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

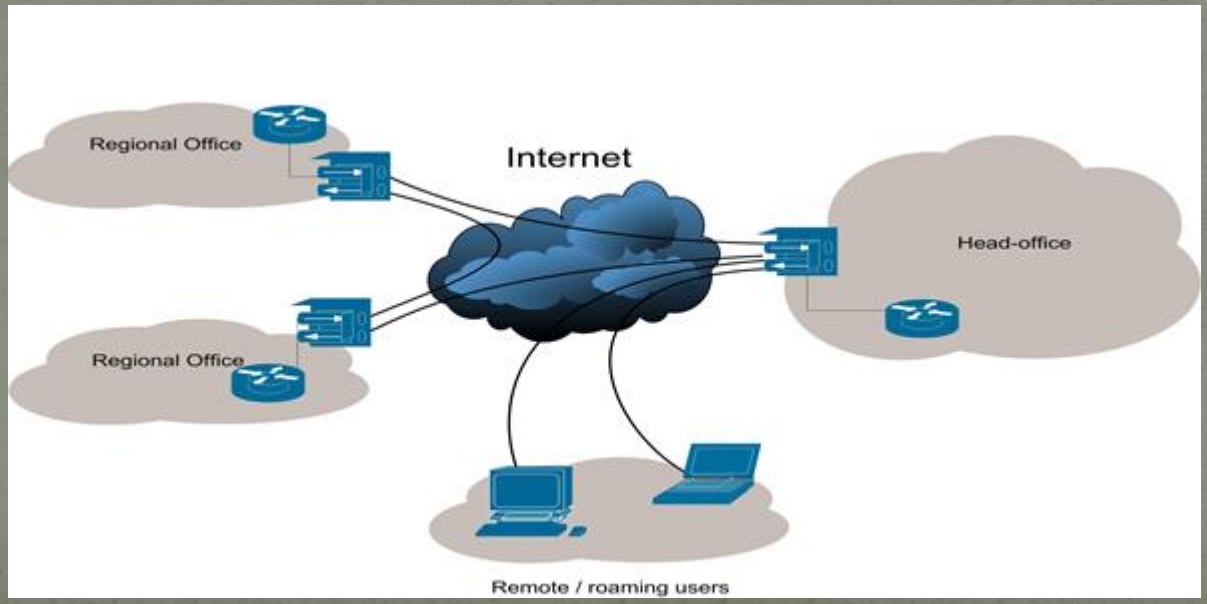
Метою дипломної роботи є підвищення безпеки та надійності доставки інформації в мережі шляхом створення каналу VPN з шифруванням.

Під час роботи розглядались такі питання:

1. Існуючі технологій реалізації захищенного 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.

