МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна інженерія»

Група: 2БКС-26

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання

БКС.26.02.000.КРБ

БОСТАНЖИ
ЮЛІЇ ІВАНІВНИ

м. Одеса
2022 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**
Освітня програма: **«Комп'ютерна інженерія»**
Група: **2БКС-26**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему: **«Аналіз технологій побудови захищеного доступу до мережі за допомогою віртуального локального зв'язку»**

Проектний матеріал складається з пояснювальної записки на 52 сторінках та графічного (презентаційного) матеріалу на 19 аркушах (слайдах)

Виконавець _____ (Бостанжи Ю.І.)
Керівник проекту_____(Кривченко Ю.В.)

Консультанти:
з охорони праці_____ (Чорновол Н.І.)
з дотримання вимог ЄСКД _____ (Петрашова В.І.)
старший консультант _____ (Скорнякова О.В.)

До захисту допущений
Завідувачка кафедри _____ (Іванова Л.В.)
Завідувач відділення _____ (Суліма Ю.Ю.)

Захист «____»_____ 202____ р. Протокол ДКК №_____
Оцінка ДКК _____

Секретар ДКК _____

АНОТАЦІЯ

Робота містить результати аналізу технологій побудови захищених каналів та мереж, технології організації віртуального локального зв’язку з мережею передачі даних, побудови розподільної мережі та віддаленого доступу до неї.

Опрацьовано літературні джерела стосовно поставлених задач, зокрема присвячені особливостям технології віртуального локального зв’язку (VPN).

Виконано аналіз та порівняння основних протоколів, що використовуються при створенні віртуального локального зв’язку з мережею передачі даних, побудові розподільної мережі та віддаленого доступу. Проаналізовано спектр вимог для вибору саме того протоколу, який найбільше підходить відповідно до конкретного випадку.

Виконано опис процесу адміністрування та реалізації захищеної мережі за допомогою каналів віртуального локального зв’язку.

Проаналізовано технології побудови захищених каналів та мереж та обрано найоптимальніший спосіб реалізації відповідно до передбачених умовами експерименту вимог. У якості серверних операційних систем обрані системи Kali Linux та Microsoft Windows Server 2016.

Виконано дослідження залежності часу підбору ключа шифрування RC4 у протоколі PPTP від його довжини.

Систематизовано знання існуючих технологій віртуального локального зв’язку по рівнях 7-рівневої мережевої моделі та по завданнях, виконуваних ними.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *Комп'ютерних систем* Кафедра *Комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

"_____" _____202____р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

Здобувачеві (здобувачці) освіти *Бостанжи Юлії Іванівні*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз технологій побудови захищеного доступу до мережі за допомогою віртуального локального зв'язку*

затверджена наказом по коледжу від "____"_____202____р. №_____

2. Термін здачі кваліфікаційної роботи_____ _____

3. Вихідні дані до роботи *1. Порівняти існуючі протоколи VPN по рівнях мережевої моделі OSI та по їх функціям. 2. Реалізувати доступ до VPN-серверу з шифруванням, використовуючи вбудовані служби. 3. Реалізувати тунельний канал та здійснити віддалений доступ на базі протоколу PPTP. 4. Дослідити залежність часу підбору ключа шифрування RC4 у протоколі PPTP від його довжини*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Аналіз технологій захищеного доступу до мережі

Вибір протоколу VPN віддаленого доступу

Реалізація захищеної мережі та інструментарій для її адміністрування

Дослідження надійності шифрування у протоколі PPTP

Охорона праці та техніка безпеки

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Загальна схема інтернет-трафіку та з використанням VPS; Схема VPN-мережі для організацій; Організація VPN для віддаленого користувача; VPN на базі брандмауерів, на базі маршрутизаторів, на базі шлюзів, програмних засобів; Транспортний та тунельний режим IPsec; Порівняльна характеристика IPsec та SSL / TLS; Налаштування VPN-серверу; Ілюстрація атаки MITM; Схема шифрування-дешифрування RC4; Результати підбору ключа шифрування прямим перебором; Результати підбору ключа шифрування за допомогою словнику ключів шифрування Rainbow tables; Графік залежності цінності інформації від часу

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів роботи, що стосується їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Технологічний	*Кривченко Ю.В.*		
Охорона праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Скорнякова О.В.*		

7. Дата видачі завдання _____

Керівник роботи *Кривченко Ю.В.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів кваліфікаційної роботи	Термін виконання етапів кваліфікаційної роботи	Примітка
1.	*Вступ. Постановка задач дослідження*	*5.05.2022*	
2.	*Аналіз технологій віддаленого доступу*	*7.05.2022*	
3.	*Огляд методів реалізації захищених каналів*	*9.05.2022*	
4.	*Аналітичний огляд засобів безпеки*	*11.05.2022*	
	інформаційних мереж на основі VPN		
5.	*Вивчення протоколу VPN*	*13.05.2022*	
6.	*Вивчення протоколів і алгоритмів захисту*	*16.05.2022*	
	IPsec		
7.	*Порівняння протоколів захищених мереж,*	*20.05.2022*	
	вибір найбільш відповідного		
8.	*Адміністрування і реалізація захищеної*	*23.05.2022*	
	мережі		
9.	*Налаштування VPN-серверу*	*27.05.2022*	
10.	*Дослідження надійності шифру RC4*	*30.05.2022*	
11.	*Проведення експерименту з дослідження*	*3.06.2022*	
	часу підбору ключа шифрування RC4		
12.	*Аналіз результатів, підготовка слайдів*	*6.06.2022*	
	презентації		
13.	*Розробка питань з охорони праці*	*10.06.2022*	
14.	*Підготовка до захисту*	*13.06.2022*	

Виконавець _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 26. 02 000. 00 КРБ	Випускна робота		
А4			БКС 26. 02 000. 00 КРБ ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 26. 02 000. 00 КРБ		
Розробив		Бостанжи Ю.І.			Аналіз технологій побудови захищеного доступу до мережі за допомогою віртуального локального зв'язку	Літ.	Аркуш 5 / 52
Перевірив		Кривченко Ю.В.				Н Д П	
Н. Контр.		Петрашова В.І.				ВСП "ОТФК ОНТУ" гр.2БКС-26	
Затверд.		Скорнякова О.В.					

ЗМІСТ

ВСТУП

Все більшого застосування у наш час набирає використання віддаленого доступу між територіально рознесеними інформаційними мережами. У підрозділах автоматизації підприємств це питання також важливе. Віддалений доступ до мережі реалізується з застосуванням мережевих технологій, протоколів, процедур, зокрема VPN (Virtual Private Network) – віртуальна приватна мережа.

Світова тенденція показує, що за роки з часу створення технології VPN кількість приватних і цивільних користувачів, які нею користуються, зростає експоненціально. У військових установах, сучасних компаніях малого та великого бізнесу VPN є основою комунікаційного середовища [1].

У випускній роботі розглядається захищений віддалений доступ до мережі, за допомогою якого здійснюється віртуальний локальний зв'язок між розподіленими абонентами. Необхідно дослідити метод шифрування RC4 в інформаційній мережі з тунельним доступом до неї через протокол PPTP. Таким чином, предметом дослідження буде виступати сервер віртуальної приватної мережі компанії та метод шифрування RC4, що використовується у протоколі PPTP. Метою дослідження у даній роботі є підвищення безпеки та надійності доставки інформації в мережі шляхом збільшення розміру ключа шифрування у протоколі PPTP. Для досягнення поставленої мети необхідно вирішити наступні завдання:

1) порівняти існуючі протоколи VPN по рівнях мережевої моделі OSI та по функціям, які вони виконують;
2) реалізувати на практиці доступ до VPN-сервера з шифруванням, використовуючи вбудовані в серверну операційну систему служби і програми;
3) реалізований тунельний канал за допомогою VPN-сервера з операційною системою сімейства Windows Server та здійснити віддалений доступ до мережі сервера на базі протоколу PPTP;
4) дослідити залежність часу підбору ключа шифрування RC4 від його довжини у протоколі PPTP.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Аналіз технологій захищеного доступу до мережі

В мирний час біля 90% трафіку передається через мережі загального користування. У військовий час ця доля складає біля 60% [1]. Військові покладаються на мережі загального користування тому, що розвивати власну інфраструктуру в умовах швидких технологічних змін – заняття дуже затратне, потрібне лише для критично важливих національних організацій тільки у виняткових випадках.

Найбільш поширений метод створення тунелів VPN – інкапсуляція мережевих протоколів (IP, IPX, AppleTalk і так далі) в PPP і подальша інкапсуляція утворених пакетів у протокол тунелювання. Такий підхід називається тунелюванням другого рівня, оскільки "пасажиром" тут є протокол саме другого рівня.

1.1.1 Мета застосування шифрованих VPN-каналів

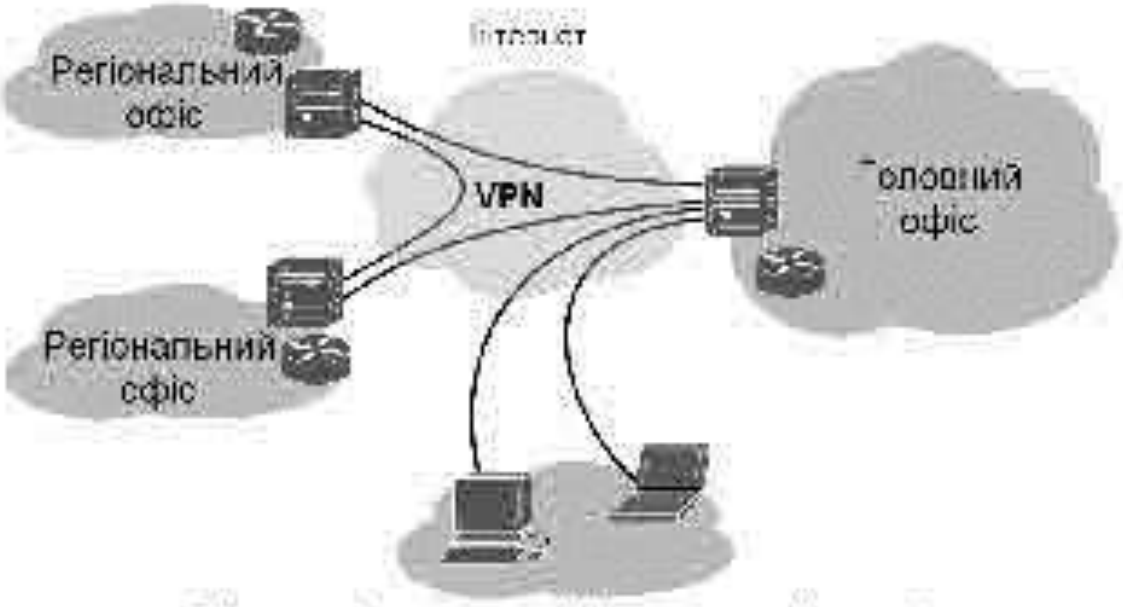


Рисунок 1.1. Загальна схема VPN-мережі для організацій

Для організації віддаленого доступу до приватної мережі за допомогою технології VPN знадобиться Інтернет і реальна IP-адреса. Будь-який користувач з

будь-якої точки земної кулі зможе зайти в нашу мережу, якщо він знає IP-адресу, логін і пароль (рис.1.1).

Головна мета VPN – прозорий доступ до ресурсів мережі, де користувач може робити все те, що він робить зазвичай незалежно від того, наскільки він віддалений. З цієї причини VPN придбав популярність серед дистанційних працівників і офісів, які потребують спільного використання ресурсів територіально розділених мереж (рис.1.2).

Рисунок 1.2. Організація VPN для віддаленого користувача

Якщо необхідна велика кількість ресурсів, розподілених в багатьох мережах і проблемою є конфіденційність переміщення інформації в цих мережах, то VPN буде потрібним вибором. В цьому полягає перевага VPN – можна дуже просто захистити від зовнішнього світу всю мережу. Якщо необхідні хости, які створюють відчуття, що вони знаходяться в одній мережі, VPN – це спосіб реалізувати подібне рішення [2]. Це дійсно зручно, якщо треба працювати з мобільними клієнтами, яким необхідний прозорий доступ до головних офісів, або треба отримати повний и безпечний доступ до домашньої мережі. У цьому випадку вже не треба турбуватися про плутанину з великою кількістю IP-адрес, мінями інфраструктуру при зміні провайдера. При використанні VPN необхідна

лише конфігурація шлюзу. Використання VPN – це відносно дешевий спосіб з'єднання фізично віддалених мереж. При цьому немає необхідності в оплаті виділених WAN-з'єднань, адже весь трафік між мережами передається за допомогою інтернету [1].

1.1.2 Методи реалізації захищених VPN-каналів

Існують різні варіанти створення VPN. При виборі рішення потрібно враховувати фактори продуктивності засобів побудови VPN. Наприклад, якщо маршрутизатор і так працює на межі потужності свого процесора, то додавання тунелів VPN і застосування шифрування/дешифрування інформації може зупинити роботу всієї мережі через те, що цей маршрутизатор не буде справлятися з простим трафіком, не кажучи вже про VPN. Досвід показує, що для побудови VPN краще всього використовувати спеціалізоване обладнання, але якщо є обмеження в засобах, то потрібно звернути увагу на повністю програмні рішення. Розглянемо деякі варіанти побудови VPN [3].

1. VPN на базі брандмауерів.

Брандмауери більшості виробників підтримують тунелювання і шифрування даних. Всі подібні продукти засновані на тому, що якщо вже трафік проходить через брандмауер, то чому б його заодно не зашифрувати. До програмного забезпечення власне брандмауера додається модуль шифрування. Недоліком даного методу можна назвати залежність продуктивності від апаратного забезпечення, на якому працює брандмауер. При використанні брандмауерів на базі ПК треба пам'ятати, що подібне рішення можна застосовувати тільки для невеликих мереж з невеликим обсягом переданої інформації (рис.1.3). У якості прикладу рішення на базі брандмауерів можна назвати FireWall-1 компанії Check Point Software Technologies. FairWall-1 використовує для побудови VPN стандартний підхід на базі IPSec [2]. Трафік, що приходить в брандмауер, дешифрується, після чого до нього застосовуються стандартні правила управління доступом. FireWall-1 працює під управлінням операційних систем Solaris і Windows.

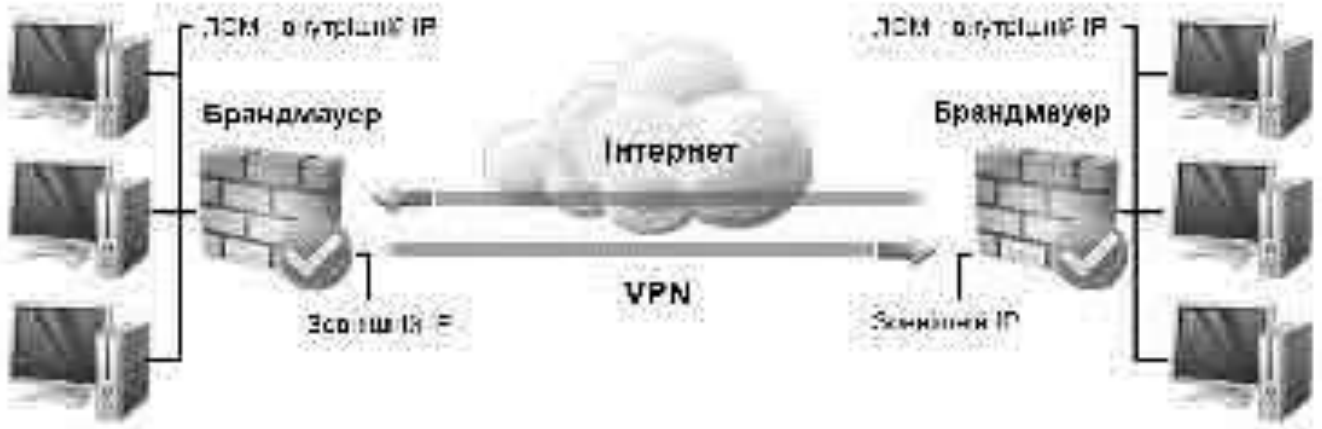


Рисунок 1.3. VPN на базі брандмауера

2. VPN на базі маршрутизаторів.

Іншим способом побудови VPN є застосування маршрутизаторів для створення захищених каналів. Зважаючи на те, що вся інформація, яка виходить з локальної мережі, проходить через маршрутизатор, то доцільно покласти на цей маршрутизатор і завдання шифрування [4].

