

Вінницький національний технічний
університет

ДИПЛОМНА РОБОТА

Тема: «Захист комп'ютерної мережі за допомогою VPN»

Керівник: старший викладач Черняк О.І

Виконав: студент групи 1КІ – 16сп

Гончарук Б.Г

Вінниця - 2017

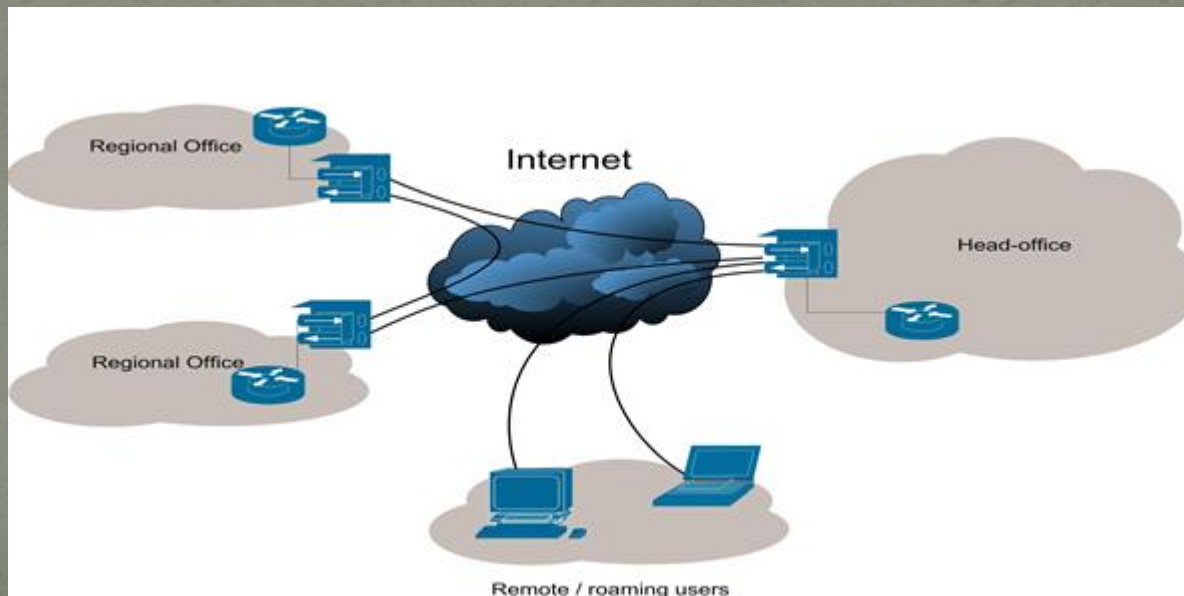
Метою дипломної роботи є підвищення безпеки та надійності доставки інформації в мережі шляхом створення каналу VPN з шифруванням.

Під час роботи розглядались такі питання:

1. Існуючі технології реалізації захищеного доступу через глобальні мережі з використанням vpn
2. Протоколи реалізації віддаленого доступу на основі vpn
3. Розробка і реалізація захищеної мережі за допомогою каналів vpn

Віртуальна приватна мережа (*VPN - Virtual Private Network*) створюється на базі загальнодоступної мережі і може гарантувати, що трафік, який направляється через цю мережу, так само захищений, як і передача усередині локальної мережі.

У той же час віртуальні мережі забезпечують істотну економію витрат в порівнянні з використанням та підтримкою власної мережі глобального масштабу.

