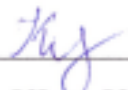


Міністерство освіти і науки України  
Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки

## ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра на тему:  
«Проект корпоративної мережі організації на основі  
IPSec VPN та міжмережного екрану Palo Alto Networks»

Виконав студент 4-го курсу групи КІ-19-1  
спеціальності 123 «Комп'ютерна інженерія»

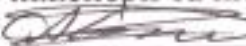
 Ілля Ковальчук  
Керівник доцент кафедри КІ та КБ, к.пед.н.

 Олена Головня  
Рецензент проф. кафедри КІ та КБ, д.т.н., доцент

 Володимир Воротніков

Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки  
Спеціальність 123 «Комп'ютерна інженерія»  
Освітня програма «Комп'ютерна інженерія»

### ЗАТВЕРДЖУЮ

Завідувач  
кафедри комп'ютерної  
інженерії та кібербезпеки  
 А.А. Єфіменко  
"1" березня 2023 року

## ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Ковальчук Ілля Володимирович

Тема проекту: Проект корпоративної мережі організації на основі IPSec VPN та міжмережного екрану Palo Alto Networks .

затверджена Наказом університету від 1 березня 2023 р. № 98/с

Термін здачі студентом закінченої роботи 21 червня 2023 р.

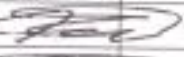
Вихідні дані до роботи (зазначається предмет і об'єкт дослідження):

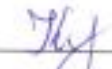
Об'єктом дослідження є процес побудови проекту корпоративної мережі організації з використанням міжмережевого екранування. Предметом дослідження є технології IPSec VPN та міжмережні екрани Palo Alto Networks для створення безпечної корпоративної мережі організації.

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 7200;
2. Комутатор Cisco 2960 та Cisco 3650;
3. Palo alto VM-8.0.0 та Palo alto VM-10.1.0;
4. Операційні системи Kali Linux, Windows XP, 7 та 10;
5. Windows Server 2019;
6. Мережевий емулятор GNS3(v.2.2.36).

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

| Розділ | Консультант   | Підпис, дата                                                                                  |                                                                                                |
|--------|---------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
|        |               | завдання видав                                                                                | завдання прийняв                                                                               |
| 1      | Єфіменко А.А. | 05.03.2023  | 05.03.2023  |
| 2      | Єфіменко А.А. | 17.04.2023  | 17.04.2023  |
| 3      | Єфіменко А.А. | 25.05.2023  | 25.05.2023  |

Студент  І.В. Ковальчук

Керівник  О.С. Головня

### КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломного проекту (роботи)                    | Строк виконання етапів проекту (роботи) | Примітка |
|-------|-------------------------------------------------------------|-----------------------------------------|----------|
| 1     | Аналіз отриманого завдання та уточнення поставлених завдань | 10.03.2023 р.                           | виконано |
| 2     | Аналіз літературних джерел                                  | 15.03.2023 р.                           | виконано |
| 3     | Аналіз об'єкта дослідження                                  | 20.03.2023 р.                           | виконано |
| 4     | Подача чернетки керівнику для перевірки                     | 03.04.2023 р.                           | виконано |
| 5     | Розробка структурної моделі                                 | 15.04.2023 р.                           | виконано |
| 6     | Розрахунок параметрів адресації                             | 23.04.2023 р.                           | виконано |
| 7     | Налаштування пристроїв та вибір обладнання                  | 30.04.2023 р.                           | виконано |
| 8     | Розробка захищеної мережі                                   | 07.05.2023 р.                           | виконано |
| 9     | Тестування працездатності мережі                            | 19.05.2023 р.                           | виконано |
| 10    | Написання пояснювальної записки                             | 27.05.2023 р.                           | виконано |
| 11    | Підготовка додаткових матеріалів                            | 07.06.2023 р.                           | виконано |
| 12    | Отримання відгуку та рецензії на кваліфікаційну роботу      | 19.06.2023 р.                           | виконано |
| 13    | Захист кваліфікаційної роботи                               | Згідно з розкладом                      | виконано |

Студент  І.В. Ковальчук

Керівник  О.С. Головня

## АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи бакалавра складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 80 сторінках друкованого тексту. Пояснювальна записка має 17 сторінок додатків. Список використаних джерел містить 18 найменувань і займає 2 сторінки. В роботі наведено 53 рисунків. Загальний обсяг роботи – 98 сторінок.

Метою кваліфікаційної роботи є побудована корпоративної мережі організації на основі IPSec VPN та міжмережного екрану Palo Alto Networks для контролю доступу та захисту від потенційних загроз.

У кваліфікаційній роботі проаналізовано теоретичні основи побудови корпоративних мереж з використанням технологій захисту Palo Alto Networks та розробки архітектури корпоративної мережі на основі IPSec VPN. Було проведено аналіз створення та проектування захищеної мережі організації, розробку топології комп'ютерної мережі та виконано проектування мережі засобами емулятора GNS3. Також здійснено аналіз і вибір обладнання, проведено його налаштування та реалізовано технологію IPSec VPN для безпечного з'єднання. Встановлено правила безпеки для захисту мережі від потенційних загроз. Результат роботи перевірений на працездатність та протестований, все відповідає поставленим вимогам.

Ключові слова: МЕРЕЖЕВЕ ЕКРАНУВАННЯ, IPSEC VPN, МАРШРУТ, КОРПОРАТИВНА МЕРЕЖА, PALO ALTO NETWORKS, ВРАЗЛИВІСТЬ.

|           |                 |            |                                                                                     |          |                                                                                                       |                   |      |        |
|-----------|-----------------|------------|-------------------------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------|-------------------|------|--------|
|           |                 |            |                                                                                     |          | КІК.КР.Б – 123 – 7 – ПЗ                                                                               |                   |      |        |
| Зм.       | Арх.            | № докум.   | Підпис                                                                              | Дата     | Проект корпоративної мережі організації на основі IPSec VPN та міжмережного екрану Palo Alto Networks | Літ.              | Арк. | Аркуші |
| Розроб.   | Ковальчук І.В.  | 7008.06.23 |  | 06.06.23 |                                                                                                       |                   |      |        |
| Керівник  | Головня О.С.    | 7008.06.23 |  | 06.06.23 |                                                                                                       |                   | 4    |        |
| Реценз.   | Воротніков В.В. | 7008.06.23 |  | 06.06.23 |                                                                                                       |                   |      |        |
| Н. контр. |                 |            |                                                                                     |          |                                                                                                       |                   |      |        |
| Затверд.  | Єфіменко А.А.   | 7008.06.23 |  | 06.06.23 |                                                                                                       | ФІКТ, Гр. КІ-19-1 |      |        |

## ANNOTATION

The explanatory note of the bachelor's degree graduation project consists of an introduction, three chapters, conclusions, a list of references, and appendices. The textual part is presented in 80 pages of printed text. The explanatory note includes 17 pages of appendices. The list of references contains 18 sources and occupies 2 pages. The project includes 53 figures. The total length of the project is 98 pages.

