РОЗДІЛ ІІ. ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

DOI: 10.25140/2411-5363-2021-4(26)-67-74
УДК 004.7:004.056.55

Євген Риндич[1], Андрій Боровик[2], Олексій Боровик[3]

[1]кандидат технічних наук, доцент, доцент кафедри інформаційних та комп'ютерних систем
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: yevhen.ryndych@stu.cn.ua. **ORCID:** https://orcid.org/0000-0002-2723-4144
ResearcherID: F-6080-2014. **SCOPUS Author ID:** 57188702150

[2]керівник групи цифрового зв'язку АТ «Чернігівобленерго» (Чернігів, Україна)
E-mail: a.borovyk@yahoo.com. **ORCID:** https://orcid.org/0000-0002-9834-325X

[3]заступник начальника відділу 3 територіального вузла урядового зв'язку
Державна служба спеціального зв'язку та захисту інформації України (Миргород, Полтавська обл., Україна)
E-mail: drpeso.jr@gmail.com. **ORCID:** https://orcid.org/0000-0001-5404-5384

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ТУНЕЛЮВАННЯ В СУЧАСНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

У статті наведено результати напівнатурного моделювання мережевої системи та аналіз використання сучасних технологій створення конфіденційних каналів зв'язку (тунелів) у публічних та приватних комп'ютерних мережах. Дослідження проведено з метою виявлення особливостей реалізації та використання програмного забезпечення за умови використання різного апаратного забезпечення відомого виробника мережевого обладнання Mikrotik. Виявлено особливості різних технологій тунелювання, що використовуються в мережевих пристроях з апаратними засобами шифрування, та надано рекомендації щодо їх використання.

Ключові слова: *комп'ютерна мережа; тунель; шифрування; конфіденційність; WireGuard; IPSec; GRE, L2TP; Open VPN; EoIP; ISP.*

Рис.: 8. Табл.: 1. Бібл.: 9.

Актуальність теми дослідження. Сучасні комп'ютерні мережі є гетерогенними, що використовують різні технології та канали зв'язку. Корпоративна мережа підприємства є сукупністю внутрішніх та зовнішніх каналів зв'язку, що поєднують частини цієї корпоративної мережі. Питання конфіденційної передачі інформації в таких мережах є актуальним. Зміни у світі, що привели до збільшення частини працівників [1; 2], що працюють у віддаленому форматі, є одним із факторів, що активно сприяє впровадженню зовнішніх захищених каналів зв'язку з інформаційними системами та підсистемами, що перебувають у внутрішній приватній частині корпоративної мережі. Вимоги, що виникають перед виробниками програмного та апаратного забезпечення комп'ютерних мереж, приводять до впровадження нових програмних та апаратних реалізацій методів і мережевих протоколів конфіденційної передачі інформації [3].

Постановка проблеми. Використання додаткових засобів шифрування дозволяє забезпечити конфіденційність зв'язку, але при цьому впливають на продуктивність систем цифрового зв'язку: завантаження каналу службовими даними, затримки, навантаження на центральний обчислювальний модуль мережевого обладнання. Впровадження та використання нових технологічних рішень у системах безперервного циклу вимагають підвищеної уваги до тих змін, що можуть негативно вплинути на роботу системи загалом. Особливо це важливо для систем критичної інфраструктури.

Для зменшення ризиків, пов'язаних із впровадженням нових рішень у системи безперервного циклу, необхідно провести аналіз та оцінити вплив на основні характеристики систем.

Аналіз останніх досліджень і публікацій. На сьогодні існує велика кількість мережевих протоколів, за допомогою яких можливе створення тунелів як конфіденційних, так і таких, що передають інформацію у відкритому вигляді [4]. Тунелі використовуються не тільки

для забезпечення конфіденційного зв'язку, а для забезпечення живучості комп'ютерних мереж [5]. Сучасне мережеве обладнання – це достатньо складні програмно-апаратні системи, що підтримують багато стандартів та протоколів. Нині відомий виробник мережевого обладнання MikroTik оновив операційну систему RouterOS до версії 7, де основною зміною є використання оновленого ядра Linux версії 5.6.3, що дозволяє використовувати маршрутизаторам декілька варіантів створення захищених з'єднань [3; 6].

Виділення недосліджених частин загальної проблеми. У сучасних дослідженнях основну увагу приділяють алгоритмам шифрування або протоколам тунелювання без урахування особливості пристроїв, що їх реалізують. У разі реалізації за допомогою обладнання або напівнатурного моделювання не оцінюють вплив використаних протоколів на характеристики мережі [7].