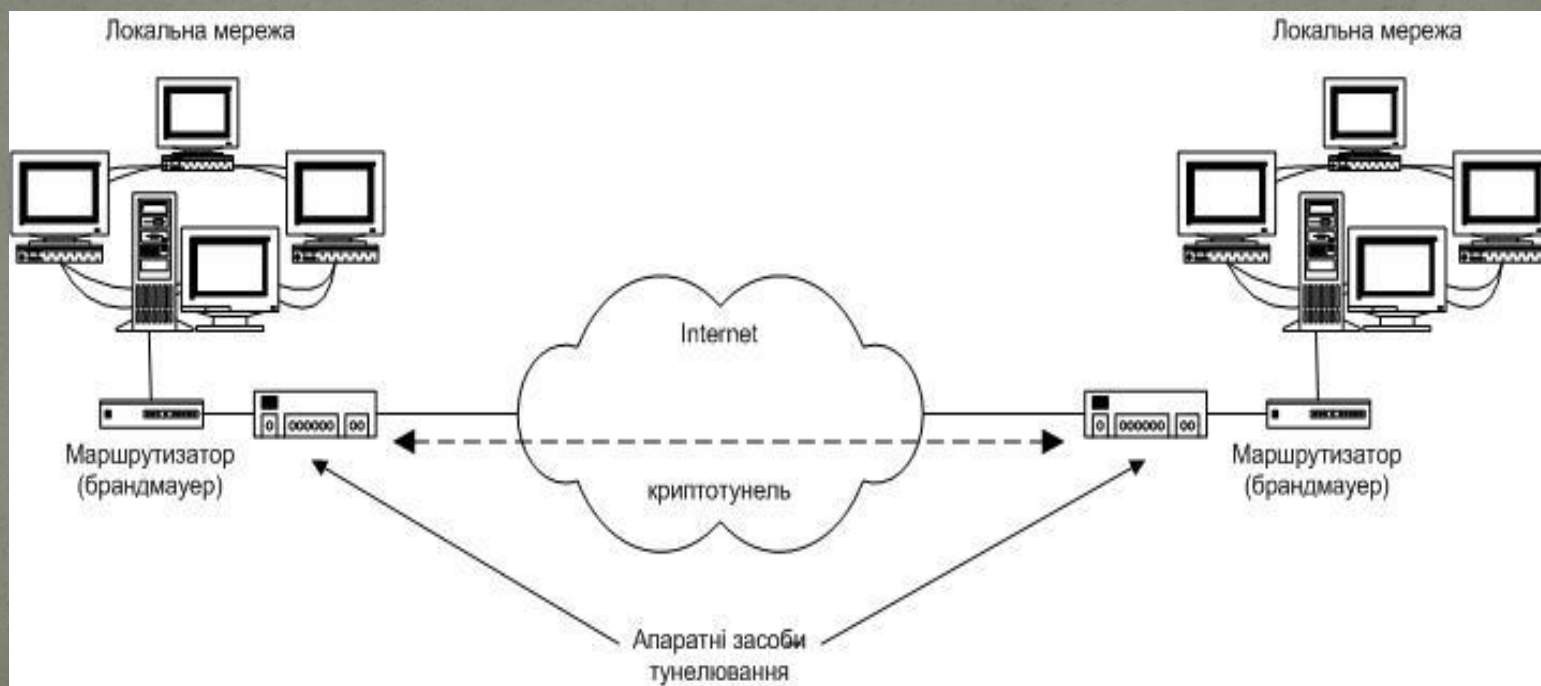


Існують різні варіанти створення VPN, такі як:

- 1) VPN на базі брандмауерів
- 2) VPN на базі маршрутизаторів
- 3) VPN на базі програмного забезпечення
- 4) VPN на базі апаратних засобів
- 5) VPN на базі мережевої ОС

При виборі рішення потрібно враховувати фактори продуктивності засобів побудови VPN.

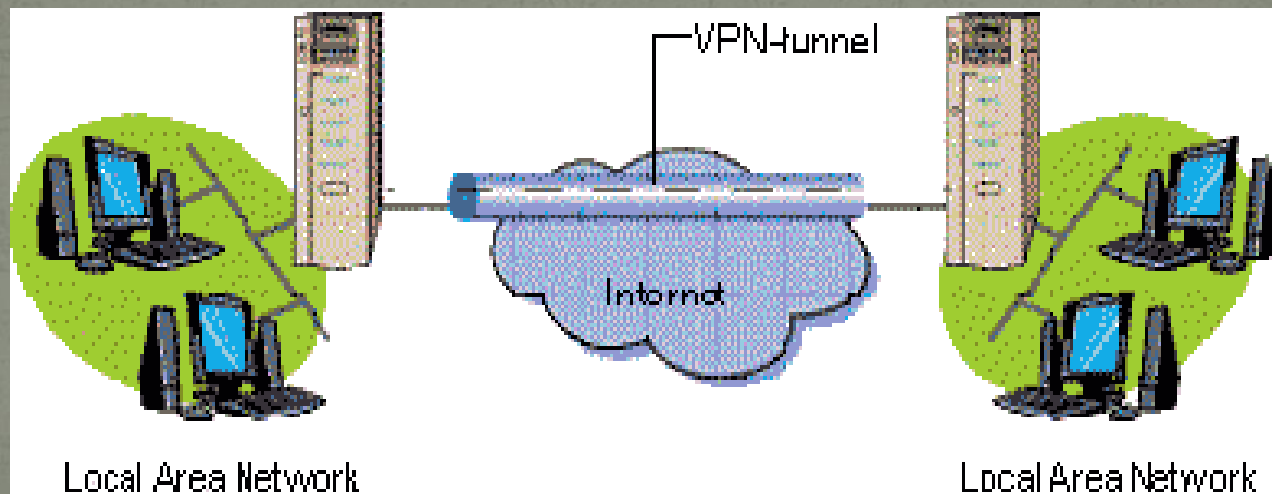
Одним з найважливіших завдань технології VPN є захист потоків корпоративних даних, що передаються по відкритих мережах. Відкриті канали можуть бути надійно захищені лише одним методом - криптографічним.



