

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

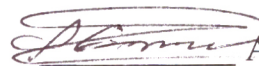
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології організації захищеного
віддаленого доступу користувачів на базі рішень
компанії Palo Alto Networks»

Виконав студент 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 Богдан Рудюк

Керівник, завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Андрій Єфіменко

Рецензент, професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

 Володимир Воротніков

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Рудюк Богдан Миколайович

Тема роботи: «Методи та технології організації захищеного віддаленого доступу користувачів на базі рішень компанії Palo Alto Networks»

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи 24 грудня 2024 р.

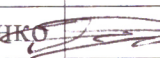
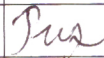
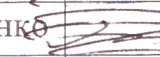
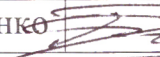
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

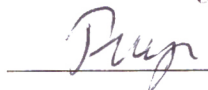
Об'єктом дослідження є організація захищеного віддаленого доступу користувачів. Предметом дослідження є методи та технології захищеного віддаленого доступу з використанням рішень Palo Alto Networks.

Обладнання та програмне забезпечення:

1. Мережевий емулятор GNS3
2. Гіпервізор Oracle VirtualBox
3. Образ міжмережного екрану Palo Alto Networks
4. GlobalProtect VPN
5. Windows 10

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

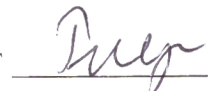
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Андрій Єфіменко	 17.09.2024	 17.09.2024
2	Андрій Єфіменко	 12.10.2024	 12.10.2024
3	Андрій Єфіменко	 17.12.2024	 17.12.2024

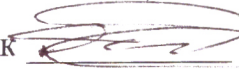
Студент  Богдан Рудюк

Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення з вимогами до виконання магістерської роботи	17.09.2024	виконано
2	Розробка плану та завдання роботи	18.09.2024 – 26.09.2024	виконано
3	Збір та аналіз літератури	27.09.2024 – 05.10.2024	виконано
4	Дослідження мереж з віддаленим доступом користувачів	06.10.2024 – 16.10.2024	виконано
5	Дослідження технологій компанії Palo Alto Networks	17.10.2024 – 29.10.2024	виконано
6	Розробка топології мережі	30.10.2024 – 09.11.2024	виконано
7	Вибір обладнання та програмного забезпечення	10.11.2024 – 17.11.2024	виконано
8	Базове налаштування проєкту	18.11.2024 – 25.11.2024	виконано
9	Налаштування міжмережного екрану	26.11.2024 – 06.12.2024	виконано
10	Тестування працездатності проєкту	07.12.2024 – 13.12.2024	виконано
11	Оформлення пояснювальної записки	14.12.2024 – 23.12.2024	виконано
12	Захист	24.12.2024	виконано

Студент  Богдан Рудюк

Керівник  Андрій Єфіменко

АНОТАЦІЯ

Кваліфікаційна робота присвячена аналізу методів захисту мереж та ключових загроз, з якими стикаються організації з віддаленими користувачами, а також особливості використання рішень компанії Palo Alto Networks для підвищення рівня безпеки мережевої інфраструктури. Текстова частина викладена на 83 сторінок друкованого тексту. Пояснювальна записка має 11 сторінок додатків. Список використаних джерел містить 33 найменування і займає 3 сторінки. В роботі наведено 48 рисунків та 3 таблиці. Загальний обсяг роботи – 94 сторінок.

Метою роботи є розробка та впровадження методів і технологій організації захищеного віддаленого доступу користувачів на базі рішень компанії Palo Alto Networks для підвищення інформаційної безпеки корпоративних мереж.

В рамках роботи було проведено аналіз сучасного стану віддаленої та гібридної роботи, визначено основні загрози для мереж із віддаленим доступом і розглянуто сучасні підходи до їх захисту. Вивчено можливості технологій Palo Alto Networks, зокрема міжмережевих екранів та VPN-рішень GlobalProtect, для забезпечення високого рівня безпеки даних. На основі отриманих даних розроблено структуру захищеної мережі для віддалених користувачів, реалізовано її налаштування та проведено тестування, яке підтвердило відповідність рішення сучасним стандартам кібербезпеки. Запропоноване рішення забезпечує надійний захист інформаційних ресурсів і є актуальним для організацій із віддаленим або гібридним форматом роботи.

КЛЮЧОВІ СЛОВА: ВІДДАЛЕНИЙ ДОСТУП, ЗАХИСТ МЕРЕЖ, PALO ALTO NETWORKS, GLOBAL PROTECT, БЕЗПЕКА ДАНИХ, МІЖМЕРЕЖНИЙ ЕКРАН НАСТУПНОГО ПОКОЛІННЯ.

ANNOTATION

The qualification work is devoted to the analysis of network protection methods and key threats faced by organizations with remote users, as well as the peculiarities of using Palo Alto Networks solutions to enhance the security of network infrastructure. The textual part comprises 83 pages of printed text. The explanatory note includes 11 pages of appendices. The list of references contains 33 items and occupies 3 pages. The work features 48 figures and 3 tables. The total volume of the work is 94 pages.

The purpose of the work is to develop and implement methods and technologies for organizing secure remote access for users based on Palo Alto Networks solutions to enhance the information security of corporate networks.

The study includes an analysis of the current state of remote and hybrid work, identification of key threats to networks with remote access, and a review of modern approaches to their protection. The capabilities of Palo Alto Networks technologies, particularly next-generation firewalls and GlobalProtect VPN solutions, were examined to ensure a high level of data security. Based on the obtained data, a secure network structure for remote users was developed, configured, and tested, confirming the solution's compliance with modern cybersecurity standards. The proposed solution provides reliable protection of information resources and is relevant for organizations with remote or hybrid work formats.

KEYWORDS: REMOTE ACCESS, NETWORK PROTECTION, PALO ALTO NETWORKS, GLOBAL PROTECT, DATA SECURITY, NEXT-GENERATION FIREWALL.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ	10
1.1 Аналіз сучасного стану віддаленої та гібридної роботи	10
1.2 Аналіз актуальних загроз та сучасних підходів до захисту в мережах з віддаленим доступом користувачів.....	15
1.3 Аналіз сучасних технологій для організації захищеного віддаленого доступу.....	26
Висновки до першого розділу	32
РОЗДІЛ 2. РОЗРОБКА ПРОЄКТУ ЗАХИЩЕНОЇ МЕРЕЖІ З ВІДДАЛЕНИМ ДОСТУПОМ КОРИСТУВАЧІВ.....	34
2.1 Проєктування структурної схеми мережі з віддаленим доступом користувачів	34
2.2 Вибір мережевого обладнання для організації роботи мережі	37
2.3 Вибір програмного забезпечення та засобів захисту мережі з віддаленим доступом користувачів.....	48
Висновки до другого розділу.....	53
РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИЩЕНОЇ МЕРЕЖІ З ВІДДАЛЕНИМ ДОСТУПОМ КОРИСТУВАЧІВ.....	54
3.1 Базове налаштування захищеної мережі та міжмережного екрану Palo Alto	54
3.2 Налаштування GlobalProtect VPN на міжмережному екрані Palo Alto для підключення віддалених користувачів.....	62
3.3 Тестування функціональних можливостей та моніторинг захищеної мережі з віддаленим доступом користувачів	71
Висновки до третього розділу	77
ВИСНОВКИ	79
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	81
ДОДАТКИ	84

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol
VPN – Virtual Private Network
NGFW – Next Generation Firewall
ZTNA – Zero Trust Network Access
GP – GlobalProtect
IoT – Internet of Thing
LAN – Local Area Network
WAN – Wide Area Network
DMZ – Demilitarized Zone
IPS – Intrusion Prevention System
NAT – Network Address Translation
PAT – Port Address Translation
HTTP – Hypertext Transfer Protocol
HTTPS – HyperText Transfer Protocol Secure
SDP – Session Description Protocol
RDP – Remote Desktop Protocol
SASE – Secure Access Service Edge
IAM – Identity and Access Management
PAM – Privileged Access Management
TLS – Transport Layer Security
SSL – Secure Sockets Layer

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку цифрових технологій організація захищеного віддаленого доступу є одним із ключових завдань для підприємств. Події останніх років, такі як пандемія COVID-19, змусили більшість компаній перейти на гібридні або повністю віддалені моделі роботи, що значно збільшило залежність від технологій віддаленого доступу. Однак цей перехід супроводжується новими викликами, серед яких найважливішим є забезпечення кібербезпеки.

Кіберзагрози, пов'язані з віддаленим доступом, зокрема фішинг, злом облікових записів та атаки на вразливі місця програмного забезпечення, становлять серйозну небезпеку для організацій. У зв'язку з цим впровадження сучасних методів і технологій забезпечення захищеного віддаленого доступу є нагальним завданням.

Рішення компанії Palo Alto Networks, такі як міжмережеві екрани нового покоління (NGFW) та платформа GlobalProtect, зарекомендували себе як ефективні інструменти для забезпечення безпеки мережевих з'єднань. Ці технології забезпечують комплексний підхід до захисту, що є критично важливим у контексті еволюції кіберзагроз.

Метою роботи є розробка та впровадження методів і технологій організації захищеного віддаленого доступу користувачів на базі рішень компанії Palo Alto Networks для підвищення інформаційної безпеки корпоративних мереж.

Об'єкт дослідження: процес організації захищеного віддаленого доступу користувачів.

Предмет дослідження: методи та технології організації захищеного віддаленого доступу на базі рішень компанії Palo Alto Networks.

Завдання роботи:

- Провести аналіз сучасних технологій організації віддаленого доступу користувачів.
- Вивчити актуальні загрози та вразливості в мережах із віддаленим доступом.

- Розробити проєкт захищеної мережі для віддалених користувачів із використанням рішень Palo Alto Networks.
- Реалізувати базові налаштування міжмережного екрану та платформи GlobalProtect.
- Провести тестування функціональності впровадженої системи.

Результати дослідження можуть бути впроваджені в організаціях, які використовують або планують використовувати рішення для віддаленого доступу. Запропоновані технології дозволяють знизити ризики витоку інформації та підвищити ефективність функціонування корпоративних мереж.

За результатами досліджень було опубліковано:

1. Рудюк Б. М., Єфіменко А. А. Забезпечення мобільності та віддаленого доступу користувачів з використанням рішень palo alto global protect. Тези доповідей XIV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2024», 28-29 березня 2024 р. Житомир: Житомирська політехніка, 2024. с.65-68

2. Рудюк Б. М., Єфіменко А. А. Порівняльний аналіз ZTNA та ZTNA 2.0. Тези доповідей XIV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2024», 28-29 березня 2024 р. Житомир: Житомирська політехніка, 2024. с.69-70

3. Рудюк Б. М., Єфіменко А. А. Способи захисту даних в умовах віддаленої та гібридної роботи. Тези доповідей VII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення – 2024», 02-03 грудня 2024 р. Житомир: Житомирська політехніка, 2024.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Аналіз сучасного стану віддаленої та гібридної роботи

З погляду інформаційної безпеки, віддалений доступ до мережі є процесом, за допомогою якого користувачі можуть з'єднуватися з центральною мережею чи іншими ресурсами, використовуючи зовнішні мережі, такі як Інтернет. Забезпечення віддаленого доступу є важливим для різних категорій користувачів, наприклад [1]:

- студентів;
- співробітників;
- окремих структурних підрозділів організації чи в цілому організацій будь-якого масштабу.

Захищений віддалений доступ відкриває перед студентами можливість брати участь у віддалених заняттях, співпрацювати над груповими проектами та користуватися різноманітними освітніми матеріалами, необхідними для їхнього успішного навчання. Важливою перевагою цього підходу є забезпечення безпеки особистих даних та збереження конфіденційності студентської інформації. Такий захищений доступ дозволяє студентам вільно використовувати ресурси та інтерактивні можливості для навчання, не хвилюючись про можливі ризики витоку особистих даних.

Працівники отримують значні переваги від надійного віддаленого доступу, оскільки він дозволяє їм працювати з будь-якого місця. Завдяки надійному віддаленому доступу, працівники можуть ефективно керувати своїм часом, пристосовуючи графік роботи до власних потреб і при цьому забезпечуючи безпеку конфіденційної інформації, що зберігається на корпоративних серверах. Такий підхід підвищує продуктивність та забезпечує комфортні умови праці, що, в свою чергу, може позитивно позначитися на загальному успіху бізнесу.

В сфері бізнесу безпечний віддалений доступ є обов'язковим. Він забезпечує можливість працювати віддалено для співробітників без ризику витоку конфіденційної інформації компанії. Завдяки цьому підходу, бізнес зберігає

стабільну продуктивність, а дані залишаються в надійній безпеці, не відкриваючи можливості для неправомірного доступу чи порушення конфіденційності. Такий захищений віддалений доступ є ключовим фактором для забезпечення безперервного функціонування бізнесу в сучасному цифровому середовищі.

У минулому віддалений доступ був послугою, яку компанії надавали через модеми з комутованим доступом. Щоб уникнути витрат на міжміські або безкоштовні телефонні лінії, компанії почали застосовувати методи віддаленого доступу, які використовують переваги загальнодоступних мереж через Інтернет. Еволюція інтернет-технологій призвела до паралельного зростання віддаленого доступу з більш адаптивними та безпечними варіантами.

Віддалений доступ, як для окремих користувачів, так і для структурних підрозділів організації чи в цілому організацій будь-якого масштабу надає такі переваги [2]:

- гнучкість доступу;
- гнучке налагодження та низька вартість;
- повний контроль над авторизацією та доступом;
- використання централізованого сховища даних та резервного копіювання;
- підвищення продуктивності співробітників.

Головною перевагою віддаленого доступу є його гнучкість та простота. У ситуаціях, коли робота в офісі стає складною або неможливою, забезпечення неперервності бізнесу стає критично важливим. Забезпечуючи віддалений доступ, працівники можуть залишатися на зв'язку, працюючи з будь-якого місця, що дозволяє уникнути втрат часу. Це також надає більшу гнучкість у структуруванні команди, дозволяючи підтримувати зв'язок під час подорожей членів команди або навіть наймати працівників з будь-якого куточка світу.

Важливим питанням організації віддаленого доступу є його гнучкість налагодження та низька вартість. Вартість та можливості налаштування мережі віддаленого доступу повністю залежать від потреб користувача. Для малих підприємств хмарні рішення можуть бути оптимальними, спрощуючи процес підключення через онлайн-інструменти. Онлайн-системи співпраці, такі як Google

Drive або Dropbox, дозволяють зберігати та обмінюватися файлами з можливістю належного авторизованого доступу, а також існують програмні засоби для віддаленого доступу до робочого столу, що дають можливість працювати з офісним комп'ютером з будь-якого місця.

Налаштування мережі віддаленого доступу дозволяє встановлювати різні рівні авторизації для різних користувачів, що гарантує доступ лише до необхідних областей мережі. Адміністратори здатні контролювати доступ та відстежувати дії користувачів, забезпечуючи додатковий рівень безпеки.

Використання віддаленого доступу дає можливість регулярно створювати резервні копії важливих даних, що значно знижує ризик втрати інформації внаслідок нещасних випадків або збоїв комп'ютерів. Це дозволяє забезпечити безпеку і надійність збереження даних, що є критичним аспектом для будь-якого бізнесу або організації. Крім того, наявність централізованого сховища даних дозволяє забезпечити надійний захист інформації від втрати та неправомірного доступу. Такий підхід до збереження даних є ключовим для забезпечення безпеки та неперервності роботи в організації.

Використання віддаленого доступу сприяє продуктивній співпраці, спрощуючи обмін та поширення інформації в команді незалежно від місця розташування користувачів.

Хоча віддалений доступ пропонує безліч переваг, але існують кілька недоліків, які важливо врахувати:

- зниження продуктивності;
- зменшення надійності;
- збільшення складності управління;
- збільшення ймовірності порушення політики безпеки.

Віддалений доступ до систем може знизити продуктивність через збільшену затримку сервера та довший цикл зворотного зв'язку при внесенні змін до локальної інфраструктури. Підключення до Інтернету та швидкість впливають на продуктивність, оскільки різні віддалені розташування можуть мати різний рівень обслуговування.

Управління дозволами та налаштування/авторизація VPN може забирати значну кількість часу в ІТ-спеціалістів. Вирішення проблем віддаленого доступу також вимагає додаткових навичок системного адміністратора, яких не завжди вистачає.

Використання служби віддаленого доступу може створювати проблеми з контролем версій, коли різні користувачі мають різні версії важливих документів з відмінностями між ними. Крім того, ризик збереження даних на пристроях співробітників може порушувати політику компанії, тому важливо навчити персонал правильному етикету під час роботи зі спільними файлами в мережі.

Віддалена та гібридна робота зазнала значного розвитку під час пандемії COVID-19, яка стала каталізатором змін у світі праці. Хоча ці моделі набували популярності ще до пандемії, обмеження, пов'язані з нею, змусили організації швидко адаптуватися до нових умов. Для багатьох компаній цей вимушений експеримент виявився успішним, що сприяло сталому переходу до гнучких форматів роботи. Такий перехід вплинув не лише на організацію праці, але й на корпоративну культуру, акцентуючи важливість самостійності працівників.

Ключовою причиною популярності віддаленої роботи стало бажання працівників мати більше гнучкості у виборі місця та часу для роботи, що позитивно впливає на баланс між роботою та особистим життям. Це особливо актуально в умовах високих витрат на транспорт, а також у постійно змінюваному економічному середовищі. Гібридна модель роботи стала оптимальним компромісом, поєднуючи переваги як віддаленої, так і офісної роботи. Вона дозволяє зберігати взаємодію в команді та забезпечувати при цьому гнучкість.

Розвиток цифрових технологій, таких як хмарні сервіси, інструменти для відеоконференцій, платформи для спільної роботи та технології захисту даних, стали основою для успішної реалізації віддаленої роботи. Без сучасних технологій була б неможлива інтеграція віддаленого і гібридного формату роботи [5].

Однак поряд із численними перевагами, віддалена та гібридна робота також мають низку викликів. Серед них — проблеми з ізоляцією працівників, емоційне вигорання та складнощі в управлінні. Відсутність фізичного контакту може

призводити до почуття відчуження серед працівників, що погіршує командну взаємодію. Для вирішення цих проблем важливо впроваджувати підтримку ментального та фізичного здоров'я співробітників, зокрема через програми для зниження стресу та забезпечення фізичної активності.

Також необхідно приділяти увагу розвитку навичок самостійного управління часом у працівників, оскільки відсутність чіткої регламентації робочого часу може призвести до перевантаження чи зниження ефективності. Важливо забезпечити правильну адаптацію нових співробітників у віддалений формат, що вимагає змін у стратегії навчання та підтримки кадрів.

З економічного погляду віддалена робота дозволяє компаніям значно знижувати витрати на утримання офісів, витрати на транспорт і комунальні послуги. Окрім цього, ці моделі роботи дозволяють залучати таланти з усього світу, що може позитивно впливати на фінансову стабільність підприємств.

Окрім того, віддалена робота дає змогу компаніям скорочувати плинність кадрів, оскільки співробітники з більшою ймовірністю залишатимуться в компаніях, які пропонують гнучкі умови роботи, що дозволяють краще поєднувати кар'єру та особисте життя.

Прогнозується, що до 2025 року близько 70% компаній по всьому світу запровадять гібридні моделі роботи як основний формат. Відповідно, організації повинні будуть активно інвестувати у цифрову інфраструктуру, покращуючи засоби для комунікації та спільної роботи, а також удосконалюючи системи кібербезпеки. Ці інвестиції допоможуть забезпечити ефективне управління віддаленими командами та оптимізувати процеси контролю за результатами праці.

Загалом, розвиток віддаленої та гібридної роботи є важливим етапом у трансформації сучасних організацій. Компанії, які адаптуються до цих змін і правильно використовують технології, зможуть забезпечити не тільки гнучкість і ефективність роботи, але й стійкість у швидко змінному світі. Інвестиції в цифрову інфраструктуру, підтримку здоров'я співробітників та навчання новим інструментам допоможуть зберегти конкурентоспроможність і забезпечити стабільний розвиток бізнесу в умовах глобалізації та цифровізації.

1.2 Аналіз актуальних загроз та сучасних підходів до захисту в мережах з віддаленим доступом користувачів

Зростання популярності віддаленої роботи та розширення використання хмарних сервісів призвели до збільшення кількості та складності загроз, з якими стикаються мережі з віддаленими користувачами. Захист таких мереж стає все більш важливим завданням для будь-якого бізнесу, який прагне зберегти свої дані та системи безпечними.

Сучасні мережі з віддаленими користувачами мають складну структуру, яка включає в себе різні компоненти, такі як користувачі (співробітники компанії або сторонні особи, які мають доступ до мережі), пристрої (комп'ютери, смартфони, планшети, IoT-пристрої), мережеве обладнання (маршрутизатори, комутатори, брандмауери та інші пристрої, які забезпечують роботу мережі), програмне забезпечення (операційні системи, служби, додатки та інші програмні продукти, які використовуються в мережі). Кожен з цих компонентів може бути мішенню для різноманітних загроз.

Далі розглянуто три основні категорії загроз:

- загрози технічного характеру;
- загрози з боку користувачів;
- загрози з боку зовнішніх атак.

Загрози технічного характеру є важливим аспектом в сучасному інформаційному середовищі, особливо в контексті мереж з віддаленими користувачами. Ці загрози можуть мати різноманітні прояви і походити від апаратних, програмних проблем, стихійних лих і несанкціонованого доступу. Далі розглянуто кожен з цих аспектів докладніше:

1. Апаратні збої є однією з найпоширеніших причин перебоїв у роботі мереж. Їх може спричинити ряд факторів, таких як старіння обладнання, перегрів, помилки виробництва або людський фактор. Наслідки апаратних збоїв можуть відрізнятися в залежності від типу та серйозності проблеми, включаючи, але не обмежуючись, перебоями в роботі мережі, повним відключенням мережі, втратою даних і фінансовими збитками. Наприклад, відмова ключового комутатора, що забезпечує

передачу даних між різними частинами мережі, може спричинити відсутність зв'язку між вузлами мережі. Це може призвести до відключення користувачів від основних ресурсів мережі, включаючи доступ до Інтернету, спільних файлів, електронної пошти та інших сервісів. Крім того, великі апаратні збої можуть мати серйозний вплив на продуктивність і функціонування організаційних процесів, збільшуючи час відновлення систем та можливі витрати на їх відновлення або заміну.

2. Відключення електроенергії є серйозною загрозою для неперервності роботи мереж. У випадку відключення живлення, якщо не вжиті додаткові заходи захисту, може відбутися відключення мережевих пристроїв, що може призвести до відсутності доступу до мережі та її ресурсів. Ця загроза набуває особливого значення у районах з нестабільним електропостачанням, де такі випадки можуть відбуватися частіше та мати більший вплив на працездатність мережі. Брак електропостачання може виникнути з різних причин, включаючи природні катастрофи, технічні несправності або планові вимкнення електромережі для обслуговування або ремонту.

3. Стихійні лиха, такі як повені, пожежі, землетруси та інші природні катастрофи, представляють серйозну загрозу для мережевої інфраструктури. Це може мати руйнівний вплив на мережеві пристрої, кабелі та інші компоненти, призводячи до фізичних пошкоджень і відмов їх роботи.

У мережах, де користувачі можуть отримувати доступ до ресурсів віддалено, існує ряд загроз, пов'язаних з їх діяльністю. Ці загрози можуть мати значний вплив на безпеку та працездатність мережі, а також на конфіденційність та цілісність даних. Далі розглянуто найпоширеніші загрози з боку користувачів:

1. Недбале поводження з даними може мати серйозні наслідки для безпеки та конфіденційності інформації. Користувачі можуть ненавмисно видалити або пошкодити важливі дані, що призведе до втрати цінної інформації та перешкодить нормальному функціонуванню системи. Крім того, небезпечне розповсюдження конфіденційної інформації може спричинити проникнення несанкціонованих осіб

до цієї інформації, що порушить її конфіденційність та може викликати серйозні проблеми з безпекою мережі.

2. Ненадійні паролі, які легко вгадати або зламати, роблять мережі та дані вразливими. Користувачі часто обирають прості або очевидні комбінації, що робить їхні акаунти мішенню для зловмисників. Також, змішування домашніх і робочих паролів і навіть повторне використання одних і тих самих паролів додає ще більше ризиків. Якщо один сайт буде зламаний, а пароль стане доступним публічно, зловмисники можуть отримати доступ до всіх облікових записів користувача, включаючи корпоративні. Ця проблема стає ще більш актуальною при віддаленій роботі, коли співробітники використовують особисті пристрої та мережі зі значно нижчими стандартами безпеки, що полегшує зловмисникам доступ до даних компанії. [4]

3. Встановлення шкідливого програмного забезпечення може стати серйозною загрозою для безпеки інформації та інфраструктури. Користувачі можуть ненавмисно встановити шкідливе програмне забезпечення на свої пристрої, що може призвести до крадіжки конфіденційних даних, порушення нормальної роботи мережі або інших серйозних проблем.

4. Недотримання правил безпеки може стати джерелом серйозних загроз для безпеки інформації та інфраструктури. Користувачі, які не дотримуються встановлених норм та процедур безпеки, можуть стати причиною витоку конфіденційної інформації, зараження мережі шкідливим програмним забезпеченням або виникнення інших серйозних проблем.

Загрози з боку зовнішніх атак у мережах з віддаленими користувачами або доступом є однією з найбільш актуальних проблем в сучасному цифровому світі. Далі розглянуто ці загрози:

1. Соціальна інженерія, яка включає в себе фішингові атаки, тепер має додаткові можливості, оскільки працівники знаходяться у різних фізичних місцях. Відсутність прямого контакту ускладнює виявлення обману, оскільки в цьому контексті виглядати як колега чи керівник стає набагато простіше. У ситуації, коли робочий процес вимагає від співробітників великої концентрації та швидкості

реакції, вони стають більш вразливими до емоційно мотивованих фішингових атак. Наслідком цього є те, що фішингові атаки стають не лише більш поширеними, але й витонченішими. Зловмисники постійно вдосконалюють свої методи, щоб обійти захист та викликати максимальний ступінь довіри серед працівників. У такому контексті важливо, щоб співробітники були добре підготовлені та свідомі ризиків, пов'язаних з фішингом, а також виявляли пильність та обережність при отриманні та обробці електронної пошти та інших комунікаційних каналів.

2. Атаки "людина посередині" (Man-in-the-Middle, MITM) визначаються як одна з найпоширеніших загроз безпеці, що стикаються з віддаленими співробітниками. Ці атаки дозволяють кіберзлочинцям прослуховувати або навіть змінювати передачу даних, виступаючи як посередники між двома взаємодіючими сторонами. Жертва, яка не підозрює нічого підозрілого, може сприйняти транзакцію як звичайну, тоді як зловмисник має можливість отримати доступ, змінити або навіть вкрати інформацію, що передається. Варіанти атак MITM можуть бути різноманітними, включаючи злам електронної пошти, прослуховування Wi-Fi, перехоплення сесії, видалення SSL та підміну системи доменних імен (DNS). Ці загрози становлять серйозну небезпеку для будь-якої організації або користувача, особливо тих, хто працює з конфіденційними даними чи корпоративною інформацією.

