

УДК 004.056

Нікулін О.Ф., д.т.н.,
Укр НДІ ЦЗ;
Давидюк В.О.,
НТУУ «КПІ»

МЕТОДИКА ПОБУДОВИ ЗАХИЩЕНОЇ БАНКІВСЬКОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ІЗ ВИКОРИСТАННЯМ VPN

Проведено порівняльний аналіз протоколів побудови приватних віртуальних мереж, що дозволило обґрунтувати вибір оптимального рішення по створенню захищеної банківської мережі. Розроблено алгоритм побудови захищеної банківської мережі із використанням пакету OpenVPN.

Проведен сравнительный анализ протоколов построения частных виртуальных сетей, что позволило обосновать выбор оптимального решения по созданию защищенной банковской сети. Разработан алгоритм построения защищенной банковской сети с использованием пакета OpenVPN.

The paper included comparative analysis of protocols for constructing virtual private networks that allowed justify the choice of the optimal solution for creating secure banking network. An algorithm for constructing a secure banking network using packet OpenVPN was developed.

Вступ. Для забезпечення безпечного мережевого з'єднання з розподіленими підрозділами компанії організовується віртуальна приватна мережа (VirtualPrivateNetworks, VPN), яка використовує набір технологій, що гарантують секретність, захист і цілісність даних, що передаються по мережі спільного користування (Інтернет). Дане рішення є оптимальним в плані фінансових витрат і дозволяє забезпечити найбільш гнучкий спосіб доступу віддалених користувачів та офісних мереж до ресурсів корпоративної мережі. Перед адміністраторами віддаленого доступу і систем VPN постає складне завдання – підготувати і спроектувати таке рішення, яке дасть можливість одночасно задовольняти потреби різних користувачів корпоративної мережі підприємства. В даний час на ринку засобів організації віртуальних приватних мереж є безліч готових рішень і технологій, частково дублюючих один одного по виконуваних функціях. Виникає необхідність проведення аналізу протоколів, що застосовуються у віртуальних приватних мережах для вирішення завдання вибору оптимального рішення віддаленого доступу до внутрішніх ресурсів корпоративної мережі.

Аналіз досліджень і публікацій. У різних інформаційних джерелах наявні подібні порівняльні аналізи протоколів побудови приватних віртуальних мереж [1], але у даній роботі аналіз буде звужений до рамок використання технологій для таких мереж, які потребують підвищеного рівня безпеки та водночас легкого захищеного віддаленого доступу (наприклад, банківські мережі). В роботах [2-4] розглядаються основні принципи побудови VPN мереж. Використовуючи досвід зазначених робіт буде розроблено новий удосконалений алгоритм побудови захищеної банківської мережі.

Постановка завдання. Таким чином *метою* даної роботи є розробка методики побудови захищеної банківської телекомунікаційної мережі за допомогою технології VPN.

Для досягнення зазначеної мети поставлені наступні завдання:

1. Огляд наявних рішень, присутніх на ринку технологій VPN.
2. Вибір технології, яка максимально підходить під поставлену задачу.
3. Розробка алгоритму побудови та налаштування мережі, перевірка його працездатності.

Вихідні умови. Наявні дві локальні мережі, що входять до складу корпоративної мережі банку (рис.1). Перша мережа знаходиться у центральному офісі (192.168.1.0/24), інша у віддаленому офісі (192.168.2.0/24).

