

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ім. Тараса Шевченка  
ФАКУЛЬТЕТ КІБЕРНЕТИКИ

РЕФЕРАТ  
на тему «віртуальні приватні мережі (VPN)»

Виконав: Процик Петро  
Група – ТТП-5

КИЇВ 2005

# ЗМІСТ

1. Вступ
2. Основи віртуальних приватних мереж
3. Еволюція віртуальних приватних мереж
4. Протоколи віртуальних приватних мереж
5. Класифікація ВПМ
6. Література

## Вступ

За останні десять років світ став свідком бурхливого росту мережі інтернет. Цей ріст був викликаний не стільки за рахунок збільшення нових користувачів, скільки проникненням інтернету у все більше сфер сучасного життя суспільства, зміною пріоритетів ведення бізнесу, появою електронної комерції.

Спочатку, компанії у всьому світі використовували інтернет для поширення інформації про нову продукцію та сервіси шляхом відкриття корпоративних веб-сайтів. З часом, увага змістилась в бік електронної комерції та електронного бізнесу. Для яких основними питанням є забезпечення захисту даних, збереження інвестицій та глобальний доступ до бізнес функціональності і необхідних даних. Більш того поява великої кількості міжнародних компаній викликала необхідність об'єднання географічно віддалених підрозділів у єдину мережу передачі даних.

Існували два принципово різних підхода до розв'язання цієї проблеми – побудова власної транспортної мережі, що означало вклад значних коштів, а іноді і не можливість реалізації такого проекту. Інший варіант – використовувати існуючі глобальні мережі передачі даних. Такою мережею майже безальтернативно визнана мережа Інтернет.

На основі мережі інтернет, як транспортної мережі виникла нова концепція віртуальних приватних мереж (Virtual Private Network, VPN). Основна ідея її така: мережею оголошується деякий набір комп'ютерів, які не обов'язково повинні перебувати в одному місці, а як канали передачі даних використовуються вже існуючі (звідси й слово «віртуальні»). У цьому випадку це - канали Інтернету. При цьому інформація передається в зашифрованому виді (звідси слово «приватна»). Схематично це може бути реалізоване в такий спосіб: на кожному з комп'ютерів майбутньої мережі встановлюється програма-клієнт. Метою програм-клієнтів є як мінімум виконання функцій firewall і шифрування інформації. Який-небудь виділений комп'ютер стає сервером, звідки можливе керування мережею і спостереження за її роботою. Залежно від складності програм користувачам мережі стають доступні різні набори додаткових сервісів, таких як захищена пошта, захищена передача електронних підписів і багато чого іншого. Дані мережі мають цілий ряд переваг. Немає необхідності побудови яких-небудь нових мереж і прокладки нових каналів зв'язку, що істотно заощаджує кошти компанії, оскільки існуючі канали Інтернету є досить дешевим засобом передачі даних. Комп'ютери не повинні бути зосереджені в одному місці або будинку. Це безсумнівно зручно, наприклад, якщо необхідно зв'язок між різними філіями компанії або, скажемо, між

виробниками продукції й дилерами. На додаток до цього при установці віртуальної приватної мережі ви одержуєте захищений трафік своїх даних — імовірність взлому стає фактично рівної нулю (середній час злому застосовуваних у цей час ключів шифрування оцінюється в сотні років). До того ж, як було сказано вище, ви можете одержати деякі додаткові сервіси.

Недивно, що, маючи такі переваги, ідея одержала швидке визнання серед провідних мережних виробників світу. Зараз багато фірм, що розробляють мережне апаратне і програмне забезпечення, створюють свої розробки, які реалізують концепцію віртуальних приватних мереж.

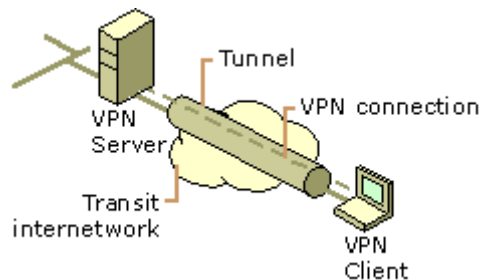
## Основи віртуальних приватних мереж

Рушійною силою всієї технології віртуальних приватних мереж (ВПМ) – є використання Інтернету та його глобальній доступності. Проте, оскільки інтернет розподілене публічне середовище, до якого можна отримати доступ влюбий час, майже з будь-якого місця, широкими апаратними засобами, обмін даними стає не безпечним. Існує велика вірогідність того, що дані будуть перехоплені зловмисником або підмінені на інші. Тому головна мета ВПМ – забезпечити безпеку, ефективність, надійність за доступну ціну.