Тому, безпечний віддалений доступ – це комплекс правил, процесів, програмного та апаратного забезпечення, спрямованих на забезпечення безпеки та доступності даних. Цей процес включає в себе забезпечення безпечного доступу до локальних мереж або хмарних сервісів для співробітників, постачальників та інших довірених партнерів, які фізично перебувають поза корпоративним приміщенням організації. Завдяки безпечному віддаленому доступу ці особи можуть користуватися тими ж ресурсами, що й співробітники, які працюють в межах офісу.

Безпечний віддалений доступ має важливе значення з трьох причин. По-перше, він сприяє захисту інтелектуальної власності, забезпечуючи безпеку даних навіть у віддалених умовах. По-друге, він підвищує продуктивність праці співробітників, дозволяючи їм працювати з будь-якого місця, що сприяє

оперативному вирішенню завдань та збільшенню ефективності. По-третє, це допомагає організаціям зберігати конкурентні переваги, оскільки співробітники можуть швидко реагувати на зміни на ринку та впроваджувати нові ідеї і рішення, навіть працюючи віддалено. [3]

Існує безліч апаратних та програмних технологій, які спільно забезпечують безпечний віддалений доступ для працівників, що працюють на відстані від офісу організації. Вибір оптимального набору технологій залежить від багатьох факторів, таких як:

- розмір організації;
- культура організації;
- співвідношення очних та віддалених співробітників.

Розмір організації є суттєвим фактором, бо великі корпорації з тисячами віддалених працівників потребуватимуть більш потужних та комплексних рішень, ніж малі підприємства з кількома віддаленими співробітниками.

Культура організації також є важливою. Деякі організації мають більш гнучкий підхід до віддаленої роботи, а інші – більш жорсткий. Це може вплинути на вибір технологій контролю та моніторингу.

Співвідношення очних та віддалених співробітників є важливим з багатьох міркувань. Якщо більшість персоналу працює віддалено, організації може знадобитися інвестувати в більш масштабовані та стійкі технології, але і передбачатиме складніші процедури їх контролю. Найпоширеніші технології безпечного віддаленого доступу:

- Віртуальна приватна мережа (VPN);
- Next-Generation Firewalls (NGFW);
- ZTNA;
- Програмно-визначуваний периметр (SDP);
- Протокол віддаленого робочого столу (RDP);
- Secure Access Service Edge (SASE);
- Управління ідентифікацією та доступом (IAM);
- Система управління привілейованим доступом (PAM).

1. VPN – це один з найпоширеніших та найефективніших методів захисту даних, які передаються між віддаленими пристроями та корпоративною мережею. Основний принцип роботи технології VPN полягає в тому, що вони створюють безпечні тунелі через нещодавно небезпечні зони, які забезпечують захист протоколів, які використовуються для передачі даних між віддаленими комп'ютерами або мережами. Тунель - це зашифрований канал, через який проходять дані між двома кінцевими точками мережі. Це забезпечує конфіденційність та захист даних, що передаються по мережі.

Існує два основних напрямки використання VPN: Remote Access VPN та Site-to-Site VPN – це дві різні технології VPN, які використовуються для створення безпечних і захищених з'єднань між комп'ютерами або локальними мережами в різних географічних місцях.

Remote Access VPN є технологією, що дозволяє віддаленим користувачам безпечно підключатися до корпоративної мережі через незахищений Інтернет. Вона забезпечує конфіденційність та безпеку даних, які передаються між віддаленим користувачем та мережею.

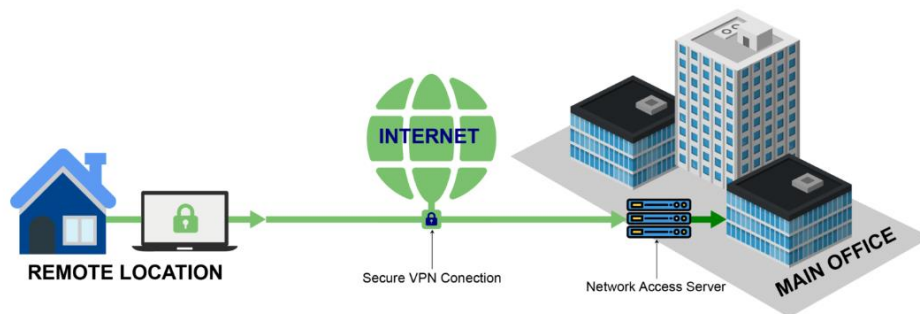


Рисунок 1.1 – Принцип роботи Remote Access VPN

Remote Access VPN дозволяє користувачам отримувати доступ до ресурсів мережі з будь-якого місця, де є підключення до Інтернету. Це особливо корисно для віддалених працівників, які працюють з дому або з інших місць поза офісом. Вони можуть безпечно отримувати доступ до файлів, додатків та інших ресурсів, що дозволяє їм бути продуктивними та забезпечує гнучкість робочого процесу. Ця технологія є незамінним інструментом для забезпечення безпеки та приватності під час віддаленого доступу до корпоративної мережі. Він забезпечує захист даних та

зручний доступ до ресурсів мережі для віддалених користувачів, що дозволяє організаціям підтримувати продуктивність та ефективність своїх робітників, незалежно від їх місця розташування [7].

2. NGFW представляють собою ще один важливий аспект захисту мережі з віддаленими користувачами. Ці міжмережеві екрани не лише аналізують трафік на рівні мережевих пакетів, але й здатні розпізнавати додаткові характеристики, такі як застосунки, користувацькі групи та контекстні дані. Це дозволяє встановлювати більш точні правила безпеки і ефективно виявляти незвичайні або підозрілі дії в мережі.

NGFW можуть блокувати шкідливий трафік, виявляти загрози, які маскуються під легітимний, та надавати детальну звітність про активність мережі. Вони також можуть інтегруватися з іншими системами безпеки, такими як системи виявлення вторгнень (IDS) та системи запобігання вторгнення (IPS), для більш ефективного виявлення та реагування на загрози. NGFW базуються на машинному навчанні і сприймають інноваційні технології, щоб забезпечити безпеку мережі.



Рисунок 1.2 – Принцип роботи міжмережевих екранів

Основні переваги брандмауера включають моніторинг та фільтрацію трафіку, запобігання вірусам, блокування доступу, забезпечення конфіденційності даних та відповідність вимогам. Брандмауер виступає як перший шар захисту в мережі, контролюючи та моніторячи вхідний і вихідний трафік, щоб запобігти небажаному доступу і атакам. Розширені переваги брандмауера полягають у забезпеченні додаткових можливостей захисту, які включають захист ідентифікаторів користувачів, контроль використання програм, безпеку зашифрованого трафіку, передбачення і виявлення загроз, таких як ATP (Advanced Threat Protection), автоматичний обмін інформацією про загрози та інтеграцію з іншими системами безпеки [8].

Використання NGFW дозволяє підвищити рівень захисту мережі, зменшити вразливість перед різноманітними загрозами та забезпечити більшу надійність в роботі мережевої інфраструктури.

3. ZTNA – це сукупність технологій, яка забезпечує безпечний віддалений доступ до програм і служб на основі визначених політик контролю доступу.

ZTNA ґрунтується на трьох основних принципах:

- Не довіряти нікому.
- Перевіряти все.
- Надавати доступ лише до того, що потрібно

Системи, які будуються на базі ZTNA, не довіряють жодному користувачеві, пристроєві чи мережі незалежно від їх розташування. Такі системи виконують перевірку всіх спроб доступу до ресурсів, незалежно від того, звідки надходять запити. Системи надають доступ користувачам лише до тих ресурсів, які їм потрібні для виконання їхніх завдань [23].

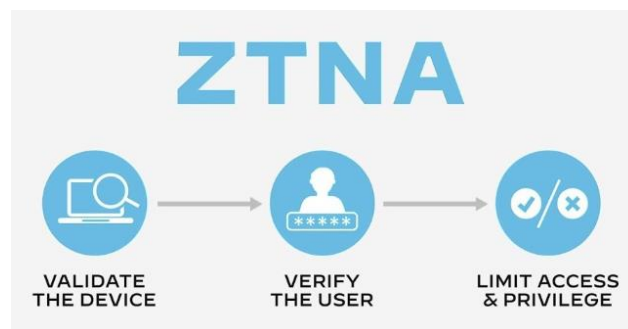


Рисунок 1.3 – Принципи ZTNA

При використанні ZTNA, доступ до конкретних програм або ресурсів надається лише після автентифікації користувача у службі ZTNA. Після успішної автентифікації ZTNA створює захищений шифрований тунель для користувача, через який надається доступ до визначеної програми. Цей тунель забезпечує додатковий рівень захисту, захищаючи програми та служби від виявлення за їх IP-адресами, які в іншому випадку могли б бути доступні.

Zero Trust Network Access 2.0 (ZTNA 2.0) вирішує проблеми, що впливають з застарілих рішень ZTNA, забезпечуючи надійне з'єднання для компаній з гібридними робочими потоками. Його основна мета – забезпечити безпечний доступ до ресурсів, зберігаючи при цьому високий рівень зручності користування.

За допомогою ідентифікації програм на 7-му рівні моделі OSI можна точно контролювати доступ на рівні окремих додатків і їх компонентів, незалежно від інших мережевих параметрів, таких як IP-адреси і номери портів. Після отримання доступу, рівень довіри постійно переоцінюється на основі змін у поведінці пристрою, користувачів та додатків. Також постійно проводиться глибока перевірка всього трафіку, включаючи дозволені з'єднання та захист від усіх видів загроз, включаючи загрози нульового дня.

4. SDP є моделлю безпеки, що базується на принципі "нульової довіри". Вона надає доступ до мережі виключно перевіреним користувачам і пристроям. Це дозволяє надавати доступ лише до тих ресурсів, на які користувачі мають відповідні дозволи, що суттєво зменшує ризики. Використовуючи політику "заборонити все", система спочатку блокує всі з'єднання, а потім вибірково надає доступ, враховуючи ідентифікацію користувача та інші критерії.

Переваги використання SDP:

Завдяки зменшенню ризиків мережа та ресурси залишаються прихованими для неперевірених користувачів і пристроїв, що не пройшли аутентифікацію або не мають доступу.

Посилюючи контроль, організації отримують можливість впроваджувати деталізовані політики доступу для кожного ресурсу.

Відсутність необхідності у VPN-клієнтах та тунелях знижує складність управління доступом.

5. RDP дозволяє користувачам безпечно підключатися до робочого комп'ютера або віртуальної машини незалежно від їхнього місця перебування. На відміну від VPN, який надає доступ до всієї мережі, або SDP, що обмежує доступ лише авторизованими додатками, RDP забезпечує пряме з'єднання із конкретною віддаленою машиною. Такий підхід мінімізує ризики несанкціонованого доступу, оскільки користувач взаємодіє тільки із зазначеним пристроєм, а не з мережею.

RDP дозволяє відображати робочий стіл віддаленого сервера і працювати з ним так, ніби користувач знаходиться безпосередньо перед ним. Крім того,

протокол спрощує управління та моніторинг користувацьких сеансів, що забезпечує надійну та безпечну роботу з віддаленими системами.

6. SASE – це сучасний підхід, який інтегрує мережеві функції та засоби безпеки в єдину хмарну платформу. На відміну від традиційних VPN, що залежать від локального обладнання та складних налаштувань, SASE використовує хмарні технології для забезпечення безпосереднього та безпечного доступу до додатків і ресурсів [13].

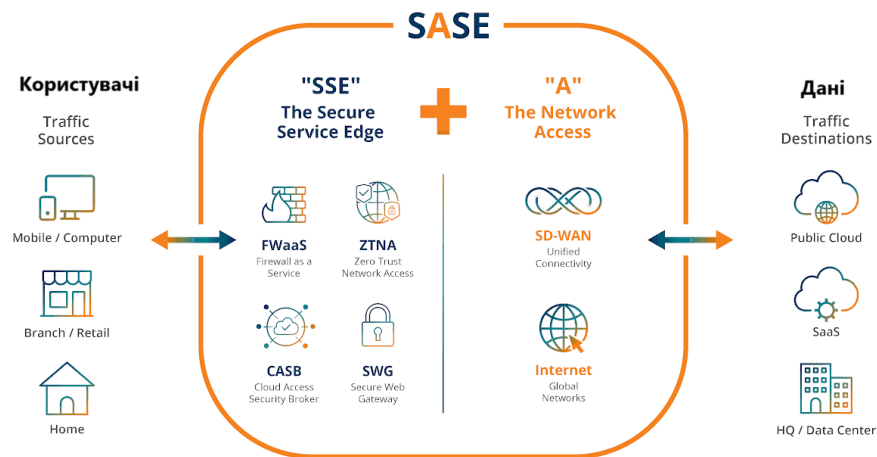


Рисунок 1.4 – Архітектура SASE

SASE спрощує управління мережею завдяки централізації політик і контролю безпеки, усуваючи необхідність у фізичному обладнанні та ручному конфігуруванні. Цей підхід гарантує захищені з'єднання та безпеку даних для віддалених користувачів незалежно від їхнього місцезнаходження.

Переваги використання підходу SASE:

Масштабованість дозволяє організаціям легко додавати або видаляти користувачів і пристрої без впливу на продуктивність чи безпеку мережі.

Покращена видимість забезпечує централізоване спостереження та звітність щодо мережевої активності та подій безпеки.

Ефективність знижує експлуатаційні витрати та спрощує управління завдяки усуненню складнощів роботи з кількома мережевими та безпековими системами.

7. Управління ідентифікацією та доступом (IAM) — це інтегрована система для централізованого керування ідентифікацією користувачів та їхнім доступом до ресурсів. Її головна мета — надавати доступ до ресурсів лише авторизованим користувачам відповідно до їхніх ролей і привілеїв.

IAM значно спрощує процеси управління доступом, дозволяючи централізовано керувати даними користувачів. Це полегшує надання та відкликання дозволів, організацію облікових записів та їхніх привілеїв.

Переваги використання IAM:

Підвищення безпеки захищає критичні ресурси, запобігаючи доступу неавторизованих або скомпрометованих користувачів і пристроїв.

Дотримання стандартів забезпечує відповідність прав доступу вимогам нормативних документів організації.

Продуктивність сприяє швидкому та зручному доступу користувачів і пристроїв до необхідних ресурсів.

IAM добре доповнює інші рішення, такі як VPN, пропонуючи централізоване управління ідентифікацією та суворою аутентифікацією. Однак IAM не замінює VPN, оскільки не забезпечує захищеного каналу для підключення до мережевих ресурсів.

8. Система управління привілейованим доступом (PAM) – це рішення, спрямоване на захист облікових записів з розширеними правами доступу до критично важливих систем і даних. Ця система забезпечує контроль і моніторинг дій привілейованих користувачів, щоб унеможливити доступ для неавторизованих осіб.

Завдяки функціям моніторингу в реальному часі та запису сеансів, PAM дозволяє фіксувати дії привілейованих користувачів, що сприяє своєчасному виявленню й усуненню підозрілих активностей. Впровадження PAM допомагає захистити сервери, бази даних і мережеве обладнання від несанкціонованого доступу чи витоку інформації.

Переваги використання PAM:

Мінімізація ризиків зменшує ймовірність витоку даних і помилок через обмеження доступу до облікових записів з підвищеними привілеями.

Дотримання стандартів підтримує відповідність принципу найменших привілеїв і внутрішнім політикам організації, а також вимогам нормативних актів.

Оптимізація продуктивності забезпечує безпечний і зручний доступ до критичних ресурсів для привілейованих користувачів і додатків.

1.3 Аналіз сучасних технологій для організації захищеного віддаленого доступу

Забезпечення безпечного та ефективного віддаленого доступу до корпоративних мереж стало особливо актуальним у сучасних умовах гібридної роботи. Ефективність впровадження тієї чи іншої технології залежить від багатьох факторів: архітектури корпоративної мережі, масштабу компанії, ресурсів на кібербезпеку та специфічних вимог до контролю доступу. В цьому контексті три провідні рішення: Palo Alto Networks GlobalProtect, Cisco AnyConnect та Fortinet FortiClient – демонструють різні підходи до забезпечення безпеки:

1. Palo Alto Networks GlobalProtect є одним з найпотужніших рішень на ринку, що поєднує у собі VPN-доступ, глибокий моніторинг мережевого трафіку та високий рівень автоматизації у виявленні загроз. Однією з головних переваг є інтеграція з Next-Generation Firewall (NGFW), що дозволяє контролювати доступ користувачів на основі політик безпеки та перевіряти трафік у реальному часі.

Ключовою особливістю GlobalProtect є HIP (Host Information Profile) – технологія, що дозволяє перевіряти стан кінцевого пристрою перед наданням доступу до мережі. Це включає аналіз оновлень операційної системи, статус антивірусного програмного забезпечення та наявність останніх патчів. Це гарантує, що лише безпечні та відповідні політикам пристрої можуть отримати доступ [22].

GlobalProtect легко масштабується завдяки використанню Prisma Access – хмарної платформи, що дозволяє організаціям об'єднати віддалених користувачів, філії та корпоративну інфраструктуру в єдину екосистему. У поєднанні з Panorama, централізованою системою управління, адміністратори отримують повний контроль над трафіком та можуть аналізувати загрози за допомогою Threat Intelligence та сервісу WildFire.

Водночас, GlobalProtect є досить дорогим рішенням, а його впровадження вимагає підготовлених фахівців. Це робить його найкращим вибором для великих корпоративних середовищ, де безпека та масштабованість стоять на першому місці.

2. Cisco AnyConnect є добре відомим рішенням у сфері VPN завдяки своїй надійності та глибокій інтеграції з екосистемою Cisco. Це рішення забезпечує

віддалений доступ за допомогою SSL VPN або IPSec VPN, що дозволяє організаціям вибирати між гнучким налаштуванням і високим рівнем захисту.

Головною перевагою AnyConnect є інтеграція з Cisco SecureX та Identity Services Engine (ISE), що дозволяє автоматизувати контроль доступу на основі ідентифікації користувачів та пристроїв. Наприклад, система може визначити, хто намагається підключитися до мережі, з якого пристрою, та застосувати політики безпеки відповідно до заданих параметрів [27].

AnyConnect підтримує Host Scan – механізм перевірки стану кінцевих пристроїв перед наданням доступу. Також він працює у зв'язці з Cisco Umbrella, що забезпечує додатковий захист на рівні DNS, блокуючи небезпечні домени до того, як вони стануть загрозою.

Недоліком Cisco AnyConnect є його залежність від інших продуктів Cisco, таких як Cisco ASA (Adaptive Security Appliance). Для організацій, які вже використовують обладнання Cisco, AnyConnect є ідеальним рішенням. Однак для підприємств, що використовують різномірну інфраструктуру, його впровадження може бути складнішим.

3. Fortinet FortiClient позиціонується як універсальне рішення для забезпечення VPN-доступу та базового захисту кінцевих точок. Це рішення є частиною Fortinet Security Fabric і тісно інтегрується з іншими продуктами компанії, такими як FortiGate та FortiSandbox.

На відміну від GlobalProtect і AnyConnect, FortiClient орієнтований на малі та середні підприємства, пропонуючи простоту впровадження та доступну вартість. Для організацій, які вже використовують FortiGate, FortiClient забезпечує безперебійне підключення за допомогою SSL VPN або IPSec VPN.

Додатковою перевагою є вбудований антивірус та веб-фільтрація, які допомагають захистити кінцеві пристрої від шкідливого ПЗ та небезпечних веб-сайтів. FortiClient також підтримує аналіз загроз zero-day через інтеграцію з FortiSandbox, що дозволяє перевіряти підозрілі файли в ізольованому середовищі.

Однак FortiClient має свої обмеження. Він не забезпечує настільки глибокого аналізу трафіку, як GlobalProtect, та не має настільки широких можливостей

інтеграції, як Cisco AnyConnect. У великих корпоративних середовищах його продуктивність може бути нижчою порівняно з конкурентами.

Palo Alto Networks GlobalProtect є лідером для підприємств, що потребують найвищого рівня безпеки, глибокого моніторингу та масштабованості. Його можливості аналізу загроз і централізованого управління через Panorama роблять його ідеальним рішенням для великих організацій.

Cisco AnyConnect забезпечує стабільний та надійний VPN-доступ з акцентом на інтеграцію в середовищі Cisco. Це рішення підходить для підприємств, які вже використовують інфраструктуру Cisco та хочуть посилити безпеку кінцевих точок.

Fortinet FortiClient є найкращим варіантом для малих і середніх підприємств завдяки своїй доступності та простоті впровадження. Його можливості базового захисту та інтеграція з FortiGate роблять його зручним інструментом для забезпечення VPN-доступу.

Вибір технології залежить від потреб підприємства. Для високої продуктивності та детального контролю краще використовувати Palo Alto Networks GlobalProtect. Для середніх рішень з глибокою інтеграцією Cisco підходить AnyConnect. А для підприємств, що орієнтуються на базовий захист з оптимальною вартістю, вигідним буде FortiClient.

Palo Alto Networks пропонує комплексний захист для організацій будь-якого розміру та галузі. Їхні ключові продукти та послуги включають:

- NGFWs
- GlobalProtect
- Prisma Access
- Cortex XSOAR
- WildFire

1. Palo Alto Networks NGFW – провідне сімейство міжмережевих екранів наступного покоління забезпечує мережеву безпеку з 2008го року. NGFW гарантують запобігання широкого спектру атак, виявляють як відомі, так і невідомі загрози за рахунок використання даних, отриманих з багатьох тисяч інстальованих пристроїв.

Міжмережеві екрани нового покоління від Palo Alto Networks захищають мережі за допомогою архітектури, орієнтованої на профілактику, яку можна легко розгорнути і використовувати. Використовуючи автоматизацію, зменшуються витрати часу на ручне управління і увага зосереджується на інших завданнях.

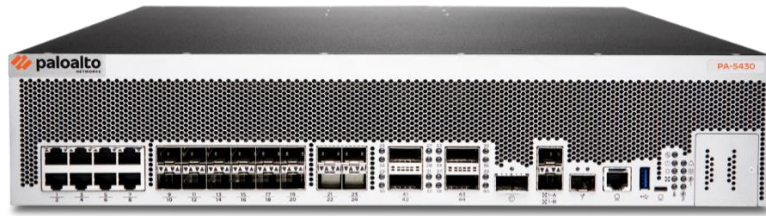


Рисунок 1.5 – Міжмережевий екран від Palo Alto Networks

Проблеми, які вирішує NGFW:

- Безпека центру обробки даних
- Безпека філій і роздрібних магазинів
- Безпека мобільних і віддалених співробітників
- Захист периметра мережі
- Безпека мобільної мережі з підтримкою 5G, IoT, мобільні і приватні

LTE мережі

2. GlobalProtect – це універсальне рішення, яке надає можливість різних сценаріїв свого використання [2], а саме:

- віддалений доступ з використанням технологій VPN;
- розширене запобігання загрозам;
- фільтрація URL-адрес;
- підтримка BYOD;
- реалізація концепції Zero Trust.

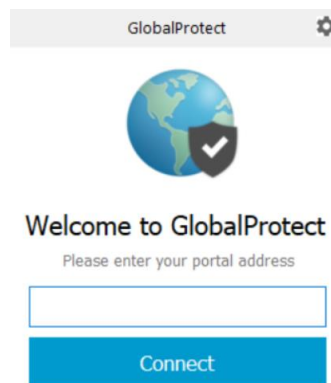


Рисунок 1.6 – GlobalProtect від Palo Alto Networks

GlobalProtect надає безпечний шлюз для доступу до внутрішніх і хмарних додатків на гарантує, що конфіденційні дані залишаються захищеними під час передавання. Для інтернет-трафіку GlobalProtect діє як механізм захисту, що перехоплює та нейтралізує загрози, перш ніж вони зможуть проникнути в кінцеву точку. Він блокує доступ до шкідливих веб-сайтів, запобігає фішингу та крадіжці облікових даних, тим самим забезпечуючи захист кінцевих точок;

3. Prisma Access призначений для запобігання успішним кібератакам, і тому він робить більше, ніж просто захищає Інтернет. Щоб зупинити кібератаки, потрібно перевіряти весь трафік. Будь-які дії, крім повної перевірки всього трафіку, створюють значну прогалину в безпеці.

Prisma Access послідовно захищає весь трафік на всіх портах та з усіх додатків, дозволяючи вашій організації:

Запобігати успішним кібератакам за допомогою перевірених принципів безпеки та аналізу загроз, що забезпечують повну прозорість і точний контроль, що охоплює всю вашу організацію.

Повністю перевіряти весь двонаправлений трафік додатків, включаючи трафік із шифруванням SSL/TLS, на всіх портах, незалежно від того, чи здійснюється зв'язок з Інтернетом, хмарою чи між філіями.

Користуватися перевагами комплексної аналітики загроз, що базується на автоматизованих даних про загрози від Palo Alto Networks та сотень сторонніх каналів.

4. Cortex XSOAR від Palo Alto Networks є однією з найпередовіших платформ у сфері автоматизації операцій безпеки (SOAR — Security Orchestration, Automation, and Response). Вона об'єднує в собі функції збору даних, аналізу, автоматизації та координації дій, що дає змогу значно підвищити ефективність роботи аналітиків безпеки та оперативних команд.

Cortex XSOAR є потужною платформою для забезпечення кібербезпеки, яка поєднує передові технології автоматизації, управління інцидентами, аналізу загроз і співпраці в режимі реального часу. Її головною метою є оптимізація роботи команд безпеки шляхом зниження часу на виконання рутинних завдань і

підвищення ефективності реагування на загрози. Ця платформа забезпечує централізоване управління всіма аспектами безпеки, що дозволяє швидко виявляти, аналізувати та усувати потенційні ризики.

Важливим аспектом Cortex XSOAR є інтегроване управління загрозами. Платформа дозволяє збирати, аналізувати та інтерпретувати дані про загрози в реальному часі. Це забезпечує командам безпеки комплексне уявлення про поточну ситуацію та допомагає приймати обґрунтовані рішення. Крім того, функції автоматизації дозволяють оперативно реагувати на виявлені загрози, виконуючи відповідні дії без затримок. Завдяки цьому організації можуть значно підвищити свою стійкість до сучасних кіберзагроз.

Cortex XSOAR є універсальною платформою, яка може використовуватись як у малих компаніях, так і у великих організаціях. Її масштабованість дозволяє адаптувати функціональність під специфічні потреби кожного підприємства. Це включає автоматизацію процесів для малого бізнесу, який прагне зменшити витрати на безпеку, і забезпечення комплексного захисту для великих корпорацій із розгалуженими інфраструктурами [16].

Унікальність платформи також полягає в її ролях і спеціалізаціях. Cortex XSOAR дозволяє командам ефективно розподіляти завдання. Наприклад, сортувальники інцидентів можуть аналізувати необроблені дані, виявляючи потенційні загрози, у той час як реагувальники можуть фокусуватися на усуненні цих загроз і визначенні їхніх першопричин. Мисливці за загрозами проводять поглиблені дослідження сучасних атак і розробляють нові стратегії їх пом'якшення. Менеджери SOC координують дії всієї команди, забезпечуючи своєчасне реагування на всі види інцидентів.