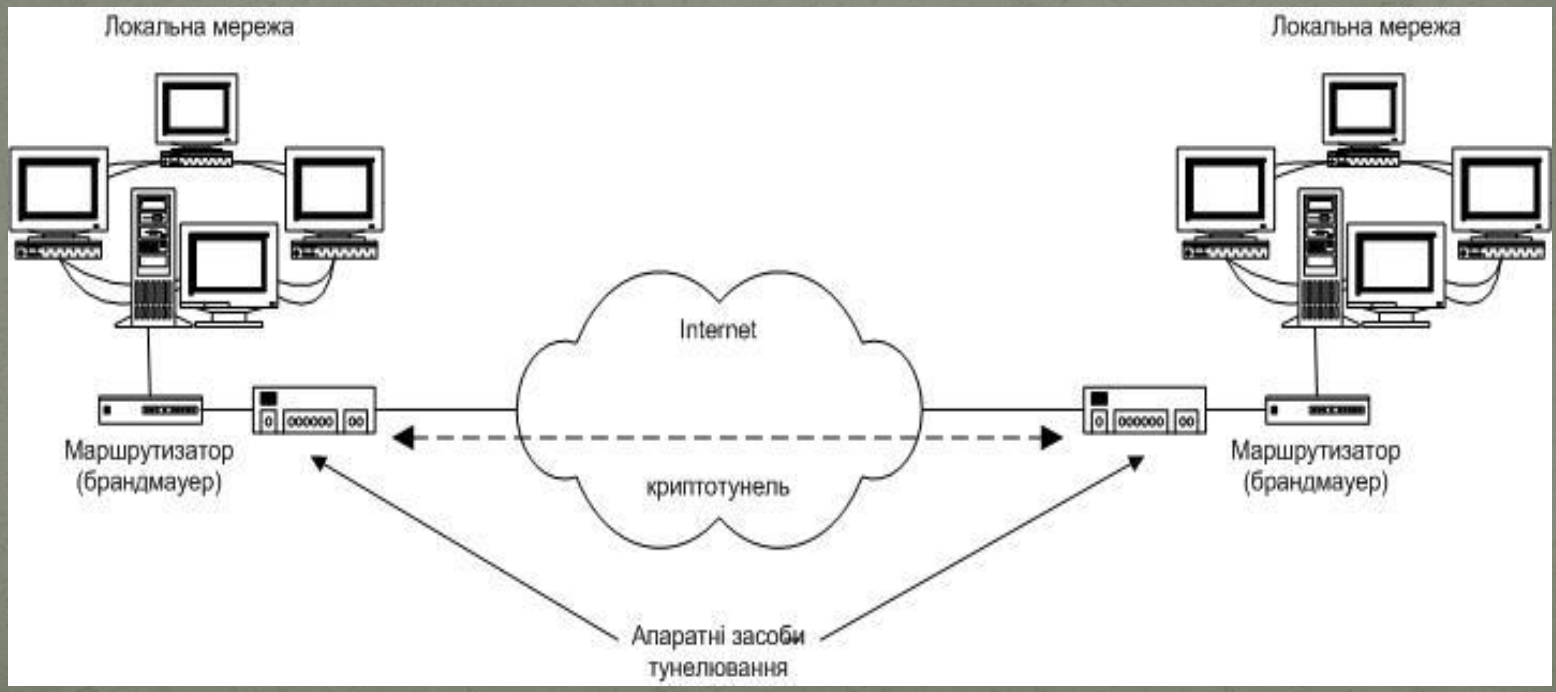


Існують різні варіанти створення VPN, такі як:

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.

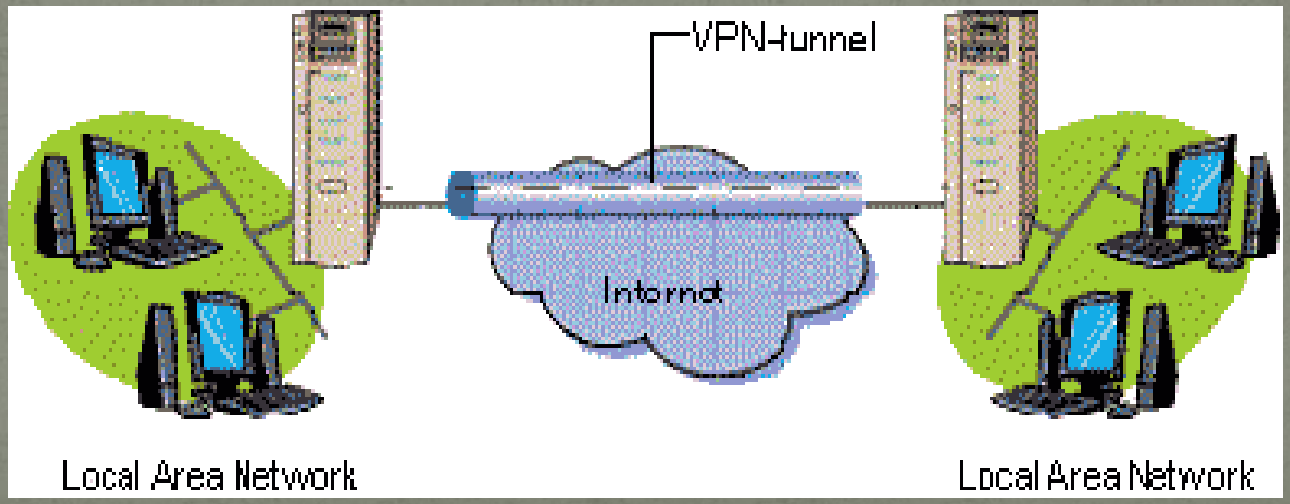
Одним з найважливіших завдань технології VPN є захист потоків корпоративних даних, що передаються по відкритих мережах. Відкриті канали можуть бути надійно захищені лише одним методом - криптографічним.