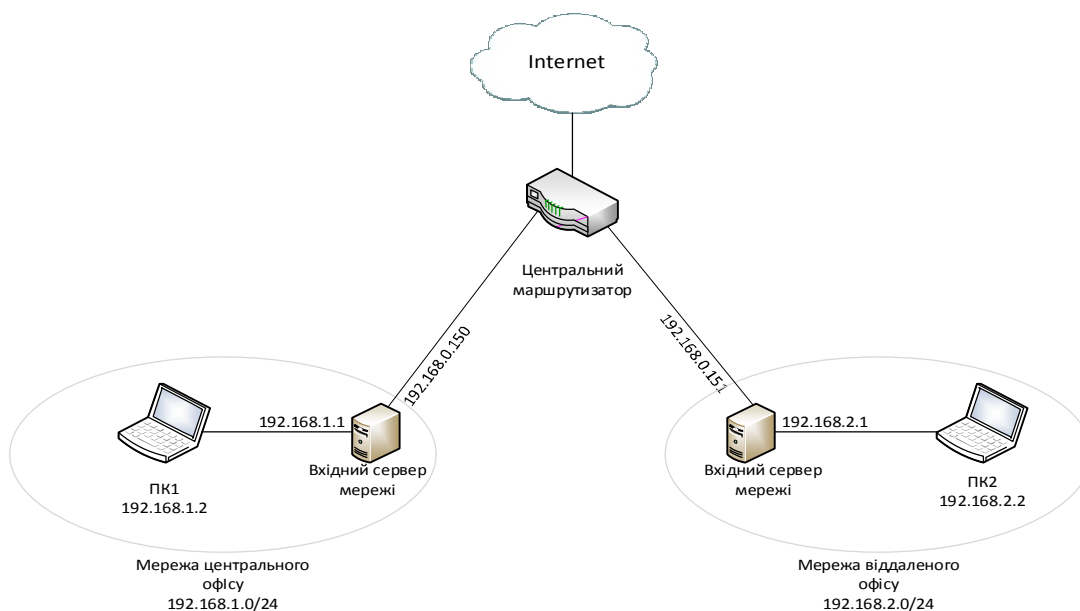


Рис. 1. Топологія мережі

На входах мереж стоять сервери під управлінням ОС WindowsXP. Обидві мережі через сервери сполучені з центральним маршрутизатором, який має доступ до Інтернет. Необхідно створити віртуальну приватну мережу, що забезпечує наступну політику маршрутизації між локальними

підмережами: з локальної підмережі центрального офісу доступні комп'ютери локальної підмережі філії, з локальної підмережі філії доступні комп'ютери локальної підмережі центрального офісу. Усі комп'ютери мережі повинні мати доступ до Інтернету, який здійснюється через центральний маршрутизатор.

Огляд наявних рішень.

IPSec. Дуже часто для побудови мереж VPN використовується технологія мережевого рівня IPSec – набір протоколів для забезпечення захисту даних, що передаються по протоколу IP. До функціоналу IPSec входять такі можливості: підтвердження достовірності (аутентифікація), перевірка цілісності та шифрування IP пакетів. IPSec також включає в себе протоколи обміну ключами в мережі Інтернет. Пакети даних шифруються по алгоритмам DES, AES та ін. Використання IPSec передбачає встановлення VPN-клієнта на термінал користувача і забезпечує доступ до ресурсів захищеної мережі так, ніби він знаходиться на своєму робочому місці в корпоративній мережі. Так, як технологія ґрунтується на мережах IP, досягається найбільша гнучкість в конфігурації мережевих налаштувань і додатків. Розглянемо яким саме чином протоколи IPSec змінюють IP-пакети задля досягнення цілей безпеки.

Аутентифікаційний заголовок (Authentication Header, AH) є додатковим заголовком пакету IP, що міститься між стандартним заголовком і полем даних. Метою введення AH є попередження несанкціонованої зміни змісту пакету та забезпечення цілісності віртуального з'єднання шляхом надійної аутентифікації джерела пакету. Заголовок ESP (Encapsulating Security Payload) може виконувати функції AH, а також додатково захищати пакет шляхом шифрування. Залежно від поставленої задачі, IPSec може функціонувати в транспортному або тунельному режимі.

Таким чином, на користувацькому рівні використання протоколів IPSec для побудови VPN має такі переваги:

- Використання прикладних додатків та клієнтів без будь-яких обмежень
- Прозорий доступ до файлів та мережевих ресурсів корпоративної мережі
- Використання обчислювальної потужності віддалених ПК
- Можливість користуватись усіми можливостями, що надаються протоколом IP (наприклад VoIP)

SSL. Протокол SSL (Secure Sockets Layer) – стандартний протокол передачі шифрованих даних, що забезпечує шифрування даних на відкритих ключах, що передаються по мережі. В загальному, принцип роботи SSL полягає в тому, що кожен користувач приватної мережі

отримує свій сертифікат, за допомогою якого автентифікується, і лише при наявності правильних сертифікатів сторони обмінюються зашифрованою інформацією, яка може бути однозначно зашифрована/дешифрована обома сторонами. Протокол набув широкого використання при передачі захищених даних через веб-браузери, електронну пошту, а також в корпоративних мережах. Перевагами SSL можна вважати:

- Необов'язковість встановлення спеціального клієнтського ПЗ: захищені SSL дані можна передавати через стандартний браузер.
- Широка підтримка операційних систем та браузерів.
- Легкий захищений доступ до ресурсів корпоративної мережі.
- Простота і надійність.

Крім переваг, VPN на основі SSL можуть мати такі недоліки:

- Прив'язаність SSL до веб-технологій.
- Обов'язкове використання зворотнього проху-сервера при використанні SSL для доступу до корпоративної мережі накладає певні обмеження на застосування передових веб-технологій, наприклад Flash, ActiveX і т.д.