The aim of the graduation project is to build a corporate network for an organization based on IPSec VPN and the Palo Alto Networks firewall for access control and protection against potential threats.

The work analyses the theoretical foundations of building corporate networks using Palo Alto Networks security technologies and the development of a corporate network architecture based on IPSec VPN. An analysis of the creation and design of a secure organization network was performed, including the development of computer network topology and the use of GNS3 software for designing. Equipment analysis and selection were also carried out, followed by configuration and implementation of IPSec VPN technology for secure connections. Security rules were established to protect the network from potential threats. The results of the work were verified for functionality and tested, meeting all the specified requirements.

Keywords: NETWORK FIREWALL, IPSEC VPN, ROUTING, CORPORATE NETWORK, PALO ALTO NETWORKS, VULNERABILITY.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 5    |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

## ЗМІСТ

|                                                                                                                           |    |
|---------------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП.....                                                                                                                | 8  |
| РОЗДІЛ 1 АНАЛІЗ ТЕОРЕТИЧНИХ ОСНОВ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ЗАХИСТУ PALO ALTO NETWORKS..... | 10 |
| 1.1 Принципи побудови корпоративної мережі та її види.....                                                                | 10 |
| 1.2 Принцип роботи та функції мережевих екранів у складі мереж організацій .....                                          | 12 |
| 1.3 Огляд наявних брандмауерів нового покоління та їх застосування .....                                                  | 17 |
| 1.4 Порівняння особливостей застосування технології IPSec з іншими технологіями VPN .....                                 | 23 |
| 1.5 Високопродуктивне запобігання загрозам Contend-ID у Palo Alto Networks Firewall.....                                  | 30 |
| РОЗДІЛ 2 ПРОЄКТУВАННЯ АРХІТЕКТУРИ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ IPSEC VPN ТА МЕРЕЖЕВОГО ЕКРАНУВАННЯ.....                 | 38 |
| 2.1. Аналіз створення та проектування захищеної мережі організації.....                                                   | 38 |
| 2.2 Розробка топології комп'ютерної мережі.....                                                                           | 41 |
| 2.3 Програмне забезпечення для проектування GNS3 (Graphical Network Simulator 3).....                                     | 48 |
| РОЗДІЛ 3 АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОРПОРАТИВНОЇ МЕРЕЖІ, РОЗРОБКА ТА ДОСЛІДЖЕННЯ РОБОТИ ЗАХИЩЕНОЇ МЕРЕЖІ .....                | 51 |
| 3.1 Вибір обладнання для організації роботи мережі.....                                                                   | 51 |
| 3.2 Налаштування обладнання мережі організації .....                                                                      | 57 |
| 3.3 Додавання правил безпеки на основі технології Content-ID та власних сигнатур.....                                     | 68 |
| 3.4 Перевірка працездатності мережі та тестування виконаних налаштувань.....                                              | 73 |
| ВИСНОВКИ.....                                                                                                             | 78 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ .....                                                                                      | 79 |
| ДОДАТКИ.....                                                                                                              | 81 |

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 6    |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – Програмне забезпечення  
IP – Internet Protocol  
VLAN - Virtual Local Area Network  
OSPF – Open Shortest Path First  
GNS – Graphical Network Simulator  
CAN — Campus Area Network  
AD – Active Directory  
PAN – Palo Alto Networks  
NGFW - Next-Generation Firewall  
VPN - Virtual Private Network  
ZBF - Zone-Based Policy firewall  
IPSec – IP Security  
TCP – Transmission Control Protocol  
UDP – User Datagram Protocol  
IPS – Intrusion Prevention System  
SSL – Secure Sockets Layer  
DNS – Domain Name System  
IKE - Internet Key Exchange  
ESP - Encapsulating Security Payload  
HTTP – HyperText Transfer Protocol  
DC- Data Center  
QoS – Quality of service  
NAT - Network Address Translation

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 7    |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

## ВСТУП

**Актуальність теми.** Кожна організація складається з різних взаємодіючих компонентів, кожен з яких має свої особливості. Ці компоненти функціонально сумісні та можуть виконувати окремі дії, які вписуються в загальні бізнес-процеси або інформаційні операції, наприклад обмін документами та замовленнями. Крім того, ці елементи можуть спілкуватися із зовнішніми системами, що може бути корисним або необхідним для їх роботи. В сучасному інформаційному суспільстві забезпечення безпеки інформаційних систем організацій є надзвичайно важливим завданням. У зв'язку зі зростанням кількості кібератак, шкідливих програм та порушень конфіденційності даних, виникає потреба у використанні надійних і ефективних інструментів захисту мережевої інфраструктури. У цьому контексті проектування корпоративної мережі з використанням безпечного з'єднання та міжмережного екрану стає надзвичайно актуальним завданням. Ця технологічна комбінація забезпечує високий рівень безпеки, надійності та швидкості обміну даними, що є критичними факторами для багатьох організацій у сучасному бізнес-середовищі.

**Метою даної кваліфікаційної роботи** є розробка та реалізація проекту корпоративної мережі організації на основі IPSec VPN та міжмережного екрану Palo Alto Networks. Головною метою є створення надійної, безпечної та ефективної мережевої інфраструктури, яка забезпечує захист конфіденційної інформації, надійний обмін даними та оптимальне використання мережевих ресурсів.

Головними завданнями роботи є:

1. Вивчення теоретичних аспектів IPSec VPN та мережних екранів Palo Alto Networks.
2. Аналіз потреб організації в безпеці мережевої інфраструктури та вимог до корпоративної мережі.
3. Проектування корпоративної мережі на основі IPSec VPN та міжмережного екрану Palo Alto Networks.
4. Розробка та впровадження проекту корпоративної мережі.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 8    |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

5. Оцінювання ефективності та надійності розробленої мережі.

**Об'єктом дослідження** є процес побудови проєкту корпоративної мережі організації з використанням міжмережного екранування.

**Предметом дослідження** є технології IPSec VPN та мережні екрани Palo Alto Networks для створення безпечної корпоративної мережі організації.

У межах дослідження розглянуто принципи проєктування мережі з використанням міжмережного екрану Palo Alto Networks, а також його впровадження та конфігурацію. Також буде з'ясовано функції та конфігурації IPSec VPN при проєктування корпоративної мережі бізнесу. Кваліфікаційна робота включатиме розробку архітектури мережі, встановлення та конфігурацію VPN, міжмережного екрану Palo Alto Networks, а також дослідження можливостей протоколу OSPF, спеціальних сигнатур вразливостей, шпигунського ПЗ та шкідливого трафіку, а також їх інтеграцію з системою управління користувачами Active Directory. Здійснено аналіз та оцінювання ефективності, безпеки та надійності розробленої корпоративної мережі.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 9    |

# РОЗДІЛ 1 АНАЛІЗ ТЕОРЕТИЧНИХ ОСНОВ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ЗАХИСТУ PALO ALTO NETWORKS

## 1.1 Принципи побудови корпоративної мережі та її види

У сучасній підприємницькій діяльності велике значення надається розвитку комп'ютерних мереж. Вони є важливим інструментом для забезпечення зв'язку між співробітниками в офісі чи будівлі, а також між різними регіонами, містами чи навіть країнами.