Це завдання вирішується при реалізації віртуальної приватної мережі, яка базується на трьох методах, що застосовуються для впровадження заходів безпеки в інформаційні мережі:

- Тунелювання;
- Аутентифікація;
- Шифрування.

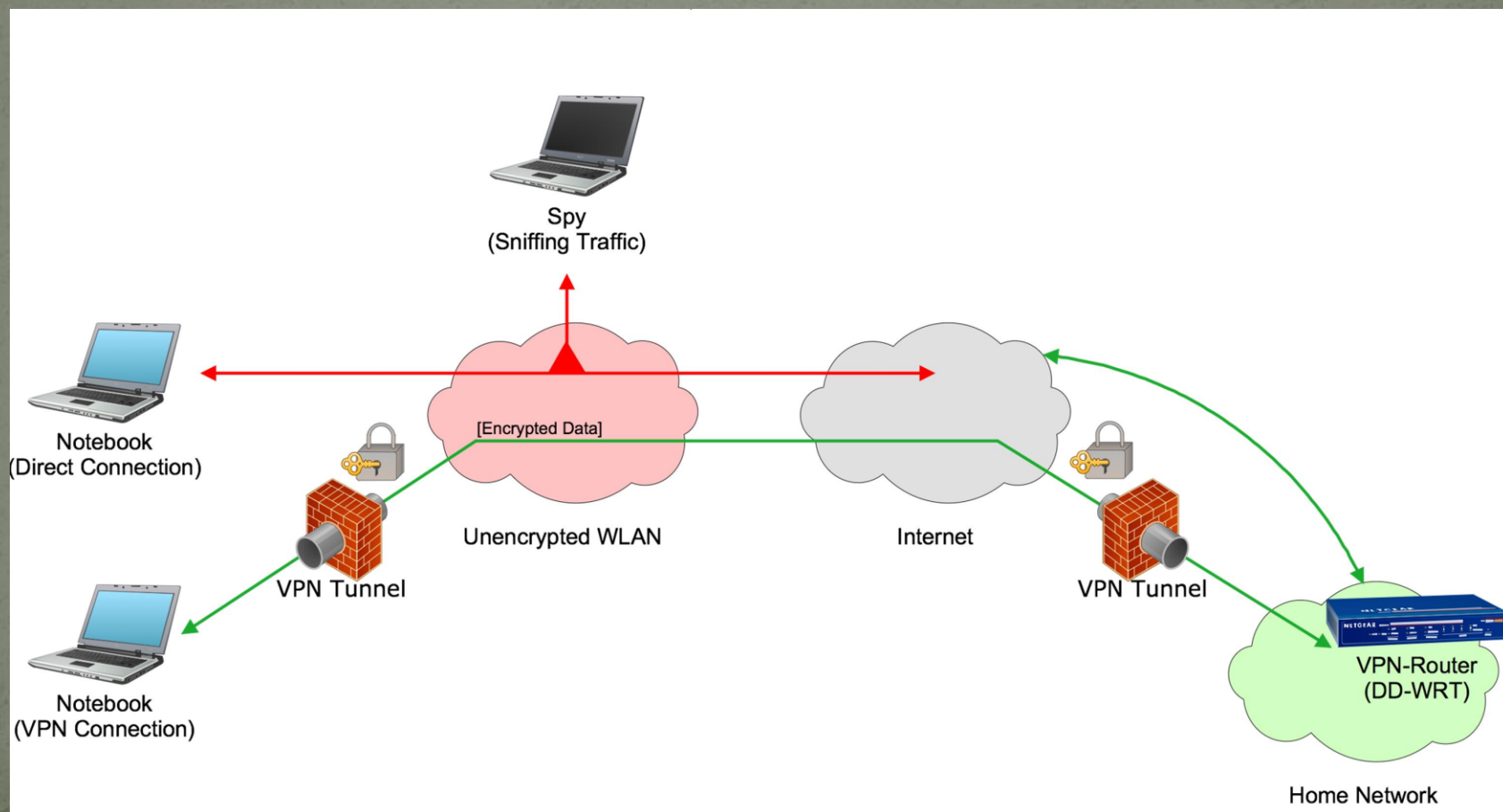
Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічному середовищі, використовуючи інший протокол. В результаті виникає можливість вирішити проблеми взаємодії декількох різнотипних мереж, починаючи з необхідності забезпечення цілісності і конфіденційності передаваних даних і закінчуючи подоланням невідповідностей зовнішніх протоколів або схем адресації.



