УДК 004.77:004.031
DOI https://doi.org/10.32689/maup.it.2024.4.16

Геннадій МОГИЛЬНИЙ
кандидат технічних наук, доцент, директор Навчально-наукового інституту математики та інформаційних технологій,
ДЗ «Луганський національний університет імені Тараса Шевченка», g.mogilniy@gmail.com
***ORCID:** 0000-0001-5317-2795*

Володимир ДОНЧЕНКО
старший викладач кафедри інформаційних технологій та систем,
ДЗ «Луганський національний університет імені Тараса Шевченка», ifmit.s.2014@gmail.com
***ORCID:** 0000-0003-0359-3051*

Світлана ДОНЧЕНКО
асистент викладач кафедри інформаційних технологій та систем,
ДЗ «Луганський національний університет імені Тараса Шевченка», donchenko.lana77@gmail.com
***ORCID:** 0000-0002-2374-2109*

ОГЛЯД ТА АНАЛІЗ ІНСТРУМЕНТІВ СТВОРЕННЯ КОРПОРАТИВНОГО СЕРЕДОВИЩА

Анотація. *Стаття присвячена аналізу сучасних підходів до створення об'єднаних інформаційних середовищ для організацій із розгалуженою структурою підрозділів. Особливу увагу приділено використанню сучасних засобів для організації віддаленого доступу для зовнішніх користувачів та інтеграції з локальною мережею підприємства. В умовах необхідності інтеграції локальних мереж підрозділів, що розташовані в різних регіонах, розглянуто рішення, які базуються на технологіях віртуальних приватних мереж (VPN), переадресації портів (PAT) і функції DMZ.*

Мета роботи *– аналіз засобів створення корпоративного середовища в умовах мінімального обсягу фінансування.*

Методологія*. Аналіз наукової літератури з питань створення корпоративного середовища. Аналіз нормативних документів з налаштування різноманітних роутерів. На засадах системного аналізу запропоновано варіанти створення корпоративного середовища в умовах швидкого впровадження нових технологій.*

Наукова новизна *дослідження полягає в обґрунтуванні варіантів створення корпоративного середовища в умовах обмеженого фінансування. Доведено, що технології DMZ та PAT можуть бути застосовано на всіх сучасних роутерах, як засоби створення корпоративного середовища. Встановлено, що використання мережевої технології VPN на клієнтських обчислювальних машинам має суттєві недоліки і може бути застосовано за умови додаткового налаштування.*

Висновки*. У роботі детально проаналізовано особливості впровадження віддаленого доступу до корпоративних ресурсів шляхом налаштування DMZ, PAT та VPN (PPTP, L2TP) на різних моделях роутерів: Tp_link TL-WR840N, Mercusys AC12g, Tp-link AX1500 та Mikrotik. На основі практичних експериментів оцінюються переваги та недоліки кожного методу. Проведений аналіз дозволяє прискорити створення корпоративних мереж у межах обмежених бюджетів, зокрема для малих підприємств і навчальних закладів. Представлено рекомендації щодо модернізації мережевої інфраструктури, вибору роутерів і впровадження засобів контролю доступу, які можуть бути застосовані для побудови інтегрованих інформаційних систем у бізнесі, освіті та інших галузях.*

Ключові слова: *корпоративна мережа, віддалений доступ, роутер, VPN, DMZ, переадресація портів.*

Hennadii MOHYLNYI, Volodymyr DONCHENKO, Svitlana DONCHENKO. REVIEW AND ANALYSIS OF TOOLS FOR CREATING A CORPORATE ENVIRONMENT

Abstract. *The article is devoted to the analysis of modern approaches to creating unified information environments for organizations with a branched structure of departments. Particular attention is paid to the use of modern tools for organizing remote access for external users and integration with the enterprise's local network. In the conditions of the need to integrate local networks of departments located in different regions, solutions based on virtual private network (VPN) technologies, port forwarding (PAT) and DMZ functions are considered.*

The purpose *of the work is to analyze the means of creating a corporate environment with minimal funding.*

Methodology. *Analysis of scientific literature on the creation of a corporate environment. Analysis of regulatory documents on the configuration of various routers. On the basis of system analysis, options for creating a corporate environment in conditions of rapid implementation of new technologies are proposed.*

The scientific novelty *of the study lies in the substantiation of options for creating a corporate environment in conditions of limited funding. It is proven that DMZ and PAT technologies can be used on all modern routers as a means of creating a corporate environment. It is established that the use of VPN network technology on client computers has significant disadvantages and can be applied subject to additional configuration.*