Яскравим прикладом обладнання для побудови VPN на маршрутизаторах є обладнання компанії Cisco Systems. Починаючи з версії програмного забезпечення IOS 11.3(3) маршрутизатори Cisco підтримують протоколи L2TP і IPSec. Крім простого шифрування інформації Cisco підтримує і інші функції VPN, такі як ідентифікація при встановленні тунельного з'єднання і обмін ключами [5].

Для побудови VPN Cisco використовує тунелювання з шифруванням будь-якого IP-потоку. При цьому тунель може бути встановлений, грунтуючись на адресах джерела і приймача, номері порту TCP (UDP) і зазначеної якості сервіу (QoS). Для підвищення продуктивності маршрутизатора може бути використаний додатковий модуль шифрування ESA (Encryption Service Adapter). Крім того, компанія Cisco System випустила спеціалізований пристрій для VPN, який називається Cisco 1720 VPN Access Router (маршрутизатор доступу до VPN), призначений для встановлення у компаніях малого і середнього розміру, а також у відділеннях великих організацій (рис.1.4).

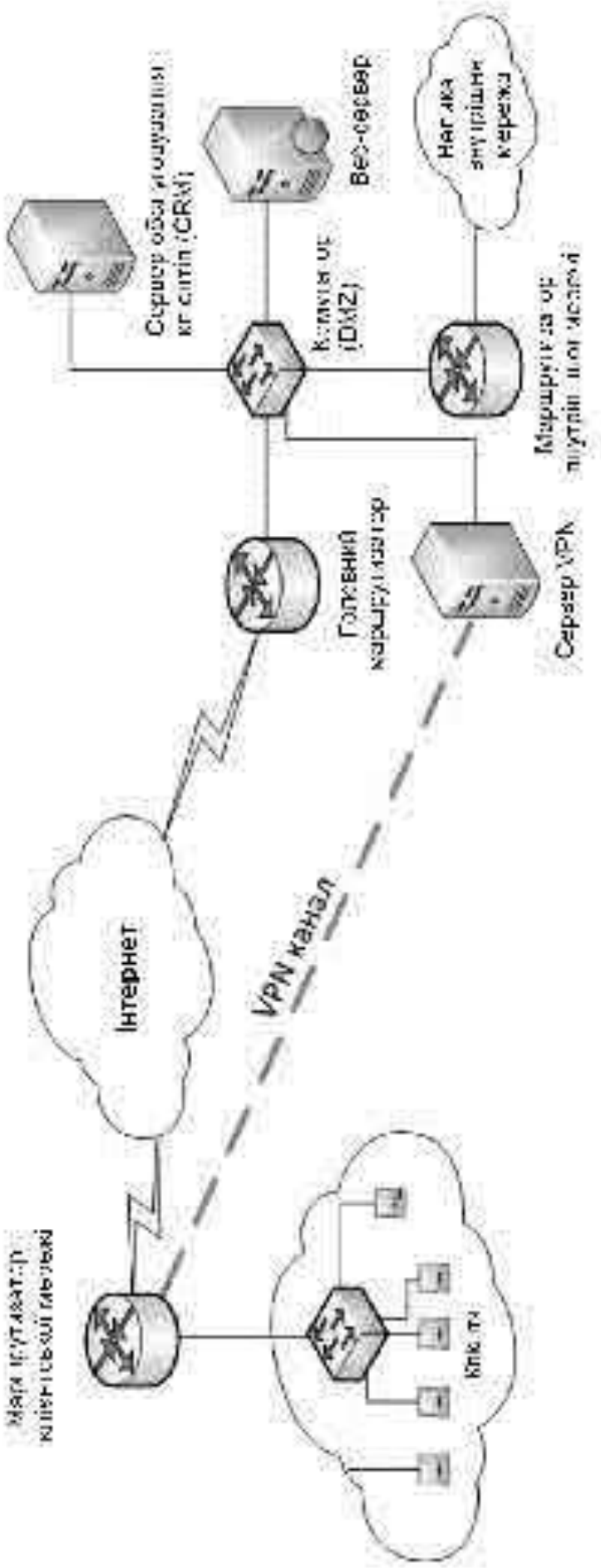


Рисунок 1.4. VPN на базі маршрутизаторів

3. VPN на базі додаткового програмного забезпечення.

Наступним підходом до побудови VPN є чисто програмні рішення. При реалізації такого рішення використовується спеціалізоване програмне забезпечення, яке працює на виділеному комп'ютері і в більшості випадків виконує роль proxy-сервера. Комп'ютер з таким програмним забезпеченням може бути розташований за брандмауером [4].

У якості прикладу такого рішення виступає програмне забезпечення iTop VPN (рис.1.5). При використанні даного ПЗ клієнт підключається до сервера Tunnel, автентифікується на ньому і обмінюється ключами. Шифрування проводиться на базі 32, 40, 56, 64, 72, 128 або 256 бітних ключів Rivest-Cipher 4, отриманих в процесі встановлення з'єднання. Далі зашифровані пакети інкапсулюються у інші IP-пакети, які в свою чергу відправляються на сервер. В ході роботи Tunnel здійснює перевірку цілісності даних за алгоритмом MD5. Позитивними якостями iTop VPN є простота установки і зручність управління. Недоліками даної системи можна вважати не високу продуктивність.

Рисунок 1.5. Програмне забезпечення iTop VPN

4. VPN на базі спеціалізованих апаратних засобів.

Варіант побудови VPN на спеціальних пристроях може бути використаний у мережах, що вимагають високої продуктивності (рис.1.6). Прикладом такого рішення є продукт cIPro-VPN компанії Radguard.

Даний продукт використовує апаратне шифрування інформації, що передається, здатний пропускати потік у 100 Мбіт/с. cIPro-VPN підтримує протокол IPSec і механізм управління ключами ISAKMP / Oakley. Крім іншого, даний пристрій підтримує засоби трансляції мережевих адрес і може бути доповнений спеціальною платою, яка додає функції брандмауера [5].

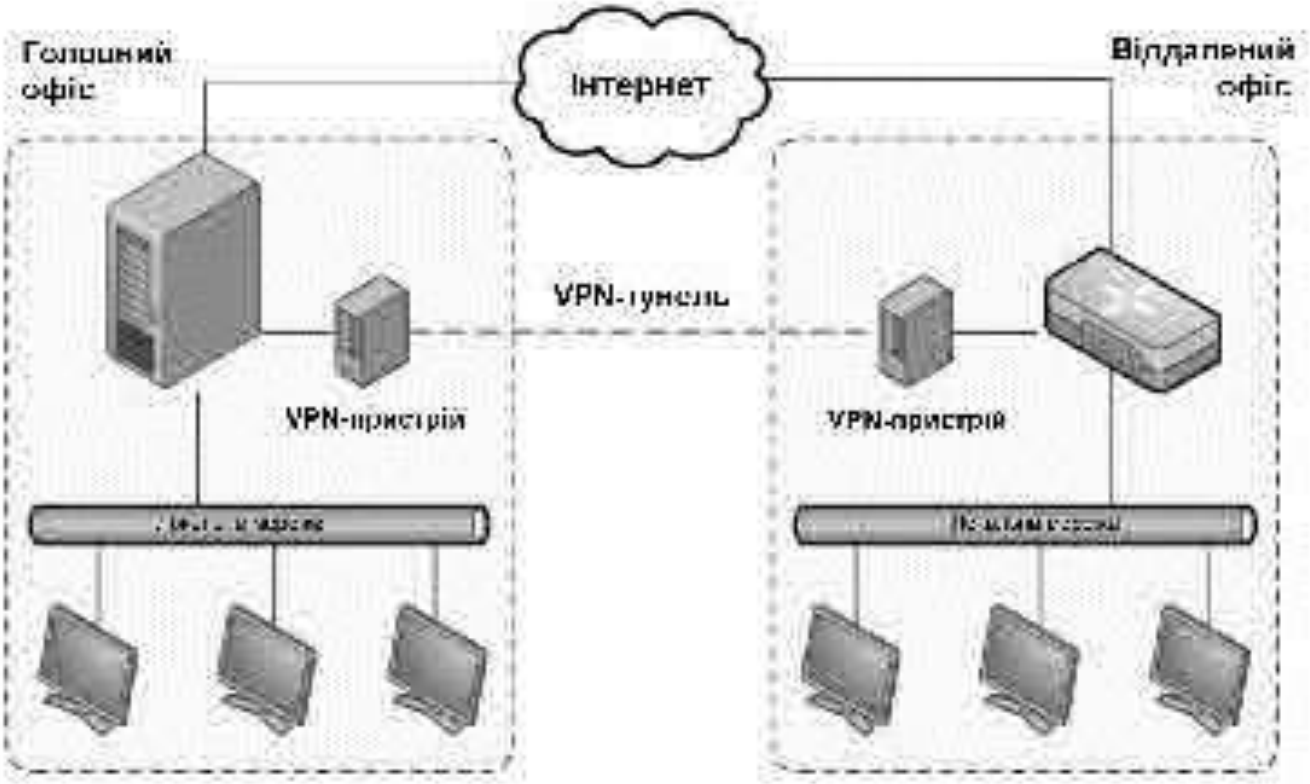


Рисунок 1.6. VPN на базі апаратних засобів

5. VPN на базі інтегрованих засобів мережевої ОС.

Рішення на базі мережевої ОС розглянемо на прикладі сімейства Windows компанії Microsoft. Для створення VPN Microsoft використовує протокол PPTP, який інтегрований у систему Windows (рис. 1.7). Дане рішення дуже привабливе для організацій, що використовують Windows у якості корпоративної операційної системи. У роботі VPN на базі Windows використовується база користувачів, що зберігається на Primary Domain Controller (PDC).

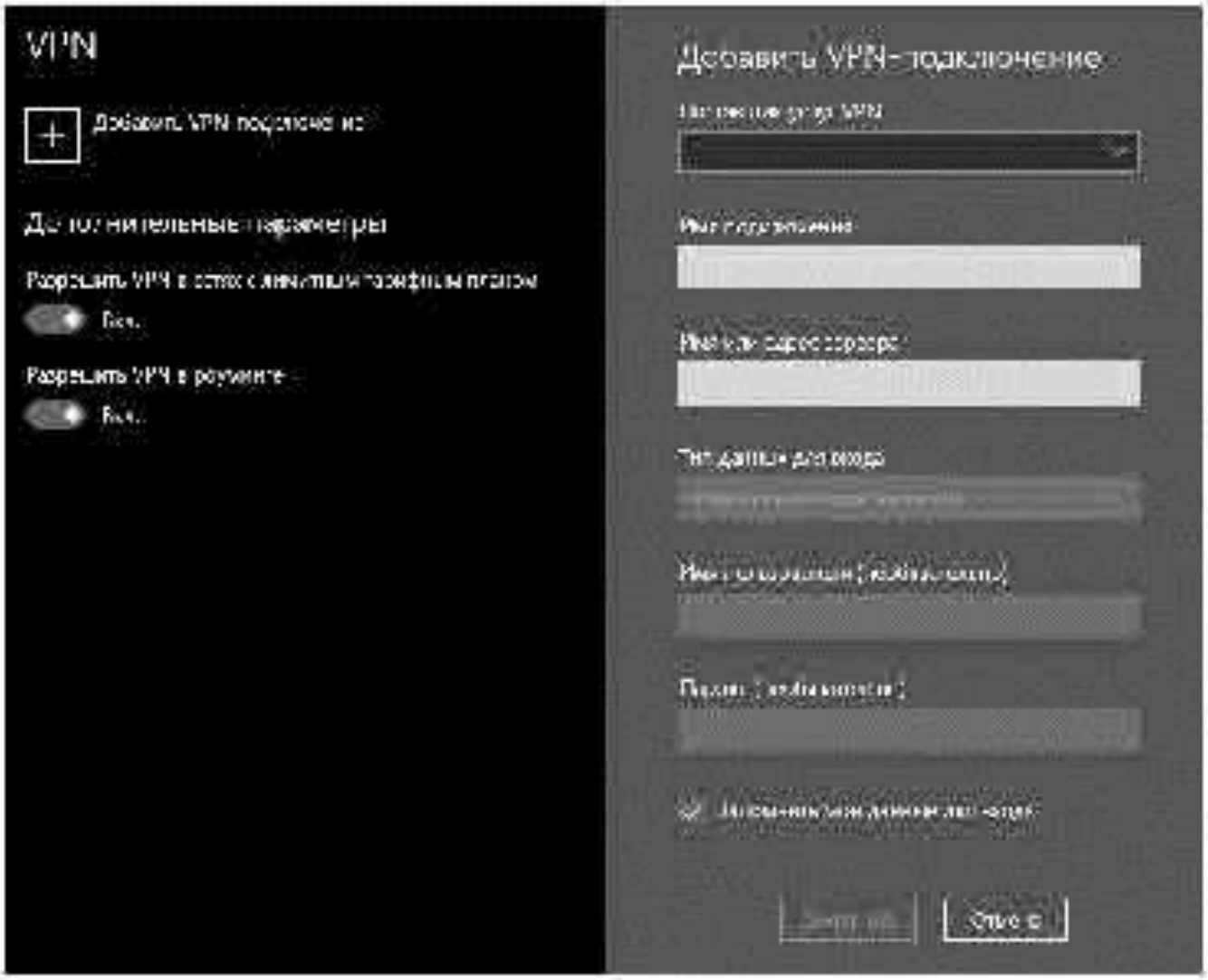


Рисунок 1.7. VPN на базі інтегрованих засобів мережевої ОС

При підключенні до PPTP-сервера користувач автентифікується за протоколами PAP, CHAP або MS-CHAP. Передані пакети інкапсулюються в пакети GRE / PPTP. Для шифрування пакетів використовується нестандартний протокол від Microsoft Point-to-Point Encryption з 32, 40, 56, 64, 72, 128 або 256 бітовим ключем, отриманим в момент встановлення з'єднання. Недоліками даної системи є відсутність перевірки цілісності даних і неможливість зміни ключів під час з'єднання. Позитивним моментом є інтеграція з ОС Windows [6].

Таким чином, будь-яка віртуальна приватна мережа базується на трьох методах, які застосовуються при реалізації заходів безпеки в мережах:

1. Тунелювання;
2. Автентифікація;
3. Шифрування.

1.1.3 Висновки за аналітичним оглядом

У даному огляді було розглянуто загальну технологію організації VPN-підключення до мережі передачі даних, побудову розподільної мережі та віддалений доступ до мережі. Схеми віддаленого доступу можуть відрізнятися також і типом служб, які підтримуються для віддаленого клієнта. Найчастіше використовується віддалений доступ до файлів, баз даних, принтерів в тому ж стилі, до якого користувач звик при роботі в локальній мережі. Такий режим називається режимом віддаленого вузлу (remote node). Інколи при віддаленому доступі реалізується обмін з центральною мережею повідомленнями електронної пошти, за допомогою якого можна в автоматичному режимі отримати запрошувані корпоративні дані, наприклад з бази даних.

Особливе місце серед всіх видів віддаленого доступу до комп'ютера є спосіб, при якому користувач має можливість віддалено працювати з комп'ютером таким самим чином, ніби він управляє ним за допомогою локального підключеного терміналу. У цьому режимі він може запускати виконання програми на віддаленому комп'ютері і бачити результати роботи у реальному часі. При цьому прийнято розділяти такий спосіб доступу на термінальний доступ і віддалене керування.

1.2 Вибір протоколу VPN віддаленого доступу

Зазвичай VPN розгортають на рівнях не вище мережевого, адже застосування криптографії на цих рівнях дозволяє використовувати в незмінному вигляді транспортні протоколи (такі як TCP, UDP).

Найчастіше для створення віртуальної мережі використовується інкапсуляція протоколу PPP в який-небудь інший протокол – IP (такий спосіб використовує реалізація PPTP – Point-to-Point Tunneling Protocol) або Ethernet (PPPoE) (хоча і вони мають відмінності). Технологія VPN останнім часом використовується не тільки для створення власне приватних мереж, але і деякими провайдерами «останньої милі» на пострадянському просторі для надання виходу в Інтернет [4].

1.2.1 VPN-протоколи рівнів мережевої моделі

Як правило, на сьогоднішній день для побудови мереж VPN використовуються протоколи наступних рівнів: канальний рівень; мережевий рівень; транспортний рівень.

На канальному рівні можуть використовуватися протоколи тунелювання даних L2TP і PPTP, які використовують авторизацію і аутентифікацію.