Для успішного управління підприємством необхідний постійний моніторинг інформаційних потоків і оперативна координація діяльності всіх співробітників і підрозділів.

Корпоративна мережа — це мережа, яка створюється для забезпечення роботи конкретного підприємства — власника мережі. Доступ до корпоративної мережі мають лише працівники цього підприємства. На відміну від операторів, корпоративні мережі зазвичай не надають послуг стороннім користувачам або компаніям. Залежно від розміру підприємства і складності завдань, що вирішуються в мережі, розрізняють відомчі мережі, кампусні мережі та корпоративні мережі.[1]

Корпоративна мережа дозволяє створити єдину базу даних для всіх підрозділів, вести електронний документообіг, організовувати відеоконференції та проводити зустрічі з віддаленими підрозділами. Він також забезпечує доступ до Інтернету та інших інтерактивних мереж, задовольняючи всі потреби організації. Все це сприяє швидкій реакції на зміни в компанії та управлінню всіма процесами в режимі реального часу.[1]

Крім того, використання корпоративної мережі допомагає зменшити залежність від операторів мобільного зв'язку та значно скоротити витрати організації. Також можлива передача конфіденційної інформації з гарантованою конфіденційністю, доступ до якої мають лише авторизовані співробітники компанії.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 10   |

Зображено загальну схему корпоративної мережі:



Рисунок 1.1 — Схема корпоративної мережі

Завдання системних інтеграторів та адміністраторів полягає у забезпеченні оптимального функціонування корпоративної мережі та забезпеченні її надійності, сприяючи швидкій передачі інформації між співробітниками та своєчасному прийняттю рішень. Оскільки швидко змінюються динаміка сучасного життя, вміст корпоративної інформації, то потоки даних та методи їх обробки постійно еволюціонують [1].

Кампусна мережа, відома також як мережа кампусу, представляє собою групу локальних мереж, що покривають відносно компактну територію та обслуговують певну організацію, наприклад, компанію, університет, офіси, оптові склади або державні установи. У таких ситуаціях усе мережеве обладнання (комутатори, маршрутизатори) та засоби передачі даних (кабелі Cat5, оптичне волокно, мідний кабель, та інше) належать власнику кампусу, будь то університет, компанія, державна установа тощо.

Основна структура кампусної мережі (CAN) полягає у великій багатосегментній локальній мережі, що охоплює кілька кілометрів у діаметрі та з'єднує локальні мережі різних будівель, розташованих поряд одна з одною. Перші приклади використання мереж кампусу зустрічаються у Стенфордському університеті з їхньою відомою мережею, проекті "Афіна" в Массачусетському технологічному інституті та проекті "Ендрю" в Університеті Карнегі-Меллон.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 11   |

Кампусні мережі здобули широку популярність та поширення, переважно серед коледжів та університетів у Сполучених Штатах. Вони використовуються для з'єднання різних будівель, розташованих на різних відстанях, включаючи адміністративні приміщення, навчальні корпуси, гуртожитки та додаткові споруди, наприклад, конференц-зали, технологічні організації та інші навчальні заклади.[12]

Зазвичай діапазон кампусної мережі становить від 1 до 5 км. Якщо дві будівлі належать до одного домену та підключені до спільної мережі, це вважається кампусною мережею. Незалежно від того, що CAN-мережі в основному використовуються для корпоративних кампусів, канали передачі даних мають високу швидкість.

Інтеграція різноманітного апаратного та програмного забезпечення становить виклик на рівні кампусної мережі. Кожний відділ може використовувати різні мережеві операційні системи, комп'ютери та мережеве обладнання, що ускладнює керування кампусними мережами. Крім того, оскільки мережі різних відділів, які входять до складу кампусної мережі, мають досить незалежну природу та часто базуються на різних технологіях, IP-протокол зазвичай використовується для їх уніфікації.

## **1.2 Принцип роботи та функції мережевих екранів у складі мереж організацій**

Мережевий брандмауер (МБ) - це пристрій, який призначений для забезпечення безпеки мережі шляхом контролювання вихідного та вхідного мережевого трафіку. Його основна мета полягає у прийнятті рішень на підставі набору правил безпеки щодо дозволу або блокування певного трафіку. Протягом понад 25 років мережеві брандмауери відіграють важливу роль у захисті мереж, виступаючи перешкодою між надійними внутрішніми мережами та ненадійними зовнішніми мережами, наприклад, Інтернетом. Існують різні типи мережевих брандмауерів, включаючи апаратні, програмні та гібридні рішення.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 12   |

Основна функція мережевого екрану полягає в аналізі структури та моніторингу вмісту вхідних пакетів даних зовнішньої мережі. Він приймає рішення, чи дозволити цим пакетам пройти до внутрішньої мережі (сегмента мережі), або повністю їх заблокувати. У разі мережевого брандмауера, що працює на платформі Windows, його ефективність полягає у повному заміщенні реалізованого стеку протоколів TCP/IP, що унеможливорює злам брандмауера шляхом спотворення зовнішніх мережевих протоколів.

Мережеві брандмауери виконують кілька важливих функцій, зокрема:

- Фізичне відокремлення робочих станцій та серверів у внутрішньому сегменті мережі від зовнішніх каналів зв'язку.
- Багатоступінчаста ідентифікація вхідних запитів до мережі.
- Перевірка привілеїв користувача та прав доступу до внутрішніх ресурсів мережі.
- Реєстрація всіх запитів до складових внутрішньої підмережі зовнішніх джерел.
- Забезпечення цілісності ПЗ та даних.
- Збереження адресного простору мережі.
- Приховування IP-адрес внутрішніх серверів для захисту від зловмисників.

Мережеві брандмауери поділяються на три типи:

1. пакетні фільтри (Packet filter);
2. сервера прикладного рівня (Application gateways);
3. сервера рівня з'єднання (Circuit gateways).