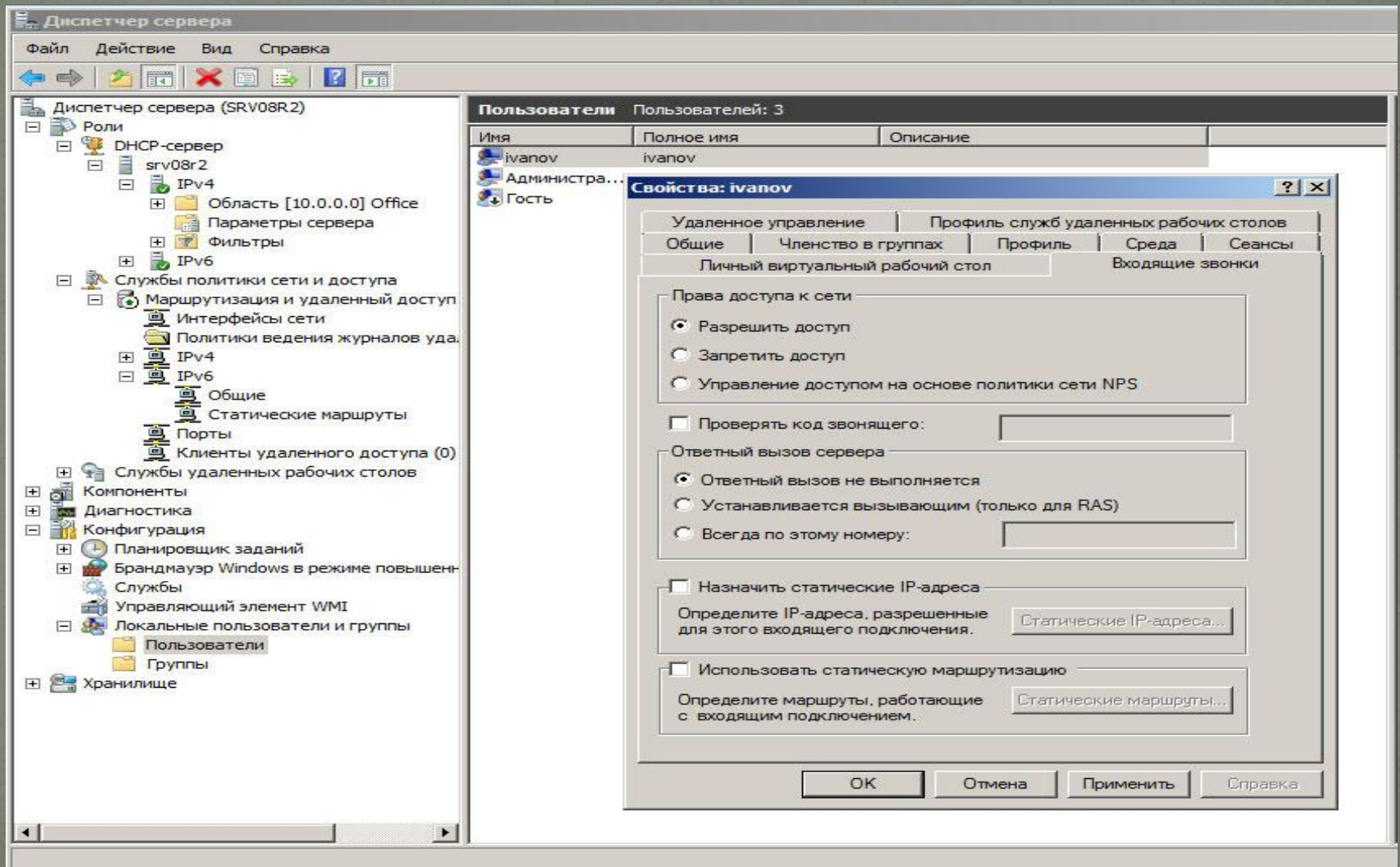
Аутентифікація застосовується для того, щоб впевнитися, що отримані дані не були прочитані, або змінені.