Мета дослідження. Метою статті є розвиток напівнатурного моделювання роботи комп'ютерних мереж та інших мережевих систем, який може використовуватися в навчальному процесі [8] та виробничих системах. Результатом моделювання є кількісні показники продуктивності мережевого обладнання та каналів зв'язку.

Виклад основного матеріалу. Напівнатурне моделювання – це моделювання з реальною апаратурою, при якому частина системи моделюється, а решта частини є реальною. Застосування такого методу моделювання стає необхідним у тих випадках, коли не вдається описати роботу деяких елементів системи математично [9].

Для моделювання корпоративної мережі використано реальне обладнання та міжміські канали зв'язку провайдерів. Для отримання точних кількісних характеристик тунелів, побудованих з використанням різних мережевих протоколів, інші види трафіку корпоративної системи приймаються рівними нулю, тобто мають бути відсутні. Запропонована напівнатурна модель з налаштованими інтерфейсами наведена на рис. 1.

Щоб результати були об'єктивними, у тестовій схемі з обох кінців встановлено обладнання MikroTik hAP ac2, у якому наявний апаратний чіп шифрування. Як програмне забезпечення маршрутизаторів використано RouterOS v.7.1. Одне з додаткових питань, які досліджуються, є взаємодія апаратного чіпа шифрування з центральним процесором. Як ISP з обох кінців використано канал 100 Mbps.

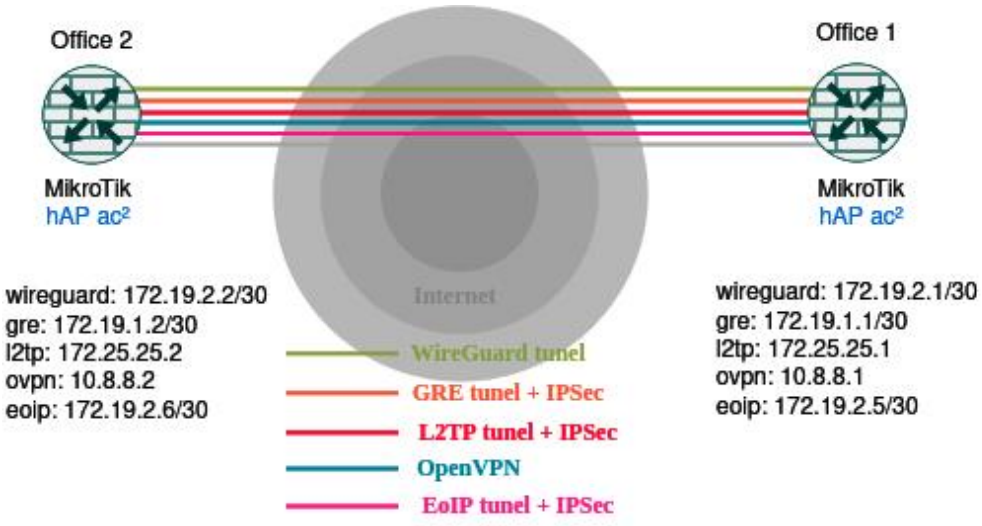

Рис. 1. Схема підключення маршрутизаторів у напівнатурній моделі комп'ютерної мережі

Критерії, які враховано при проведенні експериментів: мережевий протокол тунелювання та шифрування, тип з'єднання транспортного рівня, відправлення чи прийом даних. Як результат проведення експериментального дослідження розглянуто завантаження процесора, корисна пропускна здатність на прийом та передачу.

Для проведення експериментів послідовно налаштовувався один із зазначених типів тунелів. Також для якості зв'язку потрібно розмежувати дослідження пов'язані з транспортним рівнем моделі OSI. Тому для кожного з протоколів використано датаграмний режим передачі даних за допомогою протоколу UDP та зі встановленням з'єднання – протокол TCP.

Як генератор даних для навантаження каналу передачі даних використано стандартний вбудований у RouterOS інструмент Bandwith test. Наявність такого інструмента дозволяє проводити вимірювання саме на мережевому обладнанні та нівелює вплив роботи локальної мережі на результати експериментів. Налаштування типу потоку (транспортного рівня) знаходяться у вікні налаштування Bandwith test (рис. 2).