Що ж таке ВПМ?

Згідно стандартного визначення даного *Internet Engineering Task Force (IETF)*, ВПМ – це емуляція приватної мережі WAN, використовуючи відкриті можливості IP мереж, такі як Інтернет або приватні IP бекбони. В оригіналі: "*An emulation of private Wide Area Network (WAN) using shared or public IP facilities, such as the Internet or private IP backbones.*"

Простішими термінами ВПМ це з'єднання приватних інтранет мереж через публічну мережу (інтернет), яке гарантує захист та ефективність зв'язку між двома комунікаційними точками. Приватна інтранет мережа розширюється за рахунок приватних логічних «тунелів» (каналів). Ці тунелі дозволяють двом точкам обмінюватись даними шляхом аналогічним з'єднанню точка-точка (point-to-point connection).



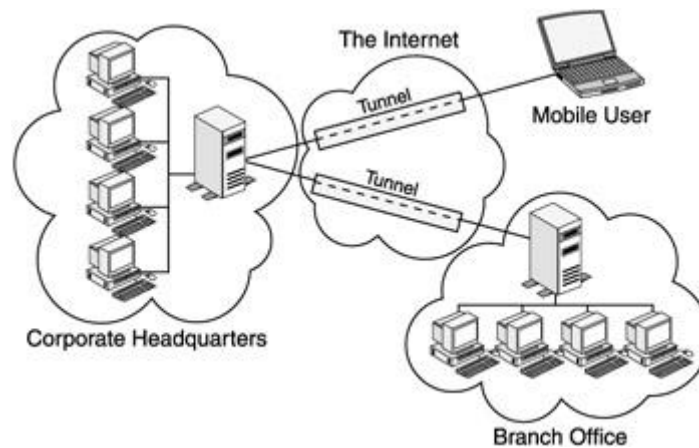
Малюнок 1, ВПМ з'єднання

Прийнято, що ВПМ з'єднання повинні складатись з трьох елементів. З'єднання вважається ВПМ коли ці три елемента коректно функціонують. Це:

- аутентифікація
- шифрування
- тунелювання

На малюнку (мал. 2) зображена типова конфігурація ВПМ з'єднання.

Хоча технологія тунелювання лежить в основі ВПМ, сюди ж включаються добре розроблені технології забезпечення надійної передачі даних по ненадійним з'єднанням. Ці механізми безпеки включають: шифрування, аутентифікацію, авторизацію.



Малюнок 2: Типова конфігурація ВПМ

#### - Шифрування.

Шифрування це процес зміни даних таким чином, щоб прочитати їх міг тільки адресат. Для того щоб прочитати повідомлення одержувач повинен мати відповідний ключ для розшифрування.

В простих схемах шифрування, відправник та одержувач використовують один і той самий ключ для шифрування та розшифрування даних. Зворотно, в схемі шифрування з відкритим ключем використовуються два ключа. Один з них відомий як відкритий ключ, який може використовувати будь-хто при шифруванні. Для кожного відкритого ключа існує відповідний приватний ключ. Приватним ключем володіє тільки один користувач, який може розшифровувати повідомлення зашифровані відповідним відкритим ключем. До схем з відкритим шифрування відносяться – PGP, DES, AES, GOST та інші.

#### - Аутентифікація.

Аутентифікація це процес упевнення, що дані доставлені тому кому вони були призначені. В доданок, аутентифікація впевнює одержувача в «чистоті»

повідомлення та відправника. Найпростіша форма аутентифікації вимагає імені користувача та пароля, для отримання доступу до деякого ресурсу. В більш складних випадках аутентифікація може базуватись на криптографічних алгоритмах із закритим та відкритим ключем.

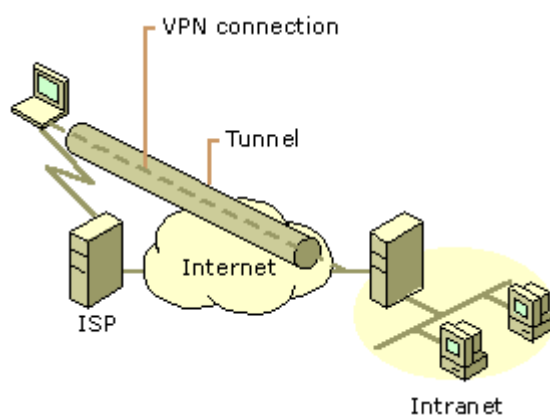
#### - **Авторизація.**

Авторизація – це процес отримання або заборони доступу до ресурсів розмішених в мережі після того як користувач був успішно ідентифікований та аутентифікований.