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.

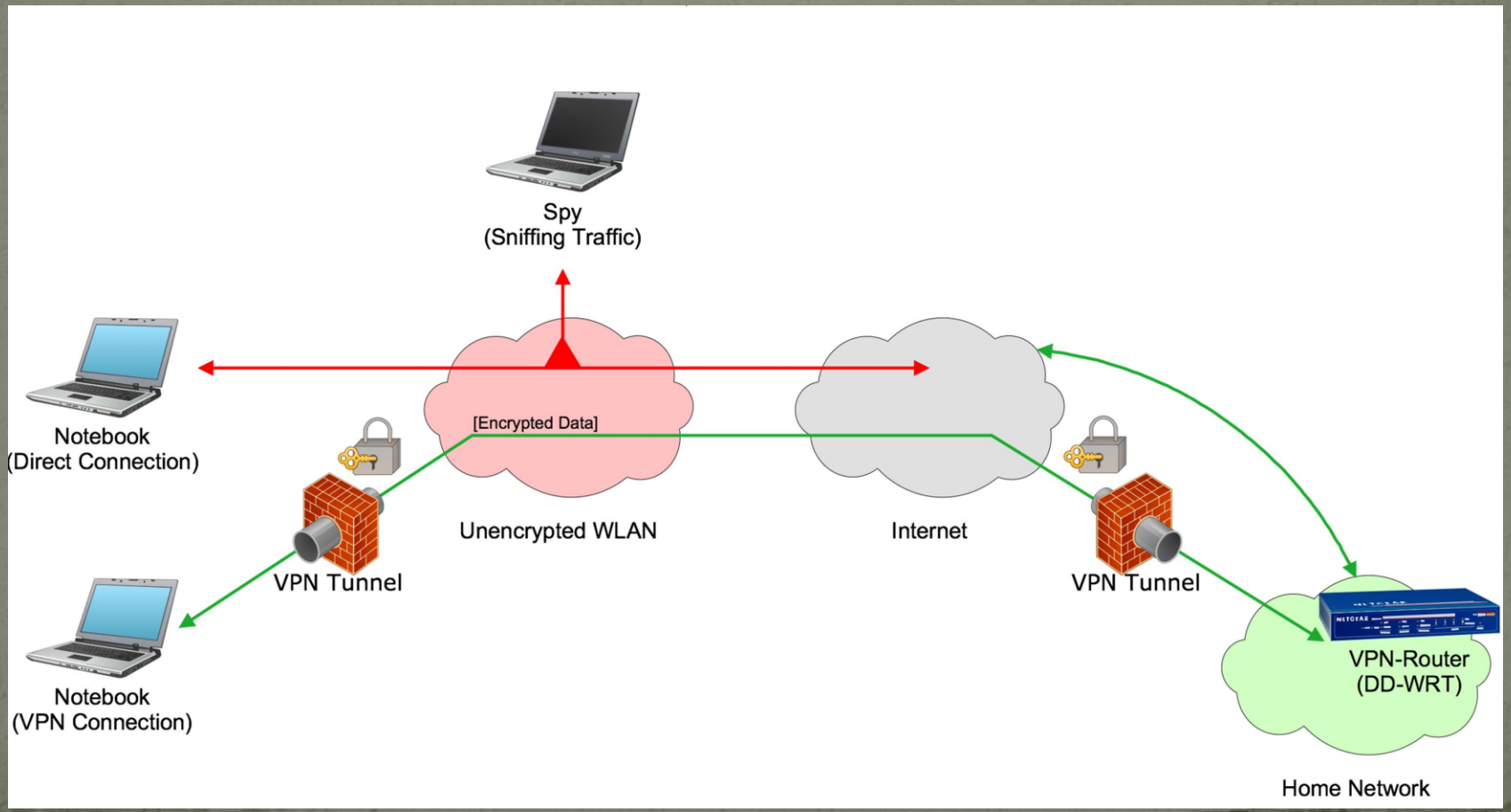
Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічному середовищі, використовуючи інший протокол. В результаті виникає можливість вирішити проблеми взаємодії декількох різнотипних мереж, починаючи з необхідності забезпечення цілісності і конфіденційності передаваних даних і закінчуючи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