Conclusions*. The paper analyzes in detail the features of implementing remote access to corporate resources by configuring DMZ, PAT and VPN (PPTP, L2TP) on different router models: Tp_link TL-WR840N, Mercusys AC12g, Tp-link AX1500 and Mikrotik. Based on practical experiments, the advantages and disadvantages of each method are assessed. The analysis allows you to accelerate the creation of corporate networks within limited budgets, in particular for small businesses and educational institutions. Recommendations are presented for the modernization of network infrastructure, the selection of routers and the implementation of access control tools that can be used to build integrated information systems in business, education and other industries.*

Key words: *corporate network, remote access, router, VPN, DMZ, port forwarding.*

Вступ. Постановка проблеми. Сьогодні багато організацій мають розгалужену мережу підрозділів, що фізично розташовані в різних регіонах. У таких умовах одним із ключових завдань стає об'єднання всіх підрозділів у єдину, надійну та безпечну локальну мережу. Таким чином, перед багатьма закладами та установами виникає питання створення загальнодоступних інформаційних баз даних та сервісів шляхом впровадження корпоративних мереж між відокремленими підрозділами та надання можливості віддаленим користувачам використовувати внутрішні локальні ресурси.

Враховуючи сучасні обставини, які виникають в умовах військового стану можна стверджувати, що різноманітні питання програмного та апаратного забезпечення, спрямовані на створення об'єднаних корпоративних мереж, є своєчасною та актуальною задачею.

Аналіз останніх досліджень і публікацій. Загальновідомі методи з'єднання віддалених підрозділів з локальною мережею полягали в тому, що підключення працювало по загальній мережі, що комутується, PSTN (public switched telephone network), або використовували спеціалізовану орендовану WAN (wide area network,), користуючись фрейм-ретранслятором або синхронною схемою протоколу PPP (Point-to-Point Protocol) [13]. Ці методи вимагають значних витрат часу на адміністрування й доволі не дешеві в обслуговуванні. Використання Internet-рішень дозволяє задовольнити потреби віддаленої роботи в організаційній мережі через кілька інтернет-підключень, наданих інтернет-провайдерами (Internet Service Providers або ISP), і VPN-сервери. У цьому контексті перспективними рішеннями є надійні та недорогі пристрої з великим вибором протоколів маршрутизації та віртуальних приватних мереж (VPN). Це дозволяє гнучко підлаштовувати пристрої під різні вимоги провайдерів інтернет-мереж, а також забезпечувати високу безпеку та надійність тунелів між підрозділами.

У роботі [3] представлено найпростіші та швидкі способи створення інформаційної системи з віддаленим доступом, описано їх реалізацію, яка не потребує значної модернізації. Проведено аналіз варіантів організації доступу до навчальної комп'ютерної лабораторії, побудованої за принципом перенаправлення окремих портів. Також розроблено рекомендації щодо модернізації обладнання лабораторії та визначено етапи налаштування системи з використанням віддаленого робочого столу. Автори [4] проаналізували різні підходи до організації віддаленого доступу до комп'ютерної лабораторії, яка може бути побудована або на базі одного вузла з різними ресурсами (інформаційними, апаратними, програмними), або декількох вузлів, серед яких є сервери віддаленого робочого столу, вебсервери та інші ресурси з окремими IP-адресами. Особливу увагу приділено структурним компонентам системи віддаленого доступу на основі VPN, надано рекомендації з їх налаштування та використання. Наведено специфіку застосування VPN за допомогою роутерів MikroTik.

У дослідженні [2] розглядаються актуальні питання захисту інформації у віртуальних приватних мережах (VPN), зокрема аспекти масштабованості, гнучкості управління, вимог до підключень та витрат на впровадження. У статті [15] досліджено сучасні методи та інструменти створення сервісу віртуальних приватних мереж, а також проведено аналіз їх реалізації за допомогою апаратно-програмних рішень на прикладі приватної мережі, побудованої з використанням CISCO FlexVPN.

У статті [5] описано принципи побудови мереж передачі даних для забезпечення послуг VPN та Інтернету на основі концепції Metro Ethernet. Запропоновано підходи до пошуку рішень, сформульовано ідеологію таких мереж, наведено їх архітектуру, параметри й характеристики. Також синтезовано структуру мережі та визначено ієрархію вузлів і обладнання. У статті [6] проаналізовано методи та способи реалізації захищених каналів VPN, їх переваги та недоліки. Розглянуто принципи функціонування та цільове призначення VPN у рамках розподілених корпоративних мереж, що використовують інфраструктуру відкритого доступу.