Щоб зрозуміти важливість ВПМ мереж розглянемо їх типові використання:

#### **Віддалений доступ через інтернет.**

ВПМ забезпечує віддалений доступ до ресурсів організації через публічний інтернет, гарантуючи захищеність даних. На малюнку зображена схема організації такої взаємодії:



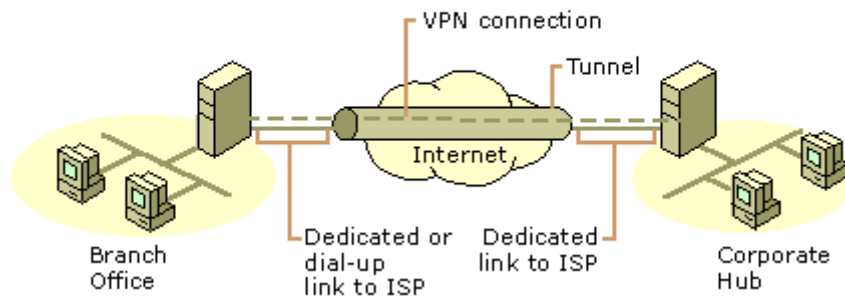
В цьому випадку замість того щоб робити дороге пряме модемне з'єднання на великі відстані, клієнт під'єднується до локального провайдера інтернет і створює ВПМ з'єднання з віддаленим сервером організації.

#### **З'єднання мереж через інтернет**

Існує два способи використання ВПМ для з'єднання локальних віддалених мереж:

- Використання виділених ліній для з'єднання віддаленого офісу з інтернетом.

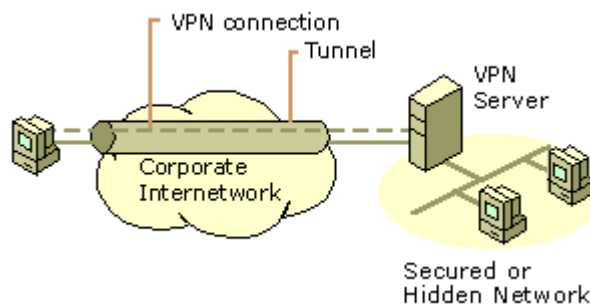
- Використання діал-ап лінії для з'єднання віддаленого офісу з інтернетом



В обох випадках, способи з'єднання віддаленого офісу з інтернетом локальні. Корпоративний маршрутизатор, працюючий як ВПМ сервер, повинен бути підключеним до локального інтернет провайдера виділеною лінією. ВПМ сервер повинен працювати 24 години на добу.

### З'єднання комп'ютерів через інтранет

Іноді буває, що в деяких організаційних одиницях, дані настільки важливі, що мережу цієї одиниці фізично розділяють від загальної мережі організації. Звичайно це суттєво знижує ризик втрати інформації, проте ускладнює доступ до неї віддалених користувачів.



ВПМ дозволяють під'єднувати відділену мережу до організаційної. ВПМ сервер буде гарантувати, що доступ до важливих даних будуть мати тільки користувачі з відповідним рівнем доступу. В такий спосіб забезпечується безпека даних, та розв'язуються проблеми з доступом.

Таким чином в цьому розділі ми розглянули базові положення на яких ґрунтуються віртуальні приватні мережі. В наступному розділі буде розглянута історія появи ВПМ.

## Еволюція віртуальних приватних мереж

Було б неправильно називати ВПМ новою технологією. На відміну від думок які можна знайти в популярних журналах, концепція ВПМ виникла близько 15 років назад та пережила декілька етапів, поки не постала в сучасному вигляді.

Найперша з відомих ВПМ була запропонована AT&T в кінці восьмидесятих років минулого століття та була відома під назвою *Software Defined Networks* (SDNs). SDN були WAN мережами на великих відстанях (long-distance WANs), які використовували як комутовані так і виділені канали, та базувались на базах даних які використовувались для класифікації кожної спроби доступу, як локального так і віддаленого. Засновуючись на цій інформації, пакет даних направлявся до пункту призначення через відкриту розподілену комутовану інфраструктуру.

