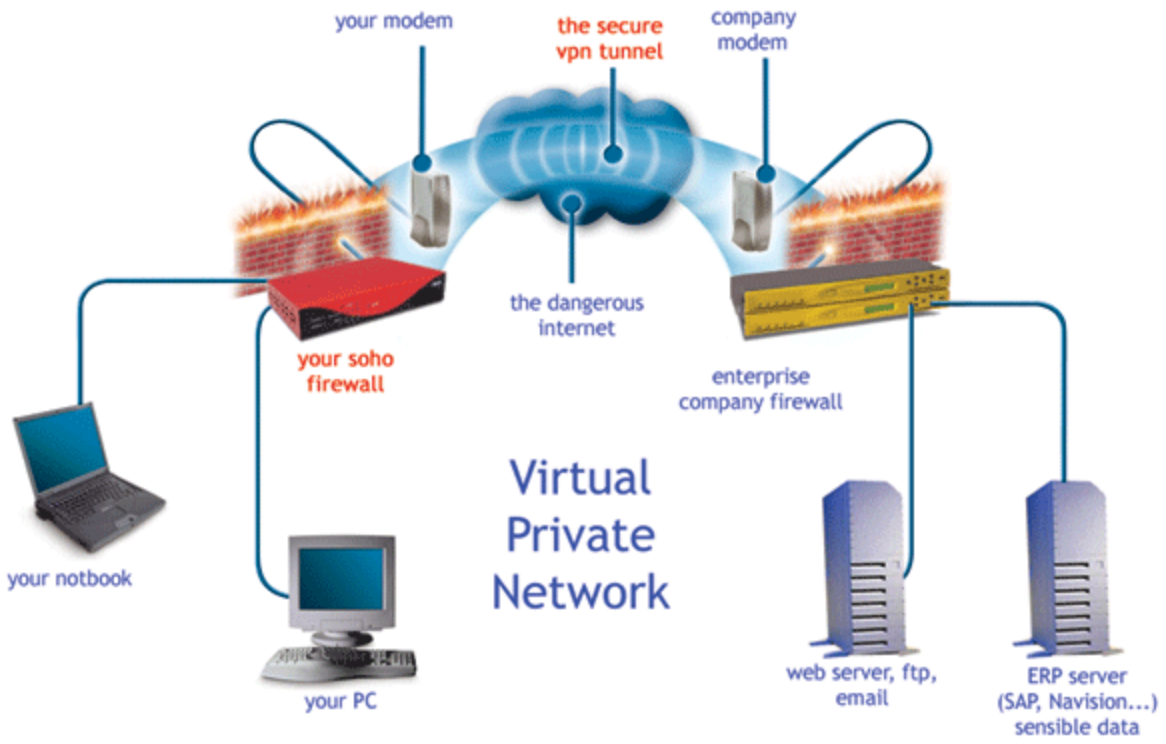
Передавання інформації через захищені мережі

Підготувала:
студентка групи СН-41
Паздрій Ганна

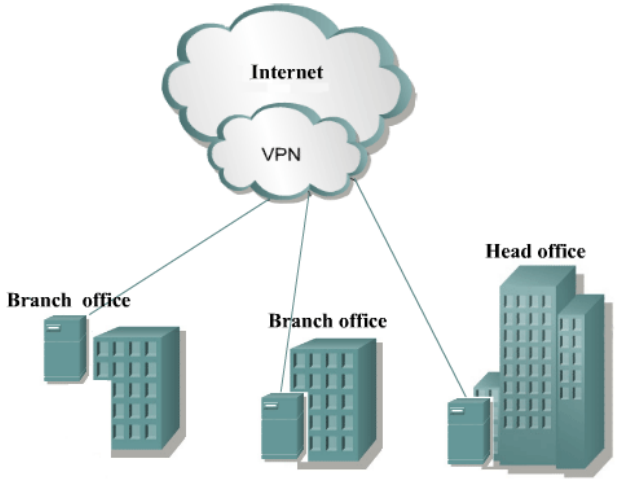
Віртуальні захищені мережі

Захищеною або приватною віртуальною мережею (Virtual Private Network, VPN) називається об'єднання локальних мереж і окремих комп'ютерів через відкрите зовнішнє середовище передавання інформації в єдину віртуальну мережу, яка забезпечує захист інформації, що в ній циркулює.