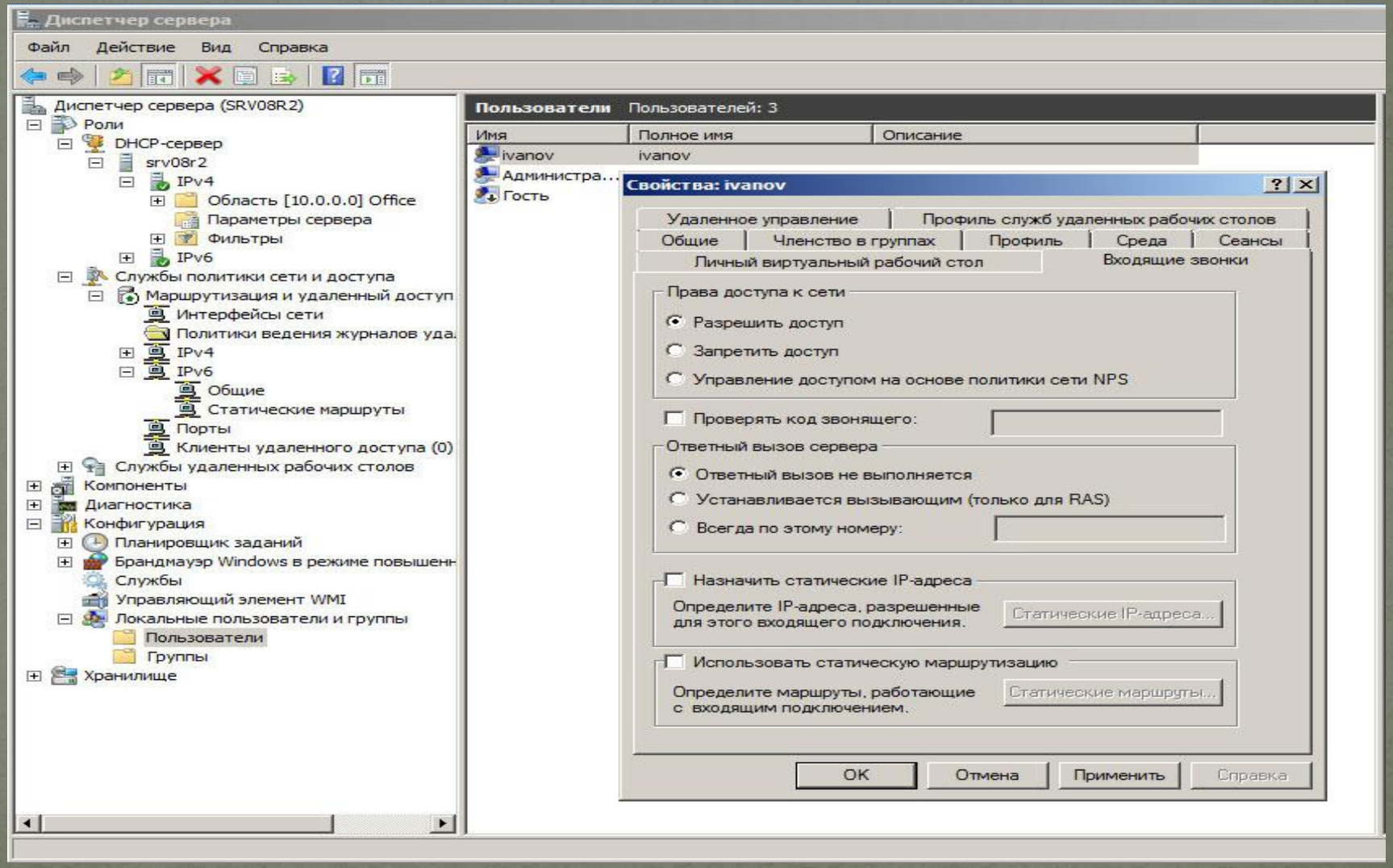
Аутентифікація застосовується для того, щоб впевнитися, що отримані дані не були прочитані, або змінені.