Брандмауери з *пакетними фільтрами* приймають рішення щодо дозволу або відкидання пакетів, аналізуючи інформацію, таку як прапорці, IP-адреси або номери портів TCP, що містяться в заголовку пакета. Інформація про номер порту та IP-адресу знаходиться на рівнях мережі та транспорту. Фільтри пакетів мають переваги, такі як низькі витрати, гнучкість при визначенні різних правил фільтрації та низьку затримку обробки пакетів, але також мають певні недоліки.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 13   |

Фільтри пакетів також мають деякі недоліки, включаючи можливість відображення локальної мережі з Інтернету, складність опису правил фільтрації пакетів, які потребують глибоких знань про технології TCP і UDP, вразливість всіх комп'ютерів у разі несправності брандмауера (що може призвести до повної незахищеності або недоступності), можливість підробки IP-адрес для обходу аутентифікації за допомогою IP-адрес (коли нападаюча система підробляє іншу систему, використовуючи її IP-адресу), а також відсутність процесу аутентифікації на рівні користувача.[8]

На прикладному рівні використовуються специфічні сервери послуг, такі як TELNET, FTP та інші. Ці служби використовують проксі-сервери, які активуються на екрані та направляють через себе весь трафік. Це встановлює дві з'єднання між сервером та клієнтом: одне від клієнта до мережевого екрану (ME), а інше від ME до призначення.

Сервери *на прикладному рівні* мають кілька переваг: вони зроблять локальну мережу невидимою в Інтернеті, забезпечуючи тим самим захист від загроз безпеці локальної мережі у разі відмови. Безпека серверів на рівні застосунків також дозволяє проводити додаткові перевірки.

Проте, цим серверам притаманні деякі недоліки, зокрема вищі витрати порівняно з пакетними фільтрами, нижча продуктивність та неможливість використання протоколів RPC та UDP.

З іншого боку, *сервер на рівні з'єднання* працює подібно до мережевого екрану на рівні застосунку, оскільки обидва вони виступають посередниками. Коли користувач встановлює з'єднання з певним портом шлюзу, шлюз підключається до порту призначення з іншого боку ME. Протягом сесії цей канал зв'язку робить копію байтів у обох напрямках. Зазвичай призначення заздалегідь визначено, тоді як джерел може бути кілька. За допомогою різних портів можна створити різноманітні конфігурації.[8]

Брандмауери нового покоління (NGFW) розширюються поза традиційне фільтрування пакетів та контроль стану сеансу. У відповідь на сучасні загрози,

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 14   |

такі як складний шкідливий код та атаки на рівні застосунків, більшість компаній використовують мережеві шлюзи наступного покоління.

Ідеальний брандмауер нового покоління повинен мати наступні функції:

- стандартні функції мережевого екрану, такі як контроль стану сеансу;
- вбудовану систему запобігання вторгнень;
- здатність розпізнавати та блокувати небезпечні програми;
- механізм оновлення, який передбачає майбутні канали інформації;
- технології безпеки, що захищають від постійно змінюваних загроз безпеці.

Хоча ці можливості поступово стають стандартом для більшості компаній, мережеві шлюзи наступного покоління пропонують ще більш розширені функціональні можливості.

Брандмауери нового покоління з функцією активного захисту відповідають на виклики звичайного брандмауера та виявлення й нейтралізацію складних загроз. Ці розширені мережеві екрани дозволяють виявляти найуразливіші ресурси завдяки комплексному контекстному розумінню. Вони також забезпечують швидку реакцію на атаки завдяки розумній автоматизації безпеки, яка встановлює політики та динамічно налаштовує захист. Крім того, вони поліпшують виявлення підозрілих дій шляхом кореляції подій у мережі та на кінцевих точках. За допомогою заходів ретроспективної безпеки значно скорочується час від виявлення до відновлення, завдяки постійному моніторингу підозрілої поведінки навіть після початкової перевірки. Єдина політика спрощує адміністрування і зменшує складність, забезпечуючи повноцінний захист протягом всього життєвого циклу атаки.[5]

Основні характеристики брандмауера наступного покоління:

- Система запобігання вторгнення (IPS)

Брандмауери наступного покоління мають вбудовану функціональність IPS, яка дозволяє виявляти та блокувати в реальному часі відомі вразливості та

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 15   |

типові атаки. Вони використовують виявлення підписів та аналіз поведінки для передбачення та захисту від мережевих загроз.

- Контроль та управління додатками

Ці брандмауери здатні проводити глибоку інспекцію пакетів для ідентифікації та контролю конкретних додатків, що працюють у мережі. Це дозволяє організаціям встановлювати політику безпеки на основі категорій додатків, їх характеристик та поведінки користувачів.

- Відстеження ідентифікації користувача

Такі брандмауери також можуть пов'язувати мережевий трафік з конкретними обліковими записами користувачів. За допомогою інтеграції з системами аутентифікації, такими як Active Directory, брандмауери можуть застосовувати політику, що залежить від користувача, та контролювати доступ до додатків та ресурсів.

- Розшифрування SSL/TLS

Брандмауери можуть розшифровувати зашифрований трафік SSL/TLS для його інспекції щодо потенційних загроз. Це дозволяє організаціям зберігати видимість шифрованих комунікацій при забезпеченні безпеки.

Брандмауери наступного покоління використовують різноманітні техніки профілактики передових загроз, включаючи пісочниці (sandboxes), розвідку загроз та машинне навчання, для виявлення та блокування складних загроз, таких як експлойти нульового дня та складне шкідливе програмне забезпечення.

Першою лінією захисту для мережевої інфраструктури організації виступають брандмауери наступного покоління. Вони захищають від несанкціонованого доступу, шкідливого програмного забезпечення та інших мережевих загроз шляхом застосування політик безпеки, блокування шкідливого трафіку та надання інформації про загрози в реальному часі.

NGFW дозволяють організаціям контролювати використання певних додатків у мережі. Це допомагає дотримуватися правил відповідності, оптимізувати використання пропускну здатності та зменшувати ризики, пов'язані з несанкціонованим або ризикованим використанням додатків.[5]

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 16   |



Рисунок 1.2 – Лого NGFW

Також ідеально підходять для захисту віддалених та філійних офісів. Вони забезпечують безпечне підключення, профілактику загроз та централізоване управління, забезпечуючи єдиний рівень безпеки по всій розподіленій мережі. Призначені для захисту хмарних середовищ, дозволяючи організаціям розширити політику безпеки та контроль до хмарних додатків та сервісів.