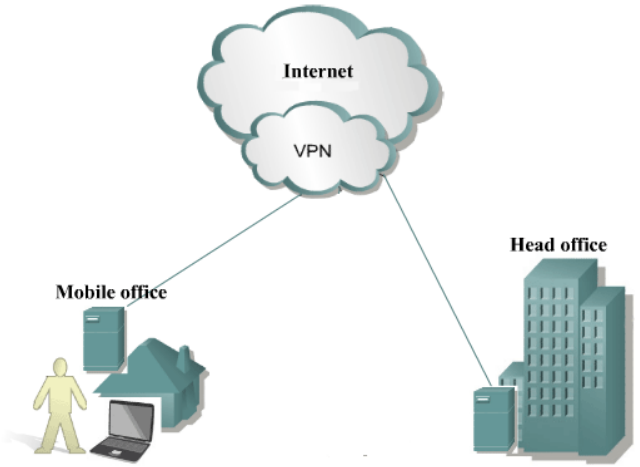


Класифікація VPN за призначенням

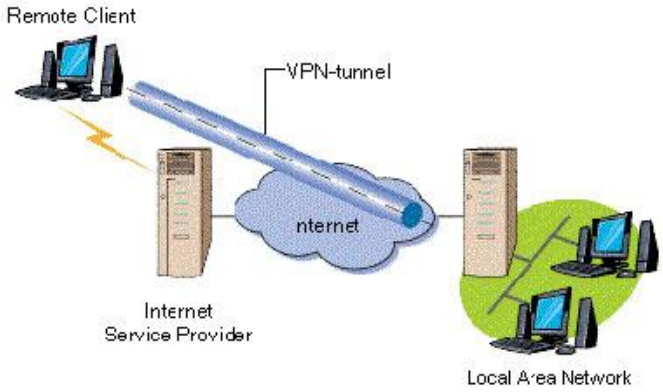
Intranet VPN



Remote Access VPN



Extranet VPN



Client / Server VPN

Internet VPN

Реалізації VPN

OpenVPN

Вільна реалізація технології VPN з відкритим вихідним кодом для створення зашифрованих каналів типу точка-точка або сервер-клієнти між комп'ютерами. Вона дозволяє встановлювати з'єднання між комп'ютерами, що знаходяться за NAT-firewall, без необхідності зміни їх налаштувань. OpenVPN була створена Джеймсом Йонаном (James Yonan) і розповсюджується під ліцензією GNU GPL.

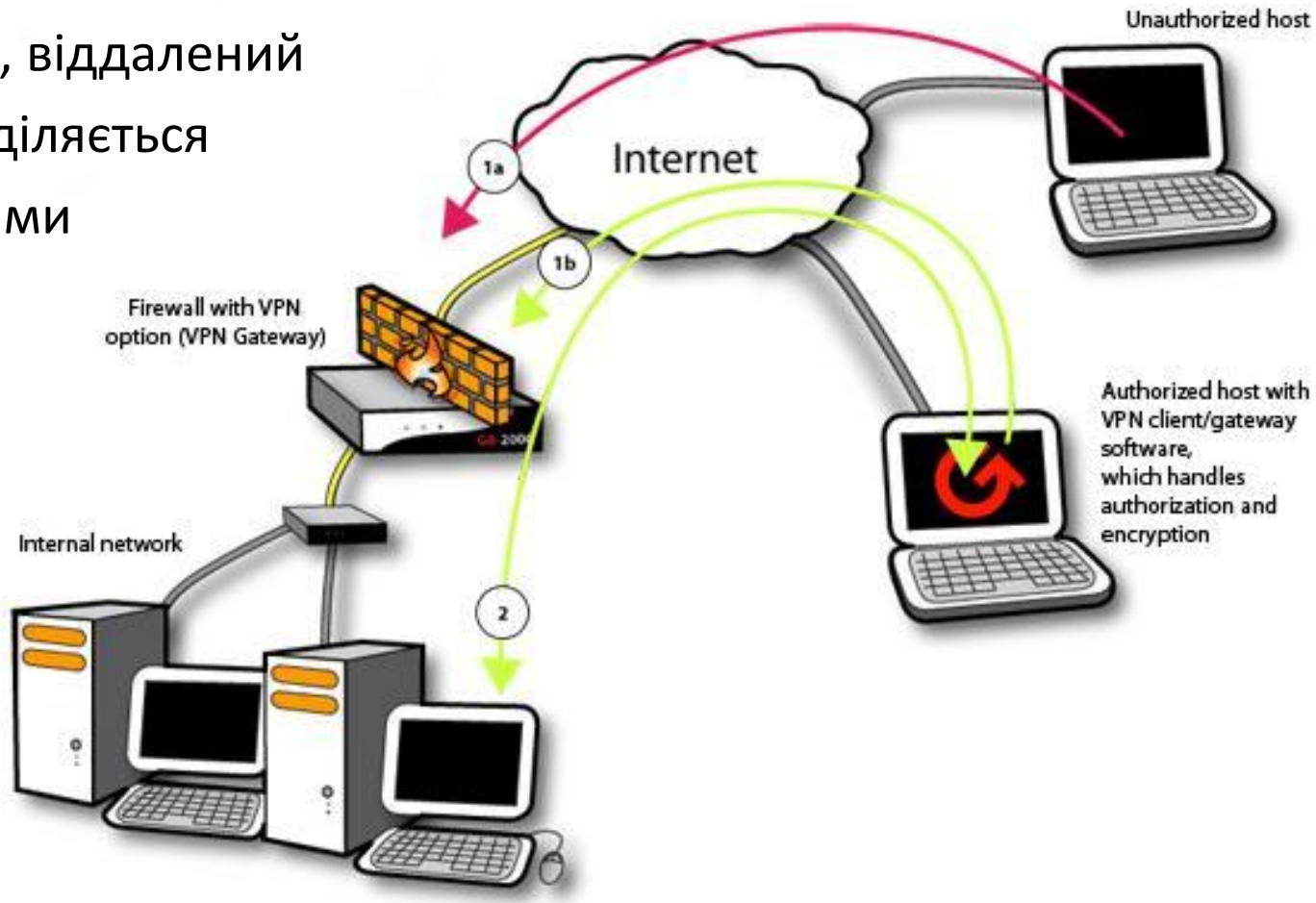
DMVPN (англ. Dynamic Multipoint Virtual Private Network - динамічна багатоточкова віртуальна приватна мережа) - технологія для створення віртуальних приватних мереж, розроблена Cisco Systems. Є подальшим розвитком VPN і грунтується на спільній роботі протоколів дозволу шлюзу NHRP, протоколу тунелювання mGRE, шифрування IPSec і протоколів динамічної маршрутизації: OSPF, ODR, RIP, EIGRP,OSPF, BGP.