Друге покоління ВПМ з'явились разом із стандартом X.25 та технологією *Services Digital Network* (ISDN) на початку 90-х років. Ці дві технології дозволяли передавати потік пакетів даних через розділені відкриті мережі. Таким чином, ідея дешевої передачі через відкриті мережі набирала популярність в рамках міжмережевої взаємодії дуже швидко. На деякий час здавалось, що протокол X.25 над ISDN стане протоколом для ВПМ. Однак, швидкість передачі даних не змогла піднятися до очікуваного рівня продуктивності і друге покоління ВПМ не змогло проіснувати достатньо довго.

Після другого покоління, ринок ВПМ мереж зменшився до появи технологій *Frame Relay* (FR) та *Asynchronous Transfer Mode* (ATM). Третє покоління ВПМ базувалось на цих технологіях. Вони (технології) на відміну від попередніх базувались на понятті віртуального каналу. Технологія віртуальних каналів дозволила значно підвищити швидкість передачі даних ніж та що була раніше. Проте технологія віртуальних каналів має і багато недоліків, серед яких складність інтеграції з IP мережами та інші проблеми.

В часи коли електронний бізнес став повноцінним способом ведення бізнесу в середині дев'яностих років, з'явились нові вимоги до ВПМ. Користувачі та організації хотіли отримати рішення, яке було б простим в реалізації, масштабованим, глобально доступним та гарантувало високий рівень захисту. Поточне покоління ВПМ – IP VPN підтримує всі ці вимоги завдяки використанню технології тунелювання.

Тунелювання це технологія інкапсулювання пакету даних в тунельний протокол, такий як *IP Security (IPSec)*, *Point-to-Point Tunneling Protocol (PPTP)* або *Layer 2 Tunneling Protocol (L2TP)* та інші, і тоді остаточно пакувати тунельний пакет в IP пакет. Отриманий таким чином пакет потім направляється до призначеної мережі використовуючи прикріплену IP інформацію. Оскільки початковий пакет може бути будь-якого типу, тунелювання може підтримувати мульти-протокольний трафік, включаючи IP, ISDN, FR та ATM.

В наступному розділі ми детальніше розглянемо протоколи тунелювання, які використовуються зараз для побудови ВПМ мереж.

## Протоколи віртуальний приватних мереж

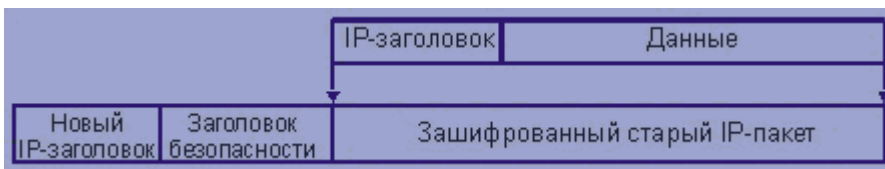
Побудувати віртуальну приватну мережу можна величезною кількістю способів, одне перерахування яких зайняло б досить багато місця. Так, користувачі UNIX давно використовують для цих цілей комбінацію ssh й rpp. Однак по-справжньому інтерес представляють, звичайно, стандартні рішення. У цей час широко відомі наступні з них:

- PPTP (Point-to-Point Tunneling Protocol), розроблений спільно Microsoft, 3Com й Ascend Communications. Цей протокол став досить популярний завдяки його включенню в операційні системи фірми Microsoft.
- L2F (Layer-2 Forwarding) - розробка фірми Cisco.
- L2TP (Layer-2 Tunneling Protocol) - розроблюваний і офіційний стандарт, що просуває, Інтернет.
- SKIP (Simple Key-management for Internet Protocols) - розробка фірми Sun.
- IPsec (Internet Protocol Security) - офіційний стандарт Інтернет.

Перші три з перерахованих протоколів орієнтовані в першу чергу на мобільних користувачів і не будуть розглядатися.

Стандартом для Інтернету є набір протоколів IPsec. Відповідно до стандарту всі пристрої, що працюють із новим IP-протоколом IPv6, зобов'язані підтримувати IPsec.

У режимі побудови ВПМ (режимі тунелювання) IPsec забезпечує безпеку зв'язку в Інтернеті «упакуванням» IP-пакета в новий IP-пакет із застосуванням до нього різних перетворень - шифрації та електронних підписів.



Справа в тому, що передача даних в Інтернеті схожа на передачу інформації на поштових

відкритках без конверта - кожен зацікавлений поштовий працівник може прочитати й навіть додати що-небудь на цю листівку. Люба людина може послати листівку від імені іншої

людини. Упакування IP-пакета в інший IP-пакет із застосуванням засобів криптографії схожі на впакування листівки в конверт, його запечатуння й підписування. Таким чином, ви можете гарантувати, що ніхто не читав інформацію в конверті, ніхто не змінив інформацію в ньому, а підпис на конверті гарантує особистість відправника.