Завдяки цим функціям Cortex XSOAR став важливим інструментом для сучасних SOC. Він не лише підвищує продуктивність команд безпеки, але й допомагає організаціям знижувати витрати, оптимізуючи операційні процеси.

Обираючи Cortex XSOAR від Palo Alto Networks, організації отримують доступ до інноваційних технологій, підтримку сертифікованих експертів та комплексні рішення, адаптовані до їхніх унікальних потреб. Платформа стає

основою для побудови стійкої та ефективної системи кібербезпеки, яка відповідає викликам сучасного цифрового світу.

5. Palo Alto Networks WildFire – це високоефективне хмарне рішення для розширеного захисту від загроз (АТР), якому довіряють організації з найрізноманітніших сфер захисту від цифрових загроз. Він розроблений, щоб дати можливість компаніям протистояти навіть найбільш обхідним загрозам і усувати їх. Він поєднує в собі багато методів для максимального підвищення рівня захисту від загроз, доступного для користувачів.

Основою WildFire є механізм виявлення зловмисного програмного забезпечення за допомогою різних методів аналізу: статичного, динамічного та хмарного. Він здатний визначати невідомі загрози, аналізуючи виконання підозрілих файлів у ізольованому середовищі (пісочниці) та використовуючи штучний інтелект для прогнозування можливих векторів атак. Унікальною перевагою платформи є її глобальна аналітична мережа, що об'єднує дані з мільйонів пристроїв клієнтів по всьому світу. Це дозволяє створювати оперативні сигнатури загроз і ділитися ними в реальному часі.

WildFire аналізує не тільки традиційні файли (наприклад, виконувані файли, документи, архіви), але й веб-контент, електронну пошту та мережевий трафік. Всі підозрілі об'єкти автоматично передаються до хмари WildFire, де вони проходять кілька етапів перевірки. Якщо об'єкт виявляється шкідливим, система миттєво оновлює бази даних сигнатур на всіх пристроях Palo Alto Networks. Значною перевагою цієї технології є масштабованість та інтеграція з іншими продуктами Palo Alto Networks [15].

Висновки до першого розділу

Перший розділ роботи присвячений аналізу теоретичних основ і практичних аспектів організації мереж з віддаленим доступом користувачів, що є ключовим елементом сучасних технологій і бізнес-процесів. Віддалений доступ користувачів став невід'ємною частиною діяльності організацій, особливо у контексті поширення мобільних технологій, хмарних сервісів і загального переходу до цифрових форм роботи. Аналіз показує, що віддалений доступ не лише спрощує

роботу і взаємодію між користувачами, а й відкриває нові можливості для підвищення ефективності бізнесу та зниження витрат. Водночас він створює і додаткові ризики, які вимагають особливої уваги до питань безпеки.

З переходом на гібридні та віддалені моделі роботи з'явилися нові виклики, які вимагають від компаній розробки гнучких та ефективних рішень для забезпечення безпеки і доступу до корпоративних ресурсів без обмежень по місцезнаходженню користувачів. Різноманітність робочих середовищ створює необхідність в інтеграції інструментів для ефективного управління доступом і моніторингу, що стало обов'язковим для забезпечення безперервної роботи підприємств у сучасних умовах.

Загрози, які супроводжують використання мереж з віддаленим доступом, є невід'ємною частиною цифрового середовища. До найбільш актуальних загроз відносяться фішинг-атаки, зловживання вразливостями програмного забезпечення та неправильне налаштування мережевих елементів, що можуть призвести до витоків конфіденційної інформації. Особливу небезпеку становлять атаки, спрямовані на слабкі місця в системах аутентифікації та ідентифікації користувачів, що є вразливими в умовах віддаленого доступу.

Забезпечення захисту мереж з віддаленим доступом користувачів потребує використання комплексного підходу. Сучасні рішення, зокрема технології, пропонувані компанією Palo Alto Networks, демонструють високу ефективність у забезпеченні безпеки мереж з віддаленим доступом. Використання їх рішень дозволяє організаціям створювати надійні бар'єри проти зовнішніх та внутрішніх загроз, завдяки інноваційним методам інтеграції міжмережевих екранів, систем управління загрозами та інтелектуальних механізмів виявлення і нейтралізації шкідливого трафіку.

Загалом, результати аналізу підтверджують важливість використання багаторівневого підходу до забезпечення безпеки мереж з віддаленим доступом, включаючи як технічні, так і організаційні заходи.

РОЗДІЛ 2. РОЗРОБКА ПРОЄКТУ ЗАХИЩЕНОЇ МЕРЕЖІ З ВІДДАЛЕНИМ ДОСТУПОМ КОРИСТУВАЧІВ

2.1 Проєктування структурної схеми мережі з віддаленим доступом користувачів

Проєктування структурної схеми мережі з віддаленими користувачами є складним та багатогранним процесом, що вимагає глибоко розуміння сучасних технологічних викликів та особливостей корпоративної інфраструктури. Проєктування є одним із найважливіших етапів у створенні ефективної системи комунікації та захисту інформації в умовах сучасного бізнес-середовища. Особливість цього процесу полягає в забезпеченні безперервності роботи користувачів у будь-якій точці світу, одночасно мінімізуючи ризики несанкціонованого доступу, втрати даних чи кібератак.

Сучасні мережі повинні відповідати декільком ключовим критеріям: забезпечення конфіденційності інформації, висока продуктивність при одночасному підключенні великої кількості користувачів, легкість у масштабуванні, а також адаптація до різних сценаріїв використання, зокрема гібридної роботи.

При розробці схеми враховуються різні типи доступу, такі як повний доступ до корпоративних ресурсів або обмежений доступ до окремих хмарних сервісів. Для забезпечення високої надійності й мінімізації затримок необхідно інтегрувати кілька рівнів доступу з використанням технологій балансування навантаження.

Для захисту мережі від загроз важливо використовувати сучасні рішення, такі як міжмережні екрани нового покоління (NGFW), які поєднують функції контролю додатків, аналізу загроз і моніторингу мережевого трафіку. Впровадження систем виявлення та запобігання вторгненням (IDS/IPS) дозволяє оперативно реагувати на підозрілу активність. Крім того, використання інструментів захисту від атак типу "відмова в обслуговуванні" (DDoS) забезпечує стабільність роботи навіть у разі масованих кіберзагроз.

Таким чином, структурна схема мережі з віддаленими користувачами повинна забезпечувати баланс між безпекою, продуктивністю та гнучкістю.

Завдяки використанню сучасних технологій та підходів до сегментації, захисту і моніторингу, компанії можуть створити ефективну й стійку до загроз інфраструктуру.

У контексті проектування структурної схеми мережі з віддаленими користувачами інтеграція міжмережєвих екранів нового покоління (NGFW) є ключовим аспектом забезпечення безпеки та продуктивності. NGFW забезпечують глибокий аналіз трафіку, дозволяючи визначати та контролювати активність на рівні додатків, користувачів та контенту.

Розміщення NGFW у структурі мережі передбачає його встановлення на кордонах мережєвих сегментів – між зовнішніми мережами, демілітаризованою зоною (DMZ) та внутрішніми корпоративними мережами. Це дозволить забезпечити ефективний моніторинг та сегментацію трафіку між локальною мережею, хмарними ресурсами та кінцевими точками.

Завдяки такій інтеграції мережа отримує як підвищений рівень захисту, так і можливість масштабування функціональності, необхідної для ефективного управління безпекою у сучасному бізнес-середовищі.

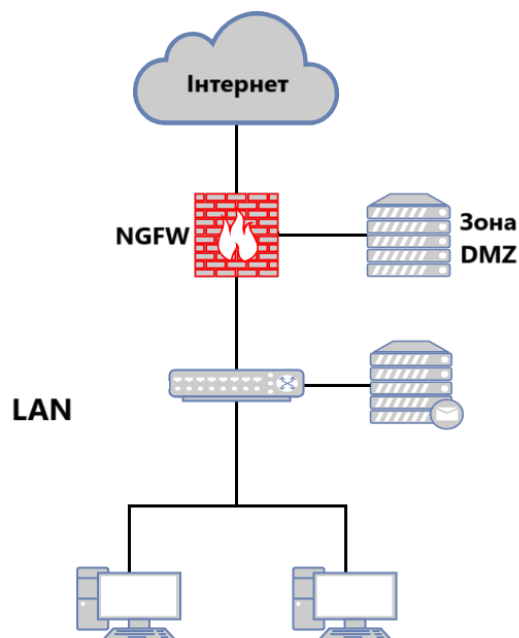


Рисунок 2.1 – NGFW як пристрій периметра

Основні переваги інтеграції NGFW як пристрій:

- Відсутність потреби у виділеному проксі-сервері;
- Вбудований IPS (Intrusion Prevention System);

- Антивірус для веб-трафіку;
- Антивірус для поштового трафіку;
- Антиспам-функціонал;
- Швидке впровадження функції "пісочниці";
- Вбудована звітність про інциденти інформаційної безпеки;
- Системна оптимізація інфраструктури безпеки.

Більшість сучасних NGFW здатні функціонувати в режимі проксі, однак основний функціонал повністю доступний і в режимі «маршруту за замовчуванням» для всіх локальних мереж. У такому випадку достатньо налаштувати шлюз за замовчуванням і потреба в ручному налаштуванні проксі в браузерах користувачів відпадає. Це спрощує адміністративне управління та зменшує кількість точок потенційного збою.

NGFW забезпечує вбудовану систему запобігання вторгненням. За необхідності можна перевести систему в режим виявлення, якщо є побоювання щодо впливу на трафік. Такий підхід дозволяє уникнути складних налаштувань для перенаправлення трафіку через окремі пристрої IPS та забезпечує швидке відновлення потоку даних у разі виникнення проблем.

Застосування NGFW дозволяє спростити схему захисту мережі, замінюючи декілька традиційних засобів безпеки єдиним рішенням. Це забезпечує легше адміністрування і знижує витрати на підтримку. Однак слід враховувати і ризик виникнення «єдиної точки відмови», коли збій NGFW може порушити роботу всієї системи безпеки. Незважаючи на це, концепція інтеграції NGFW є перспективною для організацій, що прагнуть оптимізувати свої ресурси та підвищити рівень захищеності.

Таким чином, з урахуванням аналізу основних принципів і сучасних підходів до проектування мереж із застосуванням NGFW (Next-Generation Firewall) було створено топологію мережі, яка відповідає ключовим вимогам безпеки, забезпечує високу масштабованість для подальшого розширення системи та гарантує оптимальну продуктивність під час роботи. У додатку А представлено детальну структурну схему мережі.

2.2 Вибір мережевого обладнання для організації роботи мережі

При виборі мережевого обладнання для організації роботи мережі з віддаленим доступом необхідно враховувати комплекс складних технічних, функціональних і безпекових параметрів, що забезпечують ефективну та стабільну роботу системи. Основним завданням є створення надійної інфраструктури, яка дозволяє безпечний, безперебійний і високопродуктивний доступ віддалених співробітників до корпоративних ресурсів незалежно від їхнього місцезнаходження.

Сучасні рішення вимагають використання високотехнологічного обладнання, здатного підтримувати складні протоколи автентифікації, шифрування та моніторингу мережевого трафіку. Маршрутизатори, міжмережві екрани, комутатори та спеціалізовані VPN-пристрої мають забезпечувати не тільки технічну сумісність, але й високий рівень захисту корпоративних даних.

Особливу увагу слід приділяти вибору рішень для організації захищеного віддаленого доступу, таких як брандмауери нового покоління (NGFW), що дозволяють не лише фільтрувати трафік, але й здійснювати глибокий аналіз пакетів, виявляти аномальні дії та запобігати можливим кібератакам.

Одним з найбільш ефективних рішень для організації захищеної мережі з віддаленим доступом є серія міжмережвих екранів Palo Alto Networks PA-5400. Ця лінійка обладнання представляє собою високопродуктивне рішення корпоративного класу, яке ідеально підходить для великих організацій з розподіленою мережевою інфраструктурою. Серія PA-5400 відповідає вимогам завдяки впровадженню передових технологій кібербезпеки та інтелектуального аналізу мережевого трафіку [18].

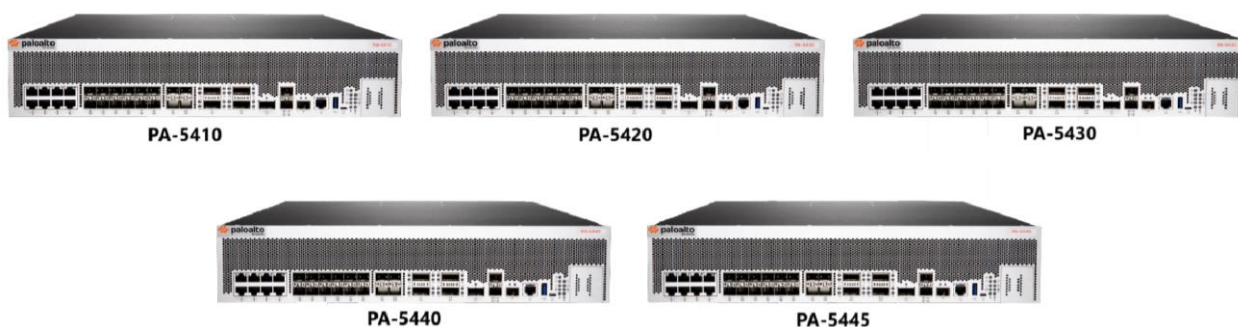


Рисунок 2.2 – Міжмережні екрани Palo Alto Networks серії PA-5400

Керуючим елементом серії PA-5400 є операційна система PAN-OS, яка є стандартною для всіх міжмережних екранів нового покоління від Palo Alto Networks.

PAN-OS автоматично класифікує весь трафік, включаючи додатки, загрози і контент та прив'язує цей трафік до конкретного користувача, незалежно від місцезнаходження або типу пристрою.

Це дозволяє створювати політики безпеки на основі додатків, контенту та користувача, що значно покращує рівень безпеки та скорочує час реагування на інциденти.

Основні функції безпеки та підключення міжмережних екранів серії PA-5400:

1. Міжмережний екран наступного покоління на основі машинного навчання:

- Вбудоване машинне навчання (ML) в основі міжмережного екрану дозволяє запобігати атакам на основі файлів без необхідності використання підписів, а також виявляти та блокувати фішингові атаки, яких не було раніше.

- Використання хмарних процесів ML для миттєвого оновлення підписів та інструкцій без затримок, які надсилаються на міжмережний екран.

- Аналіз поведінки для виявлення IoT пристроїв та автоматичні рекомендації щодо політики безпеки. Автоматичні рекомендації з політики знижують ймовірність помилок при налаштуванні політики безпеки та економлять час.

2. Ідентифікація та класифікація всіх програм і портів у будь-який час з повною перевіркою рівня 7:

- Ідентифікація програм, що проходять через мережу, незалежно від порту, протоколу, методів обходу або шифрування (SSL/TLS).

- Використання програми, а не порту, як основу для всіх рішень щодо політики безпечного доступу: дозвіл, заборона, планування, перевірка та застосування обмежень трафіку.

- Можливість створювати власні теги App-ID для власних програм або запитувати розробку App-ID для нових програм від Palo Alto Networks.

- Ідентифікація всіх корисних даних в програмах для блокування шкідливих файлів та запобігання спробам витоку даних.

- Створення стандартних та настроюваних звітів про використання програм, включаючи звіти про програмне забезпечення як послугу (SaaS), які надають уявлення про весь санкціонований та несанкціонований трафік SaaS у вашій мережі.

3. Забезпечення безпеки для користувачів у будь-якому місці, на будь-якому пристрої. Адаптація політики на основі активності користувача:

- Виявлення та застосування політик безпеки на основі користувачів та груп.
- Можливість створення динамічних груп користувачів для оперативного прийняття рішень без очікування оновлень в директоріях користувачів.
- Забезпечення однакових політик безпеки для користувачів, незалежно від їх місцезнаходження (офіс, будинок, подорожі) та пристроїв.

4. Захист від шкідливої діяльності в зашифрованому трафіку:

- Перевірка та застосування політик до зашифрованого трафіку SSL/TLS.
- Надання глибокої видимості в зашифрований трафік без необхідності його дешифрування.
- Контроль використання застарілих протоколів TLS, незахищених шифрів і неправильно налаштованих сертифікатів для зменшення ризиків.
- Можливість створення копії дешифрованого трафіку для аналізу і збереження для запобіжних цілей.

5. Універсальне керування на основі штучного інтелекту за допомогою Strata Cloud Manager:

- Прогнозування та попередження потенційних проблем з мережею за допомогою аналітики на основі AI, що дозволяє заздалегідь виявляти вузькі місця в системі.
- Забезпечення відповідності та безпеки в реальному часі за допомогою автоматичних перевірок політик і відповідності галузевим стандартам.
- Просте управління політиками безпеки через хмарні рішення для всіх типів інфраструктури, включаючи SASE, апаратні та програмні міжмережні екрани.

6. Хмарні сервіси безпеки на базі Precision AI:

- Розширена профілактика загроз: Запобігання відомих та невідомих загроз, зловмисного програмного забезпечення, шпигунського програмного забезпечення.

- Advanced WildFire: Забезпечення безпечного доступу до файлів за допомогою найбільшого в галузі механізму захисту від шкідливих програм.
- Розширена фільтрація URL: Запобігання доступу до небезпечних веб-ресурсів, зокрема фішингових сайтів.
- Розширена безпека DNS: Захист трафіку DNS та зупинка розширених загроз на рівні DNS.
- IoT Security: Безпека для всіх пристроїв, підключених до мережі, із застосуванням підходу Zero Trust.

7. Підхід до обробки пакетів з Single-Pass Architecture:

- Операції з мережею, перевірка політик, декодування додатків і порівняння з підписами відбуваються за один прохід, що значно знижує навантаження на систему. Це дозволяє забезпечити стабільну продуктивність і передбачувані результати при активованих підписах на безпеку.

8. Функціональність SD-WAN:

- Легке впровадження SD-WAN на вже наявних міжмережних екранах, що забезпечує безпеку без шкоди для продуктивності.
- Забезпечення взаємодії з кінцевими користувачами завдяки мінімізації затримки та втрат пакетів.

Враховуючи всі ці аспекти, серія PA-5400 є надзвичайно ефективним рішенням для забезпечення безпеки великих організацій з розподіленою мережевою інфраструктурою, зокрема в умовах віддаленого доступу. Вона поєднує в собі високопродуктивне обладнання з передовими технологіями безпеки, що включають машинне навчання для виявлення нових загроз, глибокий аналіз трафіку на прикладному рівні, а також можливість адаптації політик безпеки на основі користувачів та їх активності [19].

Кожна модель серії — PA-5410, PA-5420, PA-5430, PA-5440 та PA-5445 — характеризується чіткою спеціалізацією, що дозволяє ефективно задовольняти різноманітні потреби підприємств з урахуванням масштабів їхньої діяльності, рівня завантаженості мережі та вимог до безпеки. Ці моделі розроблені з урахуванням сучасних викликів інформаційної безпеки та потреб у масштабованості, що робить

їх універсальними інструментами для організації захищеного доступу та управління мережевим трафіком. Основні відмінності в продуктивності цих моделей наведена в таблиці 2.1.

Таблиця 2.1

Продуктивність міжмережних екранів серії PA-5440

	PA-5410	PA-5420	PA-5430	PA-5440	PA-5445
Пропускна здатність міжмережного екрану	52 Гбіт/с	70 Гбіт/с	80 Гбіт/с	85 Гбіт/с	90 Гбіт/с
Пропускна здатність запобігання загрозам	35 Гбіт/с	50 Гбіт/с	60 Гбіт/с	70 Гбіт/с	76 Гбіт/с
Пропускна здатність IPsec VPN	20 Гбіт/с	28 Гбіт/с	42 Гбіт/с	58 Гбіт/с	64 Гбіт/с
Максимальна кількість одночасних сеансів	5М	7М	9М	20М	48М
Кількість нових сеансів за секунду	270 000	370 000	380 000	390 000	449 000

Цільове використання міжмережний екранів серії PA-5440:

- PA-5410 та PA-5420: Найкраще підходять для малих і середніх підприємств або офісів із середнім обсягом трафіку.
- PA-5430: Ідеальне рішення для великих компаній із високими вимогами до пропускної здатності.
- PA-5440 та PA-5445: Найкраще підходять для організацій, що оперують великими обсягами даних, включаючи мультинаціональні корпорації та дата-центри.

Тому, вибір моделі міжмережного екрана Palo Alto Networks PA-5400 залежить від індивідуальних потреб, масштабів та специфіки діяльності підприємства. Визначальними факторами є обсяг мережевого трафіку, кількість співробітників, рівень кіберризиків та перспективи розвитку інфраструктури. Правильний вибір забезпечує не лише ефективний захист, але й оптимізацію витрат на мережеву безпеку.

Поряд з міжмережевими екранами Palo Alto Networks, критично важливим компонентом мережевої інфраструктури є вибір високопродуктивних та надійних маршрутизаторів. Серед провідних рішень для корпоративних мереж виділяються маршрутизатори Cisco серії ISR (Integrated Services Router), зокрема ISR 4000.

Моделі цієї серії є високопродуктивними маршрутизаторами, які підтримують інтеграцію з різними рішеннями безпеки, включаючи VPN, міжмережні екрани та IDS/IPS. Вони забезпечують необхідну продуктивність для великих підприємств та можуть бути масштабовані під конкретні потреби організації.



Рисунок 2.3 – Маршрутизатори Cisco серії ISR 4000

Маршрутизатори Cisco 4000 Integrated Services Routers (ISR) створюють програмно визначену платформу WAN, яка забезпечує високу продуктивність, безпеку та можливості конвергенції для сучасних офісів філій. Ці маршрутизатори відповідають вимогам мереж, орієнтованих на додатки, в умовах обмежених ІТ-ресурсів, забезпечуючи ефективний зв'язок з приватними та публічними хмарами через різноманітні канали, зокрема MPLS, VPN і Інтернет. Вони дозволяють організовувати мережі для розподілених корпоративних сайтів з економічними ІТ-ресурсами [20].

До сімейства Cisco 4000 Integrated Services Router (ISR) входять моделі ISR 4461, 4451, 4431, 4351, 4331, 4321 і 4221.

Сімейство маршрутизаторів ISR Cisco 4000 пропонує потужні можливості для побудови мереж нового покоління. Це забезпечується завдяки інноваційним функціям програмного забезпечення Cisco Catalyst, яке включає в себе можливості програмно керованої WAN мережі (SD-WAN) та конвергентну інфраструктуру для філій компаній. Завдяки високій пропускній здатності та розширеним можливостям, серії ISR Cisco 4000 виступають основою для створення глобальних мереж з підтримкою вимог до ефективної роботи філій в умовах складних та мінливих бізнес-середовищ.

Маршрутизатори Cisco ISR 4000 об'єднують кілька ключових ІТ-функцій, таких як мережеві, обчислювальні ресурси та ресурси зберігання, в єдину інфраструктуру філій. Це дозволяє здійснювати запуск кількох важливих служб одночасно, включаючи шифрування, управління трафіком та оптимізацію WAN, без зниження пропускної здатності. Крім того, можливість активації нових послуг через зміни ліцензій дає гнучкість у швидкому адаптуванні інфраструктури до змінюваних умов бізнесу.

Таблиця 2.2

Технічні характеристики маршрутизаторів Cisco серії ISR 4000

	Cisco 4221	Cisco 4321	Cisco 4331	Cisco 4351	Cisco 4431	Cisco 4451	Cisco 4461
Загальна пропускна здатність	35–75 Мбіт/с	50–100 Мбіт/с	100–300 Мбіт/с	200–400 Мбіт/с	0,5 – 1 Гбіт/с	1 – 2 Гбіт/с	1,5 – 3 Гбіт/с
Кількість вбудованих портів WAN або LAN	2	2	3	3	4	4	4
Порти RJ-45	2	2	2	3	4	4	4
Порти SFP	1	1	2	3	4	4	4
Розширені слоти для сервісних модулів	0	0	1	2	0	2	3
Подвійні широкі слоти для сервісних модулів	0	0	0	1	0	1	2
Слоти NIM	2	2	2	3	3	3	3
Flash пам'ять за замовчуванням	8 Гб	4 Гб	4 Гб	4 Гб	8 Гб	8 Гб	8 Гб
Максимальна flash пам'ять	8 Гб	8 Гб	16 Гб	16 Гб	32 Гб	32 Гб	32 Гб
Зовнішні слоти USB 2.0 (тип A)	1	1	1	2	2	2	2
USB консольний порт типу B mini	0	1	1	1	1	1	1
Послідовний консольний порт - RJ45	1	1	1	1	1	1	1
Послідовний допоміжний порт - RJ45	1	1	1	1	1	1	1

Cisco ISR 4321 та 4221 призначені для малих підприємств або віддалених офісів. Ці моделі мають низьку пропускну здатність, але при цьому забезпечують достатню продуктивність для малого бізнесу або невеликих філій. Вони підходять для малих офісів з обмеженими потребами у трафіку, віддалених офісів, де

потрібно з'єднання через VPN або забезпечення базових функцій маршрутизації та безпеки, а також для заміни старих мережевих рішень для малих компаній.

Cisco ISR 4331 та 4351 мають кращі характеристики продуктивності порівняно з 4321 і 4221, підтримують більшу кількість портів і мають розширену функціональність. Вони ідеально підходять для середніх за розміром підприємств з кількома філіями, мереж з високими вимогами до обробки голосового трафіку, відео або великих даних, а також для підключення віддалених офісів через MPLS або VPN з високими вимогами до швидкості.

Cisco ISR 4431 та 4451 призначені для великих підприємств або філій з високими вимогами до швидкості та безпеки. Ці маршрутизатори забезпечують ще вищу пропускну здатність і підтримують розширену функціональність для забезпечення інтенсивного трафіку. Вони підходять для великих офісів або середніх підприємств, які потребують високої пропускну здатності, організацій, що використовують ресурсоємні додатки, з високими вимогами до безпеки та ефективності, а також для мереж, що включають інтеграцію з хмарними рішеннями та підтримку великих обсягів трафіку.

Cisco ISR 4461 – це найпотужніша модель з серії ISR 4000, що підтримує високу пропускну здатність і інтеграцію з хмарними та віртуальними інфраструктурами. Цей маршрутизатор підходить для великих підприємств, які потребують великої пропускну здатності та забезпечення додаткових функцій безпеки та віртуалізації.

Тому, вибір маршрутизатора для кожної організації здійснюється індивідуально, з урахуванням її специфічних вимог щодо продуктивності та рівня безпеки. Індивідуальний підхід до вибору маршрутизатора дозволяє не лише оптимізувати роботу мережі, але й адаптувати її до змін бізнес-середовища, зберігаючи високу ефективність функціонування мережевої інфраструктури.