В даний час найбільш поширеним протоколом VPN є протокол двохточкового тунельного зв'язку або Point-to-Point Tunnelling Protocol – PPTP. PPTP використовує існуючі відкриті стандарти TCP/IP і багато в чому покладається на застарілий протокол двохточкового зв'язку PPP. На практиці PPP так і залишається комунікаційним протоколом сеансу з'єднання PPTP. PPTP створює тунель через мережу до сервера одержувача і передає по ньому PPP-пакети віддаленого користувача. Сервер і робоча станція використовують віртуальну приватну мережу і не звертають уваги на те, наскільки безпечною або доступною є глобальна мережа між ними. Завершення сеансу з'єднання з ініціативи сервера, на відміну від спеціалізованих серверів віддаленого доступу, дозволяє адміністраторам локальної мережі не пропускати віддалених користувачів за межі системи безпеки Windows Server [5].

PPTP надає компаніям можливість взаємодіяти з існуючими мережевими інфраструктурами і не завдавати шкоди власній системі безпеки. Таким чином, віддалений користувач може підключитися до Інтернету за допомогою місцевого провайдера по аналоговій телефонній лінії або каналу ISDN і встановити з'єднання з сервером. При цьому компанії не доводиться витрачати великі суми на організацію та обслуговування пулу модемів, що надає послуги віддаленого доступу.

В останній час помічено зростання кількості віртуальних приватних мереж, розгорнутих на базі нового протоколу тунелювання другого рівня Layer 2 Tunneling Protocol – L2TP.

L2TP з'явився в результаті об'єднання протоколів PPTP і L2F (Layer 2 Forwarding). PPTP дозволяє передавати через тунель пакети PPP, а L2F-пакети

SLIP і PPP. Головна перевага L2TP в тому, що цей протокол дозволяє створювати тунель не тільки в мережах IP, але і в таких, як ATM, X.25 та Frame Relay. L2TP застосовує у якості транспорту протокол UDP і використовує однаковий формат повідомлень як для управління тунелем, так і для пересилання даних [6]. L2TP в реалізації Microsoft використовує в якості контрольних повідомлень пакети UDP, що містять шифровані пакети PPP. Надійність доставки гарантує контроль послідовності пакетів.

Функціональні можливості PPTP і L2TP різні. L2TP може використовуватися не тільки в IP-мережах. Службові повідомлення для створення тунелю й пересилки по ньому даних використовують однаковий формат і протоколи. PPTP може застосовуватися тільки в IP-мережах, і йому необхідне окреме з'єднання TCP для створення і використання тунелю. L2TP поверх IPSec пропонує більше рівнів безпеки, ніж PPTP, і може гарантувати майже 100-відсоткову безпеку важливих для організації даних [7]. Особливості L2TP роблять його дуже перспективним протоколом для побудови віртуальних мереж.

Протоколи L2TP і PPTP відрізняються від протоколів тунелювання третього рівня рядом особливостей:

1. Надання корпораціям можливості самостійно обирати спосіб автентифікації користувачів та перевірки їх повноважень – на власній «території» або у провайдера інтернет-послуг. Обробляючи тунельовані пакети PPP, сервери корпоративної мережі отримують всю інформацію, необхідну для ідентифікації користувачів;

2. Підтримка комутації тунелів – завершення одного тунелю та ініціювання іншого до одного з безлічі потенційних термінаторів. Комутація тунелів дозволяє як би продовжити PPP-з'єднання до необхідної кінцевої точки;

3. Надання системним адміністраторам корпоративної мережі можливості реалізації стратегій призначення користувачам прав доступу безпосередньо на брандмауері і внутрішніх серверах. Оскільки термінатори тунелю отримують пакети PPP з відомостями про користувачів, вони в стані застосовувати сформульовані адміністраторами стратегії безпеки до трафіку окремих

користувачів. Тунелювання третього рівня не дозволяє розрізняти пакети, які надходять від провайдера, тому фільтри стратегії безпеки доводиться застосовувати на кінцевих робочих станціях і мережевих пристроях [5]. Крім того, у разі використання тунельного комутатора з'являється можливість організувати «продовження» тунелю другого рівня для безпосередньої трансляції трафіку окремих користувачів до відповідних внутрішніх серверів. На такі сервери може бути покладено завдання додаткової фільтрації пакетів.

Протокол MPLS (Multiprotocol Label Switching) – механізм передачі даних, який емулює різні властивості мереж з комутацією каналів поверх мереж з комутацією пакетів. MPLS працює на рівні, який можна було б розташувати між канальним і третім мережевим рівнями моделі OSI, і тому його зазвичай називають протоколом канально-мережевого рівня. Він був розроблений з метою забезпечення універсальної служби передачі даних як для клієнтів мереж з комутацією каналів, так і мереж з комутацією пакетів. За допомогою MPLS можна передавати трафік самої різної природи, такий як IP-пакети, ATM, SONET і кадри Ethernet.

На мережевому рівні (IP) використовується протокол IPSec, який реалізує шифрування і конфіденційність даних, а також автентифікацію абонентів. Застосування протоколу IPSec дозволяє реалізувати повнофункціональний доступ еквівалентний фізичному підключенню до корпоративної мережі [6]. Для встановлення VPN кожен з учасників повинен конфігурувати певні параметри IPSec, тобто кожен клієнт повинен мати програмне забезпечення, що реалізує IPSec.

На транспортному рівні використовується протокол SSL / TLS або Secure Socket Layer / Transport Layer Security, який реалізує шифрування і автентифікацію між транспортними рівнями приймача і передавача. SSL / TLS може застосовуватися для захисту трафіку TCP, але не може застосовуватися для захисту трафіку UDP. Для функціонування VPN на основі SSL / TLS немає необхідності в реалізації спеціального програмного забезпечення, адже кожен браузер і поштовий клієнт обладнані цими протоколами. В силу того, що SSL /

TLS реалізується на транспортному рівні, захищене з'єднання встановлюється «з-кінця-в-кінець». TLS-протокол заснований на Netscape SSL-протоколі версії 3.0 і складається з двох частин – TLS Record Protocol і TLS Handshake Protocol. Різниця між SSL 3.0 і TLS 1.0 незначна.

1.2.2 Застосування протоколу IPsec і алгоритмів захисту

IPSec (IP Security Protocol) – це розширений IP-протокол. Він пропонує службу кодування. Ця служба забезпечує автентифікацію, а також доступ і контроль за надійністю. IPSec забезпечує сервіс, схожий із SSL, але працює на мережевому рівні. Через IPSec можна створювати кодовані тунелі (VPN) або кодувати трафік між двома вузлами. У IPSec передбачене ведення бази даних політики безпеки, яка, по суті, є набором критеріїв для створення тунелів і фільтрації IP-пакетів. У цьому протоколі передбачене все необхідне, і для розробки, наприклад, програмного VPN-агенту досить лише грамотно реалізувати IPSec і передбачити інтерфейс для його адміністрування [8].

Оскільки IPSec реалізується на рівні протоколу IP, створеними з його допомогою тунелями можуть користуватися і протоколи вищих рівнів, наприклад TCP або UDP [6]. Основний недолік IPSec – здатність працювати тільки в IP-мережах – нейтралізується шляхом його застосування в комбінації з протоколами L2F (Layer 2 Forwarding, переадресація на рівні 2) і L2TP (Layer 2 Tunneling Protocol, протокол тунелювання на рівні 2), які здійснюють інкапсуляцію пакетів іншої архітектури в IP-пакети.

Протоколи управління ключами відповідають за установлення погодження щодо ключів та їх зберігання. Вони допомагають установити SA (Security Association, асоціації безпеки). Протоколи маніпуляцій з пакетами використовують SA для додавання до пакетів властивостей, зв'язаних з безпекою.

Ядро IPSec складають три протоколи:

- AH або Authentication Header;
- ESP або Encapsulating Security Payload;
- IKE або Internet Key Exchange.

AH або Authentication Header – заголовок автентифікації – гарантує цілісність і автентичність даних. Основне призначення протоколу AH – він дозволяє приймальній стороні переконатися, що:

1) пакет був відправлений стороною, з якою встановлена безпечна асоціація;

2) вміст пакета не був спотворений в процесі його передачі по мережі;

3) пакет не є дублікатом вже отриманого пакета.

Дві перші функції обов'язкові для протоколу AH, а остання обирається при встановленні асоціації за бажанням. Для виконання цих функцій протокол AH використовує спеціальний заголовок [5]. Його структура розглядається за такою схемою:

1) У полі наступного заголовку (next header) вказується код протоколу вищого рівня, тобто протоколу, повідомлення якого розміщене у полі даних IP-пакету;

2) У полі довжини корисного навантаження (payload length) міститься довжина заголовка AH;

3) Індекс параметрів безпеки (Security Parameters Index, SPI) використовується для зв'язку пакета з передбаченою для нього безпечною асоціацією;

4) Поле порядкового номеру (Sequence Number, SN) вказує на порядковий номер пакету і застосовується для захисту від його помилкового відтворення (коли третя сторона намагається повторно використовувати перехоплені захищені пакети, відправлені реально автентифікованим відправником);

5) Поле даних автентифікації (authentication data), яке містить так звane значення перевірки цілісності пакета (Integrity Check Value, ICV). Це значення обчислюється за допомогою однієї з двох обов'язково підтримуваних протоколом AH функцій MD5 або SAH-1, але може використовуватися і будь-яка інша функція.

ESP або Encapsulating Security Payload – інкапсуляція зашифрованих даних – шифрує передані дані, забезпечуючи конфіденційність, може також підтримувати автентифікацію і цілісність даних.

Протокол ESP вирішує дві групи завдань:

1. Завдання, аналогічні завданням протоколу AH, – це забезпечення автентифікації і цілісності даних на основі дайджесту;

2. Захист переданих даних шляхом їх шифрування від несанкціонованого перегляду.

Заголовок ділиться на дві частини, що розділяються полем даних. Перша частина, власне заголовок ESP, утворюється двома полями (SPI і SN), призначення яких аналогічне однойменним полям протоколу AH і розміщується перед полем даних. Решта службових полів протоколу ESP розташовані наприкінці пакету [3]. Два поля наступного заголовку і даних автентифікації – аналогічні полям заголовку AH. Поле даних автентифікації відсутнє, якщо при встановленні безпечної асоціації прийняте рішення не використовувати можливості протоколу ESP щодо забезпечення цілісності.

У транспортному режимі (рис.1.8) IPsec бере пакет, який необхідно захистити, залишає незмінним IP-заголовок пакету і замінює лише верхній шар, додавши заголовки IPsec і визначені параметри захисту між верхніми шарами і вихідним IP-заголовком. Цей режим був розроблений для використання головним чином у хостах, яким потрібно захистити трафік, який курсує між ними.

Рисунок 1.8. Транспортний режим IPsec

У тунельному режимі IPsec розглядає весь пакет як блок даних, додає новий заголовок і захищає дані (вихідний пакет), роблячи їх частиною зашифрованої корисної інформації нового пакету [8].

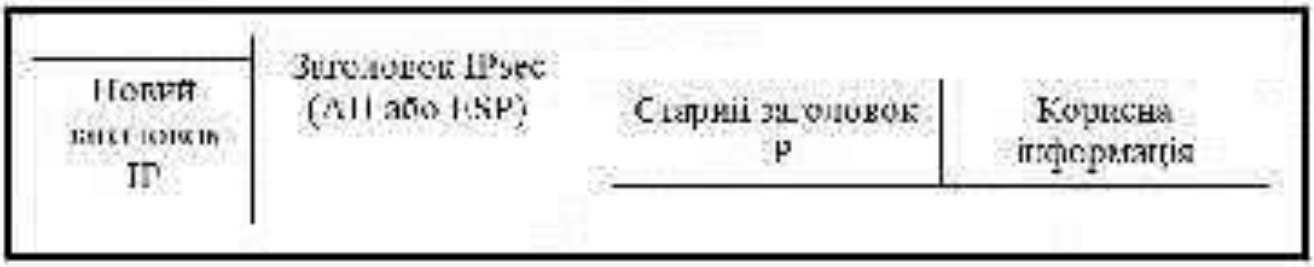


Рисунок 19. Тунельний режим IPsec

Застосування того чи іншого режиму залежить від вимог, що пред'являються до захисту даних, а також від ролі, яку відіграє в мережі вузол, який завершає захищений канал [6]. Так, вузол може бути хостом (кінцевим вузлом) або шлюзом (проміжним вузлом). Відповідно, є три схеми застосування протоколу IPSec:

- хост-хост;
- шлюз-шлюз;
- хост-шлюз.

Можливості протоколів AH і ESP частково перекриваються: протокол AH відповідає тільки за забезпечення цілісності та автентифікації даних, протокол ESP може шифрувати дані і, крім того, виконувати функції протоколу AH (в урізаному вигляді). ESP може підтримувати функції шифрування і автентифікації / цілісності в будь-яких комбінаціях, тобто або всю групу функцій, або тільки автентифікацію / цілісність, або тільки шифрування.

IKE або Internet Key Exchange (обмін ключами Інтернету) вирішує допоміжну задачу автоматичного надання кінцевим точкам захищеного каналу секретних ключів, необхідних для роботи протоколів автентифікації і шифрування даних. IKE дозволяє забезпечити передачу інформації по тунелю, виключаючи втручання ззовні. Цей протокол вирішує завдання безпечного управління та обміну криптографічними ключами між віддаленими пристроями.

IKE автоматизує процес передачі ключів, використовуючи механізм шифрування відкритим ключем для встановлення безпечного з'єднання. Крім цього, IKE дозволяє виробляти зміну ключа для вже встановленого з'єднання, що значно підвищує конфіденційність переданої інформації [3].

Автентифікація один одного хостами, що приймають участь в узгодженні по протоколу IKE, є критичним фактором. При її відсутності безпека обміну ключами буде сумнівною. Для автентифікації IKE може використовувати такі методи:

1. Розділювані ключі (Pre-shered keys, PSK). Автентифікація відбувається методом доказу володіння ключем, оскільки допускається, що тільки хости, які приймають участь у з'єднанні, можуть знати ключ. Проблема лише в безпечному розподілі ключів;

2. Алгоритми публічних ключів. При автентифікації для шифрування даних використовується публічний ключ, а для дешифрування необхідно мати приватний ключ. Метод основується на двох фактах:

А. Для використання отриманого публічного ключа необхідний приватний ключ хосту. Проблема – у безпечному розповсюдженні приватних ключів;

Б. Якщо А – дійсне, то володіння приватним ключем в сумі з раніше описаним публічним може служити доказом справжності;

3. Цифрові підписи (підписи DSS і RSA). Машина, яка має бути автентифікована, завіряє даніцифровим підписом за допомогою свого приватного ключу. Якщо підпис підтверджується за допомогою публічного ключа цього хосту, підтверджується і справжність хосту.

RSA і DSA протоколи засновані на базі спеціально створеної пари ключів, а саме публічному і приватному ключах. Це асиметричні алгоритми шифрування, тобто можна зашифрувати інформацію одним ключем, а розшифрувати іншим, на відміну, наприклад від DES, де використовується один і той же ключ для шифрування і розшифрування інформації. Доступні такі типи ключів: RSA, DSA для протоколу SSH 2 і RSA1 для SSH 1.

Алгоритм RSA базується на проблемі факторизації великих чисел. Власне, ключовим матеріалом є секретна експонента D (яка обчислюється за допомогою P і Q), відкрита експонента E, модуль N = P * Q, де P і Q – прості числа (вірніше, псевдопрості). P і Q часто також є частиною секретного ключа, оскільки дозволяють прискорити обчислення. Для шифрування береться число (воно ж – рядок байт), менше N (істотно менше не рекомендується, оскільки це спрощує злом), зводиться до ступеня E за модулем N. Для оптимізації використовується стандартне невелике значення для E, рівне 65537 (раніше було менше) – від цього стійкість алгоритму не знижується. Далі результат шифрування зводиться до ступеня D, і отримуємо теж саме значення, яке шифрували, завдяки властивостям D. Тут варто зауважити, що якщо поміняти місцями E і D (спочатку використовувати D, а потім – E), – також буде отримане вихідне число. Саме така схема і використовується для цифрового підпису – тільки власник секретної частини ключа може її згенерувати, але будь-яка інша людина може перевірити (маючи E). Завдяки цій властивості генерація цифрового підпису RSA у літературі також називається шифруванням.