### 1.3 Огляд наявних брандмауерів нового покоління та їх застосування

Наступне покоління засобів безпеки мережі стали необхідною складовою для організацій, що мають захищатися від складних кіберзагроз і забезпечувати безпеку своєї мережевої інфраструктури. Ці нові інструменти виходять за рамки традиційних брандмауерів та надають розширені можливості, такі як виявлення складних загроз, забезпечення видимості та контролю над додатками, а також комплексне управління безпекою. Згідно з визначенням Gartner, брандмауер наступного покоління повинен включати основні можливості традиційних брандмауерів, такі як перевірка стану, інтегроване запобігання вторгненням, свідомість і контроль програм, що дозволяють виявляти та блокувати ризиковані програми, шляхи оновлення для врахування майбутніх інформаційних каналів і методи для протидії новим загрозам безпеці. [3]

Рішення безпеки мережі наступного покоління від Palo Alto Networks є високопродуктивним варіантом, що пропонує широкий набір функцій та можливостей для забезпечення безпеки мережі.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 17   |

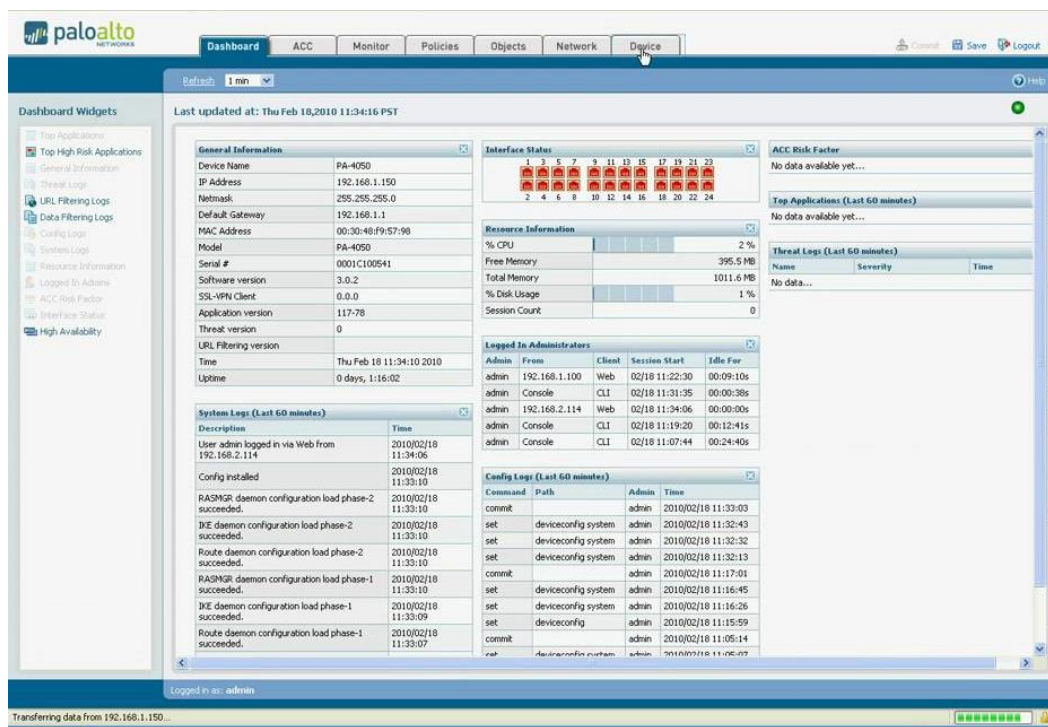


Рисунок 1.3 – Інформаційна панель Palo Alto Networks

Деякі важливі характеристики брандмауера Palo Alto Networks включають:

- Профілактика загроз

Брандмауер об'єднує кілька методів профілактики загроз, таких як система запобігання вторгненням (IPS), захист від шкідливого програмного забезпечення, фільтрацію URL-адрес та захист DNS, щоб забезпечити передовий захист від відомих і нових загроз.

- Видимість та контроль додатків

Брандмауер забезпечує глибоку видимість мережевого трафіку, що дозволяє організаціям створювати політики безпеки на основі конкретних додатків та їх категорій. Також надаються можливості контролю використання додатків та встановлення обмежень відповідно до потреб організації.

- Управління через платформу Panorama

За допомогою платформи Panorama від Palo Alto Networks забезпечується централізоване управління кількома брандмауерами наступного покоління. Це спрощує конфігурацію політик, моніторинг та звітність для всієї мережевої інфраструктури.

- Інтеграція з WildFire

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 18   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

Palo Alto Networks постійно взаємодіє з хмарною платформою WildFire для проведення піщаного тестування. Ця інтеграція розширює можливості виявлення та запобігання загроз, шляхом ідентифікації та блокування складного шкідливого програмного забезпечення та експлойтів нульового дня.

- Безпечна SD-WAN

Брандмауер включає можливості безпечної SD-WAN, що дозволяє організаціям безпечно підключати філійні офіси та віддалені розташування, забезпечуючи оптимальну продуктивність та безпеку.

Таким чином, брандмауер наступного покоління Palo Alto Networks надає надійне та масштабоване рішення для забезпечення мережевої безпеки, з високоякісною профілактикою загроз, контролем додатків та централізованим управлінням.

Для порівняння, окрім брандмауера Palo Alto Networks NGFW, на ринку також присутні ще два аналоги - Barracuda CloudGen Firewall та Cisco ASA NGFW, які користуються популярністю серед компаній.

Barracuda CloudGen Firewall представляє собою нове покоління брандмауера з вбудованими функціями, включаючи систему запобігання вторгненню (IPS), захист від шкідливого програмного забезпечення та інші функції, необхідні для захисту периметра мережі. Його встановлення та налаштування здійснюються просто й гнучко, що особливо корисно для швидкого масштабування та роботи з віддаленими користувачами, які працюють з дому або з віддалених офісів. Однією з найважливіших функцій цього брандмауера є можливість створення тунелів для кількох підключень. Крім того, CloudGen забезпечує балансування навантаження між різними місцями за допомогою різних постачальників послуг[4].