Для організації мережі з віддаленим доступом вибір комутатора є критично важливим, адже він забезпечує основну функцію маршрутизації та управління потоками даних у корпоративній інфраструктурі. Оптимальний комутатор має відповідати сучасним вимогам безпеки, продуктивності та масштабованості.

Одним із найкращих рішень для корпоративних мереж є серія комутаторів Cisco Catalyst 9000.



Рисунок 2.4 – Комутатори серії Cisco Catalyst 9000

Комутатори Catalyst 9000 оптимізовані для підтримки сучасних гібридних робочих середовищ. Висока пропускна здатність забезпечує комфортну роботу з ресурсомісткими додатками, такими як [21]:

- відеоконференції високої чіткості (720–1080p, 1–3 Мбіт/с);
- інтерактивні технології, як-от Cisco Hologram (до 20 Мбіт/с);
- потокове відео 4K та VR (15–100 Мбіт/с).

Сімейство Catalyst 9000 інтегрує провідні аналітичні інструменти Cisco для виявлення загроз, включно із зашифрованим трафіком. Постійний моніторинг, заснований на AI/ML, дозволяє адаптувати мережу до нових загроз у реальному часі.

Сімейство Catalyst 9000 включає кілька серій, кожна з яких має свої особливості та відповідає певним вимогам бізнесу. Основні серії Catalyst 9000 включають:

- Cisco Catalyst 9200;
- Cisco Catalyst 9300;
- Cisco Catalyst 9400;
- Cisco Catalyst 9500;
- Cisco Catalyst 9600.

Однією з ключових переваг Catalyst 9000 є інтеграція з Cisco Catalyst Center, яка забезпечує централізоване управління політиками та автоматизацію процесів. Це спрощує масштабування та налаштування мережі, скорочуючи час і витрати на адміністрування. Далі наведено детальний аналіз серії:

Комутатори серії Cisco Catalyst 9200 є економічно вигідною альтернативою для невеликих і середніх підприємств або філій з помірними вимогами до пропускної здатності та безпеки.

Даний комутатор підтримує Ethernet зі швидкістю до 1 Гбіт/с і є економічно ефективним варіантом для невеликих мереж, де основні задачі полягають у забезпеченні підключення користувачів до мережі та доступу до базових ресурсів.

Однією з переваг Cisco Catalyst 9200 є підтримка автоматизації та простота адміністрування, що дозволяє зменшити витрати на керування мережею

Cisco Catalyst 9300 – це найкращий варіант для мереж з середнім навантаженням, таких як офіси середнього розміру або філії. Цей комутатор підтримує Ethernet зі швидкістю до 10 Гбіт/с, що дозволяє ефективно працювати з більш потужними додатками, такими як відеоконференції високої чіткості, інтерактивні технології та стандартне відео.

Cisco Catalyst 9300 також оснащений функціями безпеки, такими як інтеграція з Cisco Umbrella для захисту від загроз, а також здатний до підтримки гнучких гібридних робочих середовищ, що є особливо важливим у сучасних умовах роботи на відстані.

Cisco Catalyst 9400 відрізняється від попередніх моделей більшою пропускною здатністю і призначений для середніх і великих підприємств, де потрібна висока продуктивність для роботи з великими обсягами даних. Цей комутатор підтримує Ethernet зі швидкістю до 40 Гбіт/с, що дозволяє ефективно працювати з важкими додатками, такими як потокове відео 4K або VR.

Крім того, Cisco Catalyst 9400 має розширену підтримку для комплексних корпоративних мереж, дозволяючи ефективно управляти політиками безпеки, масштабуванням та підключенням віддалених користувачів.

Комутатори Cisco Catalyst 9500 підходять для найбільших підприємств або центрів обробки даних з високими вимогами до пропускної здатності і продуктивності, ідеальним вибором стане Cisco Catalyst 9500. Цей комутатор підтримує Ethernet зі швидкістю до 100 Гбіт/с, що робить його найкращим рішенням для інфраструктури з великою кількістю користувачів та інтенсивними вимогами до обробки даних.

Cisco Catalyst 9500 використовується здебільшого в якості ядра мережі, де потрібна максимальна стабільність і швидкість. Включення функцій безпеки на апаратному рівні дозволяє забезпечити захист від складних кіберзагроз. Крім того, завдяки підтримці SD-Access, цей комутатор дозволяє централізовано управляти всією мережею та автоматизувати процеси.

Cisco Catalyst 9600 – це флагманський комутатор для найбільших і найскладніших мереж. Його основною перевагою є надзвичайно висока пропускна здатність, підтримка 100 Гбіт/с і здатність обробляти великі обсяги даних. Cisco Catalyst 9600 ідеально підходить для дата-центрів і корпоративних мереж, де потрібна максимальна продуктивність і масштабованість.

Загалом, вибір комутатора з серії Cisco Catalyst 9000 залежить від конкретних потреб мережі, таких як масштаб інфраструктури, обсяги мережевого трафіку, кількість підключених пристроїв, рівень безпеки та необхідність підтримки сучасних технологій. Для невеликих офісів або філій з обмеженим бюджетом і помірними вимогами до швидкості і продуктивності оптимальним варіантом буде Cisco Catalyst 9200. Якщо потрібна більша продуктивність для середнього бізнесу з розширеними вимогами до безпеки і масштабованості, найкращим вибором стане Cisco Catalyst 9300.

Для великих підприємств і центрів обробки даних, де потрібно працювати з великими обсягами даних і забезпечити високу пропускну здатність, доцільно вибрати Cisco Catalyst 9400 або 9500.

Якщо мережа має критичні вимоги до швидкості та надійності, найкраще підходить Cisco Catalyst 9600, що дозволяє масштабувати мережу на рівень великих корпоративних або дата-центрів.

2.3 Вибір програмного забезпечення та засобів захисту мережі з віддаленим доступом користувачів

Ефективність функціонування розподілених корпоративних мереж безпосередньо залежить від правильно обраного програмного забезпечення, здатного інтегрувати різноманітні технологічні рішення, забезпечити надійний захист інформаційних ресурсів та підтримати неперервність бізнес-процесів. Програмні технології в контексті мереж з віддаленим доступом виступають критичним елементом архітектури інформаційної системи, від ефективності яких залежить продуктивність, безпека та масштабованість всієї корпоративної інфраструктури.

Основна мета використання програмного забезпечення та сучасних технологій полягає у створенні захищеного середовища для передачі, обробки та зберігання інформації. Це включає широкий спектр завдань, таких як:

- забезпечення автентифікації користувачів та авторизації доступу до ресурсів;
- захист конфіденційності даних при їхньому транспортуванні через відкриті мережі;
- моніторинг активності в мережі для виявлення та запобігання загрозам;
- контроль доступу до ресурсів та управління привілеями користувачів;
- інтеграція з існуючими інфраструктурами та гнучке масштабування систем.

PAN-OS – це програмне забезпечення, яке використовується для роботи всіх міжмережевих екранів нового покоління від Palo Alto Networks. Завдяки ключовим технологіям, які інтегровані в PAN-OS – App-ID, Content-ID, Device-ID і User-ID – можна отримати повну видимість і контроль над використанням додатків усіма користувачами та пристроями в будь-якому місці й у будь-який час.

Це дозволяє забезпечити високий рівень захисту від відомих і невідомих загроз, автоматично реагуючи на зміни в мережевому середовищі та адаптуючись до нових атак. PAN-OS також підтримує централізовану політику безпеки, що дозволяє адміністраторам налаштовувати політики доступу і моніторити події на

всіх пристроях Palo Alto Networks в реальному часі. Завдяки інтеграції з іншими рішеннями безпеки, такими як Palo Alto Networks Cortex і WildFire, PAN-OS забезпечує глибоку аналітику та автоматичну реакцію на інциденти, що допомагає зменшити ризики та підвищити ефективність захисту організацій [26].

PAN-OS постійно вдосконалюється і нові версії програмного забезпечення приносять з собою додаткові можливості для оптимізації безпеки, продуктивності та зручності управління. Нижче наведено основні характеристики версій PAN-OS:

Таблиця 2.3

Основні характеристики і ключові нововведення різних версій PAN-OS

Версія PAN-OS	Основні характеристики і ключові нововведення
9.1	- Покращене управління політиками безпеки через централізовану платформу. - Підтримка автоматичного оновлення сигнатур загроз. - Інтеграція з хмарними платформами для покращеного моніторингу і виявлення загроз. - Розширена підтримка App-ID для кращої видимості додатків.
10.0	- Вдосконалена обробка трафіку для підвищення продуктивності. - Розширене виявлення і блокування нульових вразливостей. - Покращена підтримка нових протоколів і технологій, таких як HTTP/2 і QUIC. - Поліпшення роботи з Content-ID для аналізу і блокування небажаного контенту.
10.1	- Покращена інтеграція з хмарними рішеннями для гнучкості управління. - Нові можливості для виявлення й управління загрозами за допомогою автоматизованих механізмів. - Розширене управління доступом для користувачів через User-ID. - Інтерфейс користувача став більш зручним для налаштувань і моніторингу.
10.2	- Покращена продуктивність через оптимізовані алгоритми обробки даних. - Вдосконалена підтримка нових хмарних архітектур і контейнерів. - Нові можливості для централізованого управління й аналізу мережевого трафіку. - Підвищена захищеність завдяки інтеграції з системами для боротьби з кіберзлочинністю.
11.0	- Інтеграція з рішеннями для аналітики та машинного навчання для реального часу виявлення загроз. - Підвищена підтримка для Zero Trust і автентифікації користувачів. - Нові функції для розпізнавання складних загроз завдяки інтеграції з аналізом поведінки. - Підтримка додаткових можливостей для адаптації до нових типів загроз.
11.1	- Розширені можливості для автоматизації процесів управління політиками безпеки. - Підтримка нових форматів і типів даних для глибокого аналізу трафіку. - Централізоване управління через нові інтерфейси, що спрощує адміністрування. - Покращена інтеграція з третім сторонами для моніторингу й обміну даними.
11.2	- Розширена підтримка для гібридних і мультихмарних середовищ. - Покращена безпека для віддалених користувачів і мереж за допомогою новітніх функцій кіберзахисту. - Підвищена точність і швидкість виявлення загроз через покращене машинне навчання. - Інтеграція з новими рішеннями для захисту від складних кіберзагроз, включаючи APT.

Міжмережеві екрани серії PA-5400 від Palo Alto Networks підтримують версії PAN-OS 10.0 і новіше. Версії 10.0 і 10.1 оптимізовані для високої продуктивності, з підтримкою нових мережевих протоколів та інтеграцією з хмарними платформами, а також удосконаленими функціями для виявлення загроз і блокування небажаного контенту.

Використання PAN-OS дозволяє організаціям значно знизити час реагування на загрози, підвищити прозорість мережевого трафіку і забезпечити більш точний контроль за доступом до корпоративних ресурсів. Завдяки комплексному підходу до безпеки, який охоплює все – від користувачів і додатків до пристроїв і контенту, – PAN-OS є потужним інструментом для забезпечення захисту корпоративних мереж у сучасному цифровому середовищі.

GlobalProtect є одним із ключових компонентів системи Palo Alto Networks, який забезпечує захищений віддалений доступ для користувачів до корпоративних ресурсів. Це рішення працює як розширення функціоналу міжмережевого екрану наступного покоління (NGFW), використовуючи переваги PAN-OS для надійного контролю доступу, шифрування трафіку та забезпечення відповідності політикам безпеки [29].

Застосовуючи модель безпеки нульової довіри Zero Trust, GlobalProtect забезпечує надійну ідентифікацію користувачів і надає детальний контроль над доступом до ресурсів, а також впроваджує багатофакторну автентифікацію для доступу до конфіденційних ресурсів, що підвищує рівень безпеки.

GlobalProtect забезпечує безперебійне застосування політики незалежно від місця розташування користувача. Ця платформа надає адміністраторам повний набір можливостей для ефективної боротьби з кіберзагрозами. Використовуючи такі технології, як App-ID і User-ID, організації можуть адаптувати політику на основі використання програми та профілів користувачів, забезпечуючи точний контроль над доступом до мережі. Крім того, такі функції, як розшифровка SSL і захист від зловмисного програмного забезпечення WildFire, дозволяють перехоплювати загрози та пом'якшувати їх у реальному часі, зміцнюючи захист від нових кіберзагроз.

Використання Palo Alto GlobalProtect надає значні переваги організаціям, які прагнуть покращити мобільність користувачів і можливості віддаленого доступу, а саме:

- покращена безпека;
- підвищена продуктивність;
- дотримання нормативних вимог;
- економічність.

Покращена безпека здійснюється за рахунок використання надійних протоколів шифрування GlobalProtect, багатфакторної автентифікації та заходів забезпечення безпеки кінцевих точок.

Розширене запобігання загрозам зменшує ризики безпеки, пов'язані з віддаленим доступом, захищаючи критичні активи від потенційних порушень або викрадання даних.

Підвищення продуктивності забезпечує безперебійний і безпечний доступ до корпоративних ресурсів з будь-якого місця чи пристрою, GlobalProtect підвищує продуктивність робочої сили, полегшуючи співпрацю та безперервність операцій незалежно від географічних обмежень.

Дотримання нормативних вимог допомагає організаціям дотримуватися нормативних вимог, запроваджуючи суворий контроль доступу, перевіряючи дії користувачів і ведучи повні журнали для звітування про відповідність.

Функції централізованого управління та масштабованості GlobalProtect мінімізують адміністративні накладні витрати та витрати на інфраструктуру, пов'язані з наданням віддаленого доступу, створюючи економічно ефективне рішення для організацій різного розміру.

Одним з основних сценаріїв використання Palo Alto GlobalProtect є забезпечення мобільності та віддаленого доступу користувачів до корпоративних ресурсів [1].

Основні кроки цього процесу:

1. Розгортання і конфігурація.
2. Аутентифікація та авторизація.

3. Шифрування трафіку.
4. Моніторинг та аналіз.
5. Підтримка мобільних пристроїв.

Розгортання та налаштування GlobalProtect в корпоративній мережі включає в себе встановлення серверів, налаштування політик безпеки та інтеграцію з існуючими інфраструктурними рішеннями. Платформа може бути розміщена в хмарі, на власному обладнанні або в гібридній конфігурації, що робить її ідеальним рішенням для організацій будь-якого розміру та потреб. Процес розгортання може бути значно спрощений завдяки автоматизації за допомогою скриптів та інструментів оркестрування.

Для забезпечення безпеки доступу, GlobalProtect використовує різні методи аутентифікації, такі як аутентифікація за допомогою логіну та пароля, сертифікатів, а також двофакторну аутентифікацію. Крім того, адміністратор може встановлювати правила доступу до різних ресурсів мережі, контролювати час та обсяги з'єднань, а також відслідковувати активність користувачів для виявлення потенційних загроз.

Однією з ключових функцій GlobalProtect є шифрування трафіку між клієнтом та сервером, що забезпечує конфіденційність інформації, яка передається по мережі. GlobalProtect використовує стійкі алгоритми шифрування для захисту даних, що передаються між клієнтом та сервером. Залежно від конфігурації, може бути зашифровано весь трафік або лише трафік до корпоративних ресурсів. Це гарантує конфіденційність інформації та захищає її від перехоплення та несанкціонованого доступу.

GlobalProtect надає адміністраторам потужні інструменти для моніторингу та аналізу активності користувачів та трафіку. Детальні журнали та звіти дають уявлення про те, хто, коли, як і до яких ресурсів отримує доступ. Моніторинг у реальному часі дозволяє негайно реагувати на будь-які підозрілі дії.

GlobalProtect розширює свою функціональність, надаючи безпеку не лише для користувачів настільних комп'ютерів, але і для мобільних пристроїв, таких як смартфони та планшети. Ця можливість дозволяє користувачам з легкістю

отримувати доступ до корпоративних ресурсів навіть у русі, не обмежуючи їхньої продуктивності та забезпечуючи безпеку даних.

Таким чином, GlobalProtect стає життєво важливим компонентом операційної платформи безпеки Palo Alto Networks, що дає можливість організаціям розширювати надійну безпеку кінцевих точок і можливості віддаленого доступу для мобільних працівників.

Висновки до другого розділу

У другому розділі було детально розглянуто процес розробки захищеної мережі з віддаленими користувачами, що включав три основні аспекти: проектування структурної схеми, вибір мережевого обладнання та програмного забезпечення.

При проектуванні структурної схеми мережі було визначено, що ключовим елементом захисту є міжмережеві екрани нового покоління (NGFW), які забезпечують глибокий аналіз трафіку, контроль додатків та виявлення загроз у реальному часі.

В частині вибору мережевого обладнання було обґрунтовано використання міжмережевих екранів Palo Alto Networks серії PA-5400, маршрутизаторів Cisco ISR 4000 та комутаторів Cisco Catalyst 9000. Кожен компонент було обрано з урахуванням вимог до продуктивності, масштабованості та безпеки.

Щодо програмного забезпечення, було визначено, що операційна система PAN-OS та платформа GlobalProtect від Palo Alto Networks є оптимальними рішеннями для забезпечення безпеки віддаленого доступу. PAN-OS забезпечує комплексний захист завдяки технологіям App-ID, Content-ID, Device-ID та User-ID, а GlobalProtect реалізує концепцію Zero Trust та забезпечує захищений доступ до корпоративних ресурсів з будь-якої точки світу.

Таким чином, запропоноване комплексне рішення дозволяє створити надійну та захищену мережеву інфраструктуру, яка відповідає сучасним вимогам до безпеки даних та забезпечує ефективну роботу віддалених користувачів.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИЩЕНОЇ МЕРЕЖІ З ВІДДАЛЕНИМ ДОСТУПОМ КОРИСТУВАЧІВ

3.1 Базове налаштування захищеної мережі та міжмережного екрану Palo Alto

Для забезпечення коректної роботи мережі необхідно виконати налаштування з урахуванням правильних параметрів, які відповідають специфікаціям обладнання та вимогам безпеки. Крім того, слід дотримуватися чіткої послідовності налаштувань, щоб уникнути конфліктів між компонентами, забезпечити злагоджену взаємодію між пристроями та мінімізувати можливі помилки. Кожен мережевий компонент, зокрема комутатори, маршрутизатори, точки доступу та міжмережевий екран, має бути налаштований із використанням відповідних параметрів, що відповідають їхній функціональності та місцю в загальній топології мережі.

Далі наведено початкове налаштування міжмережного екрану, яке включає конфігурацію базових правил безпеки, сегментацію мережі, визначення політик доступу, а також налаштування систем моніторингу трафіку для виявлення та запобігання можливим загрозам. Таке налаштування є важливим етапом, який забезпечує захист мережі від зовнішніх атак і гарантує безпечний доступ до ресурсів.

За замовчуванням порт керування в даному міжмережному екрані має IP-адресу 192.168.1.1, доступ до якої здійснюється через веб-браузер. У разі тривалої відсутності з'єднання брандмауер автоматично вмикає DHCP на порті керування для отримання IP-адреси. Для стабільної роботи рекомендується налаштувати статичну IP-адресу.

Для налаштування статичної IP-адреси використовується режим конфігурації і наступні команди:

```
configure
set deviceconfig system type static
set deviceconfig system ip-address 192.168.1.1 netmask 255.255.255.0 default-gateway
192.168.1.254 dns-setting servers primary 8.8.8.8
commit
```

Після виконання команди `commit` доступ до веб-інтерфейсу здійснюється за IP-адресою 192.168.1.1, як наведено на рисунку 3.1.



Рисунок 3.1 – Вхід до веб-інтерфейсу міжмережного екрану

Після успішного входу в систему потрапляємо на інформаційну панель, яка показує налаштування системи та загальну інформацію про брандмауер.

Для завершення початкового налаштування вимагає коректного встановлення загальних параметрів. Для цього необхідно перейти до розділу **ПРИСТРІЙ > Налаштування > Керування** та відкрити параметри загальних налаштувань, натиснувши на відповідний інтерфейс (Рис. 3.2).

У даному розділі варто встановлювати такі параметри: коректне ім'я хоста, домен, налаштувати банер для входу та встановити точний час.

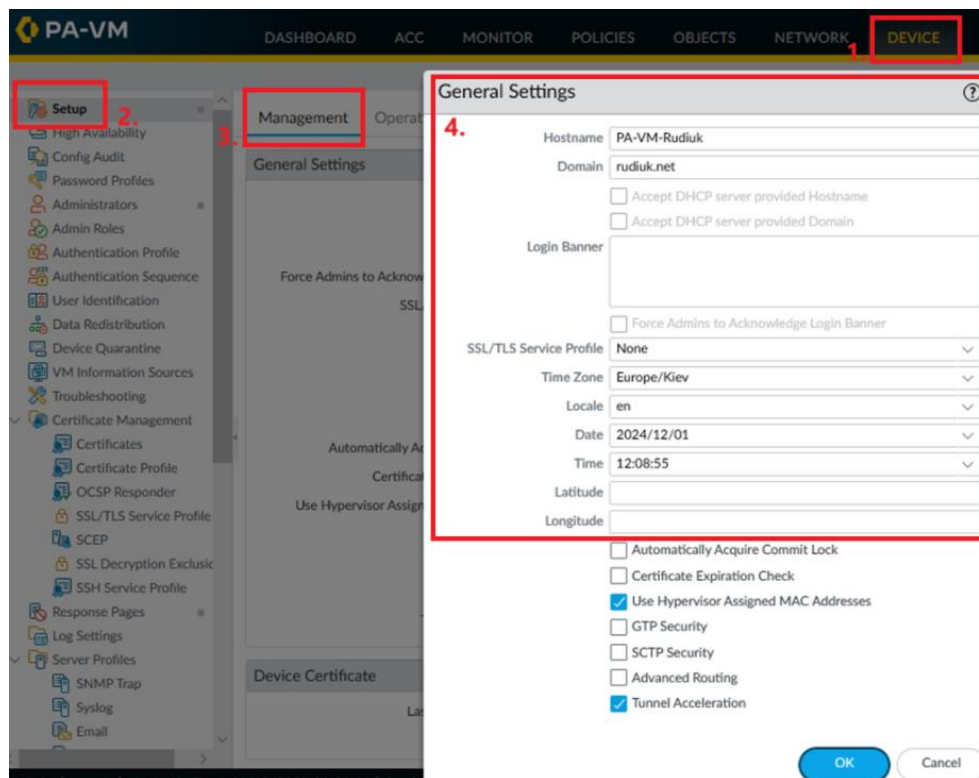


Рисунок 3.2 – Базове налаштування: ім'я хоста, домен, банер, дата та час

Для додавання додаткових DNS-серверів, NTP-серверів або HTTP-проксі, які використовуватимуться брандмауером, необхідно виконати відповідні налаштування. Для цього слід перейти до розділу **ПРИСТРІЙ > Налаштування > Служби** та відкрити параметри сервісів, натиснувши на значок шестірні у відповідному розділі (Рис. 3.3).

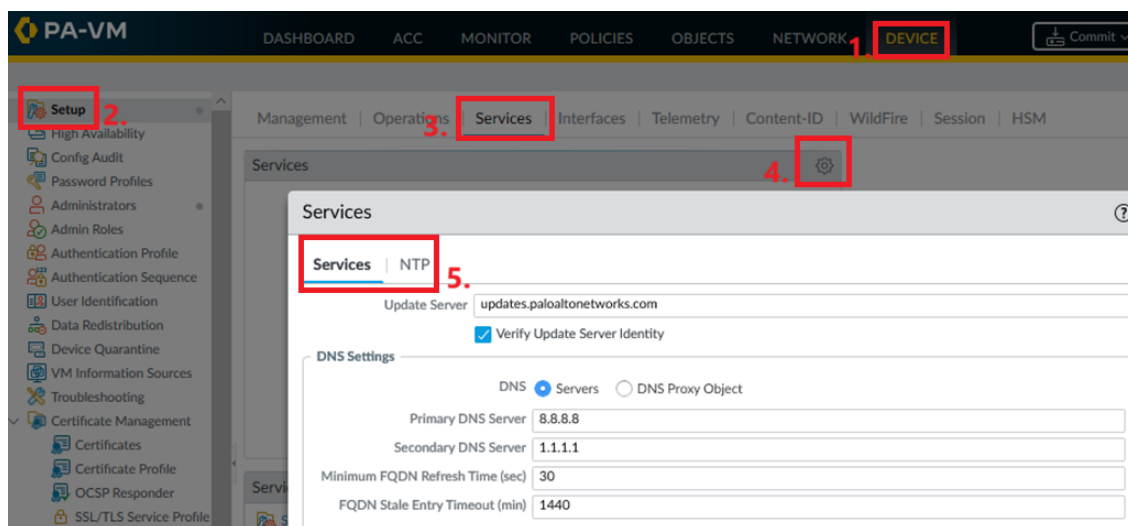


Рисунок 3.3 – Налаштування DNS, NTP або проксі

На попередніх етапах основна увага була зосереджена на налаштуваннях, що стосуються управління та функціонування самого брандмауера. Наступним кроком є створення зон безпеки, які будуть використовуватися для визначення правил доступу після призначення їм відповідних інтерфейсів.

Зони безпеки у міжмережних екранах Palo Alto Networks працюють аналогічно до концепції зон в інших типах брандмауерів. Призначення інтерфейсів або мереж різним зонам спрощує конфігурацію та полегшує її впровадження.

У межах спрощеної топології необхідно створити дві зони: INSIDE і OUTSIDE. Зону INSIDE буде призначено інтерфейсу, підключеному до клієнтів, а зону OUTSIDE — інтерфейсу, підключеному до Інтернету.

Для створення зон слід перейти до розділу **МЕРЕЖА > Зони** та натиснути кнопку **+Додати** у нижньому лівому куті.

Далі необхідно створити дві зони з назвами INSIDE і OUTSIDE, встановити параметр **Type** у значення **Layer 3**, а решту налаштувань поки залишити порожніми, як наведено на рисунку 3.4.

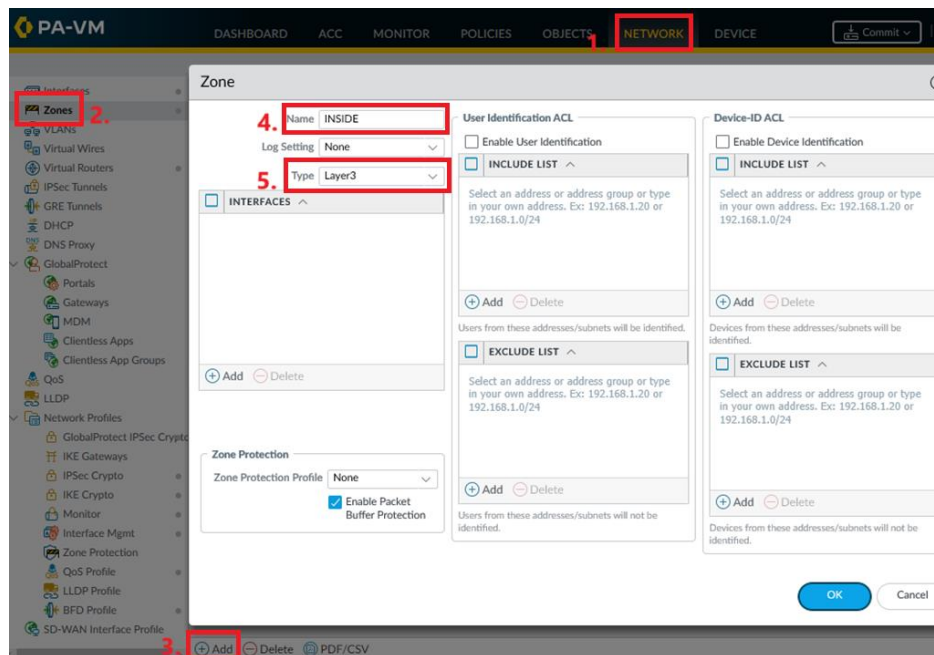


Рисунок 3.4 – Створення та налаштування зони безпеки

Необхідно повторити зазначений крок, створивши також зону OUTSIDE.