PPTP (Point-to-Point Tunneling Protocol). Даний протокол був розроблений корпорацією Microsoft сумісно з іншими ІТ-компаніями (Ascend Communications, 3 Com/Primary Access та ін.). Принцип його роботи полягає в інкапсулюванні кадрів PPP у IP-пакети та передачі їх через захищений тунель у загальнодоступній мережі. Інкапсуляція відбувається таким чином: до кадру PPP додається заголовок GRE (General Routing Encapsulation – протокол інкапсуляції компанії Cisco), а також заголовок IP. Для безпеки інформації кадр PPP шифрується методами MS-CHAP, MS-CHAPv2 (реалізації протоколу CHAP від Microsoft) або EAP-TLS. PPTP має такі переваги:

- Простота налаштування і використання.
- Вбудована підтримка майже усіма сучасними операційними системами.
- Висока швидкість.

Значним недоліком протоколу є низький ступінь захищеності і застарілість.

Порівняння протоколів. Вище були розглянуті кілька популярних протоколів для побудови віртуальних приватних мереж (VPN). Зведемо дані у таблицю задля порівняння (табл.1). Критерії обрано як найбільш критичні для реалізації даної задачі.

Таблиця 1

Характеристики протоколів для побудови мереж VPN

	IPSec	SSL	PPTP
Ключ шифр-ня	128 біт	256 біт	128 біт
Рівень захищ-ті	Добре	Відмінно	Задовільно
Необхідність встановлення додаткового ПЗ	Так	Ні	Ні
Швидкодія	Добре	Добре	Відмінно
Вартість застосування	Невисока	Невисока/безкоштовно	Безкоштовно
Область застосування	Корпоративна мережа, спрощений віддалений доступ.	Передача висококонфіденційних даних через корпоративну мережу, віддалений доступ до мережі.	Передача неконфіденційних даних або при неможливості застосування інших протоколів

Таким чином, існує велика кількість рішень даного питання, які багато разів порівнювалися по співвідношеннях функціональності/надійності/вартості. В даному випадку буде запропоновано рішення на базі безкоштовного пакету OpenVPN, що використовує сертифікати для шифрування трафіку. OpenVPN дозволяє розгорнути гнучку конфігурацію і ґрунтується на технології SSL.

Таким чином, на сервер з ОС Windows, що знаходиться на вході підмережі центрального офісу буде проінстальовано сервер OpenVPN (рис.2).

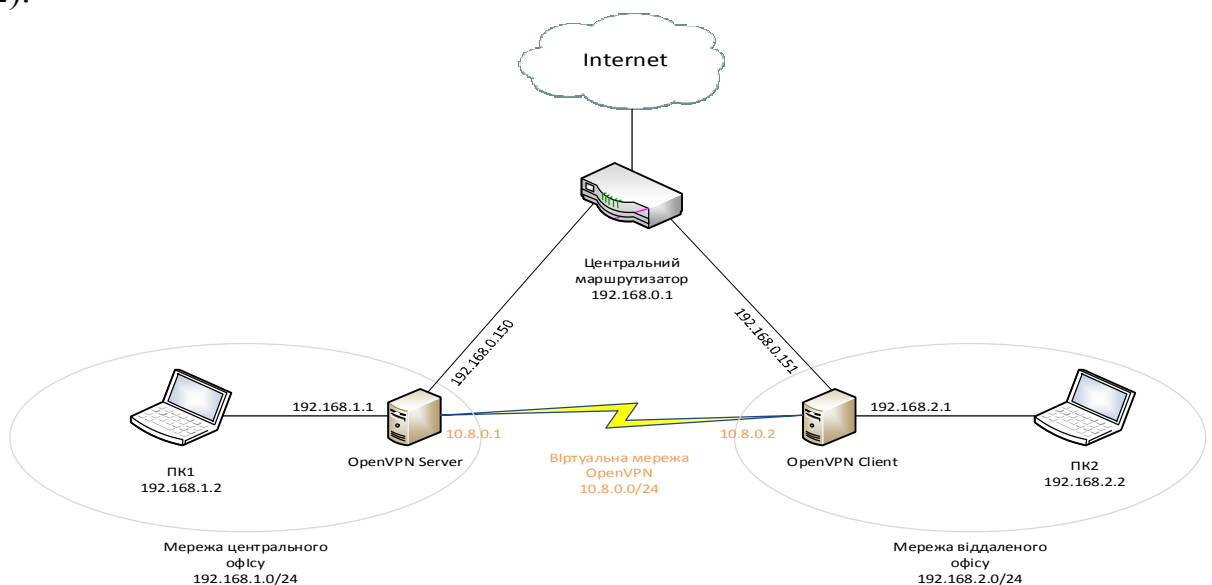


Рис.2. Запропоноване вирішення задачі

Сервер з Windows, встановлений на вході мережі віддаленої філії, відіграватиме роль клієнта OpenVPN. Обидва сервери мають фізичне підключення до центрального маршрутизатора організації. Локальна підмережа центрального офісу має адресу 192.168.1.0/24; локальна підмережа філії - 192.168.2.0/24; мережа центрального маршрутизатора - 192.168.0.0/24. Буде створена віртуальна мережа на основі OpenVPN, щозадовольнятиме усім висунутим вимогам.