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 19   |

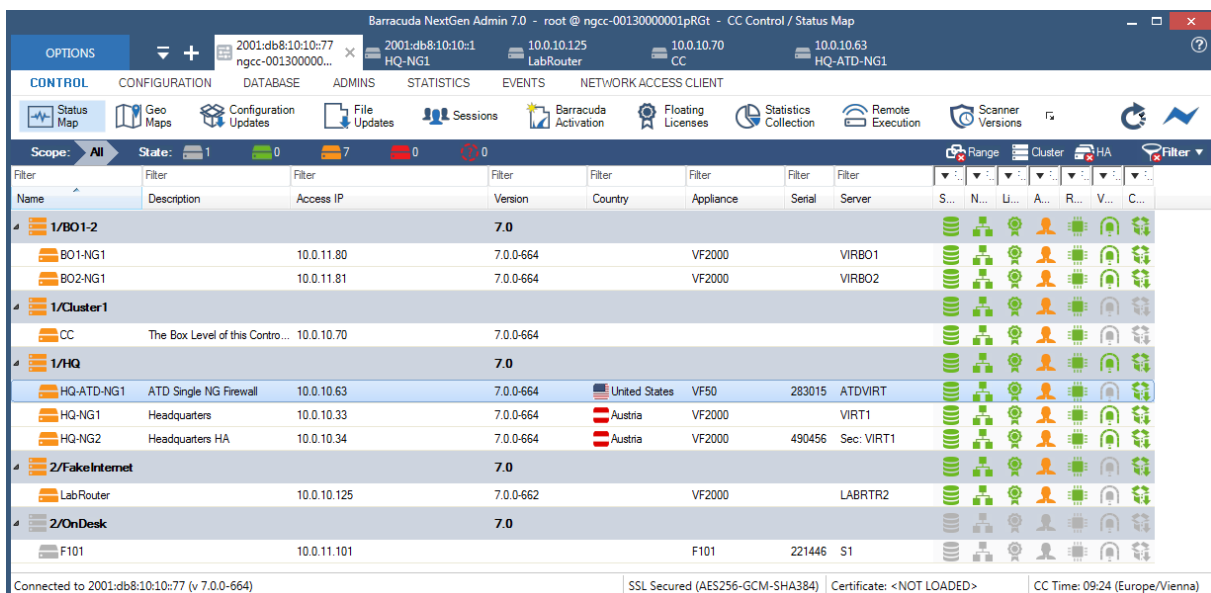


Рисунок 1.4 – Інформаційна панель Barracuda CloudGen Firewall

Брандмауер наступного покоління Cisco ASA (NGFW) є важливою складовою інтегрованої архітектури безпеки Cisco. Він надає комплексне та уніфіковане керування політикою брандмауера, контролем програм, запобіганням загрозам та розширеним захистом від шкідливого програмного забезпечення від мережі до кінцевих точок.[5]

Розглянемо їх функціонал, можливості та обґрунтуємо вибір кожного рішення. Нижче наведена таблиця з порівнянням ключових аспектів:

Таблиця 1.1 – Можливості пристроїв

| Особливість                         | Barracuda CloudGen Firewall | Palo Alto Networks NGFW | Cisco ASA NGFW |
|-------------------------------------|-----------------------------|-------------------------|----------------|
| Профілактика передових загроз       | Так                         | Так                     | Так            |
| Контроль додатків                   | Так                         | Так                     | Так            |
| Система запобігання вторгнень (IPS) | Так                         | Так                     | Так            |
| Розшифрування SSL/TLS               | Так                         | Так                     | Так            |
| Фільтрація веб-ресурсів             | Так                         | Так                     | Так            |
| Централізоване управління           | Так                         | Так                     | Так            |
| Інтеграція з хмарними сервісами     | Так                         | Так                     | Так            |

Продовження таблиці 1.1 – Можливості пристроїв

|                                    |        |          |        |
|------------------------------------|--------|----------|--------|
| Масштабованість                    | Добра  | Відмінна | Добра  |
| Продуктивність                     | Висока | Висока   | Висока |
| Інтерфейс, зручний для користувача | Так    | Так      | Так    |
| Репутація та підтримка             | Добра  | Відмінна | Добра  |

У всіх трьох рішеннях є можливості передової профілактики загроз для виявлення та запобігання складним загрозам, включаючи шкідливе програмне забезпечення, експлойти нульового дня та стійкі загрози. Вони застосовують різноманітні техніки, такі як пісочниця, аналіз поведінки та розвідка загроз, для ефективного виявлення та усунення загроз.

Barracuda CloudGen Firewall, Palo Alto Networks NGFW та Cisco ASA NGFW надають гранульований контроль за додатками, що працюють у мережі. Вони дозволяють організаціям застосовувати політики безпеки на основі конкретних додатків або категорій додатків, забезпечуючи кращу видимість та контроль над мережевим трафіком.

Кожне рішення включає систему запобігання вторгнень (IPS), яка моніторить мережевий трафік на наявність відомих патернів атак та перешкоджає спробам вторгнення. Ця функція покращує безпеку, виявляючи та блокуючи шкідливі дії в реальному часі.[4]

Кожний інструмент підтримує розшифрування SSL/TLS, що дозволяє інспектувати та аналізувати зашифрований трафік для виявлення потенційних загроз або порушень політик.

Усі три рішення пропонують можливості фільтрації веб-ресурсів для контролю та моніторингу доступу до веб-сайтів, блокування шкідливих веб-ресурсів та виконання вимог політики контенту. Ця функція допомагає організаціям захиститися від загроз, обмежити доступ до неприйняттого контенту та покращити продуктивність. Barracuda CloudGen Firewall, Palo Alto Networks NGFW та Cisco ASA NGFW надають платформи для централізованого

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 21   |

управління конфігурацією, моніторингом та звітністю мережевої інфраструктури. Це спрощує управління завданнями і забезпечує єдину картину безпеки мережі.

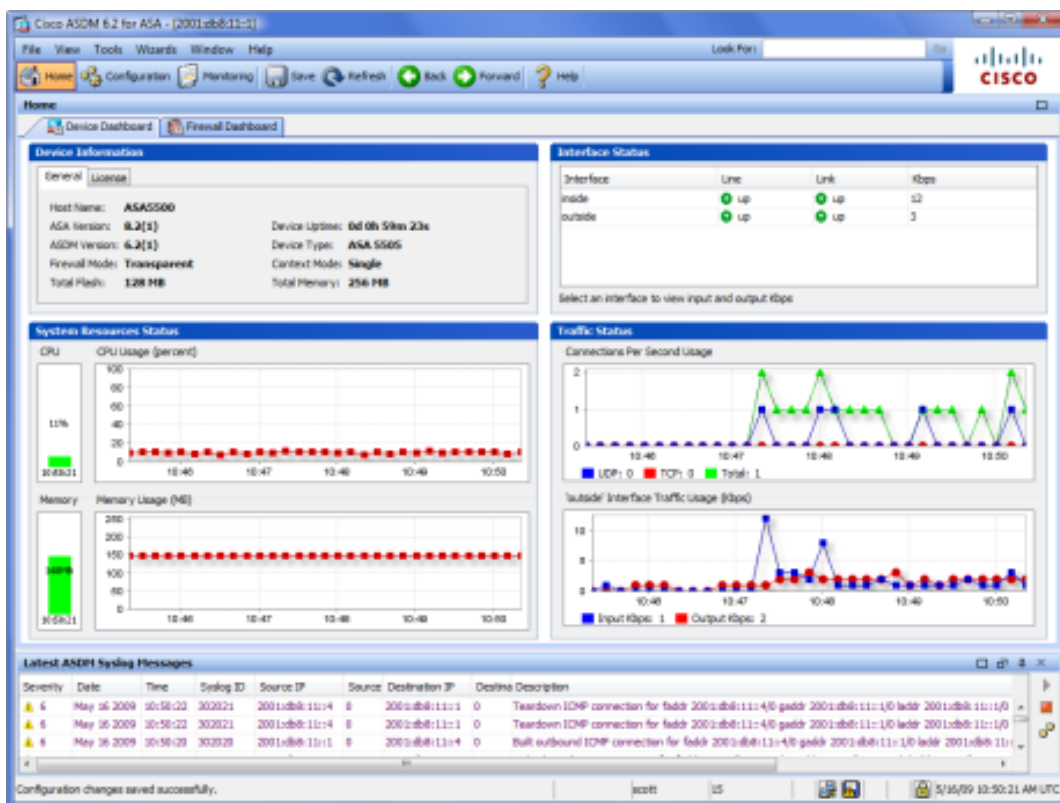


Рисунок 1.5 – Інформаційна панель Cisco ASA NGFW

Інтеграція з хмарними сервісами: Усі рішення інтегруються з хмарними сервісами, що дозволяє розширити захист мережі до хмарних інфраструктур та забезпечити безпечний доступ до хмарних додатків та ресурсів.