Слід зауважити, що оскільки розмір блоку, що шифрується, є обмеженим розміром ключа (наприклад, 2048 біт або 256 байт), і процедура такого шифрування займає набагато більше часу, ніж шифрування блоку цих же даних симетричним алгоритмом (хоча, здавалося б, за раз зашифрувати можна набагато більше), безпосередньо для шифрування даних RSA не використовується. Замість цього генерується випадковий ключ для симетричного алгоритму і передані дані шифруються ним [5]. Потім, використовуючи відкритий RSA-ключ одержувача даних, цей симетричний ключ шифрується і передається одержувачу разом із зашифрованими даними (при цьому у операції шифрування цей симетричний ключ доповнюється, щоб за розміром підходити під розмір ключа). Таким чином можна зашифрувати файл для декількох одержувачів і, таким чином, розшифрувати симетричний ключ та прочитати повідомлення зможуть тільки власники відповідних секретних ключів.

Для цифрового підпису все виконується навпаки. Власник секретного ключа пише повідомлення, розраховує від нього хеш (оскільки саме повідомлення набагато довше ключа) і шифрує (підписує) хеш від повідомлення та відсилає лист разом з цим підписом одержувачу [7]. Одержувач, маючи відкритий ключ, «розшифровує» цифровий підпис і порівнює витягнутий хеш з реальним хешем повідомлення.

Використання DSA базується на проблемі дискретного логарифмування, що дозволяє перенести алгоритм на будь-яку групу, наприклад групу точок еліптичних кривих у результаті чого отримуємо ECDSA). Процедура складніше, ніж у RSA [5]. З особливостей слід зауважити, що хеш повідомлення використовується у DSA безпосередньо, тому може використовуватися 160-бітний хеш (SHA1, як власне і описано в FIPS-186-2). Відповідно, оскільки стійкість алгоритму залежить від всіх складових ключа, не має сенсу використовувати DSA-ключі розміром більше 1024 біт. Пізніше з'явиться доповнення стандарту, що дозволяє використовувати довші хеши (SHA2 – 224, 256, 384, 512 біт) і відповідно більший розмір ключа, але це доступно поки що не у всіх реалізаціях.

Для рішення проблеми розповсюдження публічних ключів даний метод може задіяти цифрові сертифікати і у визначенні ідентичності хосту за його публічним ключем розраховувати на довірену третю сторону. В загальних рисах цей метод вважається кращим, ніж прямий обмін ключами.

На протязі першого етапу протокол IKE повинен виконати декілька важливих операцій. Однією з них є погодження криптографічних протоколів і параметрів, які будуть використовуватися для автентифікації і шифрування. Друга операція – це проведення автентифікації хостів за допомогою погоджених алгоритмів [6]. На основі цього обміну інформації встановлюються деякі спільні секретні дані. Результатом етапу 1 є безпечний канал, котрий хости можуть використовувати на етапі 2 для виконання погодження IPsec SA. Не зайвим буде відзначити, що протокол IPsec домінує у більшості реалізацій віртуальних приватних мереж. В даний час на ринку представлені як програмні реалізації

(наприклад, протокол, реалізований у операційній системі Windows компанії Microsoft), так і програмно-апаратні реалізації IPsec. Не дивлячись на велике число різних рішень, всі вони досить добре сумісні один з одним.

Робоча група інтернету (IETF) визначає IPSec як набір специфікацій для встановлення достовірності, цілісності і забезпечення конфіденційності засобами криптографії для протоколу IP [7]. IPSec призначався і фактично став стандартом для захисту інтернет-комунікацій. Розробки групи IPSec дозволяють організувати захищені тунелі між хостами, тунелі інкапсульованих даних і віртуальні приватні мережі, забезпечуючи таким чином захист протоколів, розташованих вище, ніж рівень IP.

Формати протоколу для заголовку автентифікації IPSec (Authentication Header, AH) і захищеного інкапсулювання IP (Encapsulating Security Payload, ESP) не залежать від криптографічного алгоритму, хоча деякі набори алгоритмів вказані як обов'язкові на користь забезпечення взаємодії. Так само в структурі IKE IPSec підтримуються багато алгоритмів управління ключами для захисту трафіку. Однак, не зважаючи на складність IPsec, в теперішній час він, можливо, є найкращим вибором, якщо треба отримати рішення промислових масштабів з широкою підтримкою і розповсюдженою реалізацією [9].

1.2.3 Порівняння протоколів та вибір найбільш відповідного

Для кожного типового випадку є окрема технологія VPN яка підходить найкраще. Зробити правильний вибір допоможуть правила, викладені нижче.

При використанні VPN перед адміністраторами мережі стає питання про доцільність використання саме такого захисту мережі. Але при реалізації мережі необхідно враховувати не лише переваги VPN, головними з яких є підвищена безпека, об'єднання розподілених ресурсів, прозорість для користувача та зниження затрат за рахунок використання інтернету, але й недоліки, які можуть бути несумісні з нашими вимогами до безпеки мережі. Головними ж недоліками VPN можна вважати затрати часу на реалізацію, проблематичність у виявленні проблем, які будуть з'являтися в ході експлуатації, довіра користувачам іншої

мережі при побудові топології мережа-мережа, залежність доступу від інтернет-провайдера, взаємодія між різними протоколами, апаратними та програмними засобами різних виробників. У зв'язку з цим перед плануванням мережі необхідно ретельно проаналізувати задачі, які стоять перед адміністратором мережі, та методи, якими їх можна досягти.

Найчастіше перед керівниками IT-підрозділів стоїть питання, який з протоколів вибрати для побудови корпоративної мережі VPN. Відповідь не очевидна, тому що кожен з підходів має як переваги, так і недоліки.

Як видно з аналізу характеристик протоколів IPSec та SSL / TLS, вони не є взаємозамінними і можуть функціонувати як окремо, так і паралельно, визначаючи функціональні особливості кожної з реалізованих VPN.

Вибір протоколу для побудови корпоративної мережі VPN можна здійснювати за такими критеріями:

1) Тип доступу, необхідний для користувачів мережі VPN.

При повнофункціональному постійному підключенні до корпоративної мережі рекомендується протокол IPSec. При тимчасовому підключенні, наприклад, мобільного користувача або користувача, що використовує публічний комп'ютер, з метою отримання доступу до певних послуг, наприклад, електронної пошти або бази даних рекомендовано протокол SSL / TLS, який дозволяє організувати VPN для кожної окремої послуги;

2) Чи є користувач співробітником компанії.

Якщо користувач є співробітником компанії, пристрій яким він користується для доступу до корпоративної мережі через IPSec VPN, може бути налаштований деяким певним способом. Якщо користувач не є співробітником компанії, до корпоративної мережі якої здійснюється доступ, рекомендується використовувати SSL / TLS. Це дозволить обмежити гостьовий доступ тільки певними послугами;

3) Визначення цінності інформації та рівня безпеки корпоративної мережі.

При високому рівні безпеки рекомендований вибір – протокол IPSec. Дійсно, рівень безпеки, пропонований IPSec, набагато вище рівня безпеки, пропонованого протоколом SSL / TLS в силу використання ПЗ, що

конфігурується на стороні користувача та шлюзу безпеки на стороні корпоративної мережі. При середньому рівні безпеки рекомендований вибір – протокол SSL / TLS, що дозволяє здійснювати доступ з будь-яких терміналів. Якщо в залежності від послуги рівень безпеки може бути від середнього до високого, то рекомендований вибір – комбінація протоколів IPSec (для послуг, що вимагають високий рівень безпеки) і SSL / TLS (для послуг, що вимагають середній рівень безпеки);

4) Рівень безпеки даних, переданих користувачем.

При високому рівні, наприклад, менеджменту компанії, рекомендований вибір – протокол IPSec. При середньому рівні, наприклад, партнерстві, рекомендований вибір – протокол SSL / TLS. При залежності від послуги рекомендований вибір – комбінація протоколів IPSec (для послуг, що вимагають високий рівень безпеки) і SSL / TLS (для послуг, що вимагають середній рівень безпеки);

5) Швидке розгортання VPN або масштабованість рішення в майбутньому.

При швидкому розгортанні мережі VPN з мінімальними витратами рекомендований вибір – протокол SSL / TLS. В цьому випадку немає необхідності реалізації спеціалізованого ПЗ на стороні користувача, як у випадку IPSec. При масштабованості мережі VPN і додаванні доступу до різноманітних послуг рекомендований вибір – протокол IPSec, що дозволяє здійснення доступу до всіх послуг і ресурсів корпоративної мережі. При швидкому розгортанні і масштабованості рекомендований вибір – комбінація IPSec та SSL / TLS: використання SSL / TLS на першому етапі для здійснення доступу до необхідних послуг з впровадженням IPSec.

Порівняльну характеристику протоколів IPsec та SSL / TLS, складену за наведеними вище рекомендаціями, показано у табл. 1.1

Таблиця 1.1. Порівняльна характеристика IPsec та SSL / TLS

Особливості	*IPSec*	*SSL / TLS*
Апаратна незалежність	Так	Так
Код	Не вимагається змін для додатків. Може потребувати доступ до початкового коду стека TCP/IP	Потрібні зміни у додатках. Можуть потребувати нові DLL або доступ до початкового коду додатків
Захист	IP-пакет цілком. Включає захист для протоколів вищих рівнів	Тільки рівень додатків
Фільтрація пакетів	Заснована на автентифікованих заголовках, адресах відправника і одержувача, і т.п. Проста і дешева. Підходить для роутерів	Заснована на вмісті і семантиці високого рівня. Більш інтелектуальна і складніша
Продуктивність	Менше число перемикань контексту і переміщення даних	Більше число перемикань контексту і переміщення даних. Великі блоки даних можуть забезпечити краще стиснення
Платформи	Будь-які системи, включно з роутерами	В основному кінцеві системи (клієнти/сервери), також firewalls
Firewall/VPN	Весь трафік захищений	Захищений тільки трафік рівня додатків. ICMP, RSVP, QoS і т.п. можуть бути незахищені
Прозорість	Для користувачів і додатків	Тільки для користувачів
Поточний статус	Широко використовується корпораціями	Широко використовується WWW-браузерами, також використовується деякими іншими продуктами

При виборі серед протоколів PPTP, L2TP/IPsec або SSTP для VPN-рішення віддаленого доступу слід взяти до уваги наступне:

1) Протокол PPTP підтримується різними клієнтами від Microsoft, включаючи ОС сімейства Microsoft Windows, зокрема Windows Server. На відміну від протоколу L2TP/IPsec, протокол PPTP не вимагає використання інфраструктури відкритих ключів (PKI) [8]. VPN-підключення по протоколу PPTP забезпечують конфіденційність даних за допомогою шифрування (захоплені пакети неможливо інтерпретувати без ключа шифрування). Однак VPN-підключення по протоколу PPTP не забезпечують цілісності даних (доказ незмінності даних при передачі) або перевірку достовірності даних (доказ відправки даних уповноваженим користувачем);

2) Протокол L2TP може використовуватися тільки з клієнтськими комп'ютерами під управлінням ОС сімейства Microsoft Windows, за виключенням Windows Server. Протокол L2TP підтримує методи перевірки автентичності IPsec за сертифікатами комп'ютерів і попередніми ключами. При перевірці достовірності за сертифікатом комп'ютера (рекомендований метод перевірки автентичності) для видачі цих сертифікатів комп'ютера VPN-серверу і всім комп'ютерам VPN-клієнтів потрібна інфраструктура PKI [10]. При використанні IPsec VPN-підключення по протоколу L2TP/IPsec забезпечують конфіденційність, цілісність і перевірку автентичності даних. На відміну від протоколів PPTP і SSTP, протокол L2TP/IPsec забезпечує перевірку автентичності комп'ютера на рівні IPsec і перевірку автентичності користувача на рівні PPP;

3) Протокол SSTP підтримується тільки клієнтськими комп'ютерами під управлінням ОС сімейства Microsoft Windows, зокрема Windows Server. При використанні SSL VPN-підключення по протоколу SSTP забезпечують конфіденційність, цілісність і перевірку автентичності даних;

4) Всі три типи тунелів на верхньому рівні стека мережевих протоколів передають PPP-кадри, тому загальні риси протоколу PPP, наприклад схеми перевірки автентичності, узгодження протоколу IP версії 4 (IPv4) і протоколу IP

версії 6 (IPv6), а також захист доступу до мережі (NAP), однакові для всіх трьох типів тунелів.

При правильному виборі VPN забезпечуються наступні можливості:

- користувач отримує захищені канали зв'язку за ціною доступу в інтернет, що в кілька разів дешевше виділених ліній;
- не потрібно змінювати топологію мереж, переписувати програми, навчати користувачів – все це значна економія;
- забезпечується масштабування, оскільки VPN не створює проблем росту і зберігає зроблені інвестиції;
- забезпечується незалежність від криптографії і можливість використовувати модулі криптографії будь-яких виробників у відповідності з національними стандартами тієї чи іншої країни;
- відкриті інтерфейси дозволяють інтегрувати мережу з іншими програмними продуктами та бізнес-додатками [9].

У поданому розділі були розглянуто основні протоколи, які використовуються при створенні VPN-підключення до мережі передачі даних, побудові розподільної мережі та віддаленого доступу до мережі. Їх різноманіття дає широкий спектр для вибору саме того протоколу, який найбільше підходить відповідно до конкретної задачі [10]. При проектуванні VPN необхідно пам'ятати, що існує багато протоколів та їх версій, а також можливостей їх поєднання на різних рівнях мережевої моделі OSI. Оскільки VPN-мережею, скоріше за все, будуть користуватися на різних операційних системах, то необхідно враховувати і цей фактор. Для кожного конкретного випадку потрібно ретельно розглядати вимоги, які ставляться до VPN-з'єднання та згідно з ними обирати необхідний тип організації VPN-зв'язку.

1.3 Реалізація захищеної мережі та інструментарій для її адміністрування

Після визначення вимог, які ставляться до практичної реалізації захищеної мережі у рамках даної роботи, необхідно обрати задовольняючий та доступний спосіб організації зв'язку по захищеним каналам VPN.

1.3.1 Інструментарій для адміністрування захищеної мережі

Оскільки методів і їх комбінацій при реалізації VPN існує доволі багато, необхідно враховувати, якими ресурсами можна розпоряджатися. На сьогодні VPN-з'єднання можливо реалізувати майже на будь-якій операційній системі, включаючи клієнтські версії Windows 10. Сучасні операційні системи дають можливість створювати та підтримувати шифровані канали передачі інформації за допомогою вбудованого програмного забезпечення, служб та сервісів, а також за допомогою додаткового програмного забезпечення, яке може також бути використане при налаштуванні VPN.

Перше, що потрібно зробити при практичній реалізації VPN серверу – це визначитися з операційною системою, встановити та налаштувати її базову конфігурацію. В даному випадку, використовувалася операційна система Windows Server 2016, встановлення якої було реалізоване за допомогою програми віртуалізації VirtualBox і є інтуїтивно зрозумілим і простим.

Наступним кроком має бути налаштування та запуск безпосередньо сервісів, служб та програм, які необхідні для реалізації VPN-серверу. Останнім, що необхідно зробити для повноцінної роботи VPN, буде налаштування клієнтської частини та перевірка правильності налаштувань на попередніх кроках.

1.3.2 Виконання налаштувань VPN-серверу

Першим кроком для створення VPN-серверу потрібно відкрити службу "Маршрутизація та віддалений доступ" (рис.1.10) і зайти у властивості сервера (рис. 1.11). Далі необхідно встановити параметр "локальной сети и вызова по требованию", а також "сервер удалённого доступа".