PA-VM

DASHBOARD

ACC

MONITOR

POLICIES

OBJECTS

NETWORK

DEVICE

Commit

Interfaces

Zones

VLANs

Virtual Wires

Virtual Routers

IPSec Tunnels

GRE Tunnels

DHCP

<

Рисунок 3.5 – Налаштовані INSIDE та OUTSIDE зони безпеки

Для забезпечення приймання певних мережевих служб (наприклад, ping) через стандартні мережеві інтерфейси, необхідно створити профіль керування, який дозволяє ці служби. Після цього даний профіль керування буде прикріплений до відповідних мережевих інтерфейсів.

У даному прикладі передбачається дозвіл лише для служби ping. Водночас, за необхідності, можна дозволити й інші служби керування на стандартних мережевих інтерфейсах. Проте рекомендується обмежувати доступ виключно IP-адресами мереж, що належать адміністраторам мережі або безпеки.

Для створення профілю керування необхідно перейти до розділу **МЕРЕЖА > Профілі мережі > Керування інтерфейсом**. Далі слід натиснути кнопку **+Додати** у нижньому лівому куті, створити новий профіль керування, в якому дозволити лише службу ping та завершити налаштування (Рис. 3.6).

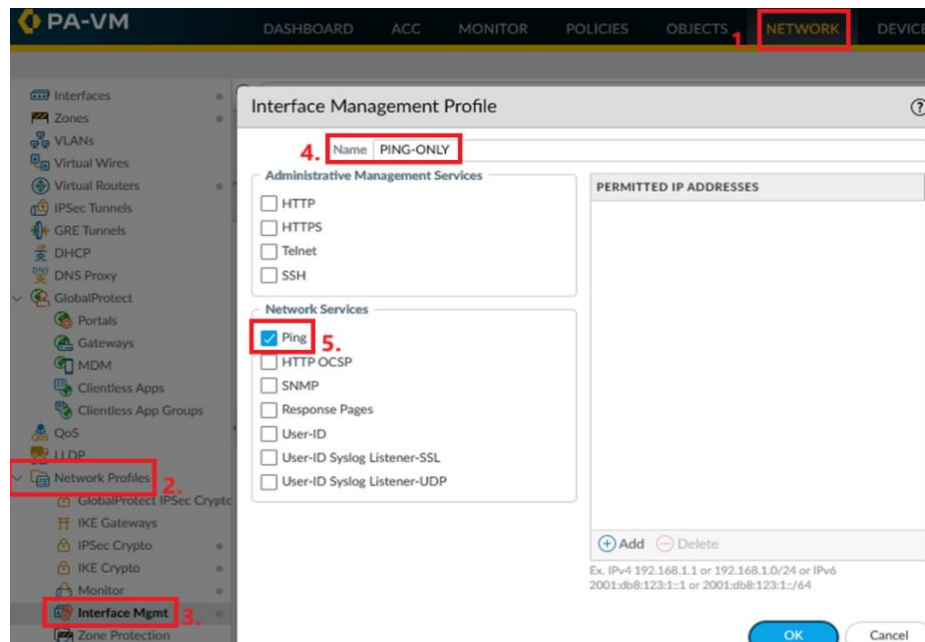


Рисунок 3.6 – Створення та налаштування профілю керування

На наступному етапі необхідно виконати остаточну конфігурацію мережевих інтерфейсів брандмауера.

Для початку слід перейти до розділу **МЕРЕЖА > Інтерфейси > Ethernet**, щоб переглянути список доступних інтерфейсів. У даному прикладі передбачено використання Ethernet1/1 для підключення до Інтернету, а Ethernet1/2 — для підключення клієнтів у внутрішній мережі (Рис. 3.7.).

Для налаштування Ethernet1/2 необхідно натиснути на відповідний інтерфейс, щоб відкрити його вікно конфігурації.

У параметрах конфігурації можна додати коментар до інтерфейсу, встановити тип інтерфейсу як Layer 3. На вкладці «Конфігурація» потрібно задати значення «за замовчуванням» для «Віртуального маршрутизатора», а для зони безпеки обрати зону OUTSIDE, створену раніше.

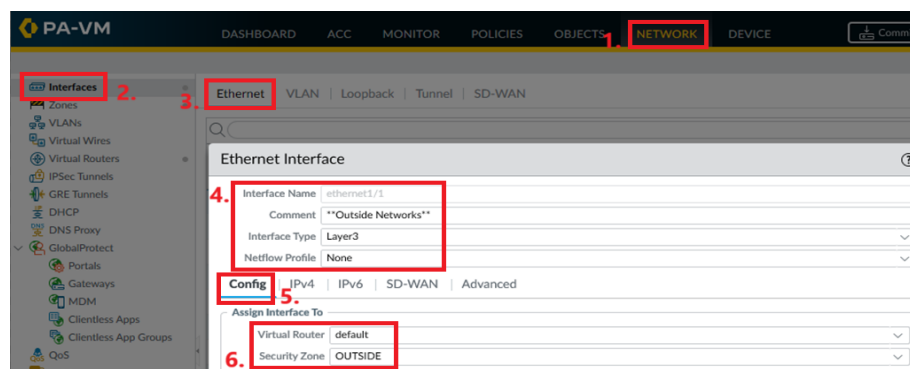


Рисунок 3.7 – Налаштування мережного інтерфейсу

Далі необхідно перейти на вкладку **IPv4**, вибрати тип «**Статичний**» та натискати кнопку **+Додати**, щоб ввести IP-адресу для цього інтерфейсу. У даному випадку інтерфейс буде використовувати IP-адресу 201.231.24.254 з маскою підмережі /24.

The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/1' and the 'Comment' is '**Outside Networks**'. The 'Interface Type' is 'Layer3' and the 'Netflow Profile' is 'None'. The 'Config' tab is selected, and the 'IPv4' sub-tab is active. The 'Type' is set to 'Static'. A list of IP addresses is shown with '201.231.24.254/24' selected. The 'Add' button is highlighted. The 'OK' button is at the bottom right.

Рисунок 3.8 – Налаштування IP-адреси на інтерфейсі

На останньому етапі потрібно перейти на вкладку «**Додатково**». У розділі «**Інша інформація**» можна обрати створений профіль керування. З міркувань безпеки профіль керування потрібно індивідуально призначати, як наведено на рисунку 3.9.

The screenshot shows the 'Ethernet Interface' configuration window, specifically the 'Advanced' tab. The 'Link Settings' section shows 'Link Speed' as 'auto', 'Link Duplex' as 'auto', and 'Link State' as 'auto'. The 'Other Info' section is expanded, showing 'Management Profile' set to 'PING-ONLY'. The 'MTU' is set to '1500'. The 'Adjust TCP MSS' section is expanded, showing 'IPv4 MSS Adjustment' as '40' and 'IPv6 MSS Adjustment' as '60'. The 'Untagged Subinterface' checkbox is unchecked. The 'OK' button is at the bottom right.

Рисунок 3.9 – Налаштування профілю керування для інтерфейса

Після завершення налаштувань інтерфейсів огляд сторінки матиме вигляд, як представлено на рисунку 3.10.

The screenshot shows the PA-VM Network configuration page. The left sidebar lists various network-related items: Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPsec Tunnels, GRE Tunnels, DHCP, and DNS Proxy. The main area displays a table of Ethernet interfaces.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE
ethernet1/1	Layer3	PING-ONLY		201.231.24.254/24	default	Untagged	none
ethernet1/2	Layer3	PING-ONLY		211.231.24.254/24	default	Untagged	none

Рисунок 3.10 – Огляд доступних налаштованих інтерфейсів

Після завершення конфігурації мережевих інтерфейсів можна приступити до налаштування маршрутизації. У рамках цього прикладу необхідно налаштувати лише маршрут за замовчуванням до провайдера.

Для цього слід перейти до розділу **МЕРЕЖА > Віртуальні маршрутизатори** та відкрити віртуальний маршрутизатор «за замовчуванням». У розділі «Налаштування маршрутизатора» будуть відображені обидва інтерфейси, які належать цьому маршрутизатору (Ethernet1/1 і Ethernet1/2).

Далі, у розділі Static Routes, потрібно натиснути кнопку +Add, щоб додати маршрут за замовчуванням (Рис. 3.11).

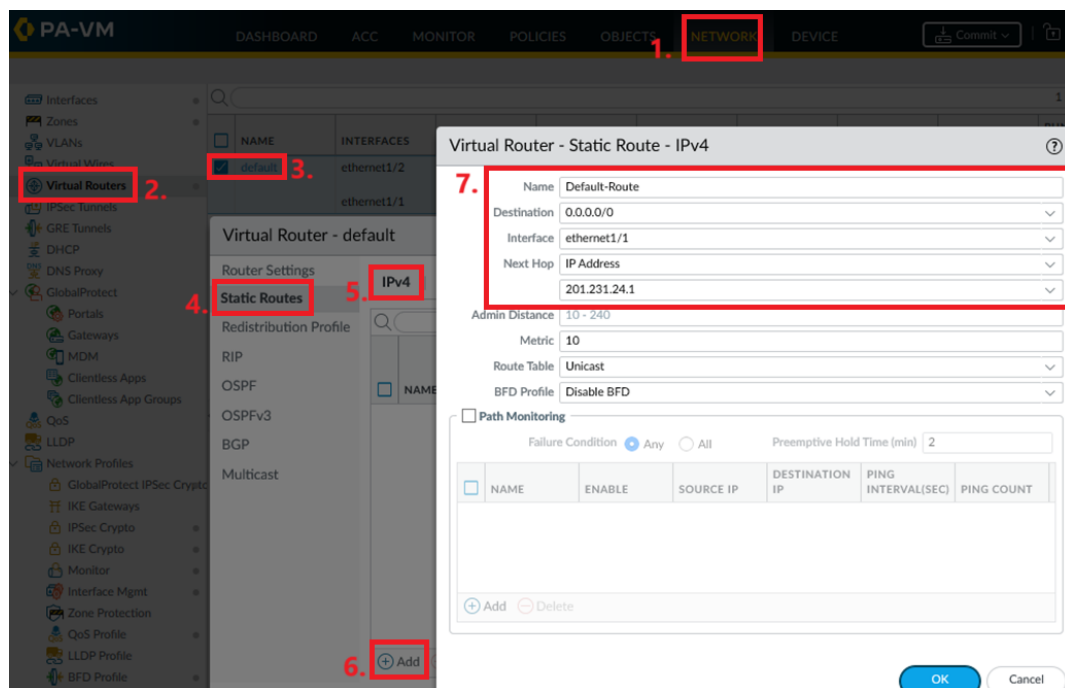


Рисунок 3.11 – Налаштування маршрутизації

Для забезпечення підключення клієнтів до Інтернету необхідно налаштувати перетворення мережевих адрес (NAT), яка забезпечує перетворення внутрішньої IP-адреси пристрою на зовнішню IP-адресу (Рис. 3.12).

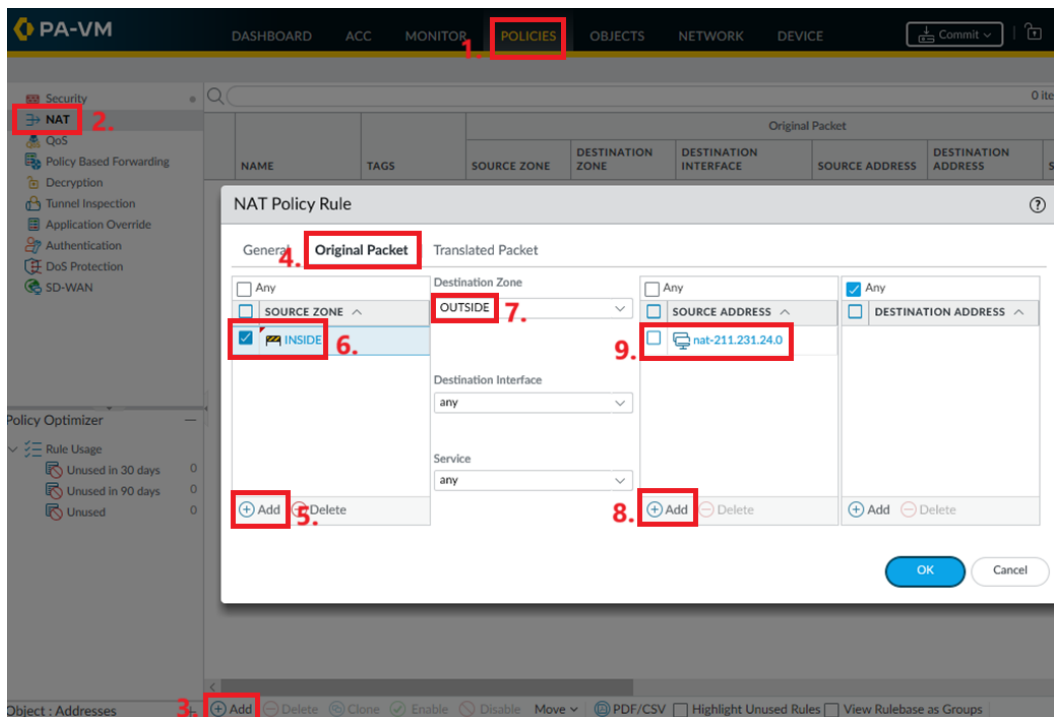


Рисунок 3.12 – Налаштування NAT

Для цього потрібно перейти до розділу **ПОЛІТИКИ > NAT** та натиснути кнопку **+Додати**, щоб створити нове правило NAT. У параметрах вихідної зони оберіть **INSIDE**, а в параметрах цільової зони — **OUTSIDE**.

На вкладці **«Трансляція пакету»** необхідно визначити спосіб трансляції трафіку, обраного на попередньому етапі. У цьому випадку внутрішня мережа буде транлюватися на IP-адресу інтерфейсу брандмауера, який забезпечує доступ до Інтернету, для трафіку, що потребує виходу у зовнішню мережу, як наведено на рисунку 3.13.

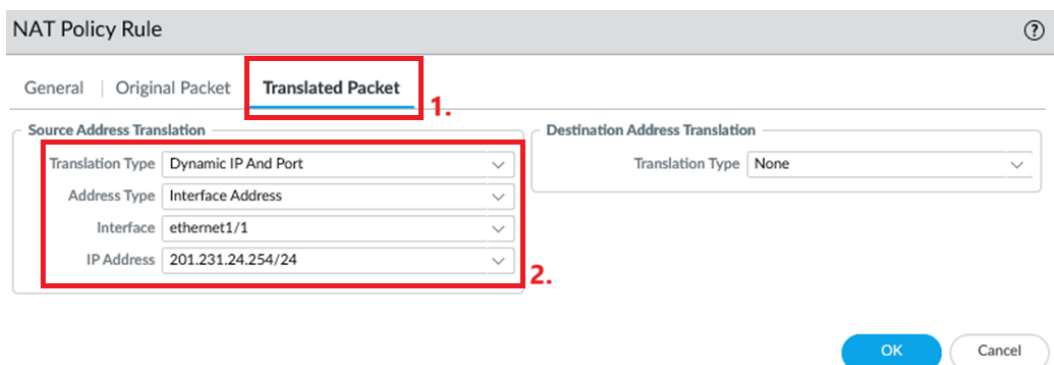


Рисунок 3.13 – Налаштування трансляції пакету

Виконавши всі наведені етапи було завершено базове налаштування міжмережного екрану.

3.2 Налаштування GlobalProtect VPN на міжмережному екрані Palo Alto для підключення віддалених користувачів

Для налаштування GlobalProtect VPN необхідно мати дійсний кореневий сертифікат центру сертифікації (ЦС), який забезпечує підтвердження автентичності і довіри до вашого VPN-з'єднання. Сертифікат відіграє ключову роль у встановленні захищених комунікацій між клієнтом і сервером, використовуючи протоколи шифрування для гарантування конфіденційності та цілісності переданих даних.

Сертифікат можна згенерувати із власним підписом безпосередньо на брандмауері Palo Alto або використати сертифікат, підписаний будь-яким зовнішнім центром сертифікації.

Щоб створити сертифікат із власним підписом, необхідно перейти до розділу **ПРИСТРІЙ > Керування сертифікатами > Сертифікати > Сертифікати пристрою** та натиснути «Згенерувати».

Далі необхідно заповнити поля сертифіката згідно з потрібними параметрами. Особливу увагу слід приділяти полю «Загальне ім'я», у якому потрібно вказати публічну IP-адресу (Рис. 3.14).

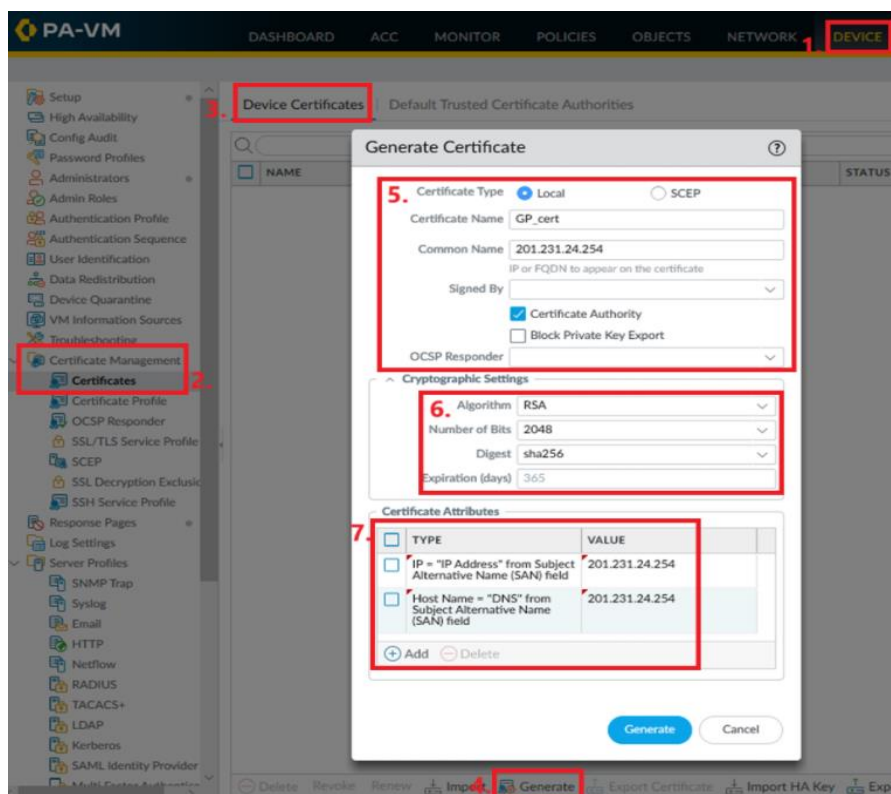


Рисунок 3.14 – Генерація сертифікату

Certificate information	
Name	GP_cert
Subject	/CN=201.231.24.254
Issuer	/CN=201.231.24.254
Not Valid Before	Dec 13 12:24:19 2024 GMT
Not Valid After	Dec 13 12:24:19 2025 GMT
Algorithm	RSA
☒ Certificate Authority ☐ Forward Trust Certificate ☐ Forward Untrust Certificate ☒ Trusted Root CA	

Рисунок 3.15 – Інформація про згенерований сертифікат

На наступному етапі необхідно створити профіль SSL/TLS, який буде використовуватися для налаштування порталу. Для цього необхідно перейти до розділу **ПРИСТРІЙ > Керування сертифікатами > Профіль служби SSL/TLS** та натиснути «Додати».

У новоствореному профілі потрібно обрати сертифікат, який був створений на попередньому етапі, а також задати мінімальну та максимальну версії протоколу TLS відповідно до вимог конфігурації.

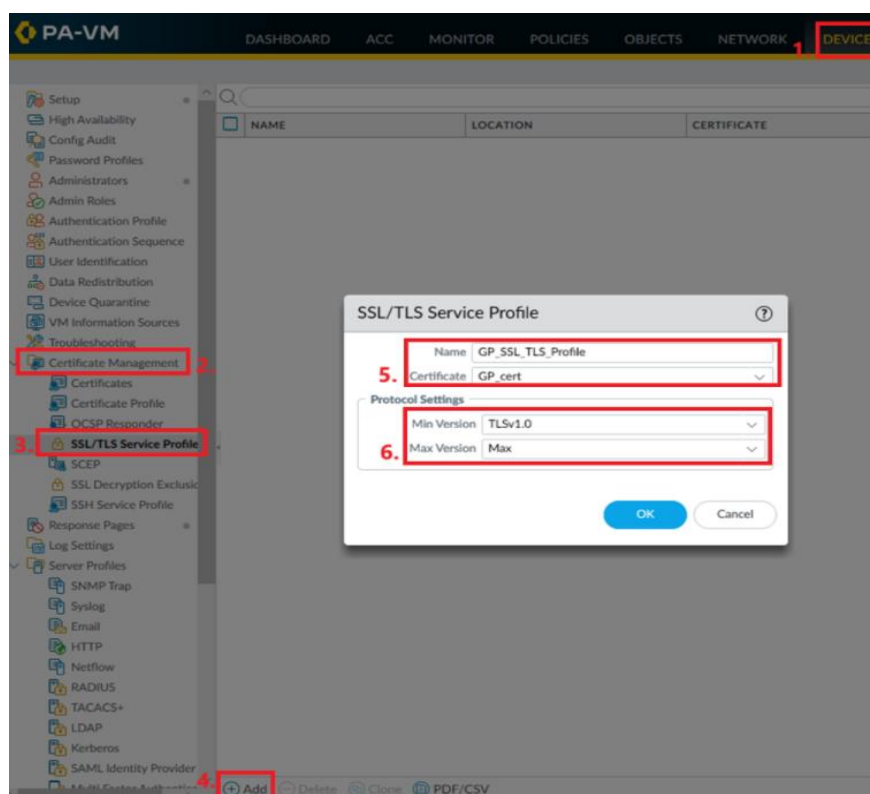


Рисунок 3.16 – Налаштування профілю служби SSL/TLS

Для функціонування GlobalProtect VPN необхідно забезпечити автентифікацію користувачів під час встановлення VPN-з'єднання. У цьому прикладі створюється локальний користувач. Для цього потрібно перейти до

розділу **ПРИСТРІЙ** > **Локальна база даних користувачів** > **Користувачі** та натиснути «Додати» (Рис. 3.17).

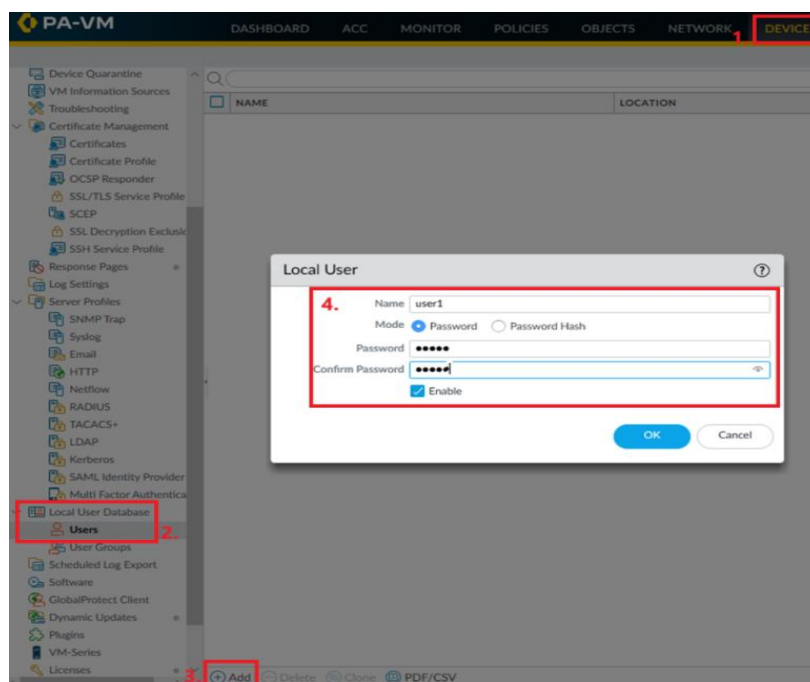


Рисунок 3.17 – Створення локальних користувачів

Для налаштування автентифікації користувачів GlobalProtect необхідно створити відповідний профіль автентифікації. Для цього потрібно перейти до розділу **ПРИСТРІЙ** > **Профіль автентифікації** та натиснути «Додати» (Рис. 3.18).

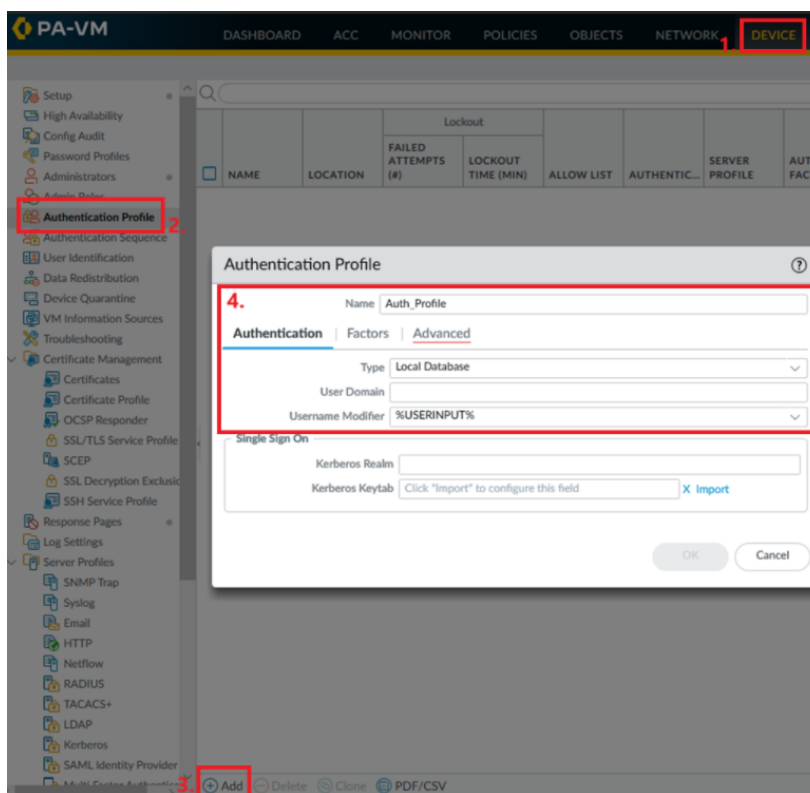


Рисунок 3.18 – Створення профілю автентифікації

На вкладці «Додатково» необхідно додати користувачів до списку дозволених, як наведено на рисунку нижче.