Метою статті є аналіз засобів створення корпоративного середовища в умовах мінімального обсягу фінансування.

Виклад основного матеріалу дослідження. В цілому задача створення корпоративного середовища це складний та багатоетапний процес. В межах цієї роботи будемо вважати, що підприємство вже має реальну IP-адресу та виконало аналіз інформаційних ресурсів, які будуть використані в об'єднаному середовищі корпоративної мережі. Таким чином, можна виділити основні складові корпоративної мережі: створення доступу окремих користувачів до внутрішніх локальних ресурсів певного підрозділу (рис. 1); об'єднання окремимих підрозділів за рахунок впровадження певного тунелю (рис. 2).

Рис. 1. Загальна схема приєднання віддалених користувачів

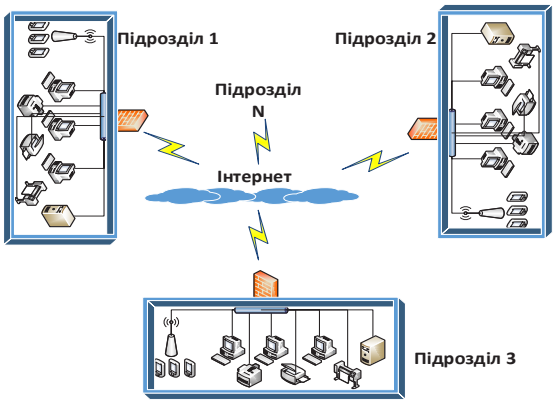


Рис. 2. Загальна схема з'єднання віддалених підрозділів

Крім того слід врахувати, що вирішення кожної задачі можливо вирішити різноманітними шляхами, однак самим поширеним є використання спеціалізованого порогового окремого роутера.

Досвід показує, що значна кількість організацій в умовах військового стану не вкладають багато коштів у мережну інфраструктуру та, в більшості випадків, використовують недорогі роутери, наприклад:

- WI-FI роутер Tp_link TL-WR840N [14] – 700 грн;
- WI-FI роутер Mercusys AC12g [7] – 1100 грн;
- WI-FI роутер Tp_link AX1500 Wi-Fi 6 [8] – 2200 грн;
- WI-FI роутер Mikrotik RBD53iG-5HacD2Hn [16] – 4000 грн.

В межах цієї роботи особливу увагу приділено вирішенню першої задачі — забезпеченню доступу віддалених користувачів до локальної мережі певного підрозділу, що є більш поширеним випадком і вимагає детального аналізу. Розглянемо декілька загальних підходів.

Наприклад, всі основні інформаційні ресурси розташовані на одному вузлі локальної мережі підрозділу (рис. 3, 4) – це найпростіший спосіб організації віддаленого доступу до інформаційних ресурсів локальної мережі, який не вимагає значних змін в інформаційній структурі підрозділу.

Встановлено, що на багатьох сучасних не дорогих роутерах можна скористатися функцією DMZ [1]. Безумовно, в такому випадку, адреса локального вузлу повинна бути статичною, тобто без використання протоколу DHCP.

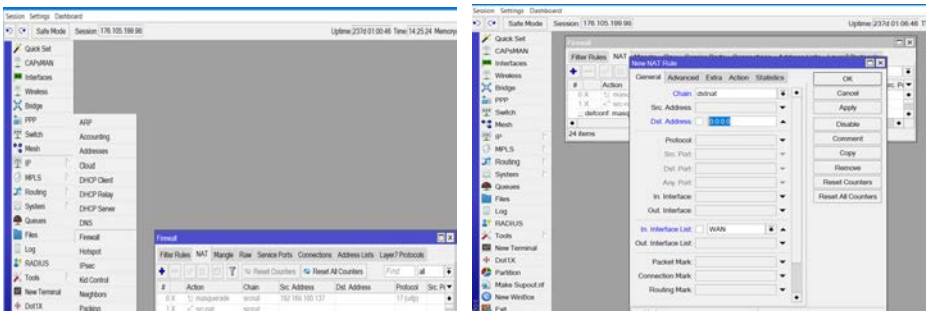
На рисунках 3–4 показано як це зробити на роутерах Mercusys AC12g та Tp_link AX1500, однак, аналогічні налаштування є на більшості роутерах та можуть бути швидко впроваджені.