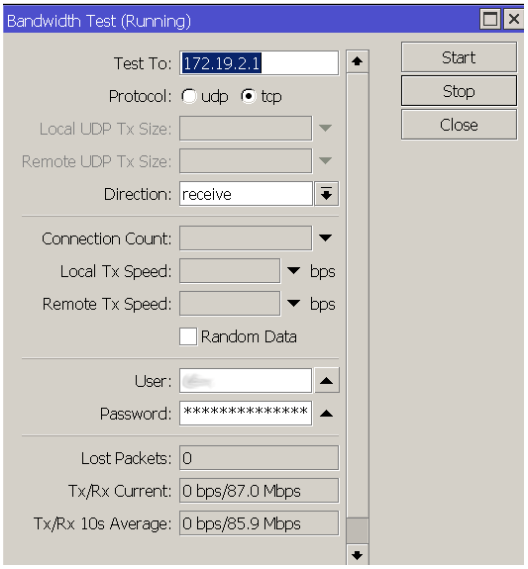

Рис. 2. Налаштування Bandwith test

На рис. 3 наведено результати тестування тунелю, який побудовано за допомогою вбудованого програмного забезпечення, що використовує протокол WireGuard. Як видно з рис. 3 основне навантаження виконується процесором, що свідчить про те, що чіп шифрування в цій реалізації не використовується.

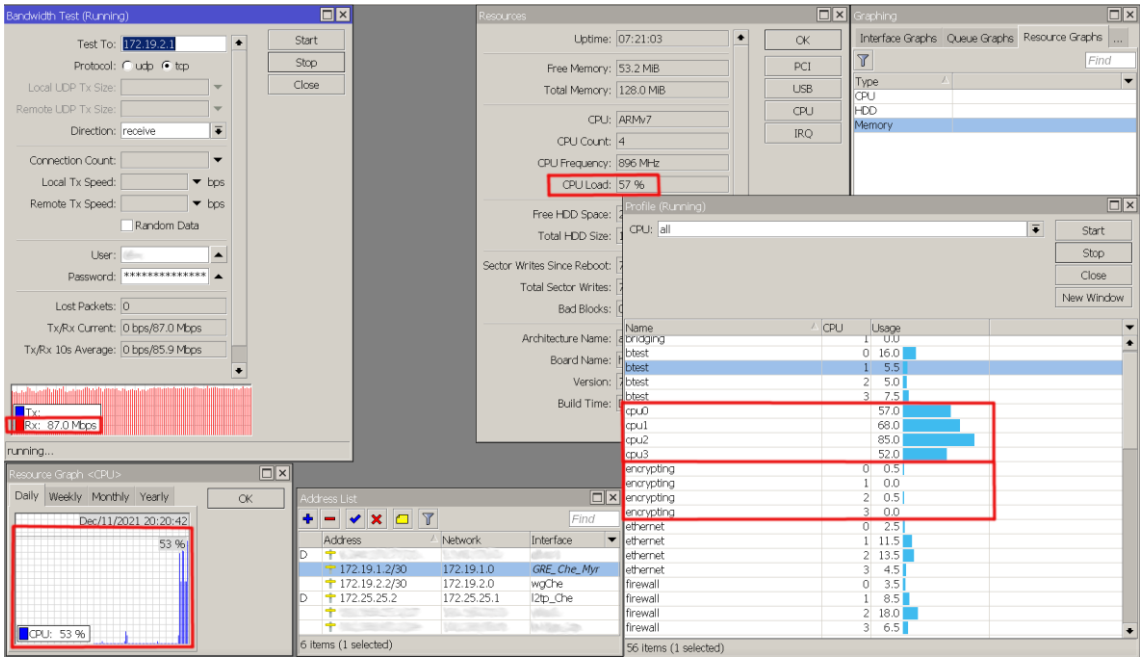

Рис. 3. Тестування тунелю з використанням протоколу WireGuard

На рис. 4 наведено результати тестування тунелю, який побудовано за допомогою вбудованого програмного забезпечення, що використовує протокол GRE + IPSec. Основне навантаження також виконується процесором, отже, чіп шифрування не використовується. Навантаження на процесор менше, ніж у попередньому експерименті.