Інсталяція та налаштування серверу OpenVPN. OpenVPN є безкоштовним програмним забезпеченням з відкритим кодом, отже знаходиться у вільному доступі. Для отримання дистрибутиву перейдемо на сайт проекту www.openvpn.net і перейдемо до сторінки завантажень (Community – Downloads). У даному випадку будемо використовувати версію OpenVPN 2.2.2. Після завантаження Windows-версії проінсталуємо програмний пакет до директорії C:\OpenVPN. Безпосередньо працювати будемо з такими директоріями, що знаходяться по даній адресі:

- ccd – файли конфігурацій віддалених клієнтів
- config – конфігурація локального сервера або клієнта OpenVPN
- easy-rsa – утіліти для генерації ключів та сертифікатів
- keys – папка, куди будуть поміщені ключі і сертифікати

Створення ключів та сертифікатів. Налаштування OpenVPN починається з генерації ключів та сертифікатів. Дані процедури виконуються на серверній частині. Генеровані ключі діляться на:

- Головний СА (Certificate Authority) сертифікат та ключ, що використовуються для підписування кожного сертифікату сервера та клієнта
- Публічний та приватний ключі для сервера та кожного клієнта окремо

Алгоритм генерації ключів такий:

- Генеруємо СА-сертифікат та ключ (ca.crt; ca.key)
- Генеруємо сертифікат та ключ сервера (server.crt; server.key)
- Генеруємо сертифікат та ключ клієнта (office1.crt; office1.key)
- Генеруємо параметри Diffie-Hellman (dh1024.pem)
- Генеруємо ключ для аутентифікації пакетів (ta.key)

Щоб приступити до генерації, через командний рядок Windows перейдемо до каталогу C:\OpenVPN\easy-rsa:

```
cd C:\OpenVPN\easy-rsa ,
```

де виконаємо файл init-config, внаслідок чого буде створений файл vars.bat, що містить усі необхідні змінні для генерації ключів

```
C:\OpenVPN\easy-rsa>init-config
```

Відредагуємо файл vars.bat. Для роботизації *.bat-файлами бажано застосовувати замість стандартного Блокноту сторонній текстовий редактор (наприклад Notepad++). Змінюємо рядок

```
set HOME=%ProgramFiles%\OpenVPN\easy-rsa
```

на

```
set HOME=C:\OpenVPN\easy-rsa
```

Додаємо рядок

```
set KEY_DIR=C:\OpenVPN\keys
```

Нижня частина файлу містить змінні, які використовуються при генерації ключів і служать для їх унікальності та інформації про власника. Після редагувань файл vars.bat, не враховуючи коментарів, виглядатиме таким чином:

```
@echooff
```

```
set HOME=C:\OpenVPN\easy-rsa
```

```
set KEY_CONFIG=openssl-1.0.0.cnf
```

```
set KEY_DIR=C:\OpenVPN\keys
```

```
set KEY_SIZE=1024
```

```
set KEY_COUNTRY=UA
```

```
set KEY_PROVINCE=KV
```

```
set KEY_CITY=Kiev
```

```
set KEY_ORG=OpenVPN
```

```
set KEY_EMAIL=mail@host.domain
```

```
set KEY_CN=server
```

```
set KEY_NAME=server
```

```
set KEY_OU=server
```

```
set PKCS11_MODULE_PATH=changeme
```

```
set PKCS11_PIN=1234
```

Змінні, починаючи з KEY_COUNTRY, можна редагувати на свій розсуд. Виконаємо даний файл, тим самим задавши значення змінних

```
C:\OpenVPN\easy-rsa>vars
```

Далі виконуємо обнуління каталогу з ключами:

```
C:\OpenVPN\easy-rsa>clean-all
```

Варто зазначити, що у деяких випадках OpenVPN може звертатись до неіснуючого конфігураційного файлу C:\openssl\ssl\openssl.cnf, що може викликати помилки. У разі виникнення такої проблеми потрібно скопіювати до даної адреси файл C:\OpenVPN\easy-rsa\openssl-1.0.0.cnf, відповідно його перейменувавши.

Генеруємо ключ і сертифікат CA

```
C:\OpenVPN\easy-rsa>build-ca
```

Погоджуємось з запропонованими варіантами відповідей на питання, CommonName задаємо наприклад як OpenVPNServer.

Згенеруємо сертифікат і ключ сервера:

```
C:\OpenVPN\easy-rsa>build-key-server server
```

Common Name задаємо як *server*, напропозицію підписати сертифікат двічі відповідаємо *Y*.

Згенеруємо ключ та сертифікат для клієнта:

```
C:\OpenVPN\easy-rsa>build-key office1
```

Common Name задаємо як *office1*.