Основним недоліком такого рішення є обмежена можливість використання різноманітного програмного забезпечення, яке зазвичай встановлюється на різних операційних системах, вимагає застосування декількох IP-адрес і не може бути розміщене на одній адресі. Безумовно створити один обчислювальний інформаційний ресурс на якому працювало б багато служб (сервісів) практично не можливо. Таким чином, використання DMZ можливе тільки для малих підприємств, які використовують обмежену кількість сервісів, що розташовані на одному вузлі.

Рис. 3. Налаштування DMZ для Mercusys AC12g

Рис. 4. Налаштування DMZ для Tp_link AX1500

Роутер Mikrotik не використовує поняття DMZ. Для такого налаштування необхідно скористатися програмою Winbox [10] та перейти до меню IP–Firewall–NAT (рис. 5,а), створити правило DST-NAT (рис. 5,б) та призначити Action dst-nat на необхідну IP-адресу.



а) б)

Рис. 5. Налаштування DMZ для Mikrotik: а) меню NAT; б) створення dst-nat

Слід відзначити [1], що використання DMZ має значну кількість недоліків з точки зору інформаційної безпеки тому, що IP вузол, у багатьох випадках, не відділяється від внутрішньої мережі та може вільно підключитися до внутрішніх ресурсів. Налаштування DMZ на всіх досліджених роутерах не дозволяє застосувати будь яких заходів безпеки. Отже для ліквідації такого суттєвого недоліку треба: встановлювати та налаштовувати додатковий міжмережевий екран у локальній мережі підрозділу або ретельно налаштувати фаєрвол вузла з контролем вхідного та вихідного трафіку.

У випадку коли, різноманітні ресурси розташовані на разних вузлах локальної мережі підрозділу, для організації віддаленого доступу необхідно ретельно проаналізувати особливості протоколів, які використовує кожен ресурс. Наприклад: веб-сервер –порти 80 і 443, e-mail сервер – 1 порти 25 і 110, FTP-сервер –порти 21, 20 і 1024–1240.

Практично для віх роутерів ця задача вирішується шляхом використання переадресації портів PAT [11], Налаштування робиться у меню «віртуальний сервер» або «port forwarding» (рис. 6).

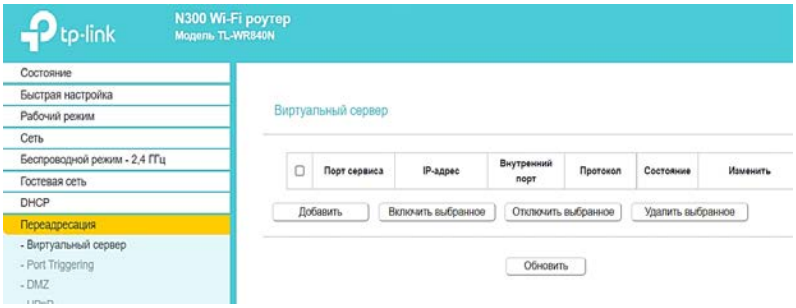


Рис. 6. Переадресація (PAT) у роутері Tp_link TL-WR840N

На рисунках 7–8 представлено відповідні меню роутерів Tp-Link TL-WR840N, Mercusys AC12G та AX1500 Wi-Fi 6. Детальне налаштування наведено лише для роутера AX1500 Wi-Fi 6 (рис. 9–10), тоді як для інших роутерів процедура є аналогічною.

Таким чином, можна створювати правила для всіх локальних інформаційних ресурсів підрозділу та контролювати використані порти. Такий підхід є доцільним для простих інформаційних систем підрозділу, де заздалегідь визначено список IP-портів, які не конфліктують між собою та можуть бути перенаправлені. Крім того, важливо враховувати, що віддалені користувачі матимуть доступ лише до зовнішньої IP-адреси пристрою, який виконує роль шлюзу. Водночас цей пристрій може стикатися з обмеженнями, пов'язаними з недостатньою кількістю місця у таблиці перенаправлення портів.