Аутентифікація здійснюється або відкритим текстом (*clear text password*), або за схемою запит / відгук (*challenge / response*). Відкрита аутентифікація практично не зустрічається. В той же час схема запит / відгук набагато більш застосована і забезпечує вищий рівень безпеки.

Шифрування при передачі даних через публічні мережі гарантує, що ніхто, крім приймаючої сторони, не зможе отримати доступ до даних при їх пересиланні через загальнодоступні публічні мережі.



Після завершення налаштування сервера, потрібно задати список користувачів яким дозволений віддалений доступ.



Інформація про підключеного клієнта

The screenshot shows the Windows Server Management console for server SRV08R2. The left-hand tree view is expanded to 'Клиенты удаленного доступа (1)'. The main pane displays a table of active remote access clients. One client is listed: 'SRV08R2\ivanov' with a duration of 00:00:32 and 1 port. A 'Состояние' (Status) dialog box is open, providing detailed statistics for this client.

Имя пользователя	Длительность	Число портов	Состояние
SRV08R2\ivanov	00:00:32	1	Не поддерживает NAP

Состояние			
Подключение:	ivanov		
Длительность:	00:00:35		
Статистика			
Вх. байт:	6 411	Исх. байт:	358
Получено кадров:	73	Отправлено кадров:	16
Сжатие при приеме:	0%	Сжатие при передаче:	0%
Ошибки			
Контр. суммы:	0	Кадрирования:	0
Таймаут:	0	Алп. переполн.:	0
Выравнивания:	0	Переполн. буфера:	0
Регистрация в сети			
IP-адрес:	10.0.10.104		
IPv6-адрес:			

Buttons: Обновить, Сброс, Разъединить, Закрыть

Відмова в доступі користувача без належних прав

The screenshot shows the Windows Server 2008 R2 Event Viewer interface. The left pane displays the 'Диспетчер сервера (SRV08R2)' tree with 'Службы политики сети и доступа' selected. The right pane shows the 'Сводка' (Summary) view of the 'Службы политики сети и доступа' service, indicating 52 events with 5 errors and 46 warnings in the last 24 hours. A specific event (ID 20271) is selected, and its properties are displayed in a dialog box.

Сводка

События: 5 ошибок, 46 предупреждений, 1 информационное за последние 24 час.

Событий: 52

Уровень	Код собы...	Дата и время	Источник
Предупреждение	20271	12.04.2017 21:45:21	RemoteAccess

Свойства событий - Событие 20271, RemoteAccess

Общие | Подробности

CoID={35A064D3-826C-412A-AC7E-BE241C34B39F}; Пользователь gutsul подключен с 10.0.0.100, но не прошел проверку подлинности по следующей причине: Учетная запись не имеет прав для дозвона.

Имя журнала:	Система		
Источник:	RemoteAccess	Дата:	12.04.2017 21:45:21
Код события:	20271	Категория задачи:	Отсутствует
Уровень:	Предупреждение	Ключевые слова:	Классический
Пользов.:	Н/Д	Компьютер:	SRV08R2
Код операции:			
Подробности:	Веб-справка журнала		

Копировать | Закрывать