Для генерації ключа Діффі-Хелмана вводимо

```
C:\OpenVPN\easy-rsa>build-dh
```

Ключ аутентифікації пакетів генерується таким чином:

```
C:\OpenVPN\easy-rsa>openvpn --genkey --secret ta.key
```

На даному етапі генерування ключів завершено.

Таким чином, сервер повинен мати такі ключі та сертифікати:

- ca.crt
- ca.key
- dh1024.pem
- server.crt
- server.key
- ta.key

На клієнт треба перенести такі файли:

- ca.crt
- office1.crt
- office1.key
- ta.key

Важливо зазначити, що файли ключів необхідно передавати лише захищеними шляхами, адже вони є секретними і будь-яке перехоплення ключа ставить під загрозу безпеку мережі.

Створення файлів конфігурації сервера. Створимо конфігураційний файл сервера. Для цього перейдемо до каталогу *C:\OpenVPN\config* та створимо текстовий файл *server.ovpn* та заповнимо таким чином:

proto udp (будемо використовувати протокол UDP)

port 1194 (стандартний порт OpenVPN)

dev tun (режим роботи – тунель)

tls-server (режим клієнт-сервер)

topology subnet (опис топології)

route-method exe (вказує що додавання маршрутів відбувається через *route.exe*)

route-delay 10 (затримка при додаванні маршруту)

server 10.8.0.0 255.255.255.0 (задається віртуальна мережа)

route-gateway 10.8.0.1 (задається шлюз)

client-config-dir "C:\\OpenVPN\\ccd" (директорія з конфігураціями клієнтів)

ca "C:\\OpenVPN\\keys\\ca.crt"

cert "C:\\OpenVPN\\keys\\server.crt"

key "C:\\OpenVPN\\keys\\server.key"


```
dh "C:\\OpenVPN\\keys\\dh1024.pem"  
tls-auth "C:\\OpenVPN\\keys\\ta.key" (шляхи до ключів та сертифікатів)  
route 10.8.0.0 255.255.255.0 (задається маршрут на мережу)  
cipher BF-CBC (вибір типу шифрування)  
comp-lzo (задається стиснення трафіку)  
verb 1 (рівень інформативності повідомлень, що виводяться у консоль)  
keepalive 5 60 (кожні 5 секунд пінгується сусід, якщо протягом 60 секунд  
нема відповіді – перезапуск тунеля)  
route 192.168.2.0 255.255.255.0 10.8.0.2 (шлях у мережу віддаленого офіса)
```

Крім власної конфігурації, на серверній частині необхідно налаштувати конфігурацію клієнта. Для цього у каталозі C:\\OpenVPN\\ссдстворюємо файл з назвою клієнта (office1). Даний файл не має розширення. Зміст файлу має бути таким:

```
ifconfig-push 10.8.0.2 255.255.255.0 (повідомляємо клієнту адресу його  
віртуального інтерфейсу)  
push "route 10.8.0.0 255.255.255.0"(передаємо маршрут на віртуальну  
мережу)  
push "route-gateway 10.8.0.1"(задаємо шлюз)  
iroute 192.168.2.0 255.255.255.0 (повідомляємо серверу, що за клієнтом  
знаходиться дана мережа)  
На даному етапі конфігурація сервера закінчена.
```

Налаштування клієнта OpenVPN. Робота з клієнтом починається аналогічно випадку з сервером: встановлюємо OpenVPN 2.2.2 у каталог C:\\OpenVPN. Далі переносимо з сервера раніше зазначені ключі і сертифікати до каталогу keys. Найкраще ці файли передавати не мережею, а за допомогою твердотільних накопичувачів: таким чином виключена можливість їх перехоплення.

Конфігурація клієнта задається шляхом створення і заповнення файлу office1.ovpn у каталозі config. Задамо такі параметри:

```
dev tun  
proto udp  
port 1194 (аналогічно налаштуванню сервера)  
remote 192.168.0.150 (IP-адреса сервера)  
tls-client (робота в режимі клієнта)  
remote-cert-tls server (захист від підміни сервера)  
route-method exe  
route-delay 10 (аналогічно налаштуванню сервера)  
route 192.168.1.0 255.255.255.0 (задається маршрут у мережу центрального  
офісу)  
pull (дозволяється отримання конфігурації від сервера)  
ca "C:\\OpenVPN\\keys\\ca.crt"
```

```
cert "C:\\OpenVPN\\keys\\office1.crt"  
key "C:\\OpenVPN\\keys\\office1.key"  
tls-auth "C:\\OpenVPN\\keys\\ta.key"  
cipher BF-CBC  
comp-lzo  
verb 1  
keepalive 5 60(аналогічно налаштуванню сервера).
```

На цьому налаштування клієнтської частини закінчено.