Рис. 7. Переадресація (PAT) у роутері Mercusys AC12g

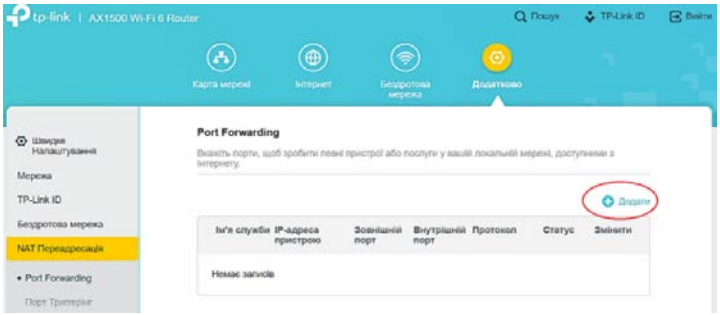


Рис. 8. Переадресація (PAT) у роутері AX1500 Wi-Fi 6

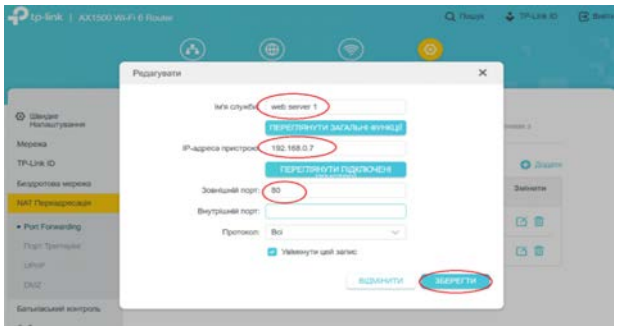


Рис. 9. Додавання вебсерверу – порт TCP/IP 80

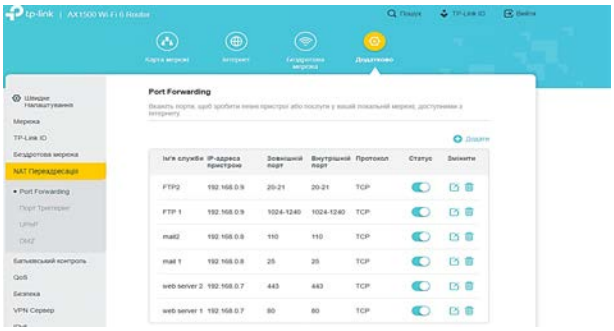


Рис. 10. Загальна таблиця налаштувань переадресування

Роутер Mikrotik не використовує поняття PAT. Таке налаштування робиться аналогічно створенню DMZ у програмі Winbox. Для цього переходимо до меню IP–Firewall–NAT (рис. 5,а), створюємо правило DST-NAT, вказуємо певні порти (рис. 5,б). Після чого треба призначити Action dst-nat на необхідну локальну IP-адресу та порт.

До недоліків цього методу відноситься складність налаштування фаєрволу на пороговому приладі, необхідність налаштування брандмауерів кожного вузла і, таким чином, необхідність індивідуальної конфігурації кожного вузла локальної мережі.

Для забезпечення повного доступу віддалених користувачів до всіх інформаційних ресурсів локальної мережі підрозділу доцільно використовувати VPN-сервіс [12]. Існує кілька типів VPN, зокрема PPTP, L2TP, SSTP, OpenVPN та різні види тунелів. Хоча це широке питання, у рамках даної роботи розглянуто організацію найпростішого типу VPN – PPTP. Цей тип має багато недоліків у сфері безпеки, однак відрізняється легкістю та швидкістю налаштування.

Використання такого сервісу дозволяє забезпечити доступ віддалених користувачів до всіх ресурсів локальної мережі та майже повністю імітувати їхню присутність у цій мережі. Водночас слід зазначити, що функція VPN інтегрована лише в обмежену кількість роутерів, вартість яких зазвичай вища. Серед роутерів, розглянутих у межах дослідження, таку можливість мають лише Wi-Fi роутер Tp-Link AX1500 Wi-Fi 6 і роутер Mikrotik.