Залежно від вимог до ВПМ використовується два види заголовків, і, відповідно, надається два режими функціональності протоколу. В одному випадку ESP (Encapsulating Security Payload) надається можливість передавати зашифровані дані, електронно підписувати передані дані та включати в заголовок спеціальний лічильник - число, що збільшується на 1 у кожному новому пакеті, запобігаючи повторному використанню даних. Таким чином, забезпечується таємність, незмінність передаваних даних, неможливість їхнього повторного використання й підтверджується особистість їхнього відправника. Причому можна використати всі ці можливості як одночасно, так і окремо. У другому випадку AH (Authentication Header) дозволяє включати електронний підпис усього пакета і лічильник. Таким чином, гарантується все те, що забезпечує ESP, крім таємності. Але AH забезпечує електронний підпис усього пакета, у тому числі і зовнішньому IP-заголовку, у той час як ESP захищає тільки впакований пакет. При необхідності ці два заголовки можуть використатися спільно, що застосовується у випадку, коли необхідно і забезпечити таємність даних, і гарантувати цілісність усього пакета.

Для того щоб два пристрої могли обмінюватися інформацією з використанням шифрованих і підписаних даних, їм необхідно знати ключ до шифру, що використовується при передачі, а також ключ до електронних підписів. Питання обміну ключами взагалі є одним з найважливіших у будь-якій системі, що використовує криптографічні методи захисту даних. Очевидно, що, яким би не був сильним протокол, якщо зловмисник має можливість украсти або підмінити ключі - всі нанівець. Іншою вимогою є досить часта зміна ключа і обмеження на кількість даних, які можуть бути передані з використанням того самого ключа. Це обмеження пов'язане з тим, що чим більше даних, зашифрованим одним ключем, і чим більше часу має зловмисник, тим легше йому «зламати» шифр. Тому обмін ключами - одна з найважливіших частин стандартів. І саме тому дані, якими обмінюються пристрої, шифруються так названим ключем сесії - випадково обраним числом, про яке сторони «домовляються» на початку обміну.

В IPsec не встановлено єдиного стандартного способу розподілу ключів. Визначено, що обов'язково повинні підтримуватися ручний розподіл ключів і спеціальний протокол -

IKE (Internet Key Exchange). Кожен постачальник вправі доповнити цей набір власними протоколами обміну ключами, однак стандартні зобов'язані бути присутніми.

Ручний розподіл ключів - дуже проста процедура: на дискеті (або будь-якому іншому носії) приноситься інформація й вноситься в комп'ютер. Все просто. Але ключі треба міняти. У деяких ситуаціях їх міняють досить часто - наприклад щогодини. Носити їхній щораз на дискеті стає важко. Можна, звичайно, згенерувати безліч ключів (на цілий рік), рознести їх один раз по всіх філіях і регулярно міняти. Загалом кажучи, це - не погане рішення. Виникає, щоправда, проблема синхронної зміни ключа. Крім того, цей метод підходить тільки при невеликій кількості сторін, що беруть участь в обміні; при збільшенні їх кількості неминуче де-небудь виникне плутанина. Виходячи із цих міркувань для розподілу ключів були розроблені протоколи обміну ключами. Одним з подібних протоколів й є IKE.

IKE-протокол дозволяє пристроям домовитися про більшість параметрів, які будуть використані в процесі обміну інформацією, про алгоритм шифрування, про ключі. IKE досить складний. Він полягає в обміні повідомленнями, що повинні здійснити сторони, перш ніж зможуть обмінюватися інформацією в безпечному режимі. У ході цієї сесії сторони спочатку обмінюються повідомленнями, що підтверджують їх особистість. Визначено кілька способів упевнитися, з ким ми маємо справу. Всі вони засновані на використанні криптографічних методів. Використовуються електронні підписи на основі загальних ключів (симетричні алгоритми), або секретних і публічних ключів (несиметричні алгоритми).