Запуск OpenVPN. Задлятого, щоб запустити OpenVPN, потрібно елементарно натиснути правою кнопкою по файлу конфігурації (*.ovpn) і обрати “StartOpenVPNonthisconfigfile”, при цьому з’явиться консоль, в якій буде виводитись стан з’єднання. Таким чином, якщо запустити сервер, а потім клієнт, вони автоматично з’єднаються, а у консолях виведуться відповідні повідомлення, при цьому віртуальний мережевий адаптер покаже, що з’явилося підключення.

Налаштування маршрутизації та брандмауера. Важливим елементом налаштування мережі є правильне конфігурування маршрутизації та брандмауера на комп’ютерах, що виконують роль клієнта та сервера OpenVPN. У будь-якому брандмауері важливо дозволити проходження ICMP-пакетів, що дозволить пінгувати хости у мережах. Також потрібно впевнитись, що дозволена передача по порту 1194 протокола UDP. Бажано додати віртуальні інтерфейси у список довірених, якщо брандмауер підтримує таку функцію.

Щодо маршрутизації, то на обох машинах будемо використовувати вбудовані засоби Windows XP. Для їх активації потрібно виконати редактор реєстру (Пуск – Выполнить – regedit.exe), перейти до розділу HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Tcpip\\Parameters, для параметра IPEnableRouter виставити значення «1». Після цього потрібно закрити редактор та перезавантажити ПК. Далі потрібно перевірити, чи запущена відповідна служба. Це можна подивитись у панелі керування (Пуск – Панель управління – Администрирование – Службы), знайти у переліку службу «Маршрутизация и удаленный доступ», у властивостях перемкнути режим запуску на «Авто», запустити службу.

Маршрутизм можна задавати як у конфігураційних файлах OpenVPN, так і у командному рядку Windows. Перший випадок розглянуто раніше, тепер розглянемо другий як альтернативу.

Синтаксис задання статичних маршрутів у Windows виглядає таким чином:

```
ROUTE -p add [destination] MASK [netmask] [gateway] , de
```

- *destination* – мережа, до якої потрібно прописати маршрут.
- *netmask* – маска даної мережі.
- *gateway* – шлюз, через який можливо дістатись даної мережі.

Ключ –розначає,що маршрут буде зберігатись постійно, а видалиться лише при введенні команди на видалення. У протилежному випадку маршрут буде видалений після перезавантаження.

Отже, сервер має направляти пакети з власної мережі 192.168.1.0/24 через віртуальну мережу 10.8.0.0/24 у мережу віддаленого офіса 192.168.2.0/24. Це реалізується такою командою з командного рядка сервера:

```
ROUTE -padd 192.168.2.0 MASK 255.255.255.0 10.8.0.2 ,
```

тобто пакети, адресовані мережі 192.168.2.0, йдуть на віртуальний інтерфейс клієнта 10.8.0.2.

Аналогічно, клієнт має направляти пакети з власної мережі 192.168.2.0/24 через віртуальну мережу 10.8.0.0/24 у мережу центрального офіса 192.168.1.0/24. Це реалізується такою командою з командного рядка клієнта:

```
ROUTE -padd 192.168.1.0 MASK 255.255.255.0 10.8.0.1
```

Обов'язково необхідно прописати шлях до сусідніх мереж для внутрішньо мережевих ПК. Це виконується таким чином:

```
ROUTE -padd 192.168.2.0 MASK 255.255.255.0 192.168.1.1 – дляПК1
```

```
ROUTE -padd 192.168.1.0 MASK 255.255.255.0 192.168.2.1 – дляПК2
```

Налаштування доступу до Інтернет на користувацьких ПК. При побудові мережі, користувачі ПК, які знаходяться у внутрішніх мережах центрального офісу та філії, не мають доступу до мережі Інтернет. До мережі підключений лише маршрутизатор, і, відповідно ПК, які відіграють роль сервера та клієнта.

Доступ комп'ютерів, які знаходяться у внутрішніх мережах, до мережі Інтернет найпростіше реалізувати за допомогою технології NAT (NetworkAddressTranslation), тобто внутрішні адреси користувацьких ПК будуть перетворюватись на адресу вхідних мережевих ПК. Користуватись будемо знову ж таки вбудованими можливостями WindowsXP.

Розглянемоце на прикладі мережі центрального офісу (192.168.1.0/24). Вхідний ПК має два фізичних інтерфейси – один з'єднаний з маршрутизатором (192.168.0.150), інший «дивиться» у внутрішню мережу (192.168.1.1). Назвемо дані інтерфейси «Internet» та «Central» відповідно.

ПроінсталуємоNAT на сервер. З командного рядка вводиться команда:

```
netshroutingipnatinstall ,
```

після чого необхідно перезавантажити ПК. Налаштовуємо інтерфейси:

```
netshroutingipnataddinterface "Internet" full
```

```
netsh routing ipnat add interface "Central" private
```

Налаштуваннямережевогоінтерфейсу на користувацькому ПК мають бути такі:

- IP-адреса: 192.168.1.2

- Маска: 255.255.255.0
- Шлюз: 192.168.1.1
- DNS: 8.8.8.8 (DNS-сервер Google, доступний для будь-якого користувача)

Після виконання цих дій для користувача внутрішньомережевого ПК буде доступна мережа Інтернет.