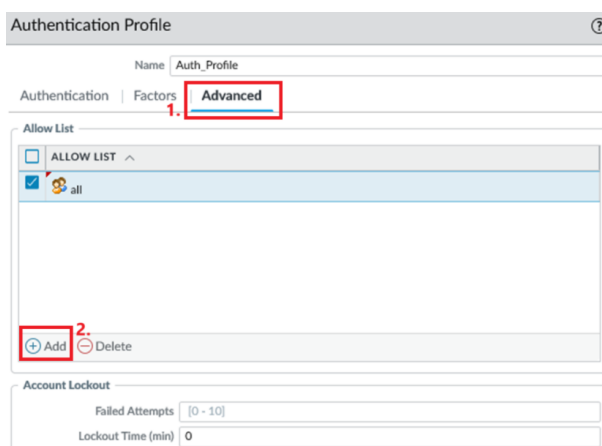


Рисунок 3.19 – Додавання необхідних користувачів до списку дозволених

Далі для GlobalProtect VPN необхідно створити зону для інтерфейсу тунелю. Хоча можна використовувати одну з наявних зон, рекомендується створювати нову, щоб забезпечити точний контроль над трафіком GlobalProtect.

Для цього необхідно перейти до розділу **МЕРЕЖА > Зони** та натиснути «Додати». Далі вибрати тип зони Рівень 3 та активувати параметр «Увімкнути ідентифікацію користувача».

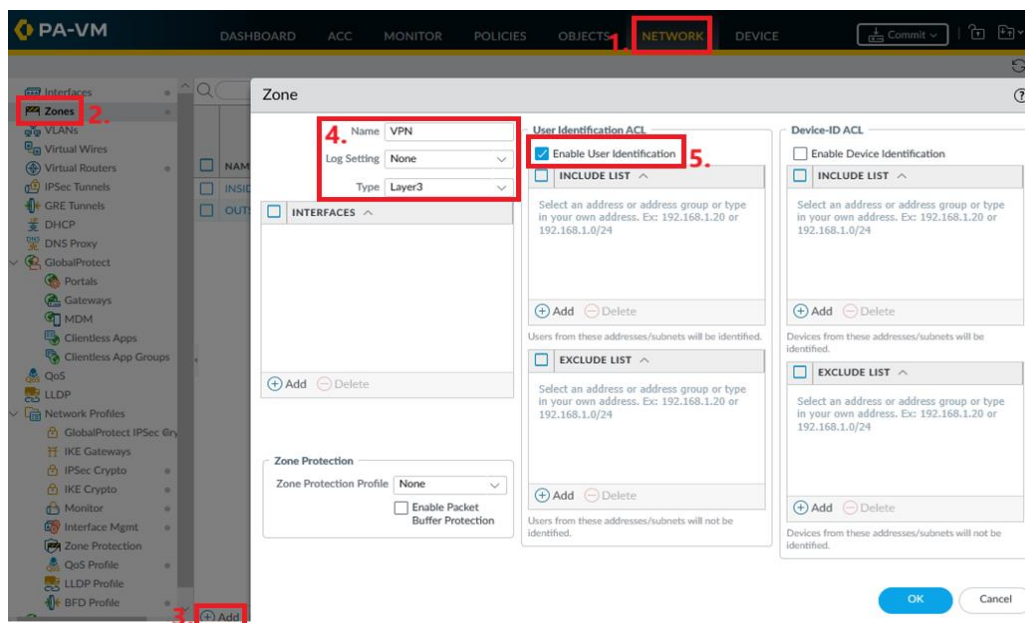


Рисунок 3.20 – Створення зони для трафіку GlobalProtect

Також, для GlobalProtect VPN необхідно створити окремий інтерфейс тунелю. Для цього потрібно перейти до **МЕРЕЖА > Інтерфейси > Тунель** та натиснути «Додати», щоб створити новий інтерфейс тунелю.

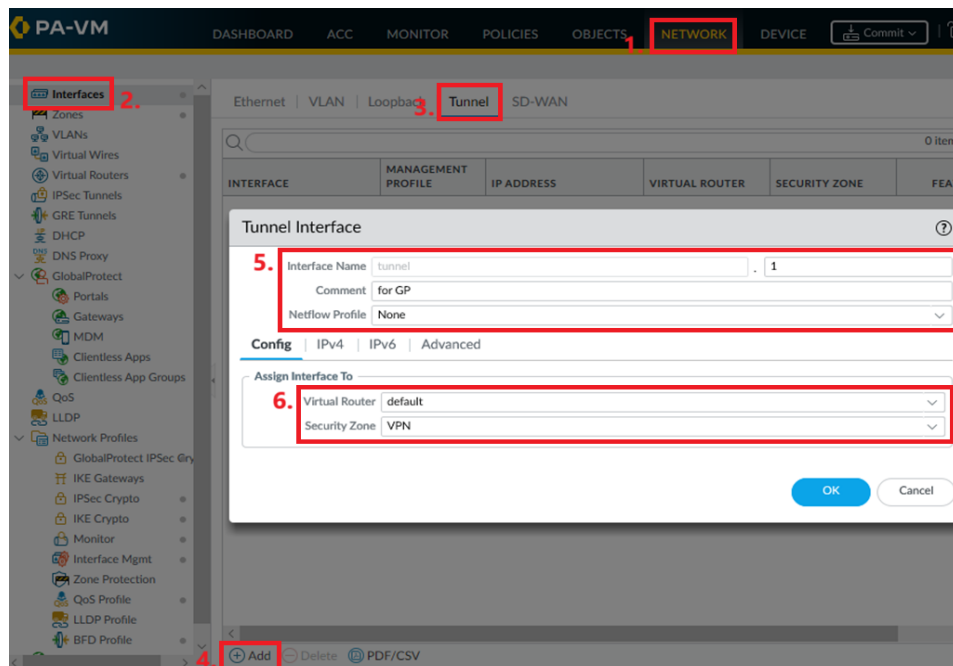


Рисунок 3.21 – Створення інтерфейсу тунеля

Обов'язково потрібно призначити цьому інтерфейсу ту ж зону безпеки, яку було створено на попередньому етапі. За потреби можна додати до інтерфейсу тунелю профіль керування відповідно до необхідних вимог.

Далі можна розпочати налаштування фактичної конфігурації для GlobalProtect. Для цього потрібно перейти до **МЕРЕЖА > GlobalProtect > Portals > Додати**. На вкладці «Загальні» необхідно ввести назву для конфігурації порталу GlobalProtect. У розділі налаштувань мережі вибрати інтерфейс, через який міжмережний екран буде приймати запити від клієнтів GlobalProtect (Рис. 3.22).

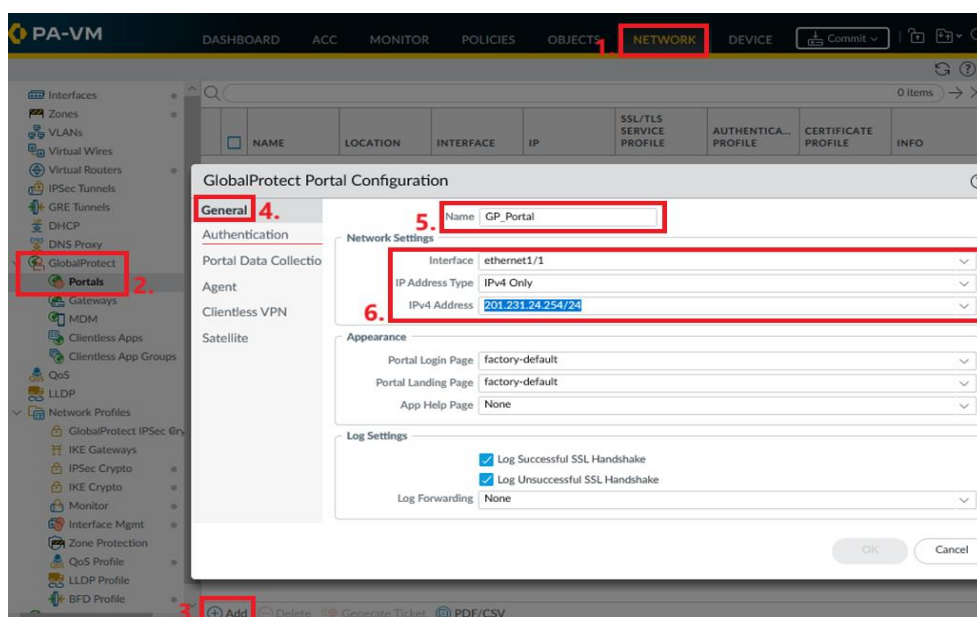


Рисунок 3.22 – Налаштування фактичної конфігурації для GlobalProtect

На наступному кроці потрібно перейти на вкладку «**Автентифікація**» та вибрати профіль служби SSL/TLS, який був створений на попередньому етапі. На цьому етапі потрібно вказати зручну назву для автентифікації клієнта та обрати операційні системи, на яких буде використовуватися GlobalProtect.

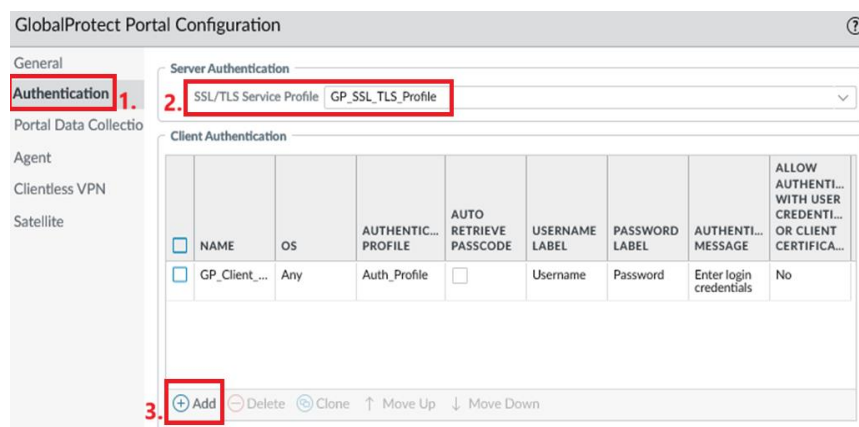


Рисунок 3.23 – Налаштування автентифікації для фактичної конфігурації GlobalProtect

Тепер потрібно перейти на вкладку «**Агент**» та вибрати довірений кореневий центр сертифікації, який був створений на першому етапі. Потім натиснути «**Додати агента**» і надати агенту зручне ім'я (Рис. 3.24).

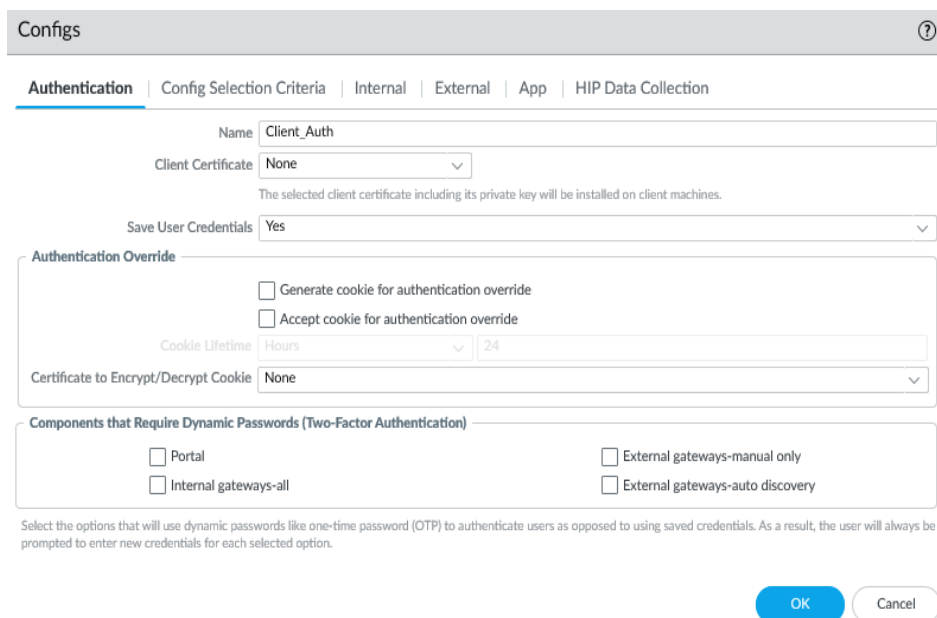


Рисунок 3.24 – Створення агента GlobalProtect

Далі потрібно перейти на вкладку «**Зовнішні**» та додати зовнішній шлюз. Необхідно ввести ім'я шлюзу, його IP-адресу, регіон джерела, а також налаштувати параметри пріоритету.

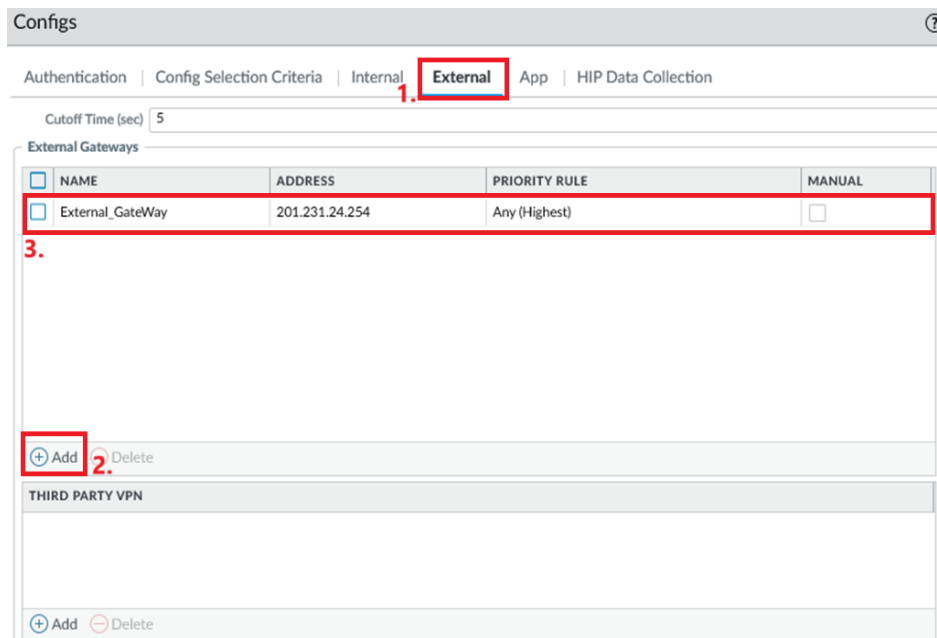


Рисунок 3.25 – Додавання зовнішнього шлюзу

Після конфігурації порталу GlobalProtect необхідно налаштувати шлюз для GlobalProtect VPN. Для цього потрібно перейти до **МЕРЕЖА > GlobalProtect > Шлюзи** та натиснути «Додати» (Рис. 3.26).

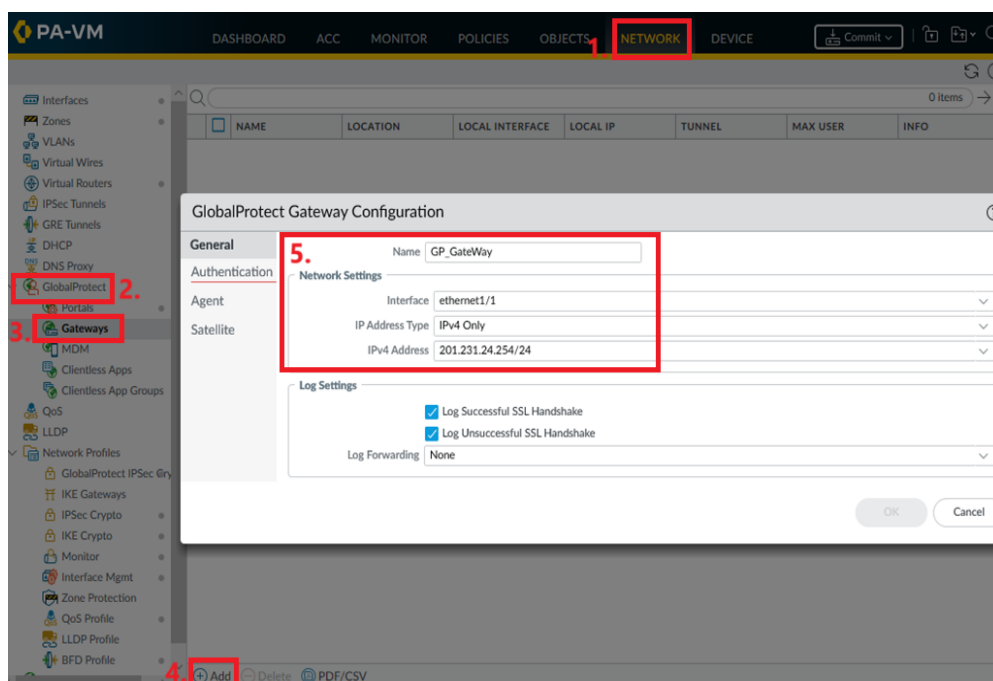


Рисунок 3.26 – Додавання шлюзу для GlobalProtect VPN

Далі потрібно перейти на вкладку «**Автентифікація**», обрати профіль SSL/TLS і натиснути «Додати», щоб додати профіль автентифікації для клієнта. У цьому розділі необхідно вказати назву, операційну систему та профіль автентифікації.

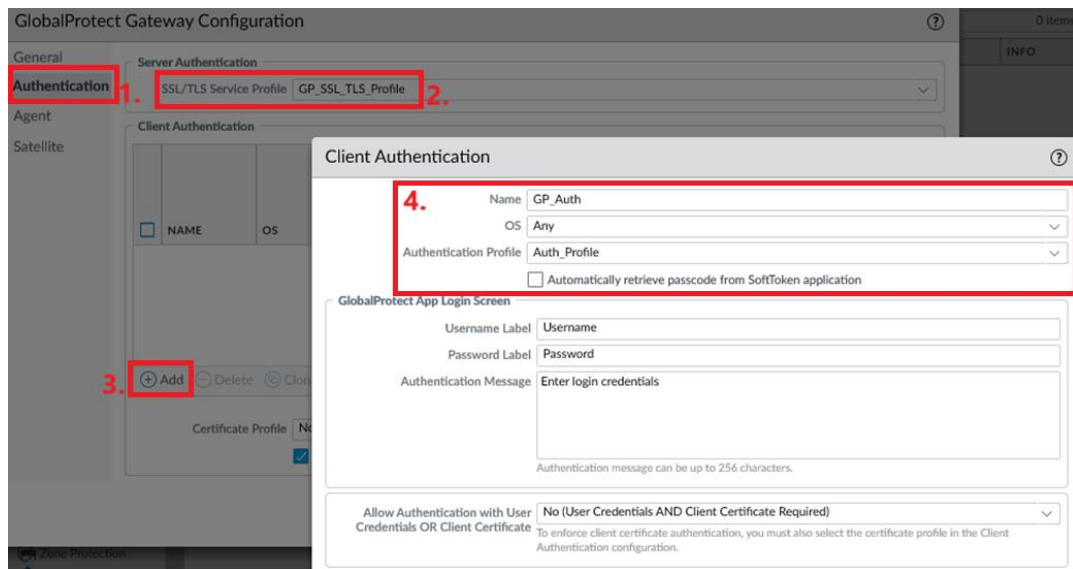


Рисунок 3.27 – Додавання профілю автентифікації для клієнтів

Далі на вкладці «Агент» необхідно увімкнути режим тунелю та вибрати інтерфейс тунелю який був створений на попередньому кроці.

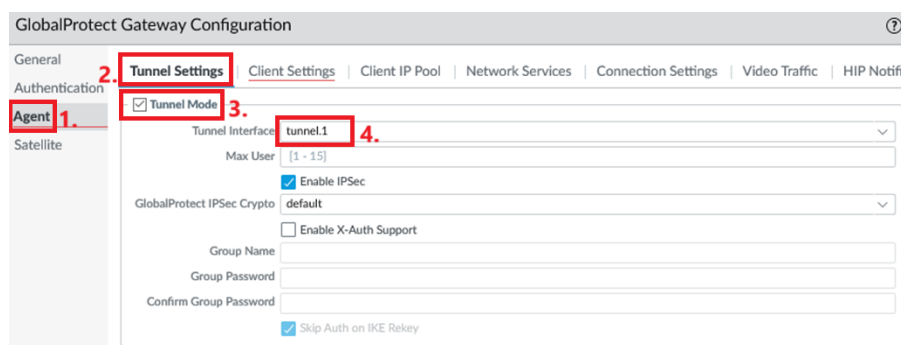


Рисунок 3.28 – Увімкнення режиму тунеля

Далі на вкладці «Параметри клієнта» потрібно додати налаштування клієнта.

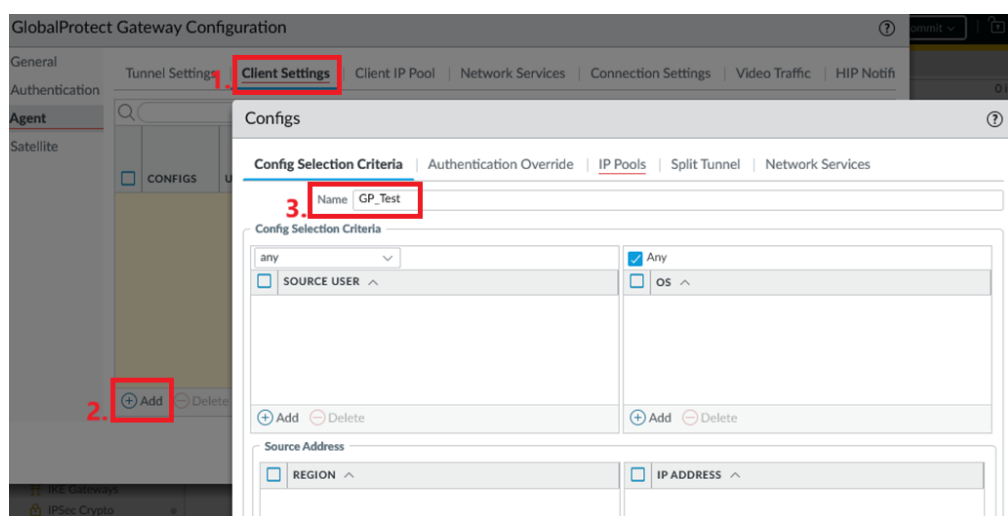


Рисунок 3.29 – Додавання налаштувань клієнта

Тепер необхідно перейти до IP-пулів і вказати IP-діапазон або підмережу, які будуть використовуватися для надання IP-адреси після успішної автентифікації клієнта через GlobalProtect.

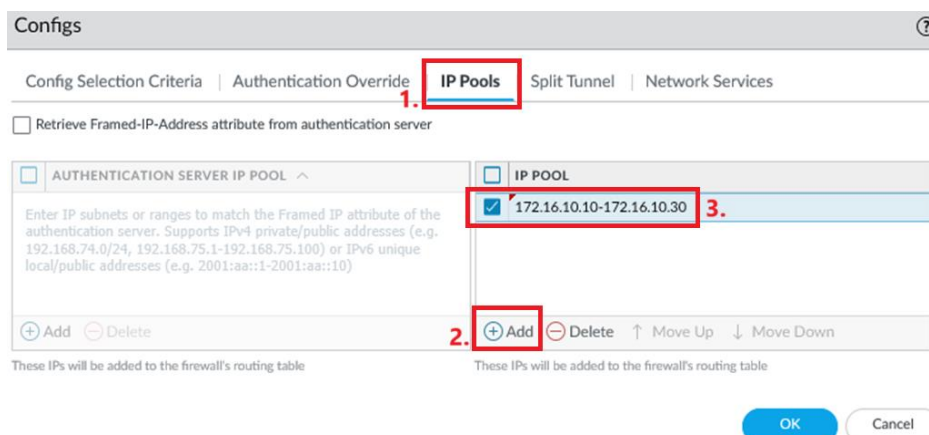


Рисунок 3.30 – Створення IP-пулів

Далі потрібно перейти на вкладку «Розділений тунель» і увімкнути доступ до всіх мереж, які будуть доступними для віддалених клієнтів.

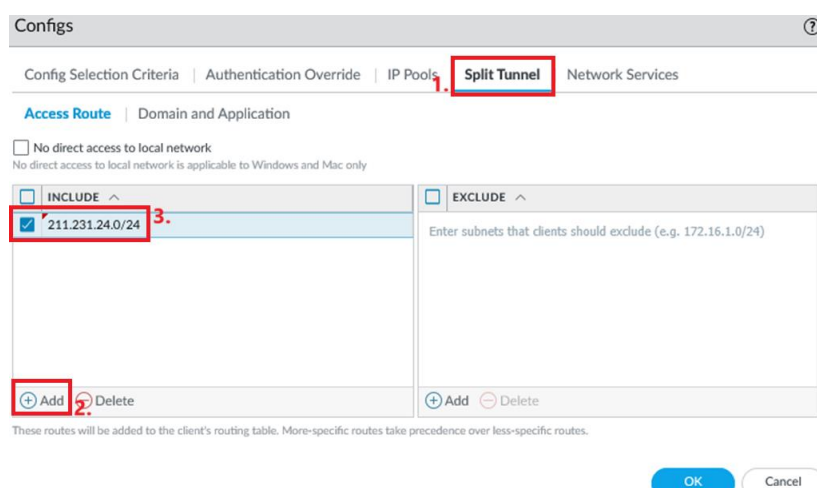


Рисунок 3.31 – Увімкнення доступу до мереж віддалених користувачів

Таким чином, впровадження рішення Palo Alto Networks VPN на базі технологій Palo Alto Networks дозволяє забезпечити високий рівень захисту віддаленого доступу користувачів до корпоративної мережі. Також, поєднання мережевих технологій Palo Alto Networks з комплексними засобами безпеки сприяє підвищенню продуктивності користувачів, забезпечуючи стабільний та безпечний зв'язок незалежно від їхнього місцезнаходження. Це дозволяє компанії ефективно реалізовувати гібридні або повністю віддалені моделі роботи, відповідаючи сучасним вимогам безпеки та гнучкості бізнес-процесів.

3.3 Тестування функціональних можливостей та моніторинг захищеної мережі з віддаленим доступом користувачів

Тестування є завершальним етапом впровадження захищеної мережі, що дозволяє перевірити працездатність налаштувань, надійність мережі та відповідність очікуваним вимогам. Основна мета тестування – виявлення можливих помилок конфігурації, перевірка пропускної здатності мережі, стабільності з'єднання та безпеки обміну даними між віддаленими користувачами та корпоративною мережею.