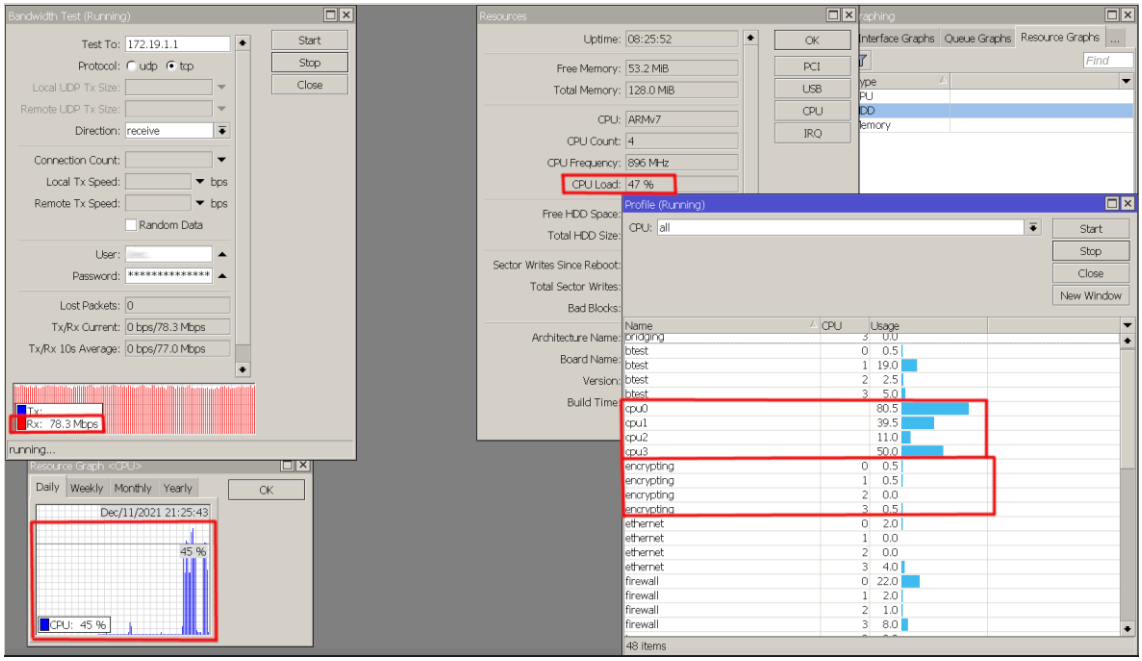

Рис. 4. Тестування тунелю з використанням GRE + IPSec

На рис. 5 наведено результати тестування тунелю, який побудовано за допомогою вбудованого програмного забезпечення, що використовує протокол L2TP + IPSec. Основне навантаження виконується процесором, що означає, що чіп шифрування не використовується. Слід зазначити, що не завжди розподіл навантаження на обчислювальні елементи пропорційний. Це особливо помітно, коли використовується протокол TCP. Згідно з припущенням при встановленні TCP з'єднання весь потік/сеанс оброблюється одним обчислювальним елементом і не змінюється динамічно залежно від навантаження.

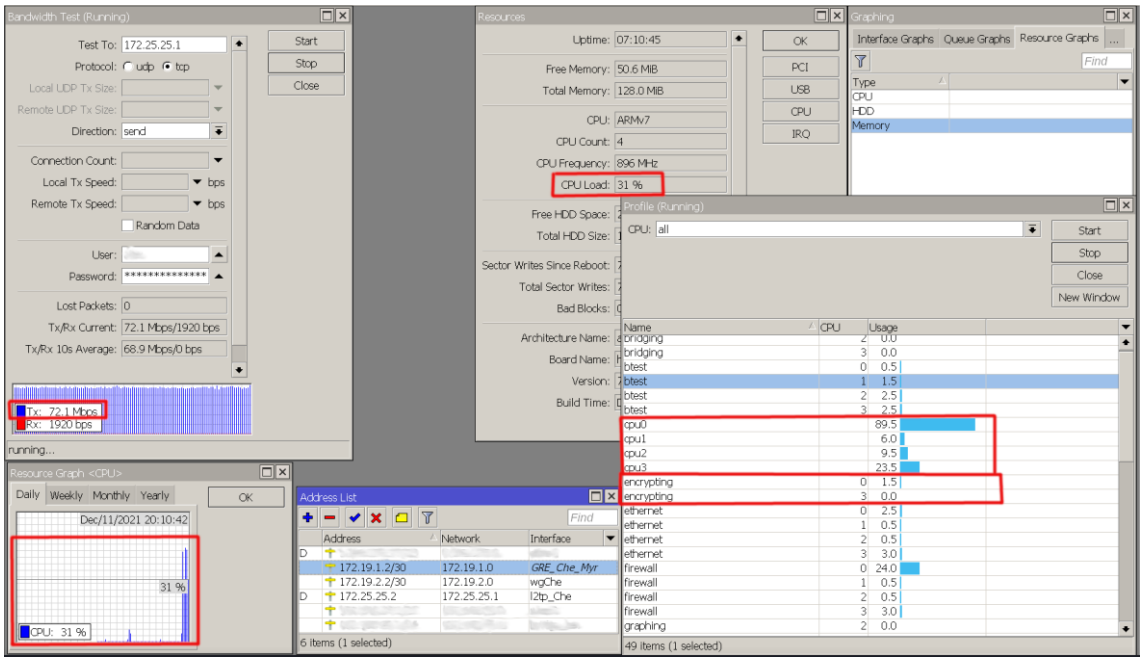

Рис. 5. Тестування тунелю з використанням L2TP + IPSec

На рис. 6 наведено результати тестування тунелю, який побудовано за допомогою вбудованого програмного забезпечення, що використовує протокол EoIP + IPSec. Основне навантаження виконується процесором, що означає, що чіп шифрування не використовується.