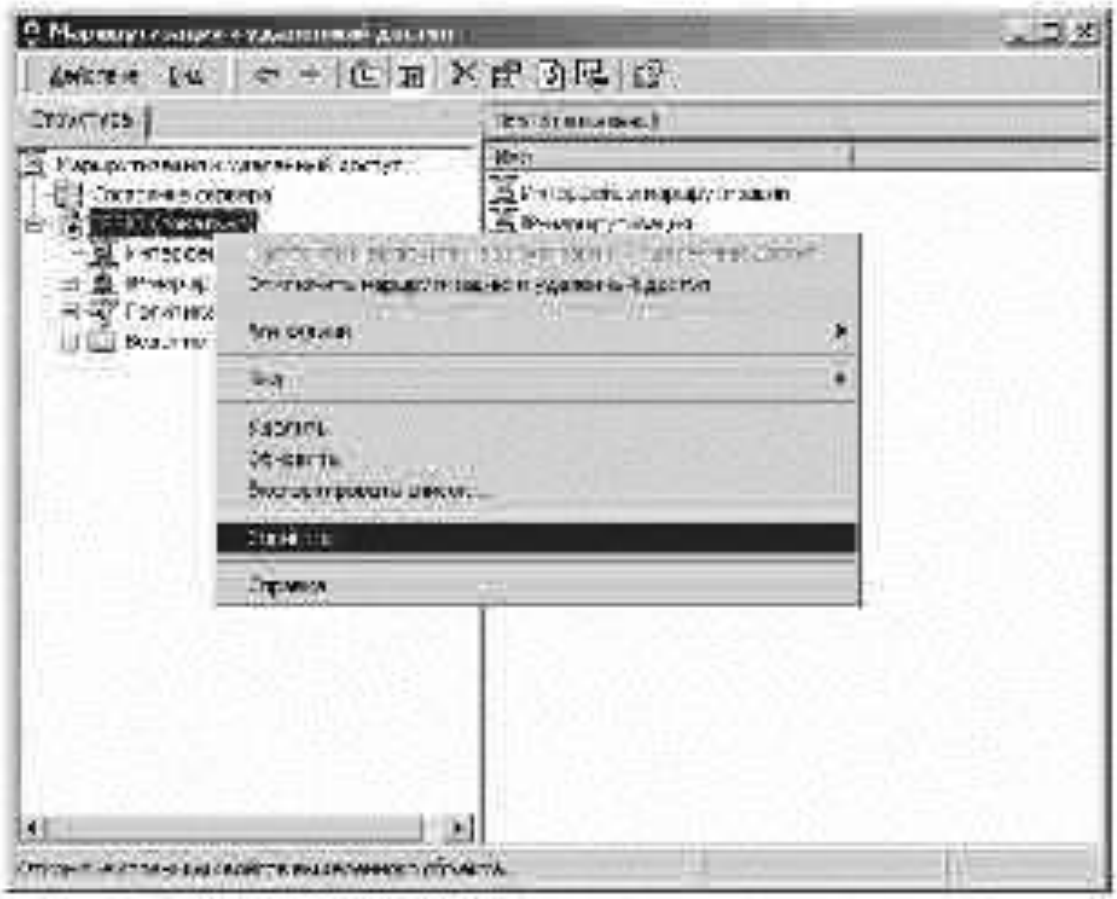


Рисунок 1.10. Маршрутизація і віддалений доступ

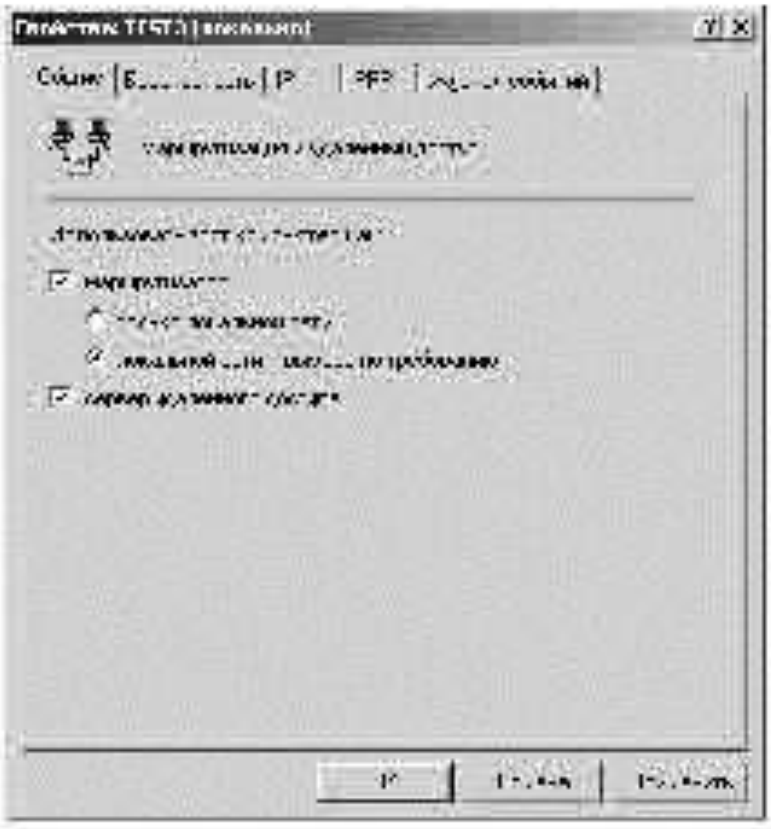


Рисунок 1.11. Загальні налаштування маршрутизації і віддаленого сервера

Після даних налашгувань зайти у вкладку "IP" (рис. 1.12) та вибрати назву внутрішнього адаптеру, а також створити статичний пул адрес, який буде присвоюватися VPN-клієнтам (рис. 1.13).

Рисунок 1.12. Вибір статичного пулу адрес

Рисунок 1.13. Встановлення діапазону IP-адрес

Після даних налашгувань треба включити ведення журналу подій у вкладці «Журнал событий» та зняти позначку з пункту «Многоканальные подключения», що прискорить роботу мережі.

Другим етапом налаштувань VPN-серверу буде конфігурація портів (рис. 1.14). Для цього необхідно зайти у властивості серверу, на вкладку "Порты" (рис. 1.15).

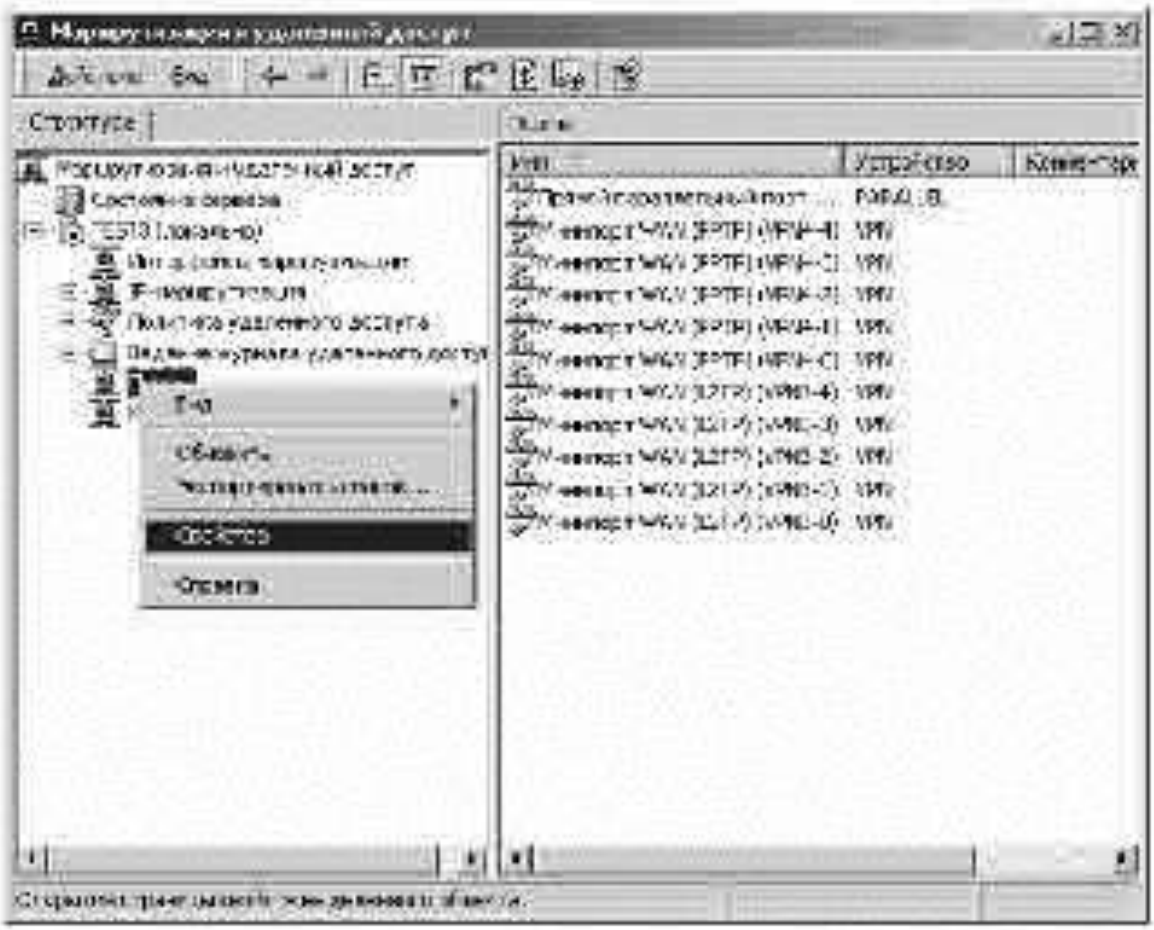


Рисунок 1.14. Вікно конфігурації портів

За замовчуванням RRAS створить 5 "PPTP", 5 "L2TP" і 1 "Прямой параллельный" порти. Для стабільної роботи сервера рекомендується видалити непотрібні порти і створити необхідну кількість портів, яких повинно бути більше ніж одночасних підключень.

Наступним кроком має бути видалення внутрішнього інтерфейсу з «IP-маршрутизация» / «NAT-преобразование сетевых адресов» (рис. 3.7), якщо необхідно надавати доступ тільки по VPN-з'єднанню. В разі використання ОС Windows Server необхідно зайти у властивості зовнішнього підключення і відключити basic firewall. Його використання при наявності утиліти Traffic Inspector може призвести до конфліктів.

Рисунок 1.15. Налаштування портів

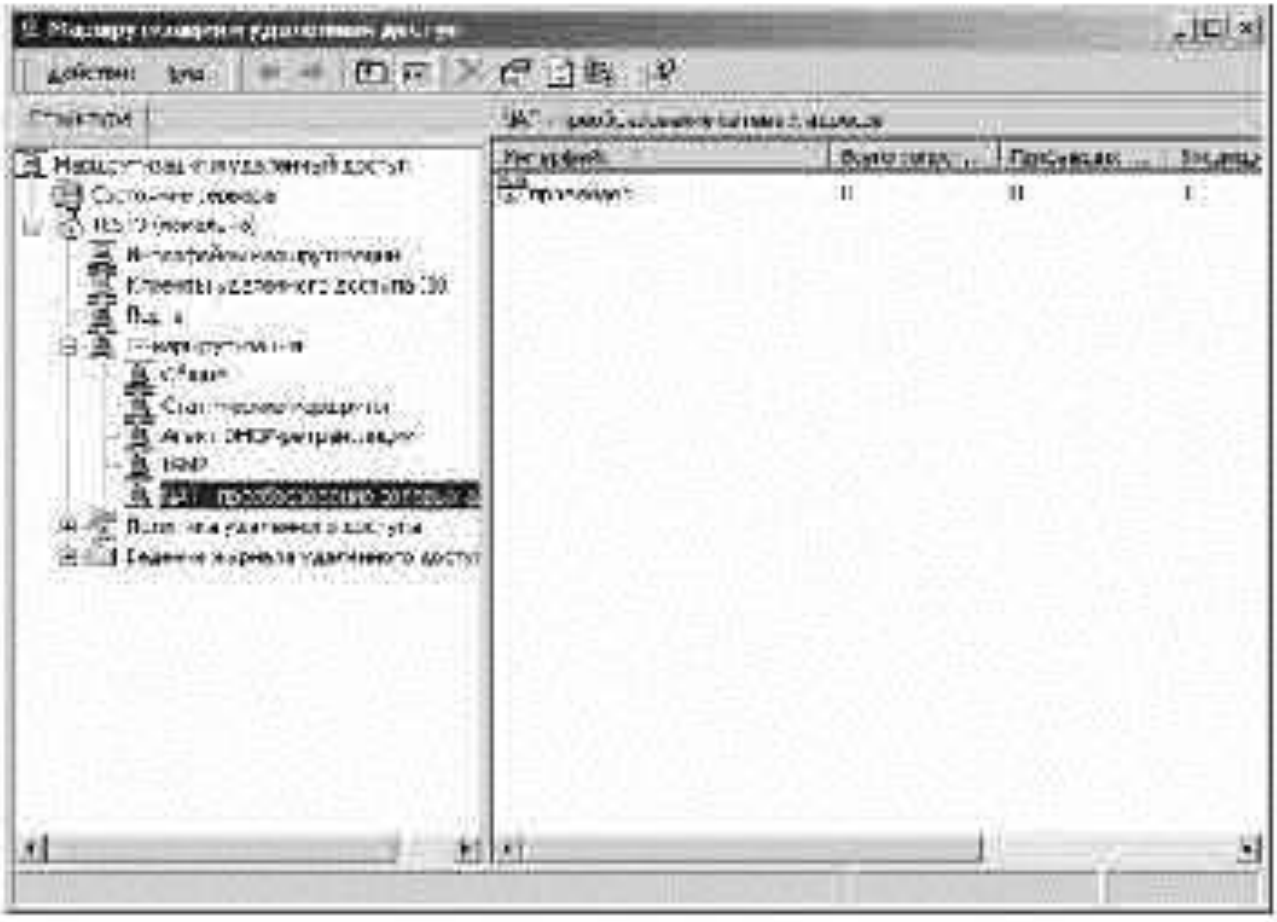


Рисунок 1.16. Налаштування інтерфейсів та NAT

Рисунок 1.17. Налаштування властивостей користувача

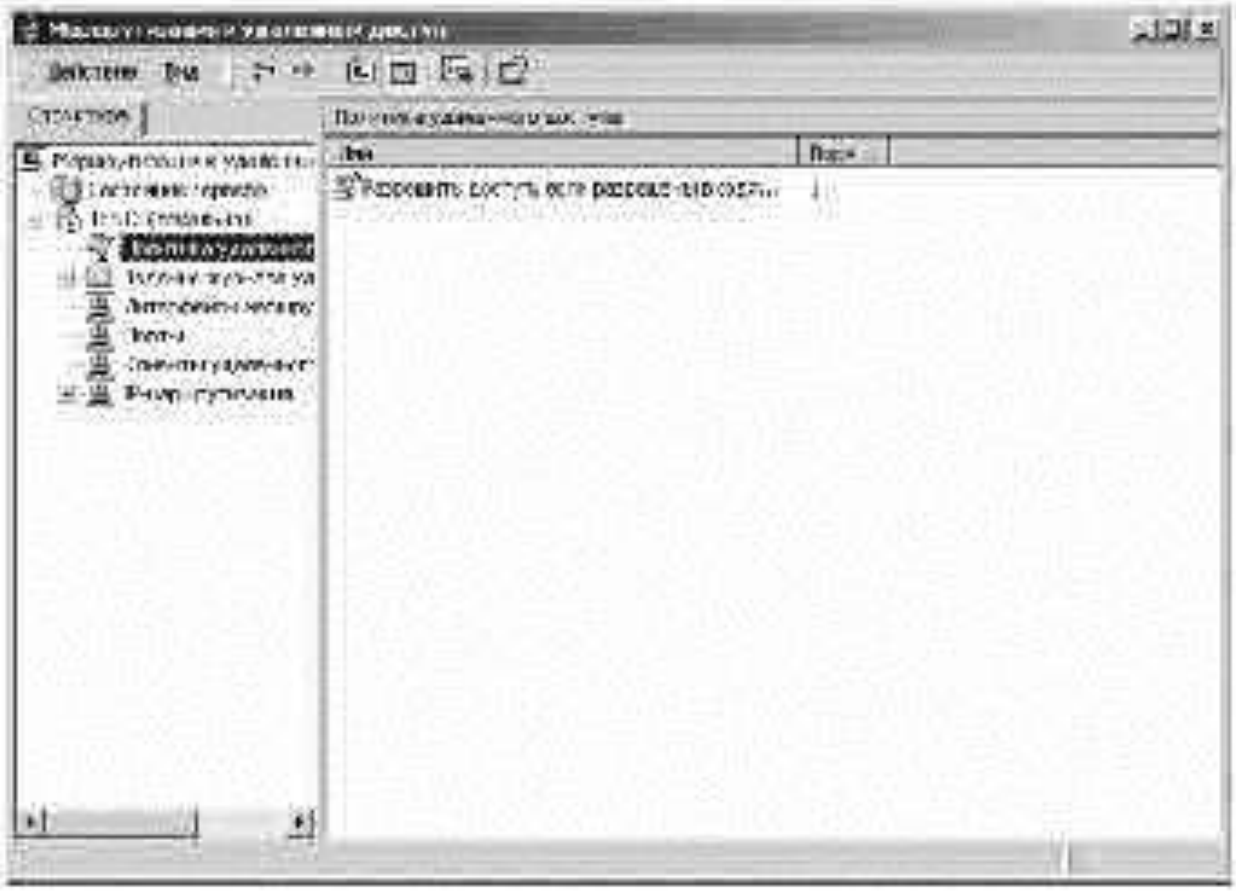


Рисунок 1.18. Дозвіл вхідного підключення

Після даних налаштувань слід створити клієнтів VPN-мережі. Для цього потрібно зайти в "Управление компьютером", далі в "Локальные пользователи и группы", "Пользователи" та створити користувача. Далі необхідно зайти у вкладку "Входящие звонки" (рис. 1.17).