Для забезпечення тестування функціональності захищеної мережі з віддаленими користувачами використовується програмне забезпечення GlobalProtect від Palo Alto Networks. Перш ніж почати підключення до мережі за допомогою GlobalProtect, необхідно завантажити та встановити програму на кінцевій точці. Це можна зробити лише через портал GlobalProtect організації. На сайті Palo Alto Networks відсутнє пряме посилання для завантаження програми, оскільки кожна організація використовує унікальні налаштування для розгортання GlobalProtect або Prisma Access. Для завантаження програми необхідно отримати від адміністратора IP-адресу або повне доменне ім'я порталу (FQDN).

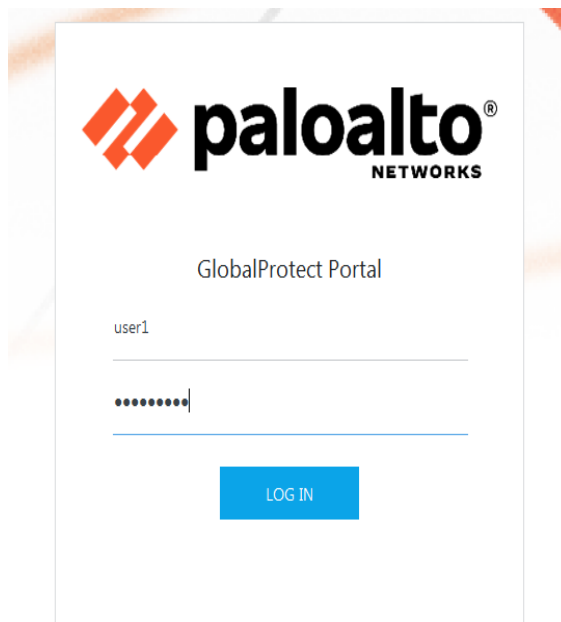


Рисунок 3.32 – Початкова сторінка входу на порталі GlobalProtect

Після успішного входу з'явиться сторінка завантаження, де є можливість отримати останню версію програмного забезпечення.



Рисунок 3.33 – Сторінка завантаження останньої версії GlobalProtect

Після встановлення GlobalProtect потрібно запустити програму, ввести адресу порталу, надану адміністратором і натиснути «Connect». У процесі підключення система може запропонувати додаткову автентифікацію, наприклад, двофакторну.

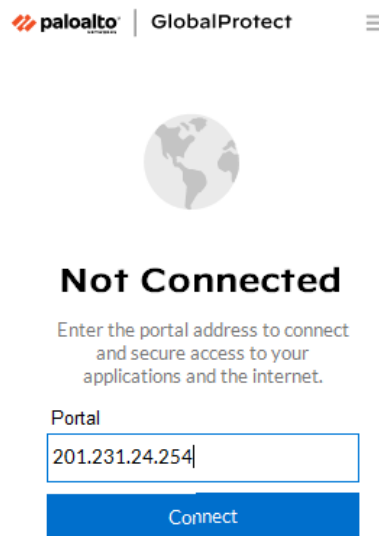


Рисунок 3.34 – Підключення клієнта GlobalProtect

Після успішного входу можна відкрити панель налаштувань GlobalProtect, яка дозволяє користувачам змінювати параметри програми, переглядати портали, шлюзи та статистику підключень. Вкладка «Параметри» надає доступ до функцій, таких як біометрична автентифікація, вибір SSL або IPSec, автоматичний запуск діагностики та керування журналами. Вкладка «Усунення несправностей» дозволяє збирати журнали, налаштовувати рівень журналювання, переглядати

інформацію про мережеву конфігурацію та запускати тести DEM. «Сповіщення» відображають інформацію про дії програми, а вкладка «Інформація про профіль хоста» демонструє дані кінцевої точки для моніторингу безпеки. На вкладці «Про програму» можна переглянути версію програми та оновлення.

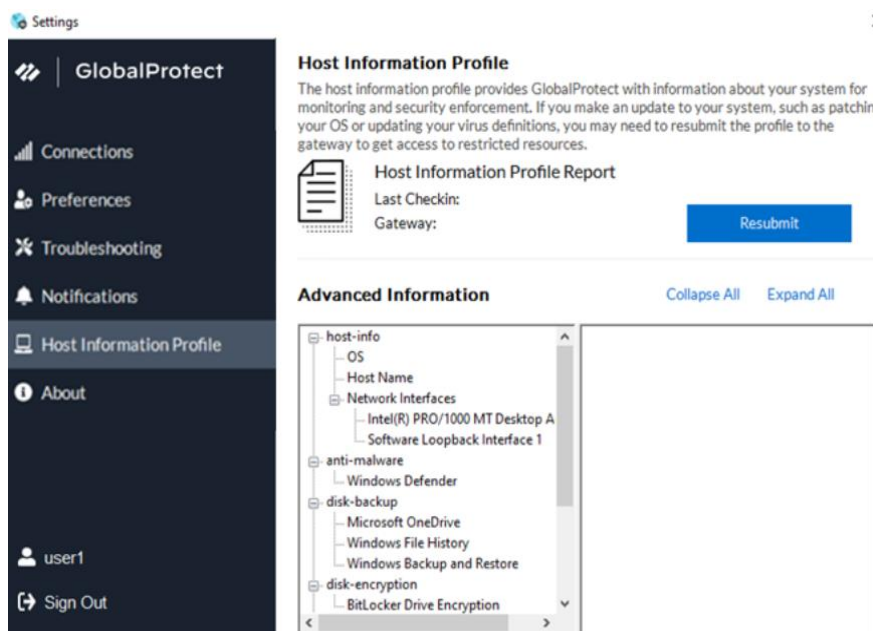


Рисунок 3.35 – Панель налаштувань клієнта GlobalProtect

Після успішної перевірки працездатності підключення клієнта GlobalProtect наступним етапом є моніторинг. Він у контексті NGFW відіграє фундаментальну роль у забезпеченні безпеки мережі. Моніторинг включає аналіз трафіку в реальному часі, деталізоване логування подій, профілювання загроз та виявлення аномалій. Унікальність підходу Palo Alto полягає у здатності аналізувати не лише метадані, але й зміст трафіку, ідентифікувати додатки, користувачів та типи загроз. Завдяки цьому NGFW стає не просто засобом контролю доступу, а повноцінною платформою для активного захисту мережі.

Інформаційна панель дозволяє відображати загальну інформацію про міжмережевий екран, включаючи стан роботи кожного інтерфейсу, версії програмного забезпечення, використання ресурсів та 10 останніх записів у системних журналах, журналах конфігурацій і загроз. Усі доступні віджети відображаються за замовчуванням, однак їх можна додавати або видаляти за необхідністю. Оновлення інформації на панелі може виконуватись вручну за допомогою відповідної іконки або автоматично з інтервалами в 1-5 хвилин.

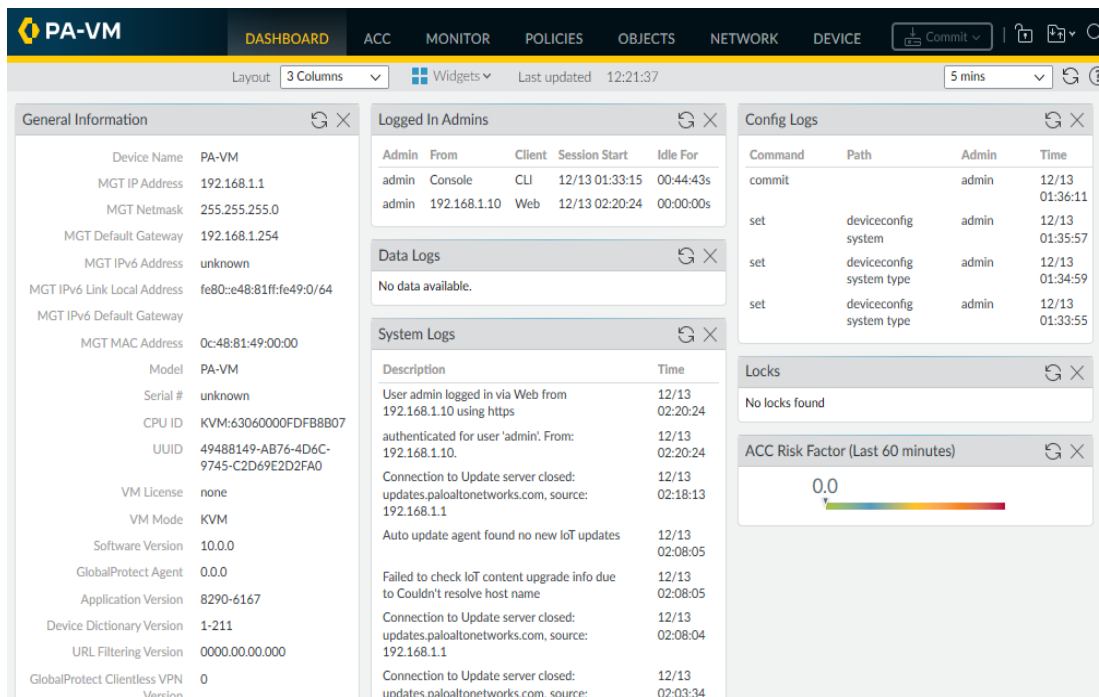


Рисунок 3.35 – Інформаційна панель міжмережного екрана

На інформаційній панелі представлені графіки та журнали, зокрема: найбільш популярні додатки, додатки з високим ризиком, загальна інформація, стан інтерфейсів, журнали загроз, журнали конфігурацій, журнали фільтрації даних, фільтрації URL, системні журнали, ресурси системи, авторизовані адміністратори, коефіцієнт ризику ACC, стан високої доступності та блокування.

Центр команд управління додатками (Application Command Center, ACC) – це інтерактивне графічне представлення користувачів, додатків, загроз, URL-адрес та контенту, що проходить через мережу. ACC використовує журнали міжмережного екрану для аналізу трафіку, забезпечуючи огляд його закономірностей і надаючи можливість отримати дієву інформацію про загрози.

Графічний інтерфейс ACC дозволяє взаємодіяти з даними, одночасно візуалізуючи взаємозв'язки між подіями в мережі. Це сприяє виявленню аномалій та розробці способів покращення правил мережевої безпеки. Для персоналізації вигляду мережі користувачі можуть додавати власні вкладки та віджети з інформацією, яка є найважливішою для їхніх завдань.

ACC включає широкий набір віджетів, які охоплюють мережеву активність, використання додатків, активність користувачів, активність джерел IP-адрес та активність цільових IP-адрес.

Завдяки АСС користувачі можуть використовувати журнали міжмережевого екрану для аналізу мережеских закономірностей. Центр пропонує три попередньо налаштовані вкладки для перегляду мережевого трафіку, активності загроз та заблокованої активності. Кожен графік має інтерактивні віджети, які дозволяють детально аналізувати дані для отримання додаткової інформації.

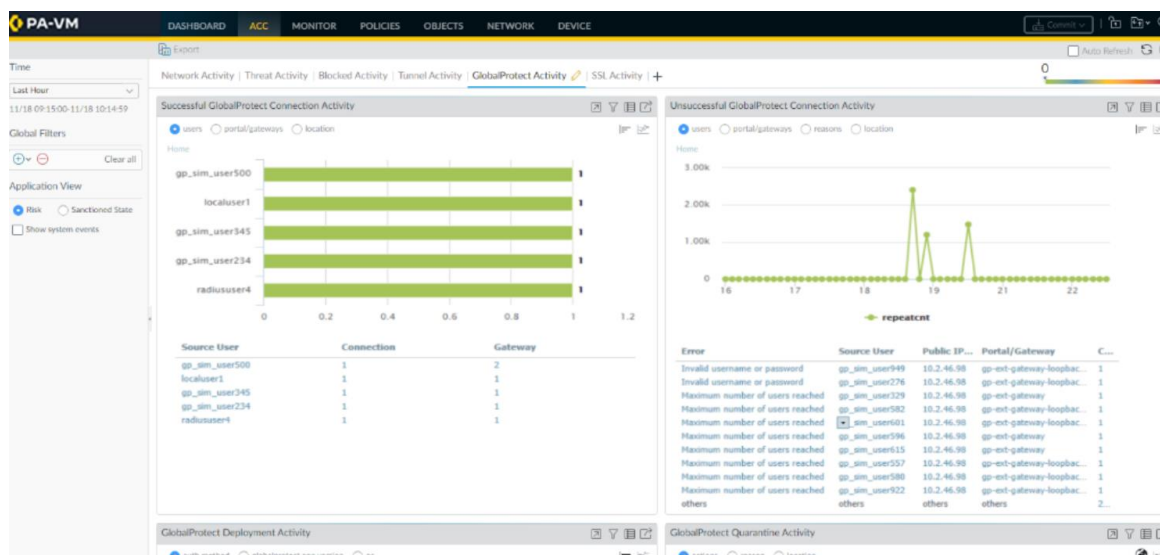


Рисунок 3.36 – Графічний інтерфейс АСС

Вкладка Monitor є центральним інструментом для аналізу всіх аспектів роботи мережі. Вона надає адміністраторам доступ до детальних логів, які відображають трафік, загрози, використання додатків, VPN-з'єднання, URL-фільтрацію та інші аспекти функціонування мережі. Це забезпечує повний огляд стану мережевої безпеки і дозволяє оперативно реагувати на потенційні проблеми.

	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION
	07/25 03:02:42	end	GP-VPN	untrust	192.168.1.1	0300		8.8.8.8
	07/25 03:02:42	end	GP-VPN	untrust	192.168.1.1	0300		8.8.8.8
	07/25 03:02:37	end	GP-VPN	untrust	192.168.1.1	0300		8.8.8.8
	07/25 03:02:17	end	GP-VPN	untrust	192.168.1.1	0300		8.8.8.8
	07/25 03:02:17	end	GP-VPN	untrust	192.168.1.1	0300		8.8.8.8

Рисунок 3.37 – Відображення журналу трафіку

Вкладка «Monitor» містить наступні розділи:

- Traffic;
- Threat;
- URL Filtering;

- WildFire Submissions;
- Data Filtering;
- HIP Match;
- GlobalProtect;
- IP-Tag;
- User-ID;
- Configuration;
- System.

Журнали трафіку відображають усі сесії, що проходять через міжмережевий екран. Адміністратор може побачити джерело, ціль, IP-адреси, зони, а також статус кожної сесії. Ці дані допомагають виявити несанкціоновані сесії, аналізувати рух між різними зонами безпеки та забезпечувати відповідність політикам мережі.

Розділ Threat відображає інформацію про всі загрози, виявлені міжмережевим екраном. Логи містять дані про шкідливі додатки, експлойти, атаки, а також деталі, такі як рівень загрози, ідентифікатор загрози, IP-адреси джерела та призначення.

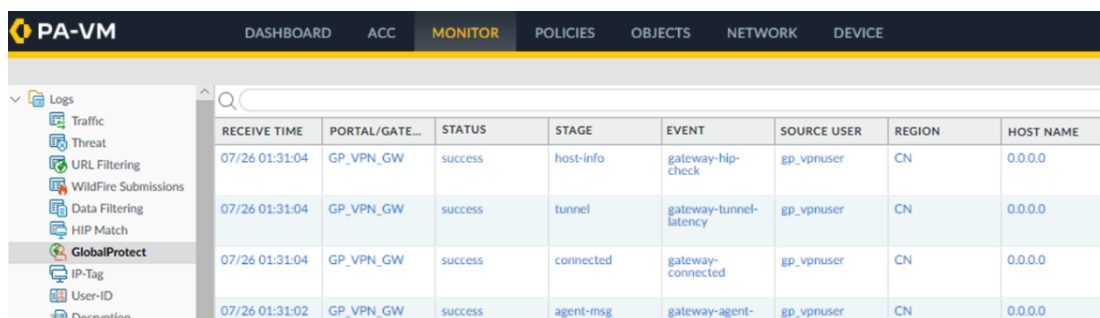
Журнали URL-фільтрації містять інформацію про активність користувачів у веб-просторі. Вони відображають відвідані URL-адреси, категорії веб-сайтів, результат політики та дату події.

У розділі WildFire Submissions відображаються дані про файли та об'єкти, які були відправлені в сервіс WildFire для аналізу на шкідливий код. Логи містять інформацію про джерело, тип об'єкта, результат аналізу та рівень загрози. Це корисно для виявлення та блокування нових і невідомих загроз.

Розділ Data Filtering фіксує всі випадки передачі конфіденційних даних через мережу. Він дозволяє виявляти порушення політик Data Loss Prevention (DLP), наприклад, надсилання файлів, які містять фінансові чи особисті дані.

Цей Розділ HIP Match фіксує відповідність пристроїв вимогам безпеки на основі Host Information Profile (HIP). Журнали включають деталі про перевірку відповідності пристрою, такі як стан операційної системи, наявність антивірусного ПЗ, брандмауерів тощо.

Журнали GlobalProtect містять деталі про всі VPN-з'єднання. Поля включають статус підключення, етапи створення тунелю, події, ім'я користувача та джерело підключення. Цей розділ дозволяє контролювати роботу VPN-з'єднань та вирішувати проблеми з доступом.



RECEIVE TIME	PORTAL/GATE...	STATUS	STAGE	EVENT	SOURCE USER	REGION	HOST NAME
07/26 01:31:04	GP_VPN_GW	success	host-info	gateway-hip-check	gp_vpnuser	CN	0.0.0.0
07/26 01:31:04	GP_VPN_GW	success	tunnel	gateway-tunnel-latency	gp_vpnuser	CN	0.0.0.0
07/26 01:31:04	GP_VPN_GW	success	connected	gateway-connected	gp_vpnuser	CN	0.0.0.0
07/26 01:31:02	GP_VPN_GW	success	agent-msg	gateway-agent-mca	gp_vpnuser	CN	0.0.0.0

Рисунок 3.38 – Відображення журналу GlobalProtect

Розділ IP-Tag призначений для відстеження та управління прив'язками IP-адрес до тегів. Теги дозволяють адміністратору динамічно класифікувати трафік або пристрої, пов'язуючи IP-адреси з певними категоріями для подальшого застосування політик безпеки, маршрутизації чи аналізу трафіку.

Розділ User-ID містить інформацію про користувачів, ідентифікованих у мережі. Логи показують IP-адресу, ім'я користувача та активність у мережі.

Журнали конфігурації записують усі зміни, внесені в систему адміністратором. Вони включають ім'я користувача, час і дату зміни, а також опис внесених змін.

Системні журнали фіксують внутрішні події міжмережевого екрану, такі як помилки, стан роботи системи, перезавантаження та інші події. Вони є ключовими для діагностики технічних проблем і підтримки працездатності пристрою.

Вкладка Monitor є важливим інструментом для адміністраторів, дозволяючи підтримувати прозорість роботи мережі, забезпечувати її безпеку та оперативно реагувати на інциденти.

Висновки до третього розділу

У третьому розділі було детально розглянуто практичну реалізацію захищеної мережі з віддаленими користувачами на базі міжмережного екрану Palo Alto. Процес впровадження включав три основні етапи.

Перший етап охопив базове налаштування міжмережного екрану, включаючи конфігурацію мережевих інтерфейсів, створення зон безпеки, налаштування маршрутизації та NAT. Ці базові налаштування заклали фундамент для подальшого розгортання захищеної мережевої інфраструктури.

Другий етап був присвячений налаштуванню GlobalProtect VPN для забезпечення безпечного віддаленого доступу. Процес включав створення та налаштування сертифікатів, профілів SSL/TLS, конфігурацію автентифікації користувачів, створення тунельного інтерфейсу та налаштування порталу і шлюзу GlobalProtect. Впровадження цього рішення дозволило забезпечити захищений доступ віддалених користувачів до корпоративних ресурсів.

Третій етап охопив тестування функціональності та моніторинг захищеної мережі. Було продемонстровано процес підключення клієнта GlobalProtect та розглянуто потужні інструменти моніторингу Palo Alto, включаючи інформаційну панель, центр управління додатками (ACC) та детальну систему журналювання. Ці інструменти забезпечують повну видимість мережевої активності, дозволяють виявляти загрози та оперативно реагувати на інциденти безпеки.

Таким чином, реалізоване рішення забезпечує високий рівень захисту корпоративної мережі та віддалених користувачів, відповідаючи сучасним вимогам до інформаційної безпеки та надаючи гнучкі можливості для моніторингу та управління мережевою інфраструктурою.

ВИСНОВКИ

У результаті виконання магістерської роботи були досліджені методи та технології організації захищеного віддаленого доступу користувачів на базі рішень компанії Palo Alto Networks. Важливість цих рішень стала очевидною в умовах сучасних викликів у сфері кібербезпеки, зокрема в умовах переходу на віддалену та гібридну форму роботи.

Під час дослідження було виявлено, що використання міжмережевих екранів нового покоління (NGFW) та платформ, таких як GlobalProtect, дозволяє значно підвищити рівень безпеки при віддаленому доступі. Завдяки вбудованим функціям глибокого аналізу трафіку, динамічному управлінню політиками доступу, а також можливостям інтеграції з сучасними системами ідентифікації та багатофакторної автентифікації, ці рішення забезпечують комплексний підхід до захисту корпоративної інфраструктури.

У першому розділі було проаналізовано теоретичні основи та проблеми організації захищеного віддаленого доступу. Особливу увагу приділено питанням безпеки мереж з віддаленими користувачами, зокрема найбільш актуальним загрозам, таким як фішинг, зловживання вразливостями програмного забезпечення та атаки на системи автентифікації.

Розгляд сучасних рішень компанії Palo Alto Networks показав, що їх технології надають ефективні інструменти для захисту від зовнішніх та внутрішніх загроз, завдяки багаторівневому підходу та інтеграції різних сучасних механізмів безпеки.

Другий розділ роботи був присвячений проектуванню захищеної мережі для віддалених користувачів. Було детально розглянуто вибір мережевого обладнання та програмного забезпечення для організації захищеного віддаленого доступу. Рішення, що базуються на міжмережевих екранах Palo Alto Networks серії PA-5400, були вибрані для забезпечення високої продуктивності та масштабованості мережі. Завдяки використанню платформи GlobalProtect, було реалізовано рішення для захищеного доступу через VPN, що підтримує сучасні стандарти безпеки і відповідає вимогам корпоративних клієнтів.

У третьому розділі було описано практичну реалізацію проекту на базі міжмережного екрану Palo Alto. Процес налаштування включав конфігурацію мережевих інтерфейсів, створення зон безпеки та налаштування VPN з використанням GlobalProtect. Тестування функціональності та моніторинг захищеної мережі продемонстрували високу ефективність реалізованого рішення, що включає інструменти моніторингу та детальну систему журналювання для виявлення загроз та швидкої реакції на інциденти.

Загалом, проведені дослідження та реалізація системи захищеного віддаленого доступу на базі рішень Palo Alto Networks показали високий рівень надійності та ефективності запропонованого підходу.

Впровадження таких рішень дозволяє організаціям забезпечити захист своїх корпоративних мереж і ресурсів, мінімізуючи ризики безпеки. Подальші напрямки дослідження можуть бути спрямовані на вдосконалення існуючих технологій, інтеграцію нових інструментів для виявлення аномалій та автоматизацію процесів безпеки з використанням штучного інтелекту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is Remote Access?. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-remote-access>
2. Advantages and Disadvantages of Remote Access Service - Abacus. Abacus. URL: <https://goabacus.com/advantages-and-disadvantages-of-remote-access-service/>
3. Secure Remote Access | Protect Remote Employees from Cyberthreats. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/secure-remote-access-understand-how-to-protect-remote-employees>
4. Five Remote Access Security Risks And How To Protect Against Them. Palo Alto Networks Blog. URL: <https://www.paloaltonetworks.com/blog/2020/04/cortex-remote-access-security-risks/>
5. Gale G. Remote work the new normal. Independently Published, 2020. 175 с.
6. Kirvan P., Contributor T. What Is Remote Access? | Definition from TechTarget. Search Security. URL: <https://www.techtarget.com/searchsecurity/definition/remote-access>
7. Oteir N. Альтернативи VPN для віддаленого доступу. INTROSERV. URL: <https://introserv.com/ua/blog/alternativi-vpn-dlya-viddalenogo-dostupu/>
8. Miller L. C. Next-Generation Firewalls for Dummies, 2nd Palo Alto Special Edition (Custom). Wiley & Sons, Incorporated, John, 2019. 80 с.
9. Tom Piens. Securing Remote Access in Palo Alto Networks: Practical Techniques to Enable and Protect Remote Users, Improve Your Security Posture, and Troubleshoot Next-Generation Firewalls. Packt Publishing, 2021. 336 с.
10. Blokdyk G. Remote Desktop Software a Complete Guide - 2020 Edition. Emereo Pty Limited, 2020. 308 с.
11. What Is Zero Trust Network Access (ZTNA). Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna>
12. What is Zero Trust Network Access (ZTNA) 2.0. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-2-0>
13. What Is SASE?. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-sase>

14. PaloGuard - Enterprise Security Platforms. Palo Alto Networks Products & Solutions | PaloGuard.com. URL: <https://www.paloguard.com/GlobalProtect.asp>
15. Palo Alto GlobalProtect Cloud Service - Protecting the Extended Perimeter - Laketec. Laketec. URL: <https://www.laketec.com/resource/palo-alto-globalprotect-cloud-service-2>
16. Palo Alto GlobalProtect » Network Interview. Network Interview. URL: <https://networkinterview.com/palo-alto-globalprotect>
17. Secure Remote Access | GlobalProtect - Palo Alto Networks. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/sase/globalprotect>
18. PaloGuard - Enterprise Security Platforms. Palo Alto Networks Products & Solutions | PaloGuard.com. URL: <https://www.paloguard.com/Firewall-PA-5410.asp>
19. PA-5400 Series Next-Gen Firewall Hardware Reference. Santa Clara : Palo Alto Networks, 2024. 128 с.
20. Cisco 4000 Series Integrated Services Routers. Cisco. URL: <https://www.cisco.com/site/us/en/products/networking/sdwan-routers/4000-series-integrated-services-routers/index.html>
21. Products - Cisco Catalyst 9000 At-a-Glance. Cisco. URL: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/nb-06-cat-9k-aag-cte-en.html>
22. Рудюк Б. М., Єфіменко А. А. Забезпечення мобільності та віддаленого доступу користувачів з використанням рішень palo alto global protect. Тези доповідей XIV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2024», 28-29 березня 2024 р. Житомир: Житомирська політехніка, 2024. с.65-68
23. Рудюк Б. М., Єфіменко А. А. Порівняльний аналіз ZTNA та ZTNA 2.0. Тези доповідей XIV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2024», 28-29 березня 2024 р. Житомир: Житомирська політехніка, 2024. с.69-70
24. Рудюк Б. М., Єфіменко А. А. Способи захисту даних в умовах віддаленої та гібридної роботи. Тези доповідей VII Всеукраїнської науково-технічної

конференції «Комп'ютерні технології: інновації, проблеми, рішення – 2024», 02-03 грудня 2024 р. Житомир: Житомирська політехніка, 2024.