При використанні електронного підпису кожен пристрій має два ключа - секретний і публічний. Ці ключі розраховуються по спеціальному алгоритмі й взаємозалежні. Секретний ключ відомий тільки власникові, публічний ключ може поширюватися вільно. Існує як мінімум дві різні схеми з асиметричними ключами. В одному (алгоритм RSA) повідомлення, зашифроване секретним ключем, можна розшифрувати, тільки використовуючи відповідний публічний ключ, і навпаки. Таким чином, якщо відоме повідомлення правильно розшифровується публічним ключем, виходить, автор повідомлення - власник цього ключа. В іншому (алгоритм Diffie-Hellman) секретний ключ відправника і публічний ключ одержувача використовуються для обчислення так званого взаємного ключа. Виявляється, що той же самий взаємний ключ можна обчислити, знаючи секретний ключ одержувача і публічний ключ відправника. Таким чином, взаємний ключ можна обчислити, тільки знаючи одну з пар - секретний ключ відправника й публічний ключ одержувача або секретний ключ одержувача і публічний ключ відправника. А оскільки секретний ключ знає тільки його

власник, тільки одержувач і відправник можуть знати взаємний ключ. Керуючись цим фактом, одержувач може бути впевнений, що відправник повідомлення, зашифрованого взаємним ключем, - саме той, за кого він себе видає. Очевидно, у випадку використання несиметричних алгоритмів шифрування кожному пристрою необхідна тільки пара ключів - незалежно від числа співрозмовників. У стандарті й для цього випадку також відсутня тверда фіксація конкретного алгоритму. Визначено тільки, що реалізація обов'язково повинна підтримувати алгоритм Diffie-Hellman.

Всі ці методи вимагають наявності попереднього знання деякого ключа, що буде використаним для підтвердження особистості. Але оскільки цим ключем шифрують дуже мало інформації, його можна міняти набагато рідше (період дії ключа може становити місяці й навіть роки). Попередній обмін підтвердженнями особистості запобігає можливість для зловмисника підсунути свій ключ і «зламати» систему.

Встановивши особистість співрозмовника, пристрої обмінюються пропозиціями по різних параметрах - алгоритмам шифрування, ключам сесії. Ключі сесії - тимчасові і можуть мінятися досить часто. Після того як домовленість досягнута, можна починати передачу інформації. Звичайно, процедура обміну ключами забирає час, і, поки вона не завершена, жоден пакет з даними не може бути переданий між пристроями в безпечному режимі. У несприятливих випадках затримка, викликана необхідністю попереднього відкриття сесії, може скласти кілька секунд, а у випадку одночасного відкриття багатьох сесій (наприклад, на початку робочого дня, після перезапуску системи) - і більше.

Трохи інакше підійшли до обміну ключами розробники протоколу SKIP. SKIP (акронім від Simple Key-management for Internet Protocols - «простий протокол обміну ключами для Інтернету») - розробка фірми Sun і призначений, як це випливає з назви, для обміну ключами. Цей протокол може бути використаний як разом з IPsec разом з іншими протоколами, так і самостійно. Саме тому про нього і говориться як про окремий протокол.

При використанні SKIP ключ, необхідний для розшифровки повідомлення (ключ сесії), зберігається в самому пакеті, у заголовку SKIP.

IP-заголовок	SKIP-заголовок	IP-пакет, зашифрований ключами з SKIP-заголовка
--------------	----------------	---

Для того щоб пакет міг бути розшифрований тільки адресатом, цей ключ, у свою чергу, зашифрований. Алгоритм і ключ шифрування обрані так, щоб його легко можна було обчислити без попереднього

обміну. Для обчислення взаємного ключа використовується вже згадуваний алгоритм Diffie-Hellman (взаємний ключ розраховується із секретного ключа відправника і публічного ключа одержувачів або публічного ключа відправника і секретного ключа одержувача). Але і цей ключ для шифрування безпосередньо не використовується. Він використовується разом з деяким числом-лічильником для одержання іншого ключа. Для цього із взаємним ключем і лічильником виконується математична операція по алгоритму MD5, що дає новий ключ. Саме цим ключем і виробляється код ключа сесії. Значення лічильника також передається разом з пакетом. Таким чином, вся інформація, необхідна для розшифровки даних у пакеті, утримується в заголовку пакета, і не потрібно ніякого попереднього обміну (крім, звичайно, знання відповідного секретного й публічного ключа). Така тріступінчаста схема дозволяє міняти ключі сесії досить часто. Ключ сесії може бути різним у різних пакетах, переданих по мережі, - більше часті зміни уявити собі важко. Крім того, наявність рівномірно зростаючого лічильника дозволяє уникнути повторного використання шифрованого пакета. Очевидно, що SKIP істотно простіше, ніж IKE, хоча і менш гнучкий.