Система безпеки VPN

Управління доступом, аутентифікація та шифрування - найважливіші елементи захищеного з'єднання.

Інформація передається в зашифрованому вигляді. Найбільш часто використовуваним алгоритмом кодування є Triple DES, який забезпечує потрійне шифрування (168 розрядів) з використанням трьох різних ключів.

Підтвердження достовірності включає в себе перевірку цілісності даних та аутентифікацію користувачів, задіяних у VPN. Сервер доступу вимагає проходження процесу **ідентифікації**, а потім процесу **аутентифікації**. Після успішного проходження обох процесів, віддалений користувач наділяється повноваженнями для роботи в мережі, тобто відбувається процес **авторизації.**



Основи тунелювання

Тунелювання (tunneling) або інкапсуляція (encapsulation) - це спосіб передачі корисної інформації через проміжну мережу.Такою інформацією можуть бути кадри (або пакети) іншого протоколу. При інкапсуляції кадр не передається в згенерованому вузлом-відправником вигляді, а забезпечується додатковим заголовком, містить інформацію про маршрут, що дозволяє інкапсульованим пакетам проходити через проміжну мережу (Internet). На кінці тунелю кадри деінкапсулюються і передаються одержувачу.

Цей процес (що включає інкапсуляцію і передачу пакетів) і є тунелювання. Логічний шлях пересування інкапсульованих пакетів в транзитній мережі називається тунелем.

VPN працює на основі протоколу PPP (Point-to-Point Protocol)

Основні компоненти PPP:

Протокол LCP - PPP задає гнучкий LCP для встановлення, налаштування та перевірки каналу зв'язку. LCP забезпечує узгодження формату інкапсуляції, розміру пакету, параметри установки і розриву з'єднання, а також параметри аутентифікації. Як протоколи аутентифікації можуть використовуватися PAP, CHAP і ін.

Протоколи управління мережею - надають специфічні конфігураційні параметри для відповідних транспортних протоколів. Наприклад, IPCP протокол управління IP.

Для формування тунелів VPN використовуються протоколи: PPTP, L2TP, IPsec, IP-IP.

Протокол PPTP - дозволяє інкапсулювати IP-, IPX- і NetBEUI-трафік в заголовки IP для передачі по IP-мережі, наприклад Internet.

Протокол L2TP - дозволяє шифрувати і передавати IP-трафік з використанням будь-яких протоколів, що підтримують режим "точка-точка" доставки дейтаграм. Наприклад, до них відносяться протокол IP, ретрансляція кадрів і асинхронний режим передачі (ATM).

Протокол IPsec - дозволяє шифрувати та інкапсулювати корисну інформацію протоколу IP в заголовки IP для передачі по IP-мережі.

Протокол IP-IP – IP-дейтаграма інкапсулюється за допомогою додаткового заголовка IP. Головне призначення IP-IP - тунелювання багатоадресного трафіку в частинах мережі, що не підтримують багатоадресну маршрутизацію.

Список використаних джерел

1. http://www.hub.ru/archives/2261
2. http://uk.wikipedia.org/wiki/VPN
3. http://www.3dnews.ru/communication/postroenie_bezopasnih_setei_na_osnove_vpn
4. http://ru.wikipedia.org/wiki/OpenVPN
5. http://ru.wikipedia.org/wiki/Dynamic_Multipoint_Virtual_Private_Network
6. Грайворонський М. В., Новіков О. М. Г14 Безпека інформаційно-комунікаційних систем. — К.: Видавнича група ВНУ, 2009. — 608 с.

Дякую за увагу!