25. A Guide to Remote Access Security for SMEs. NetBird - Connect and Secure Your IT Infrastructure in Minutes. URL: <https://netbird.io/knowledge-hub/remote-access-security-for-sme>

26. Piens T. Mastering Palo Alto Networks: Deploy and manage industry-leading PAN-OS 10.x solutions to secure your users and infrastructure. Packt Publishing, 2020. 514 p.

27. Agarwal K. GlobalProtect, FortiClient, AnyConnect, etc. hand-in-hand with dope.security. The Fly-Direct Secure Web Gateway. URL: <https://dope.security/post/globalprotect-forticlient-anyconnect-etc-hand-in-hand-with-dope-security>

28. Top Palo Alto Networks Firewall Interview Questions - 2023. GNS3 Network. URL: <https://www.gns3network.com/palo-alto-networks-firewall-interview-questions-and-answers/>

29. GlobalProtect. Palo Alto Networks | TechDocs Home. URL: <https://docs.paloaltonetworks.com/globalprotect>

30. Monitoring. Palo Alto Networks | TechDocs Home. URL: <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring>

31. Monitoring Your Palo Alto Networks VM-Series Firewall with a Syslog Sidecar | Amazon Web Services. Amazon Web Services. URL: <https://aws.amazon.com/blogs/apn/monitoring-your-palo-alto-networks-vm-series-firewall-with-a-syslog-sidecar>

32. 5 Ways to Monitor Activity on Palo Alto Firewalls. CBT Nuggets. URL: <https://www.cbtnuggets.com/blog/certifications/security/5-ways-to-monitor-activity-on-palo-alto-firewalls>

33. GlobalProtect - захист віддалених користувачів | Palo Alto Networks. ESKA. URL: <https://eska.global/products/palo-alto-networks-globalprotect>

ДОДАТКИ

Топологія мережі для модельного прикладу

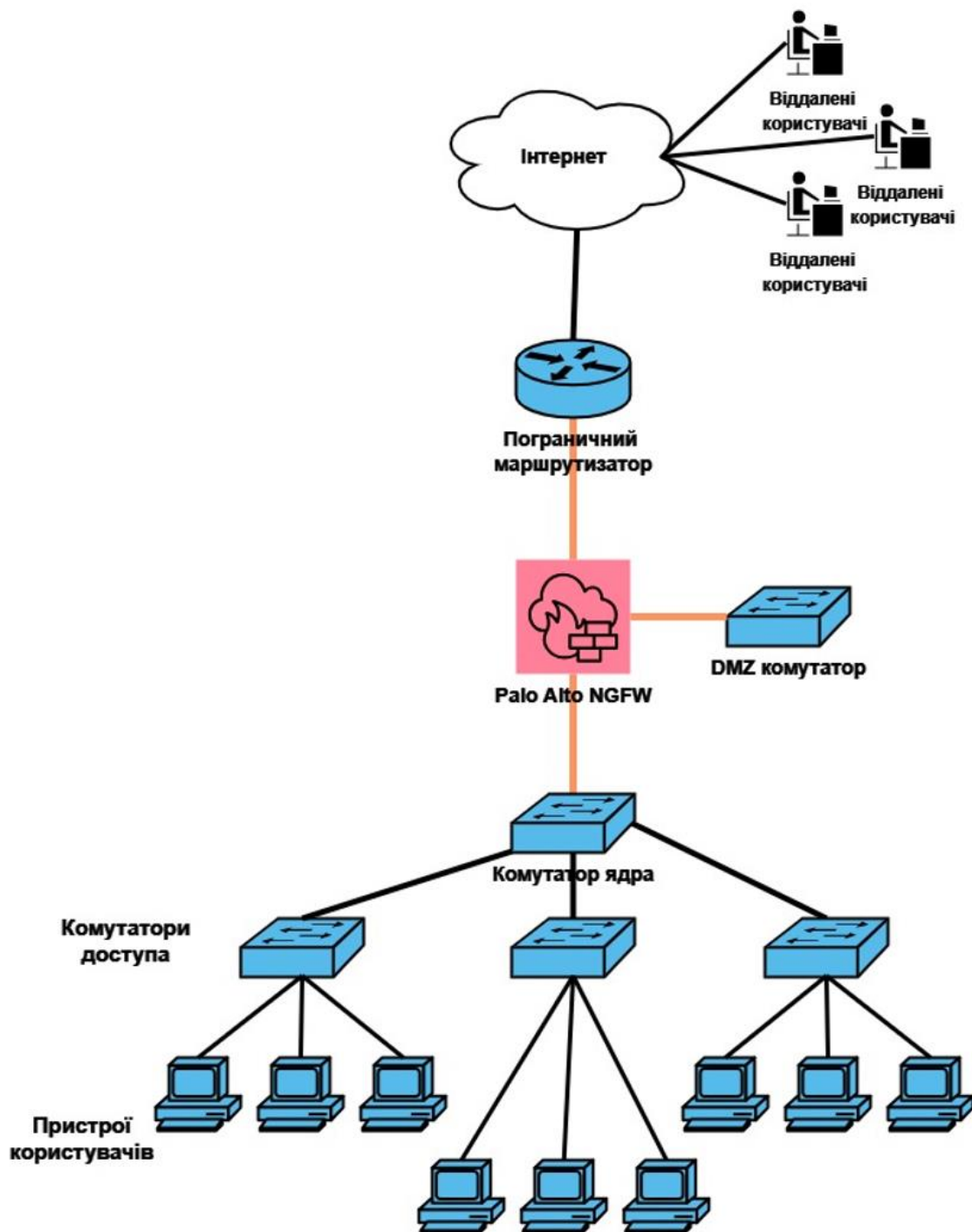


Рисунок А.1 – Топологія мережі для модельного прикладу

Лістинг конфігураційного файлу міжмережного екрану для модельного прикладу

```

admin@PA-VM-Rudiuk> show config running

config {
  mgt-config {
    users {
      admin {
        phash $1$xebkxjyy$zzJ/rIvfQ0rvv9/f7xpP60;
        permissions {
          role-based {
            superuser yes;
          }
        }
      }
    }
  }
  password-complexity {
    enabled yes;
    minimum-length 8;
  }
}
shared {
  application;
  application-group;
  service;
  service-group;
  botnet {
    configuration {
      http {
        dynamic-dns {
          enabled yes;
          threshold 5;
        }
        malware-sites {
          enabled yes;
          threshold 5;
        }
        recent-domains {
          enabled yes;
          threshold 5;
        }
        ip-domains {
          enabled yes;
          threshold 10;
        }
        executables-from-unknown-sites {
          enabled yes;
          threshold 5;
        }
      }
    }
  }
  other-applications {
    irc yes;
  }
}
}
unknown-applications {
  unknown-tcp {
    destinations-per-hour 10;
    sessions-per-hour 10;
    session-length {
      maximum-bytes 100;
      minimum-bytes 50;
    }
  }
  unknown-udp {
    destinations-per-hour 10;
    sessions-per-hour 10;
    session-length {
      maximum-bytes 100;
      minimum-bytes 50;
    }
  }
}
report {
  topn 100;
  scheduled yes;
}
certificate {
  GP_cert {
    subject-hash 5a7cec6f;
    issuer-hash 5a7cec6f;
    not-valid-before "Dec 13 12:24:19 2024 GMT";
    issuer /CN=201.231.24.254;
    not-valid-after "Dec 13 12:24:19 2025 GMT";
    common-name 201.231.24.254;
    expiry-epoch 1765628659;
    ca yes;
    subject /CN=201.231.24.254;
    public-key "-----BEGIN CERTIFICATE-----
MIIC8zCCAdugAwIBAgIJAJtYDicIvU7jMA0GC
SqGSIb3DQEBCwUAMBkxFzAVBgNV
BAMTDjIwMS4yMzEuMjQuMjU0MB4XDTI0M
TIxMzEyMjQxOVVoXDTI1MTIxMzEyMjQx
OVowGTEXMBUGA1UEAxMOMjU0MjU0MjU0
NC4yNTQwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQDhM7NE+B6HQcSot1
s30SIXZcbHt1CXOO14QLaqRB7VAza5
sOi+42+D/J3wjB6MTmE1YvOK74lChllCfL9gE5
EsxwDuUIZOxgrI+JJ8gJdRtDdQ
TUsRrICSh8tM/g0oGmZao46jdPL5UbIYxtczyKP
OFISL7HS0eDzqd112NuwsSYXN
-----"
  }
}

```

7M0D4vuRk1BbOALZtz42Ghzl785ADSKZ78+8Z
 ThoEdtXIP4EAnrrSHWRzRgRpX3a
 I24rEN9wwtOvnJEJELuUjyStQja1uOgBGK5G0d
 8pyiNCV4sRqvVld2WFr3J5ipxV
 juNorgRuwVpUYQtlmT4eV5BHA2UDz53j6kOSp
 WCdAgMBAAGjPjA8MAwGA1UdEwQF
 MAMBAf8wCwYDVR0PBAQDAgIEMB8GA1U
 dEQQYMBaCDjIwMS4yMzEuMjQuMjU0hwTJ
 5xj+MA0GCSqGSIB3DQEBBCwUAA4IBAQB++Z
 bR+Dwv/By0G7bKf/YCbCUavWvUczaj
 RQMoIslUKMw45qJRF+uBheG3MyhJDQSiHlKP
 UAXWxwUI/tC9cuNa78/wQIHehWXv
 aGlRf8gEbsdBYnt6Cizf1PBqjl7vWACsAGu4LPoc
 XJOpjNbkvSnMN1E2ROGrBvmB
 xRXvsBb084XUnNHE+i1pCfM2V4GmKxBbeid9j
 wmQRCamjGyGX+BL0EwOO3w2577r
 E5BgCZ/GRfcj02cbeBTefOZ8WTVsYJbVi5t1+/P
 dY5VW2TEPDnGb0aQr31w5MVx
 IzU8z5sOj2uLk9uqwqc5dd8SeMMNniiemtH6qLzs
 sjfHD8RkikEQ
 -----END CERTIFICATE-----

";

algorithm RSA;

private-key

AQ==Z+cl5AhyT/Xj9Q3Mk/EVnH5qk7I=wfl5Zc
 +wUAak+B7CnAVY6NdutYWtt67XvF+yGHFGS
 +uStOxD5MLQytEGaNevSeA2galb1SrO2a4MRto
 gN3e5quMQkxb0k3m2FqL5yKa6MQz/unoahRghJ
 rhSSHCKAyinobpP5fS7yVWVrSJfPYzM/uF4oq3
 aRQoaqaOsy/dngZrv5Ug05gGhSnzsM1Fj30Hjxju
 AYcG5YeciKk+R49x/18bDllo5X/6A0ms1YvApen
 sYGlXeRaw0/IWaHPiI+ENB1l7remfNvZiIgzlPm0
 SzwGE54Lo8VrERnJIJ/vX9UbOpR4Ni0pHzbN/H
 7M9GdaVggbt5CvnF0yj6l9YCM2hJCqTn7H7F+
 WedBkOzuSeozE/ZHOM9WFDbsBmn/GkchUqK
 sL6f8O9sRRdZrF5XdW5VG5tbdH7ejAOkwMFqY
 6i3l5B/zys9am6IEzjcEclbmP5Hv9dcXxYljhPJ2ho
 8o71gZFro1g2jOeCOU7hBW9C4MKUQMguWqe
 eQ3o+mCHEuWtUWE/UgN0dofmX4hCz8gr4RHq
 S/q/i/nhx7QKl3uUpVS0WRQlHYk3idqRp7h1Qtcs
 Bv0/qpC8kMPnZYsmmhUWchGIqLc3mIIOpGJO
 DOzl+rc3IEMQxIDItsaeV/MkRyU6rL+ZgOuQFc
 MhoK0m5qISglS/bVHu0jq1bahyhw2Xp7uM9Pb53
 VHIWYbGS/YDjsrBsVX3QtMagTjVgN8tuXa/jnp
 mCzuISUVmTAVVj+yEN7E4FOKfltlYHa0aaV1k
 nrN0XrZ2iNhCeHU6unfNvhSp426//kMxeSLu6uK
 VwC1PdrQv5IlhHq2u+8EdVxs3TCXVKzty1koRH
 0q3c7eBwliC2WHF4wk0F7M4zlbKZOcbSkq6Q6f
 0bokYRn2qEFv0fnDxY2vVY3p18zOODJi4L1ntP
 u0cCHtWduxZH7+pMZPFdyMih6z49VojwHIBU
 cYmt3rkxeSa65nvdPbRls5XslT8AyWnD0dgK09G
 jxjNLnm2J619Xv+xmK7P8Uh4xitBj0RcaGOebK
 G54z/J4GbrSTeGiZuu92UOkemHmXnZi8CRS+zS
 R8dGR5qOXGp/frEbnIIPnYAYncbh5UeADINox
 W+KHqiq490+2oGVUvZ+LTCR387tiCTKtSY4na
 ku43L21P5/vUaqIXMOFJT9PNKjRkkfgMFQApG+
 G+QgRU7VMHk5NNQHk9B2V6jltGebarzGopTl
 Wn6oUjZlezEZRjtXknjIPBlFFe64Ar5S69q0JN3aI

9fP8FY4Y1/IHLbkmcUqp2EVl3QIJegZYDZJNNg
 Tr1oyl6JSgNdm8JeB3oCyO2qQ6UVEjcx1k8KT
 6oAyhPEtWvsGvK/ryOwCptc9CaZ9wiPmmUKJN
 EJqizpjL/6zZ4D1KwjrgRKB3NM8Xy6luOTHTo7
 5cFaMXeAAvE0LDyYknVf6oBYf9V/EWkFE/d5f
 lY7wg4xxLVBttrkwKNeHrwuAGmOT9nAK5oA
 RTkWC+HJX5tMgRqWbCZHy5FUj3l+89u2HlhlL
 Pa0LP5d2JQcjHMAXwAQN9vRHtwGSyWgdv5A
 epQI+3afzwi8dL08s2kZlhelYtd+d9PU2Rf7aQves
 BDRf8ML07AE+B1I3FQuP/GcHnL0WErCf0E/oj
 q1zgcen/eTj0EFTok8knWyYz4Hm5Cnz1tB37iuiH5
 SSA/W3SCC+irAzw+q3rU3VF5rV2Q4YjubpXk5j
 zhv6byxCZtBMiuknVYkDdWkoS7RYJMnA4a2kI
 RIK07Yu2W3F92KaJBuTRq6rZz5K4H3HLAUC9
 mcUFDV0eoRHUvUNP98KYdbOh+oqVSH/Wlcp
 7mrCabEhcUvMYqTYs427Zgj1N6+703vyBphe2
 5ADDlNYHttMT9wXcrKKzTAVMN3HFVjCnEZ
 kfes4ShvVK6GfIWqjUX7tCVBNOgMY+BvXvly
 D3NwmUW2lkeE7g4luCWUYAmDiLl5Dcc5lfK9
 yEmGLEcEEH2DeHN81PbgGrOle48hjfMlZnDdlb
 Qw2qzyjkhbWiIHqorJASftmIQtoCqY+7MKikZbk
 pKdZ2uZQOXtoJ/wk+dFD9r+XUAJ0dolYXCoy
 G2WuUU9lXehpzn7UE0Fqho3Bi04AcZRZyZkV
 ByfmwuU3nWKCIY/WrZVo9WNzXVGDl0vfMN
 fiWVxsDRz5KgKd3QKDJ6l6jby3K0aQRcRFY
 XxLSf/I6hU5Efg5Nz9cb4KOAOZDRrWwa08KGk
 mSn4SnwYO2QY0TnHVN2DvWe;

}

}

```
ssl-decrypt {
    trusted-root-CA GP_cert;
}
```

```
ssl-tls-service-profile {
    GP_SSL_TLS_Profile {
        protocol-settings {
            min-version tls1-0;
            max-version max;
        }
        certificate GP_cert;
    }
}
```

```
local-user-database {
```

```
    user {
```

```
        user1 {
```

```
            phash
```

```
$1$svgxheos$UZWqU8DGMN4EUljJEQMu4/;
```

```
        }
```

```
        user2 {
```

```
            phash
```

```
$1$suspmdfvq$cLLfDZ0PQVYxWPcT6DVh3.;
```

```
        }
```

```
        user3 {
```

```
            phash
```

```
$1$nnosrin$Nbg5bABAYC9IoY1.7FihF.;
```

```
        }
```

```
    }
```

```
authentication-profile {
```

```

Auth_Profile {
  multi-factor-auth {
    mfa-enable no;
  }
  method {
    local-database;
  }
  allow-list all;
}
log-settings {
  system {
    match-list {
      all1 {
        filter "All Logs";
      }
    }
  }
  config {
    match-list {
      all2 {
        filter "All Logs";
      }
    }
  }
  userid {
    match-list {
      all3 {
        filter "All Logs";
      }
    }
  }
  hipmatch {
    match-list {
      all4 {
        filter "All Logs";
      }
    }
  }
  globalprotect {
    match-list {
      all5 {
        filter "All Logs";
      }
    }
  }
  iptag {
    match-list {
      all6 {
        filter "All Logs";
      }
    }
  }
}
devices {
  localhost.localdomain {
    network {

```

```

interface {
  ethernet {
    ethernet1/1 {
      layer3 {
        ndp-proxy {
          enabled no;
        }
      }
      ip {
        201.231.24.254/24;
      }
      lldp {
        enable no;
      }
      interface-management-profile    PING-
ONLY;
    }
    comment "***Outside Networks***";
  }
  ethernet1/2 {
    layer3 {
      ndp-proxy {
        enabled no;
      }
      ip {
        211.231.24.254/24;
      }
      lldp {
        enable no;
      }
      interface-management-profile    PING-
ONLY;
    }
    comment "***Inside Networks***";
  }
  tunnel {
    units {
      tunnel.1 {
        comment "for GP";
      }
    }
  }
}
profiles {
  monitor-profile {
    default {
      interval 3;
      threshold 5;
      action wait-recover;
    }
  }
  interface-management-profile {
    PING-ONLY {
      ping yes;
    }
  }
}
ike {

```

```

crypto-profiles {
  ike-crypto-profiles {
    default {
      encryption [ aes-128-cbc 3des];
      hash sha1;
      dh-group group2;
      lifetime {
        hours 8;
      }
    }
  }
  Suite-B-GCM-128 {
    encryption aes-128-cbc;
    hash sha256;
    dh-group group19;
    lifetime {
      hours 8;
    }
  }
  Suite-B-GCM-256 {
    encryption aes-256-cbc;
    hash sha384;
    dh-group group20;
    lifetime {
      hours 8;
    }
  }
}
ipsec-crypto-profiles {
  default {
    esp {
      encryption [ aes-128-cbc 3des];
      authentication sha1;
    }
    dh-group group2;
    lifetime {
      hours 1;
    }
  }
  Suite-B-GCM-128 {
    esp {
      encryption aes-128-gcm;
      authentication none;
    }
    dh-group group19;
    lifetime {
      hours 1;
    }
  }
  Suite-B-GCM-256 {
    esp {
      encryption aes-256-gcm;
      authentication none;
    }
    dh-group group20;
    lifetime {
      hours 1;
    }
  }
}
}

global-protect-app-crypto-profiles {
  default {
    encryption aes-128-cbc;
    authentication sha1;
  }
}

qos {
  profile {
    default {
      class-bandwidth-type {
        mbps {
          class {
            class1 {
              priority real-time;
            }
            class2 {
              priority high;
            }
            class3 {
              priority high;
            }
            class4 {
              priority medium;
            }
            class5 {
              priority medium;
            }
            class6 {
              priority low;
            }
            class7 {
              priority low;
            }
            class8 {
              priority low;
            }
          }
        }
      }
    }
  }
}

virtual-router {
  default {
    protocol {
      bgp {
        enable no;
        dampening-profile {
          default {
            cutoff 1.25;
            reuse 0.5;
            max-hold-time 900;
            decay-half-life-reachable 300;
            decay-half-life-unreachable 900;
            enable yes;
          }
        }
      }
    }
  }
}

```

```

}
}
routing-options {
    graceful-restart {
        enable yes;
    }
}
}
rip {
    enable no;
}
ospf {
    enable no;
}
ospfv3 {
    enable no;
}
}
interface [ ethernet1/1 ethernet1/2 tunnel.1];
ecmp {
    algorithm {
        ip-modulo;
    }
}
routing-table {
    ip {
        static-route {
            Default-Route {
                path-monitor {
                    enable no;
                    failure-condition any;
                    hold-time 2;
                }
                nexthop {
                    ip-address 201.231.24.2;
                }
                bfd {
                    profile None;
                }
            }
            interface ethernet1/1;
            metric 10;
            destination 0.0.0.0/0;
            route-table {
                unicast;
            }
        }
    }
}
}
}
}
tunnel {
    global-protect-gateway {
        GP_GateWay-N {
            local-address {
                ip {
                    ipv4 201.231.24.254/24;
                }
            }
        }
    }
}

```

```

management {
    hostname-type-in-syslog FQDN;
}
}
auto-mac-detect yes;
}
}
vsys {
    vsys1 {
        application;
        application-group;
        zone {
            INSIDE {
                network {
                    layer3 ethernet1/2;
                }
            }
            OUTSIDE {
                network {
                    layer3 ethernet1/1;
                }
            }
            VPN {
                network {
                    layer3 tunnel.1;
                    enable-packet-buffer-protection no;
                }
                enable-user-identification yes;
            }
        }
        service;
        service-group;
        schedule;
        rulebase {
            nat {
                rules {
                    NAT          3935a797-a375-421f-8db7-
586270fce82b {
                        source-translation {
                            dynamic-ip-and-port {
                                interface-address {
                                    ip 201.231.24.254/24;
                                    interface ethernet1/1;
                                }
                            }
                        }
                        to OUTSIDE;
                        from INSIDE;
                        source nat-211.231.24.0;
                        destination any;
                        service any;
                    }
                }
            }
            security {
                rules {
                    DENY-ALL    1f24941c-d16c-441a-8d9c-
2de743e18035 {
                        to any;
                        from any;
                        source any;
                        destination any;
                        source-user any;
                        category any;
                        application any;
                        service application-default;
                        source-hip any;
                        destination-hip any;
                        action allow;
                    }
                }
            }
            import {
                network {
                    interface [ ethernet1/1 ethernet1/2 tunnel.1];
                }
            }
            address {
                nat {
                    ip-netmask 211.231.24.0;
                }
                nat-211.231.24.0 {
                    ip-netmask 211.231.24.0/24;
                }
            }
            global-protect {
                global-protect-portal {
                    GP_Portal {
                        portal-config {
                            local-address {
                                ip {
                                    ipv4 201.231.24.254/24;
                                }
                            }
                            interface ethernet1/1;
                        }
                        client-auth {
                            GP_Client_Auth {
                                user-credential-or-client-cert-required
no;
                                os Any;
                                authentication-profile Auth_Profile;
                                authentication-message "Enter login
credentials";
                                auto-retrieve-passcode no;
                                username-label Username;
                                password-label Password;
                            }
                        }
                        log-success yes;
                        custom-login-page factory-default;
                        custom-home-page factory-default;
                        ssl-tls-service-profile
GP_SSL_TLS_Profile;
                    }
                    client-config {
                        configs {

```

```

Client_Auth {
  hip-collection {
    max-wait-time 20;
    collect-hip-data yes;
  }
  gateways {
    external {
      list {
        External_GateWay {
          ip {
            ipv4 201.231.24.254;
          }
          priority-rule {
            Any {
              priority 1;
            }
          }
          manual no;
        }
      }
      cutoff-time 5;
    }
  }
  authentication-override {
    generate-cookie no;
  }
  source-user any;
  os any;
  agent-ui {
    max-agent-user-overrides 0;
    agent-user-override-timeout 0;
  }
  gp-app-config {
    config {
      connect-method {
        value user-logon;
      }
      refresh-config-interval {
        value 24;
      }
      agent-user-override {
        value allowed;
      }
      uninstall {
        value allowed;
      }
      client-upgrade {
        value prompt;
      }
      enable-signout {
        value yes;
      }
      use-sso {
        value yes;
      }
      use-sso-macos {
        value no;
      }
    }
  }
  logout-remove-sso {
    value yes;
  }
  krb-auth-fail-fallback {
    value yes;
  }
  default-browser {
    value no;
  }
  retry-tunnel {
    value 30;
  }
  retry-timeout {
    value 5;
  }
  enforce-globalprotect {
    value no;
  }
  captive-portal-exception-timeout {
    value 0;
  }
  traffic-blocking-notification-delay {
    value 15;
  }
  display-traffic-blocking-
notification-msg {
    value yes;
  }
  traffic-blocking-notification-msg {
    value "<div style='font-
family:Helvetica Neue';"><h1
style='color:red;text-align:center; margin: 0; font-
size: 30px;'>Notice</h1><p style='margin: 0;font-
size: 15px; line-height: 1.2em;'>To access the
network, you must first connect to
GlobalProtect.</p></div>";
  }
  allow-traffic-blocking-notification-
dismissal {
    value yes;
  }
  display-captive-portal-detection-
msg {
    value no;
  }
  captive-portal-detection-msg {
    value "<div style='font-
family:Helvetica Neue';"><h1
style='color:red;text-align:center; margin: 0; font-
size: 30px;'>Captive Portal Detected</h1><p
style='margin: 0; font-size: 15px; line-height:
1.2em;'>GlobalProtect has temporarily permitted
network access for you to connect to the Internet.
Follow instructions from your internet
provider.</p><p style='margin: 0; font-size: 15px;
line-height: 1.2em;'>If you let the connection time
out, open GlobalProtect and click Connect to try
again.</p></div>";
  }

```

	<pre> } captive-portal-notification-delay { value 5; } certificate-store-lookup { value user-and-machine; } scep-certificate-renewal-period { value 7; } retain-connection-smartcard- removal { value yes; } enable-advanced-view { value yes; } enable-do-not-display-this- welcome-page-again { value yes; } rediscover-network { value yes; } resubmit-host-info { value yes; } can-change-portal { value yes; } can-continue-if-portal-cert-invalid { value yes; } show-agent-icon { value yes; } user-switch-tunnel-rename-timeout { value 0; } pre-logon-tunnel-rename-timeout { value -1; } preserve-tunnel-upon-user-logoff- timeout { value 0; } ipsec-failover-ssl { value 0; } ssl-only-selection { value 0; } max-internal-gateway-connection- attempts { value 0; } portal-timeout { </pre>	<pre> value 5; } connect-timeout { value 5; } receive-timeout { value 30; } split-tunnel-option { value network-traffic; } enforce-dns { value yes; } append-local-search-domain { value no; } flush-dns { value no; } proxy-multiple-autodetect { value no; } use-proxy { value yes; } wsc-autodetect { value yes; } mfa-enabled { value no; } mfa-listening-port { value 4501; } mfa-notification-msg { value "You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at"; } mfa-prompt-suppress-time { value 0; } ipv6-preferred { value yes; } log-gateway { value no; } quarantine-add-message { value "Access to the network from this device has been restricted as per your organization's security policy. Please contact your IT Administrator."; } quarantine-remove-message { </pre>
--	--	--