NGFW мають різні рівні масштабованості. Palo Alto Networks відомий своєю високою масштабованістю, що дозволяє розширювати мережу та додавати нові об'єкти без значного впливу на продуктивність.

Кожен виробник ставить на перший план зручність використання своїх рішень, тому брандмауери надають інтуїтивно зрозумілі та легко налаштовувані інтерфейси для користувачів.

## 1.4 Порівняння особливостей застосування технології IPSec з іншими технологіями VPN

Безпека та конфіденційність в Інтернеті є важливими аспектами для багатьох людей, які не хочуть бути під наглядом або спостереженням, навіть якщо у них немає нічого незаконного або неприпустимого. В таких випадках використання VPN є надзвичайно важливим для забезпечення конфіденційності. Наприклад, підключення до публічної Wi-Fi мережі може стати ризиком, оскільки зловмисники можуть легко перехопити ваші дані. VPN дозволяє зашифрувати ваш трафік і зробити його невидимим для потенційних загроз.

Урядові установи, маркетологи та постачальники інтернет-послуг можуть відстежувати та збирати вашу приватну інформацію, включаючи історію перегляду та повідомлення. VPN є ефективним інструментом для приховування цих даних та забезпечення вашої приватності.

Технологія VPN використовується для створення приватних мереж, які дозволяють підключати користувачів до окремих мереж або ресурсів через захищений канал передачі даних. Вона використовує глобальні канали, захищені протоколи та маршрутизатори для забезпечення безпеки та конфіденційності.[11]

VPN-сервіси також можуть допомогти обійти обмеження мережевого трафіку, які накладають деякі постачальники інтернет-послуг (ISP). Наприклад, якщо ваш постачальник послуг обмежує швидкість передачі даних після досягнення певного ліміту, використання VPN може допомогти уникнути цього обмеження та забезпечити безперебійний інтернет-трафік. Проте, варто зазначити, що використання VPN може призвести до деякого зниження швидкості підключення через додатковий процес маршрутизації трафіку через VPN-сервер.

При підключенні до VPN, весь ваш інтернет-трафік проходить через інфраструктуру VPN-провайдера. Важливо враховувати ризики, пов'язані з цим, оскільки VPN-провайдер може мати доступ до вашої приватної інформації, якщо вони не дотримують належних стандартів безпеки та конфіденційності. Тому

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 23   |

перед вибором VPN-провайдера варто докладно ознайомитися з їх політикою конфіденційності та заходами безпеки, які вони приймають.

Наразі ринок VPN-послуг для споживачів все ще розвивається, і не завжди легко визначити надійного провайдера. У рейтингах і оглядах VPN-послуг, таких як ті, що проводяться [rstag.com](http://rstag.com), акцентується увага на різних аспектах, включаючи юридичну основу, заходи безпеки та політику щодо зберігання та використання користувацьких даних. Ознайомлення з цими оглядами допоможе отримати більш глибоке розуміння того, як кожен VPN-сервіс забезпечує конфіденційність користувачів.[7]

Також варто враховувати, що самостійне встановлення VPN-сервера має свої особливості, і його використання може бути необхідним для робочих потреб.

Спеціальні віртуальні окремі канали використовуються для інтеграції локальних мереж в єдину віртуальну мережу. Це досягається за допомогою механізму тунелювання. Ініціатор тунелю вкладає пакети з локальної мережі в нові IP-пакети, які містять адресу тунелю ініціатора та адресу тунелю термінатора у своїх заголовках. При отриманні такого пакета кінцевий користувач (термінатор тунелю) розшифровує отриманий пакет за допомогою зворотного процесу.

При використанні цього типу передачі критично враховувати конфіденційність та цілісність даних, оскільки саме тунелювання не може гарантувати ці аспекти. Для забезпечення конфіденційності інформації під час передачі використовується конкретний алгоритм шифрування. Важливо, щоб як відправник, так і одержувач використовували однаковий алгоритм і мали виключні знання про нього. Крім того, вони повинні мати ключі шифрування та розшифрування. Протоколи шифрування можуть варіюватись в залежності від підтримуваного протоколу тунелювання конкретного VPN-рішення [12].

Однією з важливих характеристик рішень VPN є набір підтримуваних протоколів аутентифікації. Загалом, більшість популярних продуктів працюють з відкритими стандартами ключів. Внаслідок цього безпеку віртуальної мережі

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 24   |

можна збільшити за допомогою відповідного протоколу аутентифікації, який дозволяє доступ до захищених каналів лише конкретним користувачам [15].

Зашифровані VPN можна розділити на різні типи. Віддалений доступ до VPN дозволяє розширити практично будь-яку додаткову, голосову або відео програму до віддаленого пристрою, також відомого як "кінцева точка" або хост. Розширені технології VPN дозволяють проводити перевірку безпеки на кінцевих точках, щоб переконатися, що вони відповідають певним критеріям, перш ніж отримати доступ до мережі.[7]

Secure Sockets Layer (SSL) VPN і Internet Protocol Security (IPsec) є прикладами технологій тунелювання та аутентифікації. Залежно від вимог розгортання, компанії можуть використовувати SSL VPN, IPsec або комбінацію обох для впровадження віддаленого доступу до VPN. SSL VPN та IPsec захищають дані, що передаються через VPN, від несанкціонованого доступу.

Для доступу до IPsec VPN користувачам потрібно ввести програму або "клієнт" VPN. Зазвичай це вимагає встановлення програмного забезпечення на їх пристрої [14].

**SSL VPN** для безпечного віддаленого доступу покладається на протокол Transport Layer Security (TLS), який замінив старий протокол SSL. SSL VPN дозволяє автентифікованим користувачам створювати безпечні з'єднання з внутрішніми службами HTTP і HTTPS через стандартні веб-браузери або користувацькі програми, що надають прямий доступ до мережі.

SSL VPN можна розділити на два основних типи: портал VPN і тунель VPN. SSL VPN-портал надає одночасні з'єднання SSL VPN з віддаленими веб-сайтами. Віддалені користувачі отримують доступ до шлюзу SSL VPN через свої веб-браузери після аутентифікації за допомогою підтримуваного методу. Доступ здійснюється через веб-сторінку, що виступає як портал до інших служб.

З іншого боку, SSL VPN-тунель дозволяє користувачам безпечно отримувати доступ до різних мережевих служб через стандартні веб-браузери, а також інші протоколи та програми без веб-інтерфейсу. VPN-тунель встановлює канал між віддаленим користувачем і сервером VPN. Сервер може підключатися до одного

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 25   |

або декількох віддалених веб-сайтів, мережевих служб або ресурсів від імені клієнта. Для роботи з SSL VPN-тунелю веб-браузер повинен обробляти активний контент і надавати функціональність, недоступну через SSL VPN-портал.