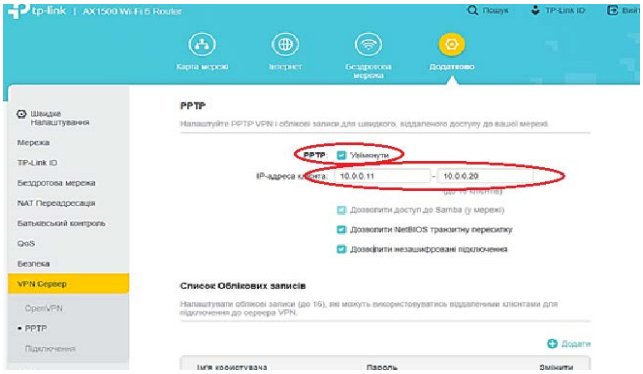


Рис. 11. Налаштування VPN PPTP на роутері Tp_link AX1500

Для створення VPN PPTP на роутері Tp_link AX1500 необхідно перейти на вебсторінку керування приладом та обрати меню «Додатково» – «VPN Сервер» – «PPTP» (рис. 11–12). Включити «PPTP», призначити діапазон IP-адрес користувачів, додати користувачів, вказавши їх паролі та імена.

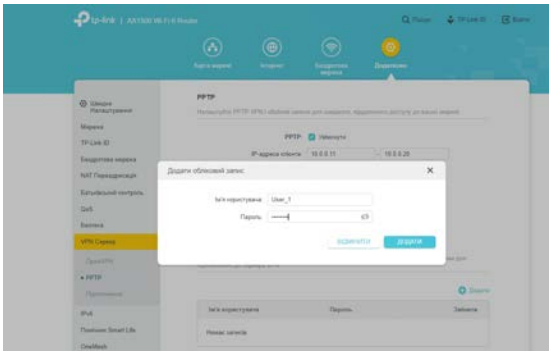
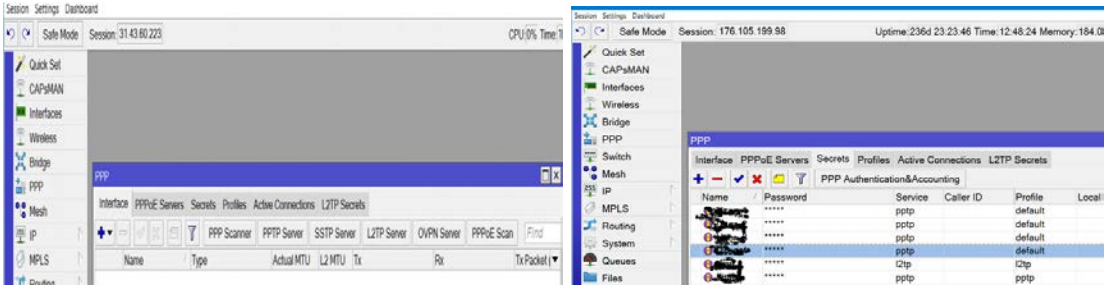


Рис. 12. Створення користувача на роутері Tp_link AX1500 у VPN PPTP

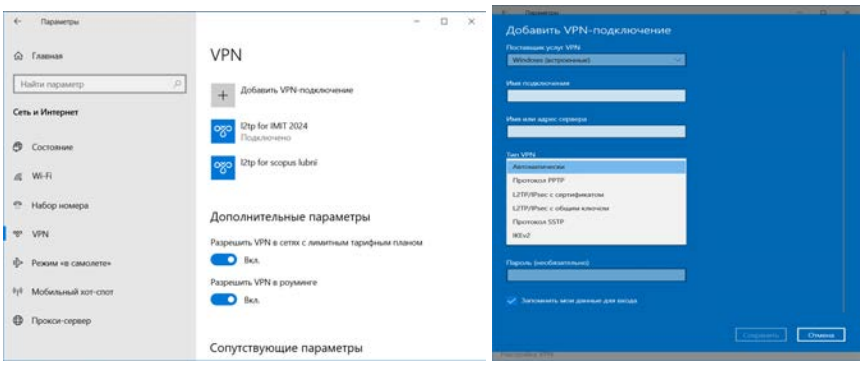
Слід відзначити, що для цього роутера є можливість створити до 16 користувачів, але одночасно можуть працювати тільки 10. Однак, роутер Miktotik такого обмеження не має [9]. У роутері Mikrotik для налаштування PPTP/L2tp/SSTP/OVPN у програмі Winbox [10] треба перейти до меню PPP/interface (рис. 13) та виконати налаштування та активізацію PPTP Server, L2TP Server, а потім налаштувати користувачів та профілі їх приєднання.



а) б)

Рис. 13. Меню Winbox для налаштування VPN у роутері Mikrotik:
а) створення VPN; б) створення користувачів

Усі створені користувачі зможуть підключатися до VPN на своїх персональних комп'ютерах після відповідного налаштування. Наприклад, у ОС Windows 10 це виконується через додаток «Параметри»: потрібно перейти до розділу «Мережа та Інтернет» – VPN – і вибрати «+ Додати VPN-підключення» (рис. 14).