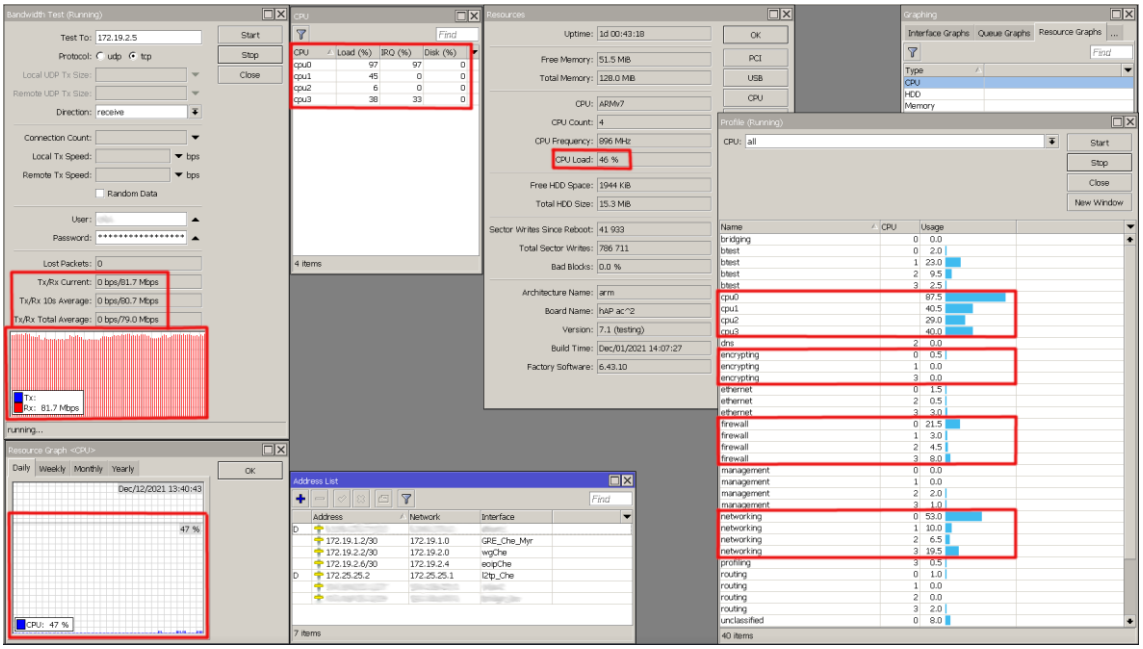

Рис. 6. Тестування тунелю з використанням EoIP + IPSec

На рис. 7 наведено результати тестування тунелю, який побудовано за допомогою вбудованого програмного забезпечення, що використовує протокол OpenVPN. Для цього протоколу передбачено шифрування з використанням апаратного шифрування, що одразу помітно, оскільки навантаження на центральний процесор менше, ніж у попередніх експериментах.