Далі потрібно провести налаштування властивостей VPN-з'єднання. Для цього у групі "Политика удалённого доступа" треба зайти у властивості "Разрешить доступ, если разрешены входящие подключения" (рис. 1.18). Потрібно натиснути на кнопку "Изменить профиль" (рис. 1.19).

Рисунок 1.19. Налаштування прав віддаленого доступу

Потім потрібно зайти у вкладку "Проверка аутентичности" і залишити два параметри перевірки автентичності MS-CHAP v2 для ОС Windows і CHAP для інших ОС. Далі у вкладці "Шифрование" (рис. 1.20) потрібно вибрати параметри шифрування. Всі виконані налаштування повинні бути ідентичні при налаштуванні VPN-з'єднання у клієнтів.

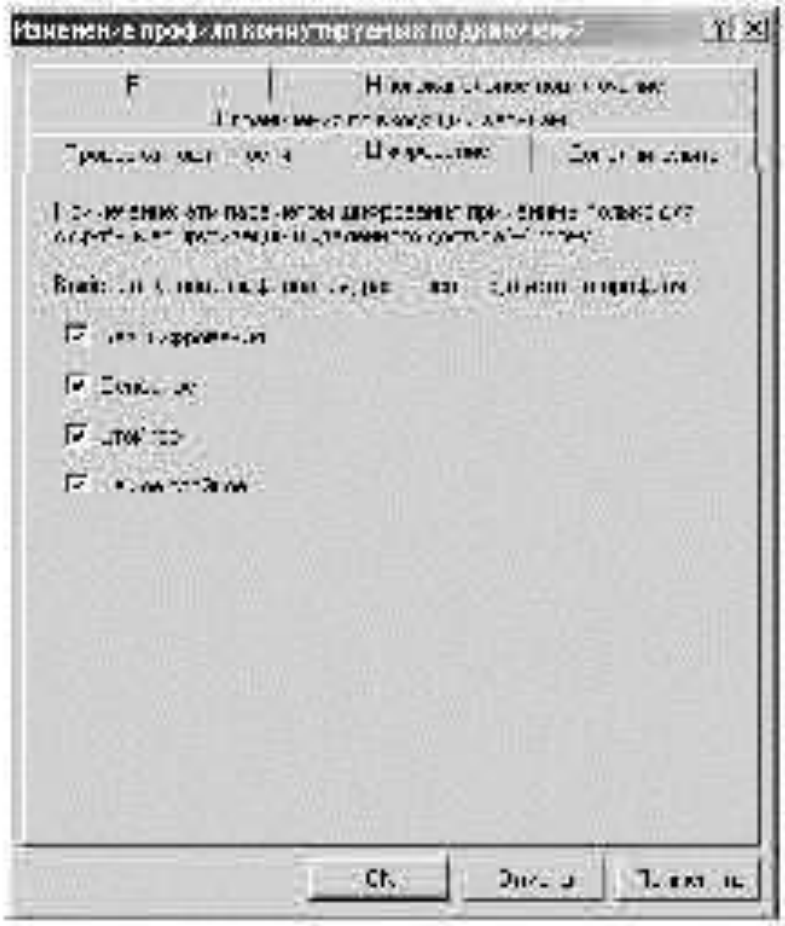


Рисунок 1.20. Налаштування VPN-шифрування

Після цього треба налаштувати клієнтську частину. Тобто, на кожному приладі, який буде підключатися до створеного VPN-з'єднання, необхідно ввести доменну або IP-адресу сервера та логін і пароль користувача, який має право доступу до цього серверу. Після авторизації та автентифікації користувач може безпечно користуватися захищеним каналом VPN.

Таким чином, для налаштування VPN-з'єднання були використані стандартні, вбудовані в операційну систему служби і додатки, призначені для вирішення задач, таких як "Маршрутизація та віддалений доступ", "NAT-перетворення мережеих адрес", "Керування комп'ютером", "Політика віддаленого доступу" та інші. У якості протоколу тунелювання був вибраний PPTP, який використовує існуючі відкриті стандарти TCP/IP, дозволяє взаємодіяти з існуючими мережеими інфраструктурами і не завдавати шкоди власній системі безпеки.

1.4 Дослідження надійності шифрування у протоколі PPTP

Тунельний протокол типу PPTP встановлює захищене з'єднання з сервером за рахунок шифрування PPE (Point-to-Point Encryption), створеного компанією Microsoft. Шифрування даних, що використовується в цьому протоколі відповідає алгоритму RC4 (Rivest cipher 4). Даний шифр є симетричним. Це означає, що ключ шифрування і розшифрування є однаковим. Потокові алгоритми шифрування послідовно обробляють текст повідомлення. Ідеальним варіантом з точки зору стійкості для потокового шифру є розмір ключу, який можна зіставити з розміром шифрованих даних. Тоді кожен біт відкритого тексту об'єднується з відповідним бітом ключу за допомогою суми по модулю 2 (XOR), утворюючи зашифровану послідовність. Для розшифрування потрібно виконати ту ж операцію ще раз на приймаючій стороні.

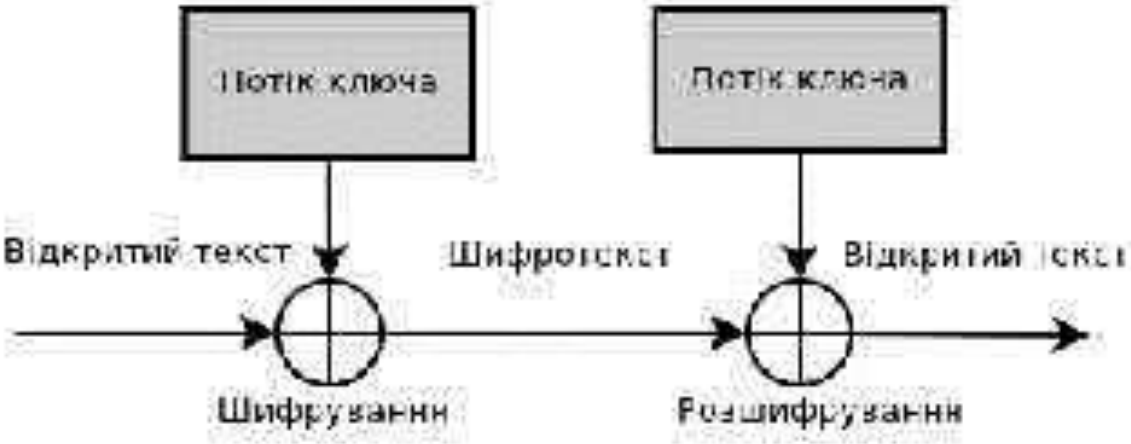


Рисунок 1.21. Схема шифрування-дешифрування RC4

При необхідності довжина ключу може бути задана у 32, 40, 56, 64, 72, 128 або 256 біт. Перелічені значення є вхідними даними для подальшого дослідження у даному розділі.

1.4.1 Умови перехоплення трафіку шляхом атаки MITM на абонента мережі VPN

При проведенні технічного аудиту віртуальних приватних з'єднань спеціалісти з комп'ютерної безпеки використовують різні способи – від соціальної інженерії та методів стеження, до цілого переліку кібератак.

Наприклад, при експлуатації вразливостей операційних систем і програмного забезпечення найпоширенішою атакою є так звана атака «людина посередині» MITM (Man in the midle). Це ситуація, коли крипто-аналітик здатний перехоплювати мережевий трафік, виступаючи посередником зв'язку.

Рисунок 1.2.2. Атака «людина посередині» MITM (Man in the midle)

Атака починається з прослуховування каналу зв'язку у публічному місці або біля офісу компанії та закінчується тим, що крипто-аналітик намагається підмінити перехоплене повідомлення, витягти з нього корисну інформацію або перенаправити його на який-небудь зовнішній ресурс. Такий вид втручання у мережу неможливо виявити і тому є дуже дієвим.

Зазвичай перехоплений трафік – це дамп пам'яті маршрутизатора або комп'ютера, за яким працює жертва. Він виглядає як файл формату [назва файлу. PCAPNG] і містить данні у шістнадцятковому вигляді. Використовується для зберігання даних, отриманих з мережі за допомогою мережевого інтерфейсу Wireshark, яким був здобутий цей файл.

Якщо трафік, що перехоплюється, переданий VPN-каналом, то цей файл буде зашифрований тим алгоритмом шифрування, який вказаний у налаштуваннях VPN-сервера. У випадку, який досліджується – це 7 файлів, які містять однакову інформацію і зашифровані алгоритмом RC4 (Rivest cipher 4).

Кожен файл має свій ключ шифрування конкретної довжини 32,40,56,64,72,128 та 256 біт.

1.4.2 Технічні умови проведення експерименту

Для досліджуваної інфраструктури був використаний сервіс хмарних обчислень Caspio (PaaS Provider).

Операційна система, на якій проводився експеримент – Kali Linux. Дана версія ОС є дистрибутивом типу Debian Linux, призначеним для цифрової криміналістики і тестування на проникнення.

Методи, якими було виконано підбір ключа шифрування:

1. Програма для підбору прямим перебором ARCFOURdecrypt, яка виконує обчислення на відеокарті (GPU) та (або) на процесорі (CPU);

2. Програма підбору Rainbowcrpt, у якій підбір ключа здійснюється за допомогою словників або Райдужних таблиць (Rainbow tables). Таблиці – це особливий тип словника, який містить список паролів і дозволяє підібрати пароль протягом меншого часу з ймовірністю 85-99%.

1.4.3 Результати експерименту та їх аналіз

У цьому розділі визначено залежність часу підбору ключа шифрування RC4 від його довжини. З метою отримання об'єктивних результатів тестування виконувалось наступним чином. Для кожного методу, яким було проведено підбір ключа, виконано 2 раунди підбору.

Для методу прямого перебору ключів перший раунд шифрування виконувався обчислювальними засобами процесора (CPU), а другий – обчислювальними засобами відеокарти (GPU). Підбір ключа шифрування за допомогою словника ключів шифрування Райдужних таблиць (Rainbow tables) не дає точної гарантії підбору, тому деякі значення були упущені. В результаті побудовано дві таблиці замірів часу для кожного методу підбору ключа з усіма необхідними показниками (табл. 1.2, табл. 1.3). У таблицях вказані також використовувані при виконанні досліджень апаратні засоби (центральний процесор на графічний процесор).

Таблиця 1.2. Підбір ключу шифрування за методом прямого перебору

Розрядність ключу	Перший раунд (на центральному процесорі Core i7-6700K), годин	Другий раунд (на графічному процесорі NVIDIA GTX1060), годин	Усереднений час підбору, годин
256 біт	-	-	-
128 біт	68,4	69,1	68,75
72 біт	33,8	34,0	33,94
64 біт	22,8	21,2	23,9
56 біт	11,3	10,4	10,8
40 біт	5,6	3,9	4,75
32 біт	3,7	1,9	2,8

Таблиця 1.3. Підбір ключу шифрування за допомогою Райдужних таблиць

Розрядність ключу	Перший раунд (на центральному процесорі Core i7-6700K), годин	Другий раунд (на центральному процесорі Core i7-6700K), годин	Усереднений час підбору, годин
256 біт	79,1	82,3	80,7
128 біт	58,2	-	58,2
72 біт	28,6	29,8	29,2
64 біт	18,8	19,5	19,15
56 біт	-	9,4	9,4
40 біт	4,7	3,8	4,25
32 біт	0,43	0,95	0,69

Аналізуючи таблиці можна побачити, що є пряма залежність часу підбору ключа шифрування від довжини цього ключа. Чим більша довжина ключа шифрування, тим довше виконується його підбір.

Для будь-якої криптографічної системи завжди існує поняття цінності інформації.

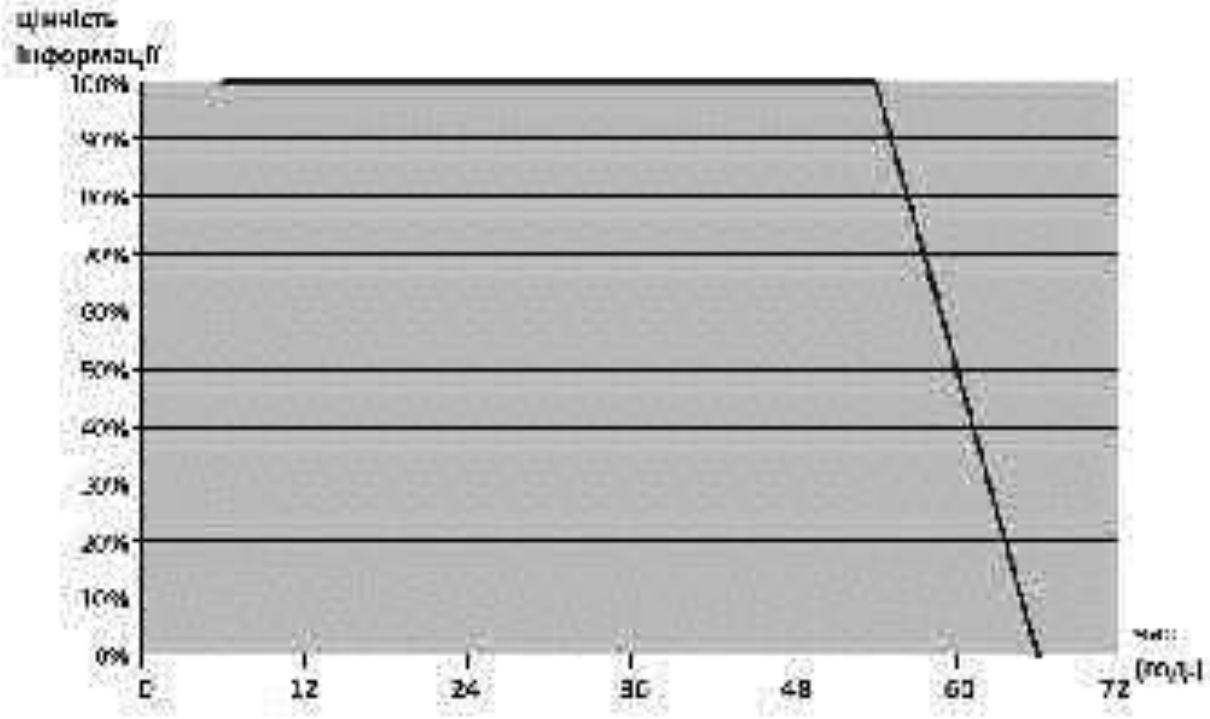


Рисунок 1.23. Графік цінності інформації від часу

Наведений графік ілюструє залежність цінності добутої інформації від часу у даному експерименті. Він показує, що для криптоаналітика після проходження певного часу інформація втрачає свою цінність. Тому, для підвищення надійності передачі даних по каналах VPN з використанням PPTP слід використовувати найбільшу з можливих довжину ключа шифрування, яку будуть підтримувати усі пристрої у мережі.

2 ОХОРОНА ПРАЦІ

2.1 Вступ

Відповідно до Конституції України, громадянам забезпечується рівноправність у області праці, незалежно від національності і раси.

Умови праці впливають на здоров'я, працездатність і всебічний розвиток особи трудящого. Узагальнюючи приведені вище положення, можна зробити висновок, що чим вища культура виробництва, тим краще умови праці, а отже, забезпечуються здоров'я і безпека працівників.

Робоче місце користувача послуг апаратно-програмного комплексу комп'ютерного зору складається з персонального комп'ютеру з програмним забезпеченням та може бути організовано в спеціалізованих закладах нагляду за станом дорожнього руху.

Тому для нього застосовуються звичайні вимоги до організації робочого місця користувача персонального комп'ютеру.

2.2 Коротка характеристика і основні вимоги безпеки до мікроклімату виробничих приміщень, освітлення, шуму, вібрації, ультразвуку, інфразвуку, виробничих випромінювань, небезпека ураження електричним струмом

Під час роботи на робочому місці користувача ПК виникають небезпечні та шкідливі фактори:

- підвищений рівень шуму;
- несприятливі мікрокліматичні умови;
- недостатній рівень освітленості приміщення та робочого місця;
- підвищений рівень електромагнітних випромінювань радіочастот;
- висока напруга електричної мережі;
- статична електрика та інші.