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 вищій рівень безпеки.

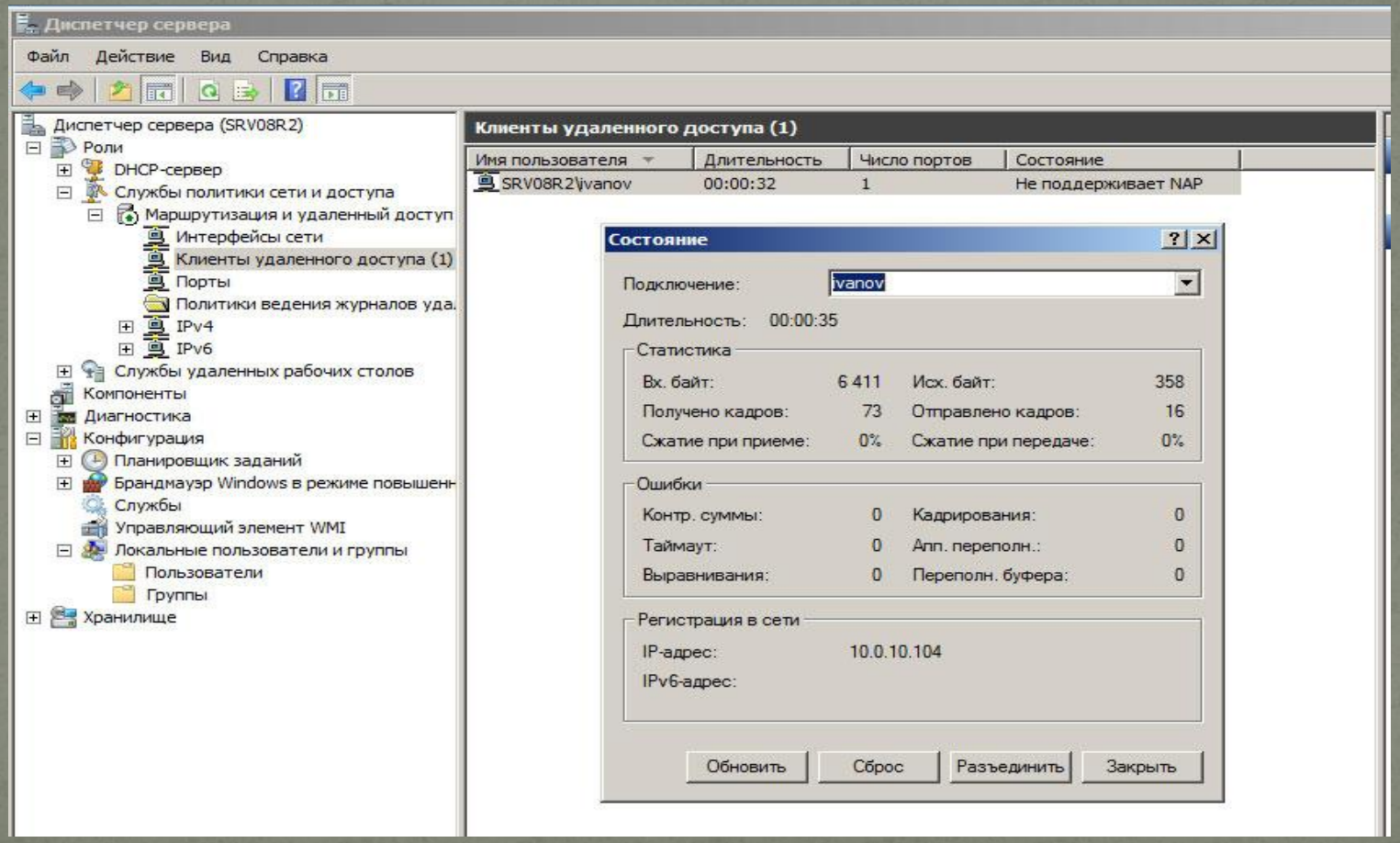
Шифрування при передачі данних через публічні мережі гарантує, що ніхто, крім приймаючої сторони, не зможе отримати доступ до даних при їх пересиланні через загальнодоступні публічні мережі.



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



Інформація про підключеного клієнта



Відмова в доступі користувача без належних прав