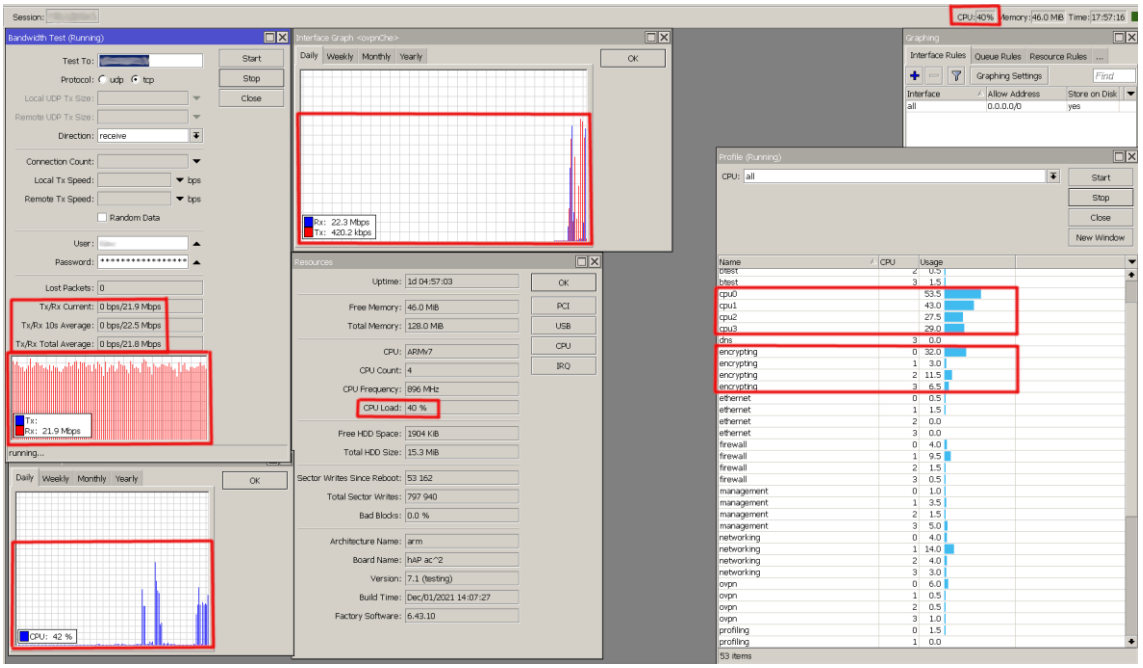

Рис. 7. Тестування тунелю з використанням OpenVPN

Для тунелів, для яких можливо використовувати як транспортний протокол TCP та UDP, було проведеного два експерименти, що підтвердили вже отримані результати.

Одним з основних критеріїв використання тунелів є корисна пропускна здатність каналу (рис. 8). Загальні результати моделювання наведено в таблиці.