Робота з ПК супроводжується також підвищеним ступенем напруженості трудового процесу. При систематичному впливі виробничих факторів, які не

відповідають нормативним показникам, зростає рівень професійно зумовленої захворюваності працюючих та можуть виникнути професійні захворювання органів зору, ружу, нервової системи. Таким чином, вивчення умов праці на робочому місці користувача ПК є необхідною умовою запобігання негативних наслідків впливу небезпечних та шкідливих факторів.

Головним завданням будь-якої галузі промисловості є збільшення продуктивності праці. Разом з тим, людина що працює, проводить на виробництві значну частину свого життя. Тому для її нормальної життєдіяльності в умовах виробництва треба створити санітарні умови, які б дали змогу їй плідно працювати не перевтомлюючись та зберігати своє здоров'я. Для цього треба, щоб енергетичні витрати при праці компенсувалися відпочинком та умовами оточуючого середовища. Ці умови створюються забезпеченням для працюючого:

1) зручного робочого місця;
2) чистого повітря;
3) нормованої освітленості;
4) захисту від шуму та вібрацій;
5) захисту від дії шкідливих речовин та випромінювань;
6) робочим одягом та різними засобами індивідуального захисту;
7) побутовими приміщеннями та спеціальними службами, що призначені
8) створювати безпечні та нормальні умови праці.

2.2.1 Мікроклімат виробничих приміщень

Основні нормативні документи, де наводяться норми мікроклімату – це санітарні норми та стандарти безпеки праці. Виробничий мікроклімат характеризується температурою й вологістю повітря, швидкістю його руху, а також інтенсивністю радіації і повинен відповідати ГОСТ 12.1.005-88 і СНиП 2.04.05-86.

Оптимальні значення параметру мікроклімату повинно становити: температуру повітря від 18-22 градусів Цельсію, вологість повітря від 40%-60%, та швидкість повітря від 0,1-0,2 м/с.

Для підтримки в приміщеннях нормального, що відповідає гігієнічним вимогам складу повітря, видалення з нього шкідливих газів, пару і пилу використають вентиляцію. В приміщеннях з ПК це змішана вентиляція – природна та механічна.

У приміщеннях, де відбувається робота програміста вимоги до параметрів мікроклімату в цілому виконанні.

2.2.2 Освітлення виробничих приміщень

Для освітлення приміщення, у якому працює користувач ПК, використовується змішане освітлення, тобто сполучення природного й штучного освітлення. Природне освітлення - здійснюється через вікна в зовнішніх стінах будинку. Штучне освітлення - використовується при недостатньому природному освітленні й здійснюється за допомогою двох систем: загального й місцевого освітлення. Для загального освітлення приміщення, використовуються газорозрядні лампи типу ЛД.

Значення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500лк.

2.2.3 Заходи щодо захисту від дії шуму та вібрації

У робочих приміщеннях основними джерелами акустичних шумів є шуми ПЕОМ. ЕОМ є також джерелами шумів електромагнітного походження (коливання елементів електромеханічних пристроїв під впливом змінних магнітних полів). Систематичний шум може викликати стомлення слуху й ослаблення звукового сприйняття, а також значне стомлення всього організму.

Зниження рівня шуму у приміщенні можна здійснити наступними методами:

- використанням блоків живлення ПК з вентиляторами на гумових підвісках;
- облицювання стелі і стін звукопоглинаючим матеріалом;
- екранування робочого місця (постановкою перегородок, діафрагм);
- раціональне планування приміщення.

2.2.4 Безпека праці

Обладнання і організація робочого місця з ВДТ мають забезпечувати відповідність конструкцій всіх елементів робочого місця та їх взаємного розташування ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності (ГОСТ 12.2.032-78, ГОСТ 22269-76, ГОСТ 21.889-76). Конструкція робочого місця й взаємне розташування всіх його елементів (сидіння, органи керування, засобу відображення інформації) відповідають антропометричним, фізіологічним і психологічним вимогам, а також характеру роботи. Конструкція робочих меблів повинна забезпечувати можливість індивідуального регулювання відповідно росту працюючих для підтримки зручної пози. Робочий стіл повинен бути пофарбований матовою фарбою. Дисплей розташований так, що його верхній край перебуває на рівні очей на відстані близько 70 см, що укладається в у припустимі рамки від 60 до 90 см. Частота мерехтіння екрана $f_{мер}$=100 Гц, що відповідає умові $f_{мер}$>70 Гц.

Робоче місце розташоване перпендикулярно віконним прорізам, це зроблено з тією метою, щоб виключити пряму й відбиту мерехтливість екрана від вікон і приладів штучного освітлення, якими є лампи накалювання. Обладнання і організація робочого місця з ВДТ мають забезпечувати відповідність конструкцій всіх елементів робочого місця та їх взаємного розташування, ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності згідно правил охорони праці під час експлуатації ЕОМ.

2.2.5 Ультразвук

Ультразвук - це коливання пружного середовища з частотою понад 20 000 Гц.

Джерелами ультразвуку можуть бути різні акустичні перетворювачі, найпоширеніший з них - магнітострикційний перетворювач, що працює від змінного струму і генерує механічні коливання з частотою понад 20 кГц.

В розроблюваному дипломному проекті не використовується.

2.2.6 Інфразвук

Основними джерелами інфразвуку на виробництві є тихохідні масивні установки та механізми (вентилятори, поршневі компресори, турбіни, електроприводи та ін.), що здійснюють обертові та зворотно-поступальні рухи з повторенням циклу менше, ніж 20 разів за секунду (інфразвук механічного походження). Інфразвук аеродинамічного походження виникає при турбулентних процесах у потоках газів чи рідин.

В розроблюваному дипломному проекті не використовується.

2.2.7 Виробничі випромінювання

У виробничих умовах випромінювання можуть бути небезпечним чи шкідливим виробничим чинником. Оптимальним рівнем аероіонізації у зоні дихання користувача вважається вміст легких аерофонів обох знаків від 150 до 5000 у 1 $см^3$ повітря.

Нормалізуючий вплив на склад повітря робочої зони справляють примусова вентиляція, захисні екрани (оснащені заземленням) та застосування іонізаторів.

2.2.8 Електробезпека

Приміщення, де використовуються імпульсні джерела живлення відповідно до ОНТП24-86 і ПУЕ-87 відноситься до класу приміщень без підвищеної небезпеки поразки персоналу електричним струмом, оскільки відносна вологість повітря не перевищує 75%, температура не більш 35°С, відсутні хімічно агресивні середовища. Живлення електроприладів усередині приміщення здійснюється від двухфазної мережі з заземленою нейтралю напругою 220 В і частотою 50 Гц із використанням автоматів токового захисту. У приміщенні повинна бути застосована схема заземлення.

Ураження людини електричним струмом може відбутися у випадку:

1. дотику до відкритих струмоведучих частин;
2. у результаті дотику до струмопровідних не струмоведучих елементів устаткування, що опинилися під напругою в результаті порушення ізоляції або з інших причин.

Заземлення повинно бути зроблено за допомогою гнучкого спіненого мідного проводу діаметром порядку 1,5 мм2. Для зменшення значень напруг дотику і відповідних їм величин струмів, при нормальному й аварійному режимах роботи устаткування необхідно виконати повторне захисне заземлення нульового проводу. Відповідно до ГОСТ-12.2.007.0-75 все устаткування (крім ЕОМ - II клас) відноситься до I класу, воно має робочу ізоляцію відповідно до вимог ГОСТ 12.1.009-76. Підключення устаткування виконане відповідно до вимог ПБЕ та ПУЕ. Додаткових заходів по електробезпечності не потрібно.

2.3 Пожежна безпека

Пожежна безпека – стан об'єкта, при якому з регламентованою ймовірністю виключається можливість виникнення та розвитку пожежі і впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей.

За стан пожежної безпеки на підприємстві відповідають її керівники, начальники цехів, майстри та інші керівники. Можливими причинами виникнення пожежі в приміщенні є:

1) коротке замикання проводки;

2) користування побутовими електрорадіоприладами.

3) не дотримання умов протипожежної безпеки.

Для гасіння пожеж на робочому місці використовують вуглекислотні та порошкові вогнегасники.

Наявність первинних засобів пожежегасіння і вогнегасників, їхня кількість і зміст відповідає вимогам ГОСТ 12.4.009-75 і ISO3941-77.

У приміщенні виконуються усі вимоги по пожежній безпеці відповідно до вимог НАПБ А.0.001-95 "Правила пожежної безпеки в Україні". У приміщенні також вивішується план евакуації на випадок виникнення пожежі.

ВИСНОВКИ

У кваліфікаційній роботі був виконаний аналіз побудови захищеного доступу до мережі, розглянуто загальну технологію організації VPN-підключення до мережі передачі даних, побудову розподільної мережі та віддалений доступ до неї. При розробці і практичній реалізації VPN-серверу були розглянуті технології побудови захищених каналів та мереж та вибраний найоптимальніший спосіб реалізації відповідно до наведених у технічному завданні та вимог.

У якості серверної операційної системи була обрана ОС фірми Microsoft Windows Server 2016, яка найкраще пристосована до роботи у мережі, де використовуються клієнтські операційні системи сімейства Windows та Kali Linux, яка використовувалась при проведенні експерименту з визначення надійності шифрування у протоколі PPTP. Для налаштування VPN-з'єднання були використані вбудовані у ОС служби та додатки, що дозволило забезпечити необхідний рівень безпеки, надійності та економічної доцільності.

У якості протоколу тунелювання був обраний PPTP, який використовує існуючі відкриті стандарти TCP/IP та дозволяє компаніям взаємодіяти з існуючими мережевими інфраструктурами не завдавчи шкоди власній системі безпеки.

Результатом роботи є дані дослідження залежності часу підбору ключа шифрування RC4 у протоколі PPTP від його довжини. З результатів експерименту випливає, що для підвищення надійності передачі даних по каналах VPN з використанням PPTP слід використовувати найбільшу з можливих довжину ключа шифрування. В результаті дослідження систематизовано знання існуючих технологій VPN по рівнях мережевої моделі OSI та по завданнях, які вони виконують.

Предметом подальших досліджень може бути перевірка VPN-протоколів на стійкість до криптографічних атак та дослідження аналогічних протоколів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Васильков, А.В. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. – М.: Форум, НИЦ ИНФРА-М, 2013. – 368 с.
2. Васильков, А.В. Информационные системы и их безопасность: Учебное пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. – М.: Форум, 2013. – 528 с.
3. Дейтел, Х.М. Операционные системы. Распределённые системы, сети, безопасность / Х.М. Дейтел, Д.Р. Чофнес. – М.: Бином, 2013 – 704 с.
4. Ерохин, В.В. Безопасность информационных систем: учеб. пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. – М.: Флинта, 2016. – 184 с.
5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. – 416 с.
6. Хетч Б., Колесников О. Создание виртуальных частных сетей (VPN) – КУДИЦ-Образ, 2004.
7. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. / Учебник. – СПб: Питер, 2002.
8. Оголюк А., Щеглов А. Технологии построения системы защиты сложных информационных систем, Экономика и производство, №3, 2001.
9. Файльнер М. Виртуальные частные сети нового поколения LAN, № 11, 2005.
10. Медведев Н. Г. Аспекти інформаційної системи віртуальних приватних мереж / Н.Г. Медведев, Д.В. Москалик – К: Европ. ун-та, 2002.

ДОДАТОК А

Слайди мультимедійної презентації

Загальна схема інтернет-трафіку під час серфінгу у інтернет

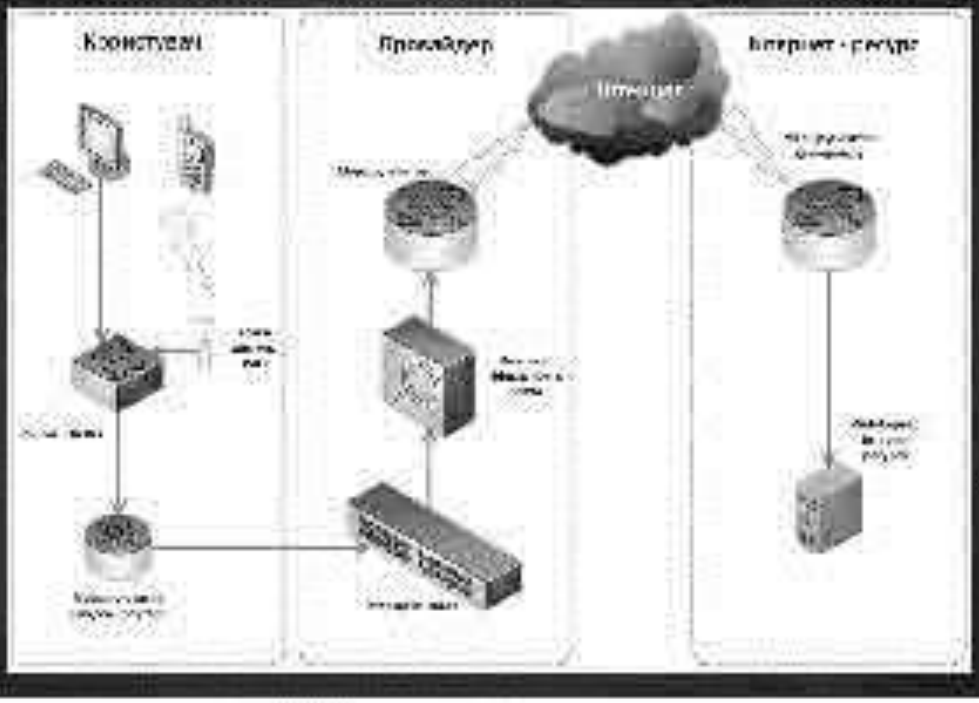
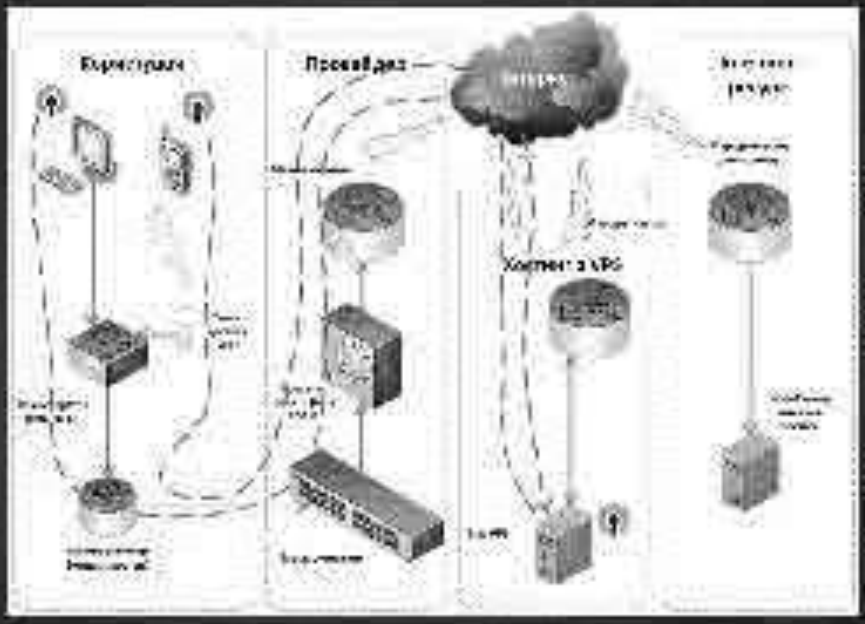
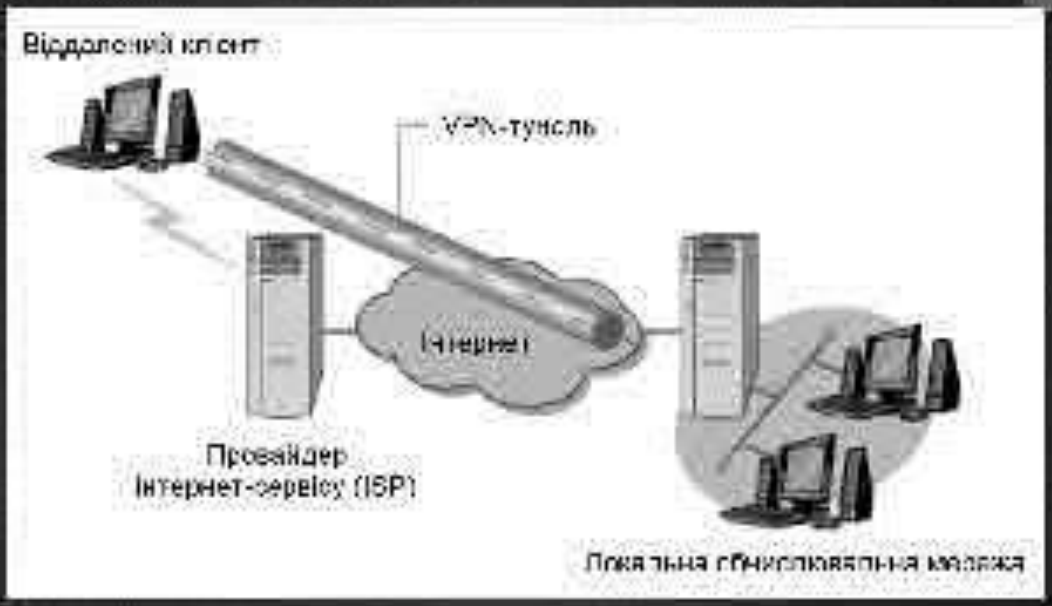