а) б)

Рис. 14. Налаштування VPN у Windows 10:
а) перелік існуючих VPN; б) процес додавання та налаштування VPN

Така система VPN потенційно може бути використана для створення корпоративного середовища для підключення віддалених користувачів. Для цього необхідно більш ретельно провести вибір та перенаалагодження порогових пристроїв, але попередньо, провести ґрунтовний аналіз безпеки ресурсів спрямованих на загальне використання.

Висновки. Серед популярних моделей роутерів лише деякі здатні забезпечувати створення інтегрованої інформаційної системи та об'єднувати користувачів із можливістю віддаленого доступу. Проведений аналіз дозволяє прискорити створення корпоративних мереж у рамках обмежених бюджетів, зокрема для малих підприємств і навчальних закладів.

1. Якщо всі ресурси зосереджені на одному сервері підрозділу, організація віддаленого доступу до нього вирішується на всіх досліджених роутерах за допомогою функції DMZ. Необхідно відзначити, що є можливість використання двох і більше вузлів. Для цього слід мати необхідну кількість реальних IP-адрес: одна адреса на кожен вузол DMZ. Однак, така можливість є тільки у роутера Mikrotik за рахунок створення окремих правил для аналізу IP-адреси призначення. З іншого боку, цей підхід можливо використати при об’єднанні декількох підрозділів. Слід відзначити [1], що, IP вузол, який призначено DMZ не відділяється від внутрішньої мережі та може вільно підключитися до внутрішніх ресурсів. Налаштування DMZ на всіх досліджених роутерах не дозволяє застосувати будь яких заходів безпеки. Для ліквідації такого суттєвого недоліку треба встановлювати та налаштовувати додатковий міжмережевий екран у локальній мережі підрозділу.

2. Коли ресурси різного типу працюють з різними протоколами та розташовані на окремих вузлах підрозділу, організація єдиного інформаційного середовища здійснюється шляхом перенаправлення цих протоколів з урахуванням відповідних портів. Більшість сучасних роутерів підтримують такий підхід, однак необхідно ретельно враховувати специфіку протоколів і портів, які використовуються кожним ресурсом, адже деякі програмні додатки можуть задіювати велику кількість портів одночасно. До недоліків цього методу відноситься складність налаштування фаєрволу й відсутність централізованого контролю доступу, що вимагає індивідуальної конфігурації на кожному вузлі локальної мережі. Водночас цей спосіб може бути застосований для інтеграції кількох підрозділів в єдину систему.

3. Найефективнішим способом організації об'єднаного інформаційного середовища є використання системи серверів VPN. Серед досліджених моделей роутерів лише Tp-Link AX1500 і Mikrotik підтримують використання VPN-серверів з протоколами PPTP/L2TP. Проте залишається актуальною проблема забезпечення безпеки інформаційних ресурсів, яка вимагає окремого налаштування фаєрволу. Практичне впровадження цього підходу також виявило ряд інших недоліків:

– У випадку (рис. 15), коли декілька користувачів знаходяться за одним приладом з NAT виникає конфлікт навіть у разі використання різних імен користувачів. Таким чином одночасно може працювати тільки один.

– З’єднання VPN у операційній системі Windows 10 призначає шлюз за замовчанням на пороговий пристрій. Це приводить до того, що увесь трафік віддаленого користувача проходить через пороговий прилад в незалежності від того використовує користувач локальні ресурси чи ні.