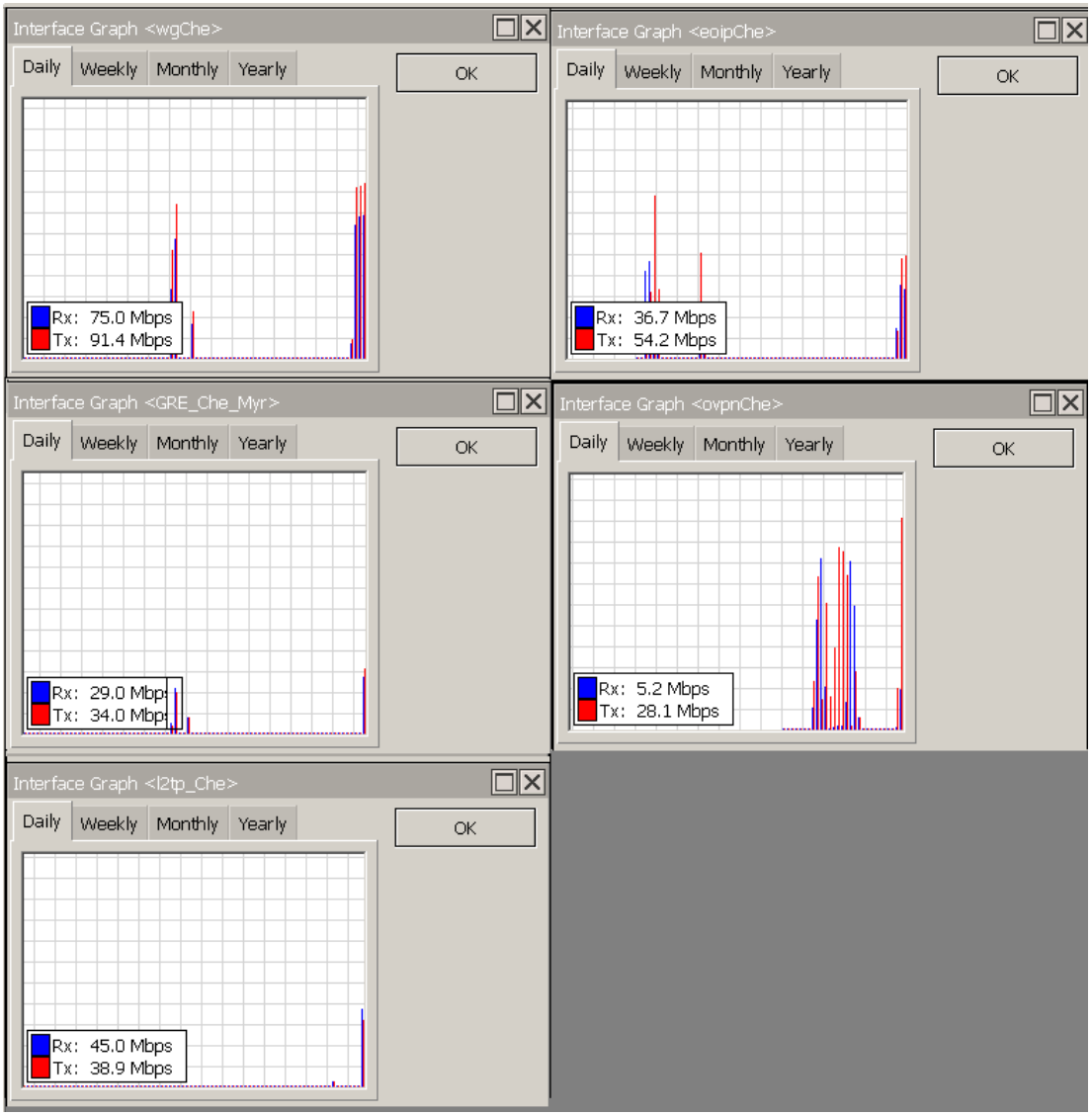

Рис. 8. Корисна пропускна здатність тунелів

Таблиця 1

Загальні результати напівнатурного моделювання

VPN Tunel	**Завантаження CPU, %**	**Rx,** Mbps	**Tx,** Mbps
WireGuard	65	69,7	89,4
GRE + IPSec	43	35,3	50,2
L2TP + IPSec	48	40,3	41,1
EoIP + IPSec	46	50,2	35,0
OpenVPN tcp	40	16,2	12,8
OpenVPN udp	24	30,2	10,4

Висновки. Була створена напівнатурна модель мережевої системи з використанням маршрутизаторів MikroTik. Проведене дослідження дозволило визначити особливості роботи сучасної версії операційної системи RouterOS, а саме визначити протоколи, для яких можливе використання апаратної реалізації алгоритмів шифрування. Особливістю цієї версії є вбудована реалізація тунелю з використанням протоколу WireGuard, який показав високу продуктивність.

Також за допомогою моделі було отримано кількісні показники продуктивності використання тунелів із різними протоколами за умови шифрування даних, що передаються. Ці результати можуть бути використані на виробництві для обґрунтування вибору протоколів та необхідних каналів зв'язку. Як видно з результатів проведених експериментів вплив протоколів та їх реалізацій на корисну пропускну здатність значний та може зменшувати її в декілька разів.

Надалі ця модель може бути використана для тестування каналів зв'язку та аналізу впливу зовнішніх факторів, у тому числі для дослідження можливості несанкціонованого доступу до інформації, що передається в тунелях. Впровадження цієї моделі до навчальних стендів вивчення мережевих технологій забезпечить можливість поглибити знання та набути практичні навички.

Список використаних джерел

1. Количество удаленных работников вырастет до 34,4 % в 2021 году [Электронный ресурс]. – Режим доступа: https://biz.liga.net/ekonomika/it/novosti/kolichestvo-udalennyh-sotrudnikov-v-mire-udvoitsya-v-2021-godu-opros.

2. Полная статистика по удалённой работе за 2021 год [Электронный ресурс]. – Режим доступа: https://promopoisk.com/articles/polnaya-statistika-po-udalyonnoy-rabote-za-2021-god.

3. MikroTik Routers and Wireless - Software [Electronic resource]. – Access mode: https://mikrotik.com/download/changelogs.

4. Generic Routing Encapsulation (GRE) [Electronic resource]. – Access mode: https://www.rfc-editor.org/rfc/pdfrfc/rfc2784.txt.pdf.

5. Коваленко А. А. Метод забезпечення живучості комп'ютерної мережі на основі vpn-тунелювання / А. А. Коваленко, Г. А. Кучук, В. М. Ткачов // Системи управління, навігації та зв'язку : зб. наук. праць. – Полтава, 2021. – Т. 1 (63). – С. 90-95.

6. Download RouterOS 7.1.1 Stable / 7.2 RC 1 / 6.48.6 LTS / 6.49.2 Stable [Electronic resource]. – Access mode: https://www.softpedia.com/get/Internet/Other-Internet-Related/RouterOS.shtml.

7. VPN Site to Site Implementation using Protocol L2TP and IPSEC / B. Santoso, A. Sani, T. Husain, N. Hendri // TEKNOKOM. – 2021. – № 4(1) – Pp. 30-36.

8. Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації / Є. В. Риндич, Т. А. Петренко, Л. Г. Черниш, С. М Семендяй, Г.С. Біленький // Технічні науки та технології. – 2020. – № 2(20). – С. 229–236.

9. Яковлев Ю. С. Принципы организации и применение полу натурного моделирования / Ю. С. Яковлев, А. А. Тимашов // Математические машины и системы. – 2019. – № 2. – С. 80–89.

References

1. Kolichestvo udalennykh rabotnikov vырastet do 34,4 % v 2021 godu [The number of remote workers will grow to 34.4% in 2021]. https://biz.liga.net/ekonomika/it/novosti/kolichestvo-udalennyh-sotrudnikov-v-mire-udvoitsya-v-2021-godu-opros.

2. Polnaia statistika po udalennoi rabote za 2021 god [Complete statistics on remote work for 2021]. https://promopoisk.com/articles/polnaya-statistika-po-udalyonnoy-rabote-za-2021-god.