Схема інтернет-трафіку під час серфінгу у інтернет з використанням VPS

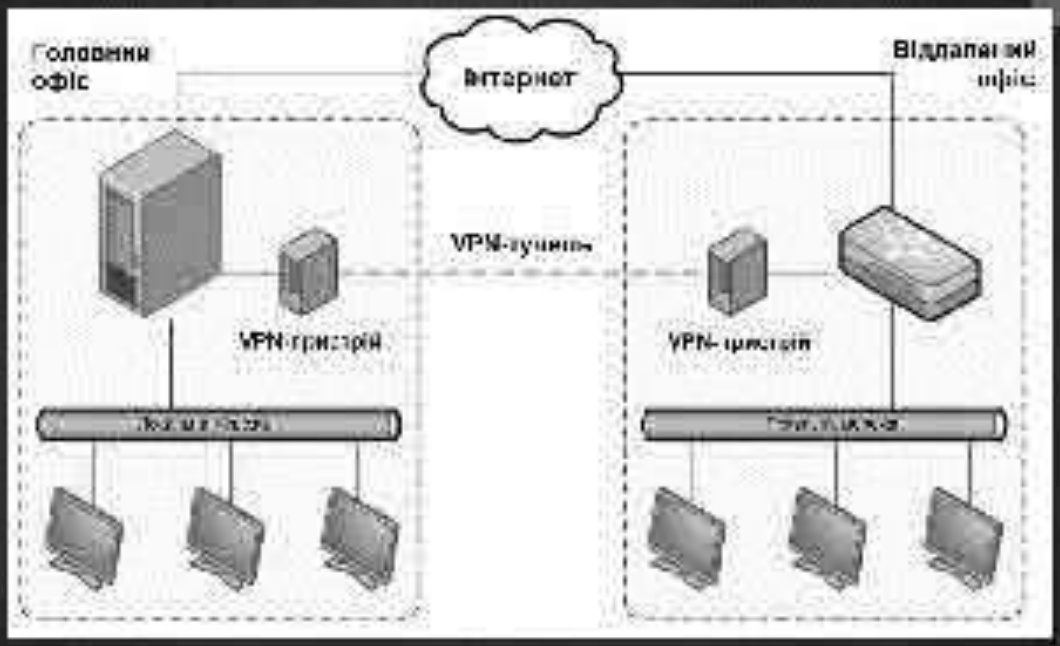


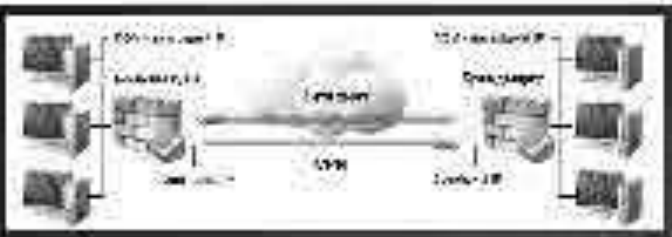
Загальна схема VPN-мережі для організацій

Організація VPN для віддаленого користувача

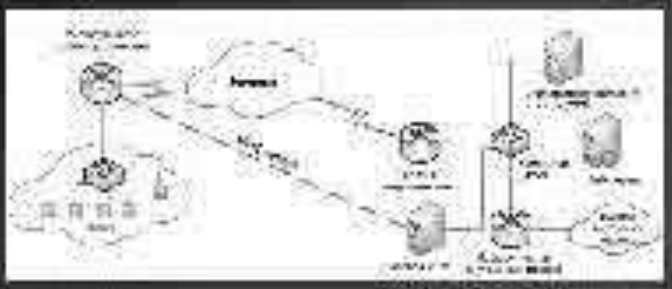


VPN на базі апаратних засобів





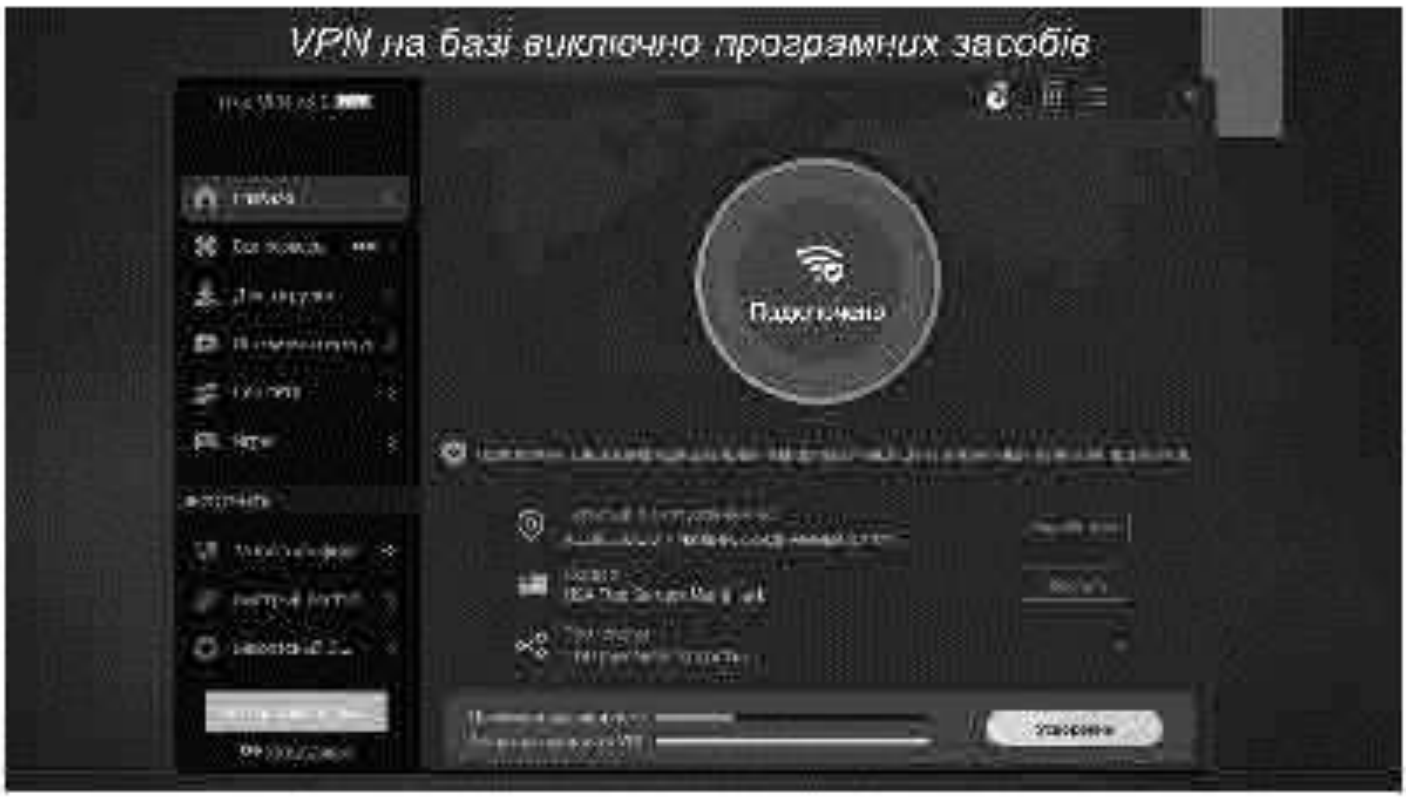
VPN на базі брандмауерів



VPN на базі маршрутизаторів

VPN на базі шлюзів

VPN на базі виключно програмних засобів



Транспортний режим IPsec

Тунельний режим IPsec

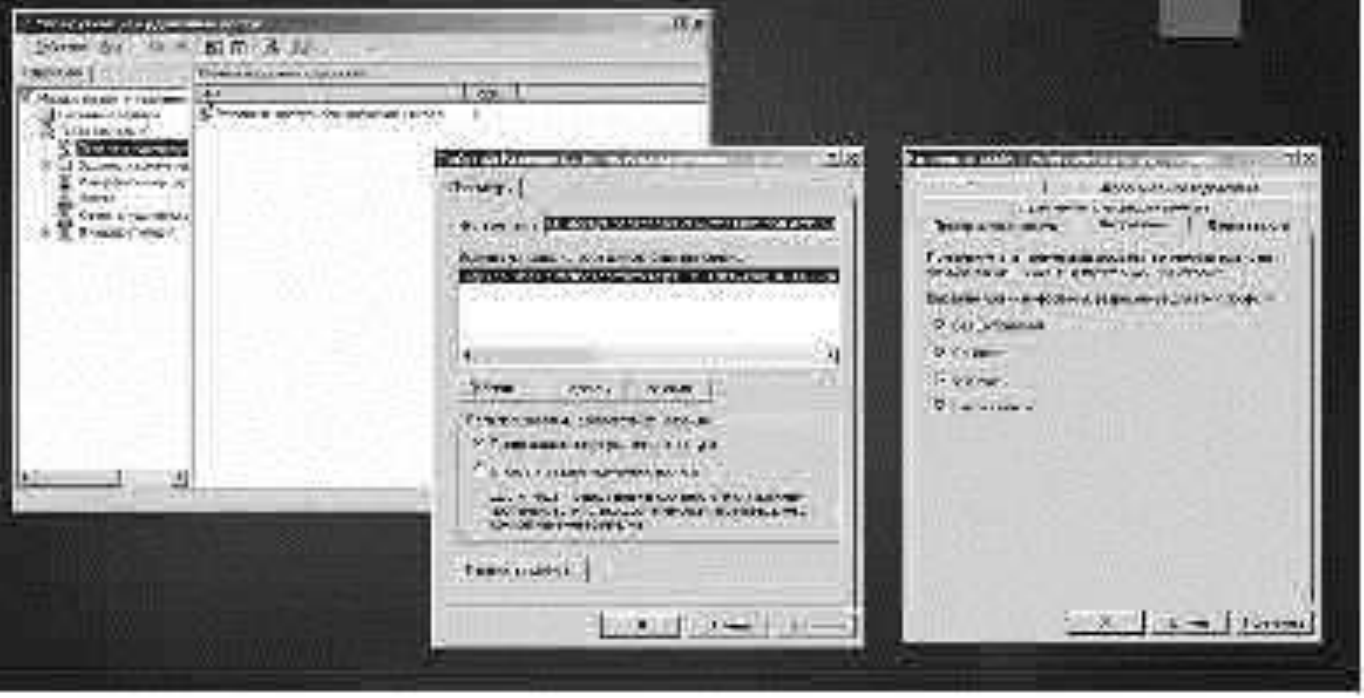
Порівняльна характеристика IPsec та SSL / TLS

Налаштування маршрутизації та віддаленого доступу

Конфігурація портів

Видалення внутрішнього інтерфейсу та створення кліснтів VPN-мережі

Налаштування властивостей VPN-з'єднання



Ілюстрація атаки MITM (Man in the middle)

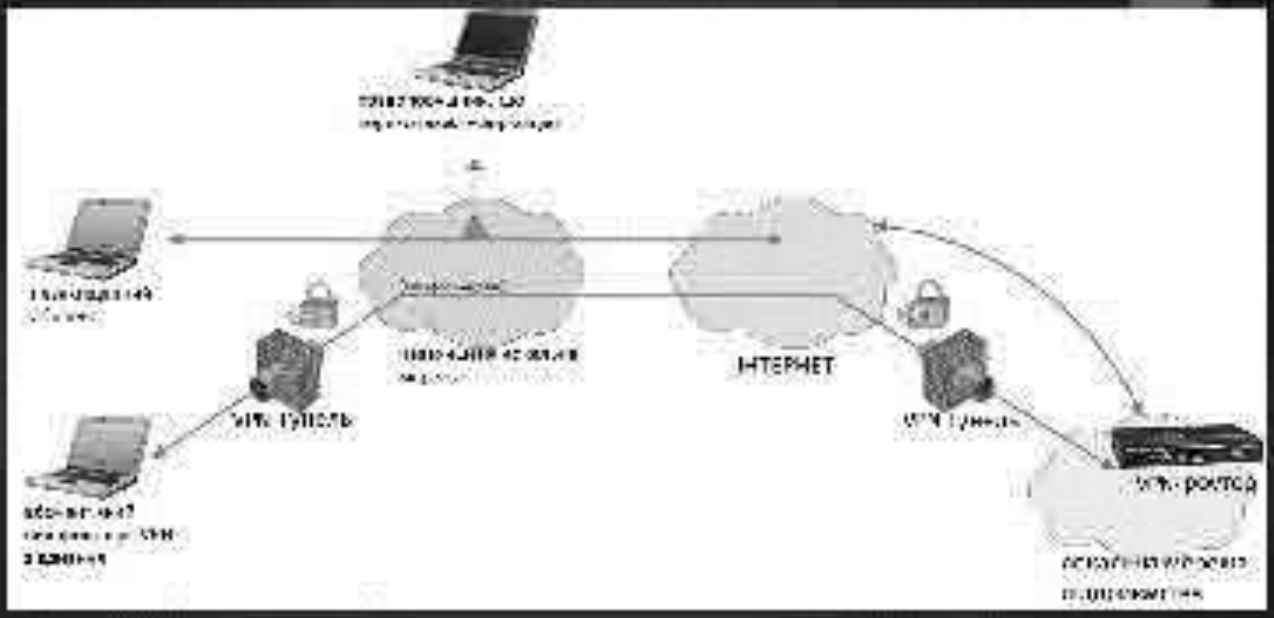
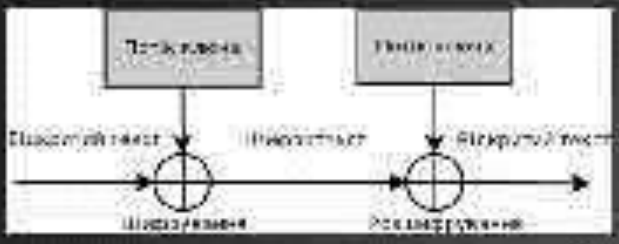
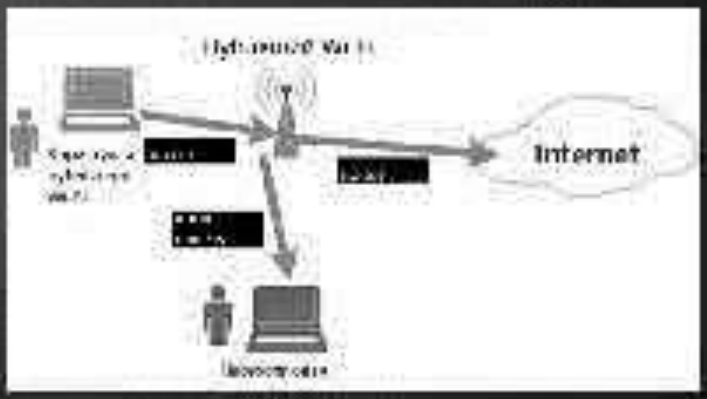


Схема шифрування-дешифрування пакетів даних за алгоритмом RC4





Результати підбору ключа шифрування прямим перебором

Розрядність ключу	Перший раунд (на одному процесорі Core i7-6700K) годин	Другий раунд (на графічному процесорі NVIDIA GTX1080) годин	Усереднений час підбору годин
32 біт	0,4	0,1	0,25
40 біт	28,4	7,1	17,75
64 біт	7284	1820	4552
80 біт	1 865	466	1165
128 біт	1	0,3	0,65
256 біт	5,2	1,3	2,25

Результати підбору ключа шифрування за допомогою Райдужних таблиць (Rainbow tables)

Довжина ключа	Перша версія (на центральному процесорі Core i7-870) годин	Друга версія (на центральному процесорі Core i7-870) годин	Усереднений час підбору, годин
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

Графік залежності цінності інформації від часу