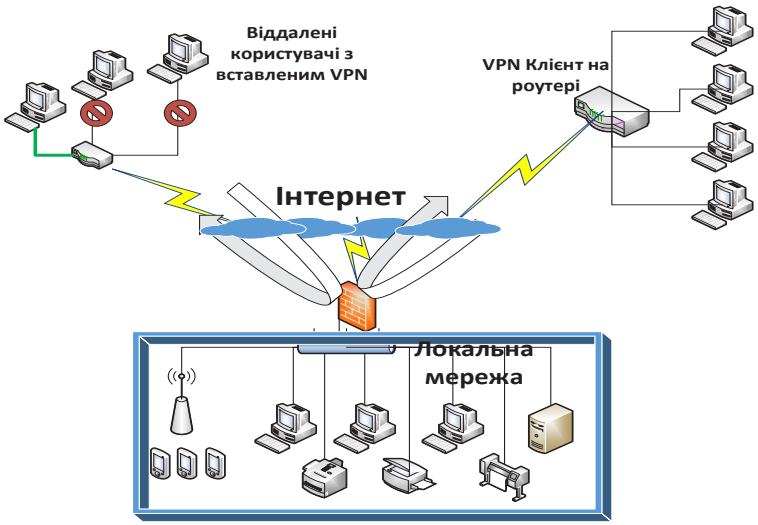


Рис. 15. Особливості VPN

Таким чином, встановлення системи VPN на користувацьких приладах це перший крок створення корпоративного інформаційного середовища, однак його не слід використовувати для об'єднання віддалених підрозділів. Для цього необхідно провести окремий аналіз можливості встановлення VPN клієнтів безпосередньо на порогових приладах віддалених підрозділів.

Отримані результати можуть бути застосовані для побудови інтегрованих інформаційних систем у бізнесі, освіті та інших галузях, які вимагають надійного й безпечного віддаленого доступу користувачів до локальних ресурсів.

Список використаних джерел:

1. Демілітаризована зона (комп'ютерні мережі) URL: https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D0%BC%D1%96%D0%BB%D1%96%D1%82%D0%B0%D1%80%D0%B8%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B0_%D0%B7%D0%BE%D0%BD%D0%B0_(%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%96_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96)#cite_ref-FOOTNOTE%D0%A1%D0%BC%D1%96%D1%822006_2-0

2. Кардашук В., Бортник К., Багнюк Н. Проблеми захисту інформації у віртуальних приватних мережах та відбиття атак на Web-додатки. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2023. № 53. С. 117–124. URL: https://doi.org/10.36910/6775-2524-0560-2023-53-18 .

3. Могильний Г. А. Аналіз програмно-апаратних засобів створення системи з віддаленим доступом до навчальних комп'ютерних лабораторій закладів середньої освіти. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2023. № 1 (277). С. 5–19. URL: https://doi.org/10.33216/1998-7927-2019-256-8-5-19.

4. Могильний Г. А., Семенов М. А., Кірєєв І. Ю. Впровадження системи віддаленого доступу до інформаційних ресурсів комп'ютерних лабораторій. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2022. № 2 (272). С. 7–14. URL: https://doi.org/10.33216/1998-7927-2022-272-2-7-14

5. Недашківський О. Принципи побудови мереж передачі даних для надання vpn і інтернет послуг. *Сучасний захист інформації*. 2017. No2(30). С. 35–41. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/1487/1419.

6. Пархоменко І., Галкін В. Способи захисту каналів корпоративних мереж на базі vpn-рішень. *Сучасний захист інформації*. 2016. № 4. С. 35–40.

7. AC12g Dvukhdyapazonnыi hyhabytnыi Wi-Fi router. URL: https://www.mercusys.com/ru/product/details/ac12g (дата звернення: 21.10.2024).

8. AX1500 Wi-Fi 6 marshrutyzator URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/archer-ax10/ (дата звернення: 21.10.2024)

9. Main Page. Welcome to the MikroTik documentation wiki. URL: https://wiki.mikrotik.com/Main_Page (дата звернення: 21.10.2024)

10. MikroTik Software. Downloads. URL: https://mikrotik.com/download (дата звернення: 21.10.2024)

11. PAT URL: https://uk.wikipedia.org/wiki/PAT (дата звернення: 21.10.2024)

12. Point-to-Point Tunneling Protocol (PPTP) URL: https://www.ietf.org/rfc/rfc2637.txt (дата звернення: 21.10.2024).

13. PPP Protocol. URL: https://www.javatpoint.com/ppp-protocol (дата звернення 21.11.2023).

14. TL-WR840N V6.20. URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/tl-wr840n/ (дата звернення: 21.10.2024).

15. Tyshyk I. CHOICE OF REMOTE ACCESS TECHNOLOGY FOR EFFECTIVE ORGANIZATION OF PROTECTION OF NETWORK CONNECTIONS. Cybersecurity: Education, Science, Technique. 2023. T. 3, № 19. С. 34–45. URL: https://doi.org/10.28925/2663-4023.2023.19.3445.

16. Wi-Fi роутер MikroTik hAP ac3 (RBD53iG-5HacD2HnD). URL: https://www.mikrotik.ua/ru/product/mikrotik-hap-ac3-rbd53ig-5hacd2hnd (дата звернення: 21.10.2024).