3. Routers and MikroTik Wireless Devices – Software. (n.d.). https://mikrotik.com/download/changelogs.

4. Generic Routing Encapsulation (GRE). (n.d.). https://www.rfc-editor.org/rfc/pdfrfc/rfc2784.txt.pdf.

5. Kovalenko, A., Kuchuk, H., & Tkachov, V. (2021). Metod zabezpechennia zhyvuchosti kompiuternoi merezhi na osnovi vpn-tuneliuvannia [Method of ensuring the survivability of a computer mesh based on vpn tunneling]. *Systemy upravlinnia, navihatsii ta zviazku – Control systems, navigation and communication* (Vol. 1(63), pp. 90-95). PNTU.

6. Download RouterOS 7.1.1 Stable / 7.2 RC 1 / 6.48.6 LTS / 6.49.2 Stable. https://www.softpedia.com/get/Internet/Other-Internet-Related/RouterOS .shtml.

7. Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN Site to Site Implementation using Protocol L2TP and IPSEC. *TEKNOKOM*, 4(1), 30-36.

8. Ryndych, Y.V., Petrenko, T.A., Chernysh, L.G., Semendiai, S.M., & Bilenkyi, H.S. (2020). Navchalnyi stend dlia vyvchennia dystsyplin iz zabezpechennia merezhevoho zakhystu informa-tsii. *Tekhnichni nauky ta tekhnolohii – Technical sciences and technologies*, (2(20)), 229-236.

9. Yakovlev, Y.S.; Timashov, A.A. (2019). Pryntsipy organizatsii i primenenie polu naturnoho modelirovaniia [Principles of organization and application of semi-natural modeling]. *Matematicheskie mashiny i sistemy – Mathematical machines and systems,* (2), 80–89.

Отримано 30.11.2021

UDC 004.7:004.056.55

Yevhen Ryndych[1], Andrii Borovyk[2], Oleksii Borovyk[3]

[1]PhD in Technical Science, Associate Professor, Associate Professor of Information and Computer Department
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: yevhen.ryndych@stu.cn.ua. **ORCID:** https://orcid.org/0000-0002-2723-4144
ResearcherID: F-6080-2014. **SCOPUS Author ID:** 57188702150

[2]Head of the digital communication group of JSC «Chernihivoblenergo» (Chernihiv, Ukraine)
E-mail: a.borovyk@yahoo.com. **ORCID:** https://orcid.org/0000-0002-9834-325X

[3]Deputy Head Department of 3 Territorial Node of Government Communications
State Service of Special Communications and Information Protection of Ukraine (Myrhorod, Poltava region, Ukraine)
E-mail: drpeso.jr@gmail.com. **ORCID:** https://orcid.org/0000-0001-5404-5384

RESEARCH OF TUNNELING TECHNOLOGIES IN MODERN COMPUTER NETWORKS

Modern corporate networks are a combination of internal and external communication channels. The issue of confidentiality in such networks is relevant. To reduce the risks associated with implementing new solutions in continuous cycle systems, it is necessary to analyze and evaluate their impact.

For now, there is a large number of network protocols that can be used to create tunnels. Modern network equipment is a rather complex software and hardware system that supports many standards and protocols. Well-known network equipment manufacturer MikroTik has upgraded the RouterOS operating system to version 7, where the main change is the use of an updated Linux kernel version 5.6.3, which allows routers to use several different ways to establish secure connections. In modern research, the main attention is paid to encryption algorithms and tunneling protocols without taking into account the peculiarities of implementation.

The aim of the article is to develop semi-natural modeling of networks that can be used in the educational process and production systems. The result of the simulation is quantitative indicators of the performance of network equipment and communication channels. The use of semi-natural modeling is necessary when it is not possible to describe the operation of some elements of the system mathematically. Real network equipment and long-distance communication channels of providers were used to model the corporate network. To make the results objective in the test scheme, MikroTik hAP ac2 equipment with a hardware encryption chip and RouterOS v.7.1 were installed on both ends. A 100 Mbps channel was used as the ISP at both ends. The standard Bandwith test tool built into RouterOS is used as a data generator. The study allowed to determine the features of the modern version of the operating system RouterOS. A feature of this version is the built-in implementation of the tunnel using the WireGuard protocol, which showed high performance. The model was also used to obtain quantitative indicators of the performance of tunnels with different protocols under the condition of encrypting the transmitted data. As can be seen from the results of the experiments, the impact of protocols and their implementations on the useful bandwidth is significant and can reduce it several times.

Keywords: *computer network; tunnel; encryption; privacy; WireGuard; IPSec; GRE; L2TP; Open VPN; EoIP; ISP.*
Fig.: 8. Table: 1. References: 9.

Риндич Є., Боровик А., Боровик О. Дослідження технологій тунелювання в сучасних комп'ютерних мережах. *Технічні науки та технології.* 2021. № 4(26). С. 67-74.