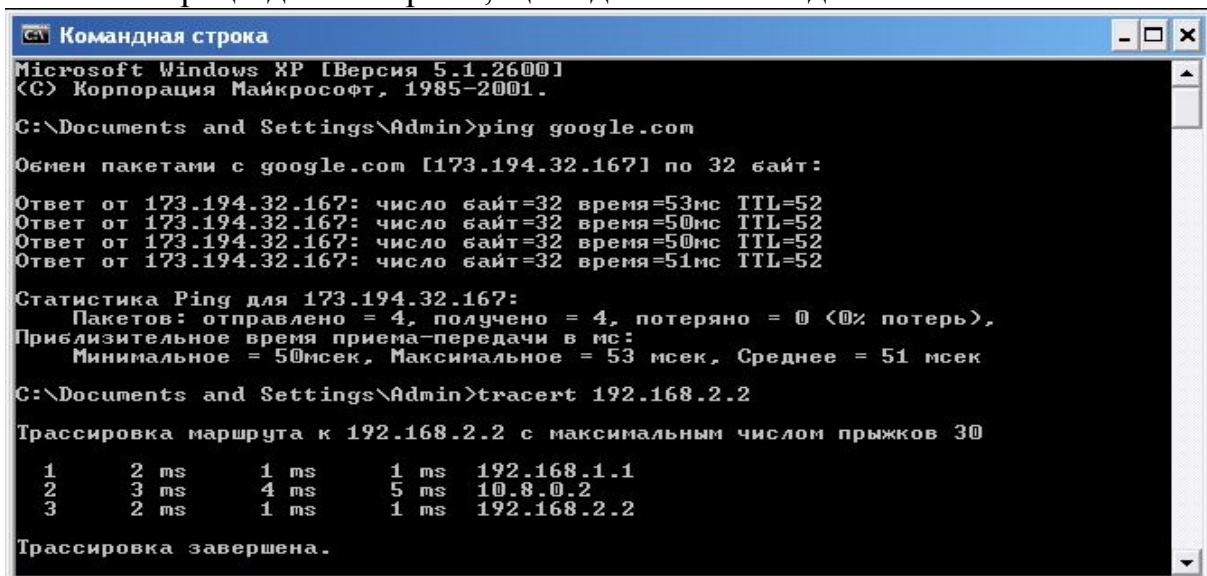
Варто зазначити, що в зв'язку з особливостями функціонування ОС WindowsXP, при використанні NAT після кожного перезапуску сервера необхідно вручну запускати службу «Брандмауер Windows/спільний доступ до інтернету (ICS)», інакше мережа не працюватиме.

На стороні філії необхідно проробити аналогічні дії.

Перевірка працездатності мережі. На даному етапі можливо виконати повну перевірку мережі задля визначення працездатності і відсутності неполадок. Будемо користуватись утилитами ping та traceroute. Процедура перевірки полягатиме у трасуванні шляху від користувацького ПК у іншу мережу, а також перевірки доступності мережі Internet.

На ПК1 (192.168.1.2) пропінгуємо адресу в Інтернеті, а також проведемо трасування для адреси 192.168.2.2 (рис.3).