Як вже говорилося, SKIP може бути використаний як з IPsec, так і без нього. При використанні SKIP без IPsec IP-пакет, призначений для передачі, шифрується і упаковується в новий IP-пакет. Новий IP-пакет містить заголовок SKIP, у якому, як ми вже згадували, утримується вся інформація, необхідна для розшифровки упакованого пакета.

IP-заголовок	SKIP-заголовок	IP сек-заголовок	Зашифрованный и / или подписанный IP-пакет
--------------	----------------	------------------	--

У випадку спільного використання SKIP та IPsec

пакет-конверт містить два заголовки - IPsec-заголовок й SKIP-заголовок. У заголовку SKIP передається ключ, а в заголовку IPsec передається додаткова інформація, необхідна для правильної розшифровки і обробки упакованого пакета.

Зараз на ринку багато продуктів для побудови VPN. Частина з них здатна реалізовувати IPsec з IKE, частина - з SKIP, деякі - SKIP без IPsec. Деякі включають підтримку і того і іншого.

Крім чисто технічних міркувань, при виборі того або іншого протоколу важливо і наявність на ринку продуктів, що реалізують цей протокол, їхня якість.

Хоча SKIP - розробка фірми Sun, багато постачальників мережного встаткування й операційних систем включають у свої продукти підтримку SKIP. SKIP доступний для Solaris, Sun OS, FreeBSD й Linux. Були створені версії і для Windows. Оскільки SKIP відносно

простий і продукти на його основі випускаються вже далеко не перший рік, можна сміло затверджувати, що це досить зрілий, розвинений протокол.

Продукти, що реалізують протоколи IPsec й IKE теж присутні на ринку. Реалізації доступні для вільно розповсюджуваних систем Linux, OpenBSD. При цьому OpenBSD містить підтримку цього стандарту в базовій конфігурації.

## Класифікація ВПМ

Враховуючи обставини описані в попередніх розділах технології реалізації ВПМ еволюціонували в трьох напрямках:

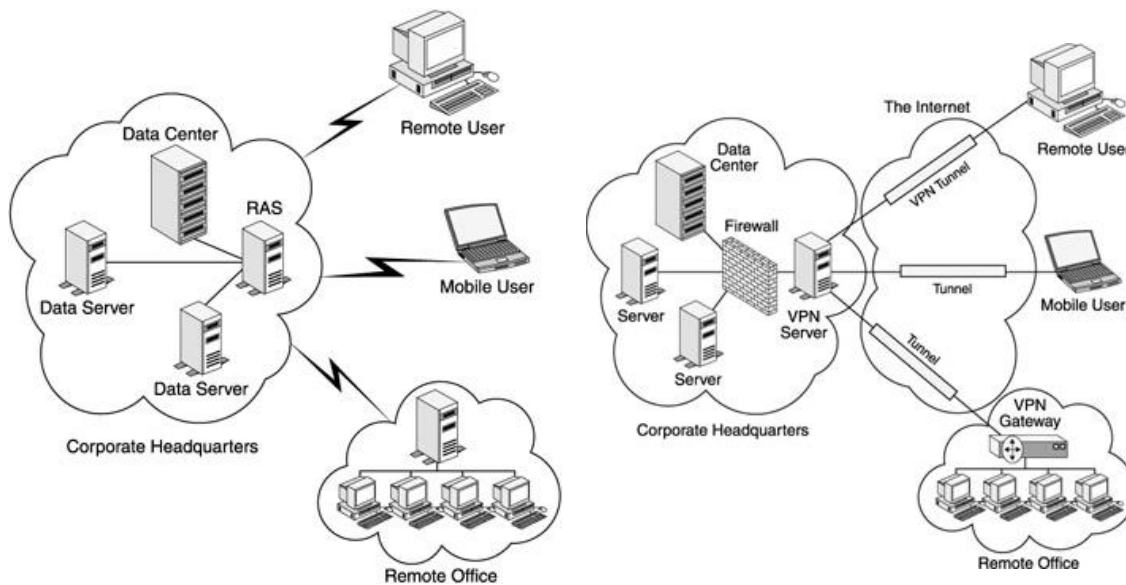
- Remote Access VPNs
- Intranet VPNs
- Extranet VPNs

### Remote Access VPNs

Як можна здогадатись з назви, Remote Access VPN забезпечують доступ в будь-який час віддалених співробітників до корпоративних ресурсів. Структура такої ВПМ складається з

- *Remote Access Server (RAS)*, який знаходиться в центральному офісі та аутентифікує та авторизує запити.
- Забезпечує діал-ап з'єднання.
- Обробляє запити віддаленого офісу.

Схеми такої взаємодії без ВПМ та з використанням ВПМ:

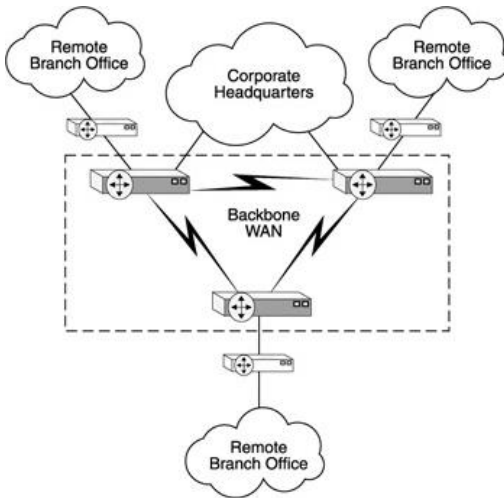


(традиційний випадок)

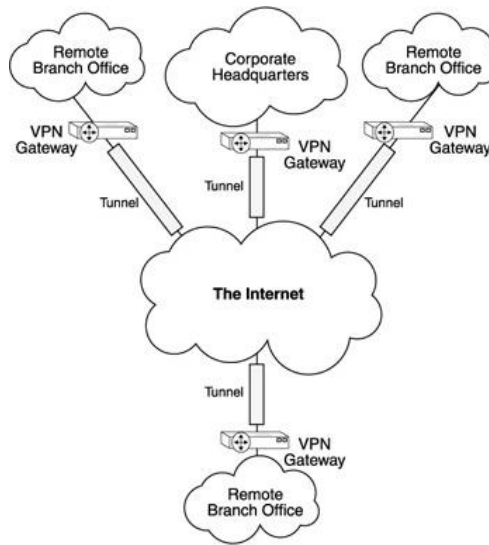
(використання ВПМ)

## Intranet VPNs

Intranet VPNs використовуються для з'єднання віддалених локальних офісних мереж з корпоративною мережею. В якості транспортного рівня виступає Інтернет.



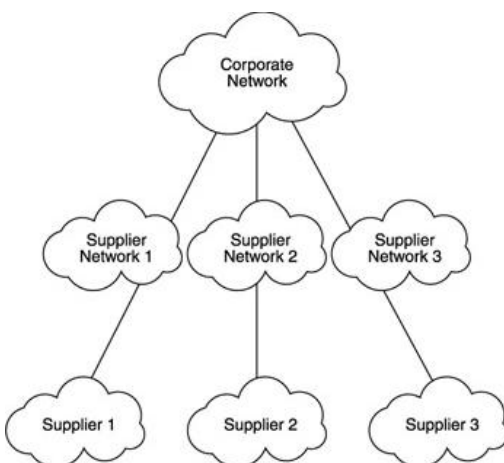
(традиційний випадок)



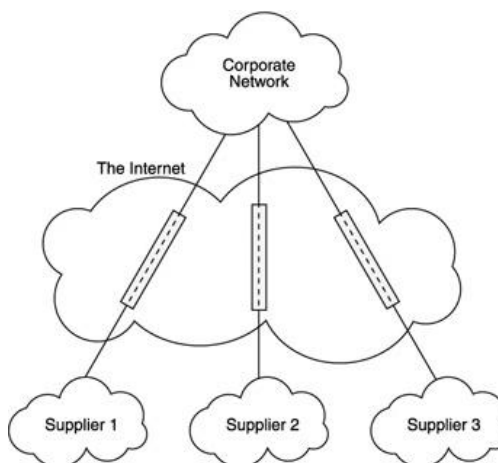
(використання ВПМ)

## Extranet VPNs

На відміну від двох попередніх випадків, екстранет ВПМ не повністю відгороджені від зовнішнього світу. Екстранет ВПМ надають контрольований доступ до необхідних мережних ресурсів, до зовнішніх бізнес-сутностей, таких як партнери, замовники, виконавці які відіграють важливу роль у веденні бізнесу.



(традиційний випадок)



(використання ВПМ)

## **Література**

- [1]. Robert Williams, Mark Walla, The Ultimate Windows Server 2003 System Administrator's Guide, Addison Wesley, 2003
- [2]. Алексей Кошелев, Виртуальные частные сети, Компьютер пресс, 11'2000
- [3]. Meeta Gupta, Building a Virtual Private Network
- [4]. Virtual Private Networking with Windows Server 2003: Overview, Microsoft Corporation, Published: March 2003