Очевидно, що мережа Інтернет досяжна, а пакети у локальну мережу віддаленого офісу прямують через віртуальну мережу, що створена OpenVPN. Виконаємо аналогічні дії на ПК2 (192.168.2.2) (рис.4). Маємо аналогічні результати. Таким чином, мета досягнута: побудована повністю працездатна мережа, що задовольняє вхідним вимогам.



```
Командная строка
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Admin>ping google.com

Обмен пакетами с google.com [173.194.32.167] по 32 байт:

Ответ от 173.194.32.167: число байт=32 время=53мс TTL=52
Ответ от 173.194.32.167: число байт=32 время=50мс TTL=52
Ответ от 173.194.32.167: число байт=32 время=50мс TTL=52
Ответ от 173.194.32.167: число байт=32 время=51мс TTL=52

Статистика Ping для 173.194.32.167:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
Приблизительное время приема-передачи в мс:
  Минимальное = 50мсек, Максимальное = 53 мсек, Среднее = 51 мсек

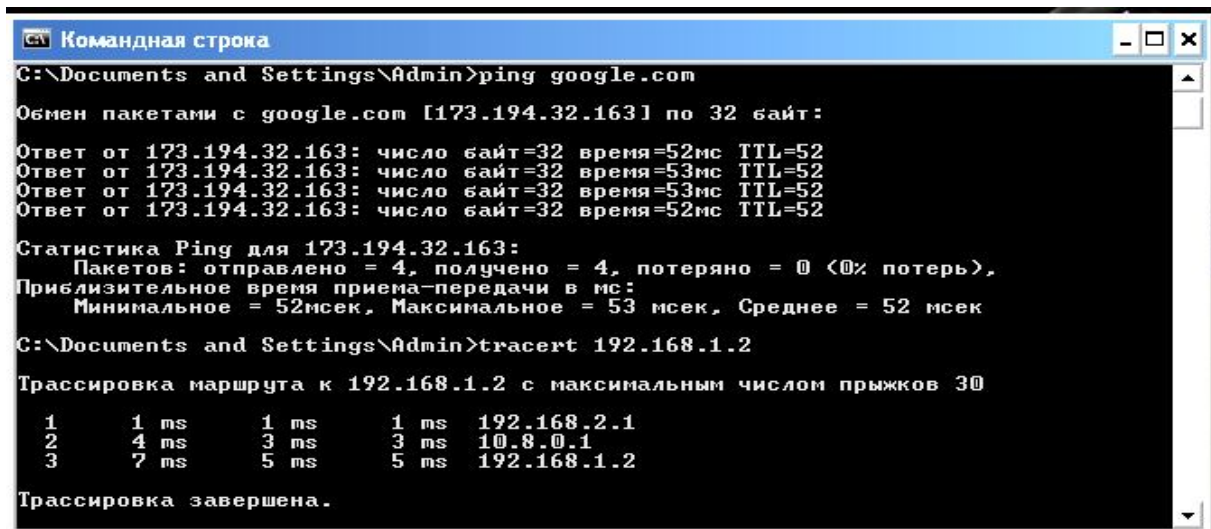
C:\Documents and Settings\Admin>tracert 192.168.2.2

Трассировка маршрута к 192.168.2.2 с максимальным числом прыжков 30

 1      2 ms      1 ms      1 ms     192.168.1.1
 2      3 ms      4 ms      5 ms     10.8.0.2
 3      2 ms      1 ms      1 ms     192.168.2.2

Трассировка завершена.
```

Рис. 3 Перевірка мережі на ПК1



```
Командная строка
C:\Documents and Settings\Admin>ping google.com

Обмен пакетами с google.com [173.194.32.163] по 32 байт:

Ответ от 173.194.32.163: число байт=32 время=52мс TTL=52
Ответ от 173.194.32.163: число байт=32 время=53мс TTL=52
Ответ от 173.194.32.163: число байт=32 время=53мс TTL=52
Ответ от 173.194.32.163: число байт=32 время=52мс TTL=52

Статистика Ping для 173.194.32.163:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
    Приблизительное время приема-передачи в мс:
        Минимальное = 52мсек, Максимальное = 53 мсек, Среднее = 52 мсек

C:\Documents and Settings\Admin>tracert 192.168.1.2

Трассировка маршрута к 192.168.1.2 с максимальным числом прыжков 30

  1         1 ms          1 ms          1 ms      192.168.2.1
  2         4 ms          3 ms          3 ms      10.8.0.1
  3         7 ms          5 ms          5 ms      192.168.1.2

Трассировка завершена.
```

Рис. 4. Перевірка мережі на ПК2

Висновки. У даній роботі були розглянуті протоколи для побудови віртуальних приватних мереж (VPN), які найчастіше використовуються на практиці, основи їх роботи, переваги та недоліки, а також проведено їх порівняння задля визначення області застосування кожного протоколу. Таким чином визначено, що найкращим протоколом за критеріями простоти та безпечності для побудови приватної корпоративної мережі, зокрема банківської, можна вважати SSL разом з похідними рішеннями (OpenSSL, OpenVPNі т.д.), оскільки разом з хорошою швидкістю та відмінним захистом, дана технологія надає доволі простий доступ до ресурсів мережі, наприклад через звичайний браузер. Окрім цього розроблено простий та дієздатний алгоритм побудови захищеної банківської мережі із використанням OpenVPN, що може використовуватись в банківських установах та в навчальних закладах для відпрацювання навичок побудови віртуальних приватних мереж.

Використані джерела інформації:

1. Finlayson M., Harrison J., Sugarman R. VPN technologies – a comparison. – Enfield: Metaswitch, 2003. – 45 p.
2. Lewis M. Comparing, Designing, and Deploying VPNs. – Indianapolis: Cisco Press, 2006. – 1043 p.
3. Keijser J. J. OpenVPN 2 Cookbook. – Birmingham: Packt Publishing, 2011. – 356 p.
4. Есартія Р.Б. Организация VPN каналов между офисами // Записки IT специалиста. – Режим доступа: http://interface31.ru/tech_it/2011/09/organizaciya-vpn-kanalov-mezhdu-ofisami.html.