Інтеграція локальних мереж в єдину віртуальну мережу здійснюється за допомогою спеціальних віртуальних окремих каналів, які використовують механізм тунелювання. Цей процес полягає в тому, що пакети з локальної мережі вкладаються в нові IP-пакети, які містять адреси тунелю ініціатора та термінатора. При отриманні такого пакета кінцевий користувач розшифровує його за допомогою зворотного процесу.

Проте важливо пам'ятати, що тунелювання само по собі не гарантує конфіденційність та цілісність даних, тому використання відповідного алгоритму шифрування є необхідним. Конфіденційність забезпечується за допомогою шифрування, яке вимагає використання одного алгоритму та відповідних ключів шифрування і розшифрування. Протоколи шифрування можуть різнитись залежно від протоколу тунелювання, який використовується в конкретному VPN-рішенні.

Крім того, одним з важливих аспектів рішень VPN є підтримка протоколів аутентифікації. Більшість продуктів використовують відкриті стандарти ключів, що дозволяє забезпечити безпеку віртуальної мережі за допомогою протоколу аутентифікації, який обмежує доступ до захищених каналів конкретним користувачам.[11]

Існує кілька типів зашифрованих VPN. Наприклад, віддалений доступ до VPN дозволяє розширити можливості практично будь-якої програми до віддаленого пристрою. Також є SSL VPN та IPsec, які використовуються для тунелювання та аутентифікації. Вони забезпечують захист передачі даних через VPN від несанкціонованого доступу.

Для доступу до IPsec VPN користувачам потрібно встановити спеціальний клієнтський програмний засіб. З іншого боку, SSL VPN використовує протокол TLS для безпечного віддаленого доступу через веб-браузери або спеціальні клієнтські програми.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 26   |

SSL VPN може бути реалізований у вигляді VPN-порталу або VPN-тунелю. VPN-портал надає з'єднання з віддаленими веб-сайтами через SSL VPN. Віддалені користувачі отримують доступ до порталу через веб-браузери і мають можливість підключатися до інших служб. За своєю чергою, VPN-тунель дозволяє безпечний доступ до мережеских служб, інших протоколів та програм без веб-інтерфейсу. VPN-тунель встановлює канал між користувачем і сервером VPN, який може підключатися до різних ресурсів від імені користувача.



Рисунок 1.6 – Робота технології VPN

Облікові дані для входу до VPN зазвичай ґрунтуються на пароліх. Хоча дані, що передаються через VPN, шифруються, якщо зломисники отримають доступ до користувацьких паролів, вони можуть несанкціоновано отримати доступ до VPN та вкрасти зашифровані дані. Використання двофакторної аутентифікації (2FA) значно підвищує безпеку IPsec VPN, оскільки це перешкоджає зломисникам отримувати доступ, навіть якщо вони отримають лише пароль.

### Особливості роботи IPsec?

IPsec проходить чотири етапи:

- Ідентифікація цікавого трафіку. Коли мережевий пристрій отримує пакет, він порівнює 5-кортеж пакета з налаштованою політикою IPsec, щоб визначити, чи його потрібно маршрутизувати через тунель IPsec. Трафік, який потребує передачі через тунель IPsec, вважається "цікавим трафіком".
- Переговори щодо асоціації безпеки (SA). SA визначає параметри безпечної передачі даних між комунікуючими сторонами. Ці параметри включають протоколи безпеки, режими інкапсуляції даних, алгоритми

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 27   |

шифрування та аутентифікації, а також ключі шифрування, які використовуються для передачі даних.

Після ідентифікації цікавого трафіку локальний мережевий пристрій ініціює переговори щодо SA з пірним пристроєм. Під час цього етапу комунікуючі сторони використовують протокол Internet Key Exchange (IKE) для установки SA IKE для аутентифікації особи та обміну ключами. Потім вони встановлюють IPsec SA для забезпечення безпечної передачі даних на основі SA IKE.

- Завершення тунелю. У більшості випадків завершення сеансу (розрив сеансу) між двома комунікуючими сторонами означає завершення обміну даними.

- Передача даних. Після встановлення IPsec SA між комунікуючими сторонами вони можуть безпечно передавати дані через тунель IPsec.

Для забезпечення безпеки передачі даних використовується або заголовок аутентифікації (AH), або захищений поліпшений пакет (ESP) для шифрування та аутентифікації даних. Механізм шифрування забезпечує захист від перехоплення даних та конфіденційність даних під час передачі. Водночас механізм аутентифікації гарантує цілісність та надійність даних, запобігаючи підробленню або несанкціонованим змінам даних під час передачі.[14]

IPsec VPN-тунель складається з налаштування тунелю та застосування безпеки. Під час налаштування тунелю вузли-піри встановлюють асоціації безпеки (SA), які визначають параметри для захисту трафіку між ними. Після встановлення IPsec-тунелю IPsec забезпечує безпеку передаваного трафіку між кінцями тунелю шляхом застосування параметрів безпеки, визначених SA під час налаштування тунелю. У реалізації Junos OS IPsec працює у режимі тунелю, який підтримує протоколи Encapsulating Security Payload (ESP) та Authentication Header (AH).

У режимі тунелю повний початковий IP-пакет, включаючи корисне навантаження та заголовок, укладається в інший IP-навантажувач. Додається новий заголовок, як показано на рисунку 1.7. Весь початковий пакет може бути

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 28   |

зашифрований, аутентифікований або обома способами. Протокол заголовка аутентифікації (AH) аутентифікує як заголовок AH, так і новий заголовок, тоді як протокол захищеного поліпшеного пакету (ESP) також може аутентифікувати заголовок ESP.[15]

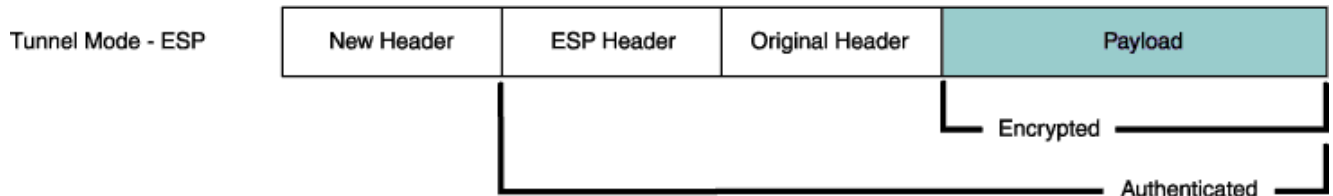


Рисунок 1.7- Режим тунелю, додавання нового заголовку

У випадку VPN типу "сайт-сайт" IP-адреси вихідного інтерфейсу використовуються як адреси джерела та призначення у новому заголовку (див. рис. 1.8).

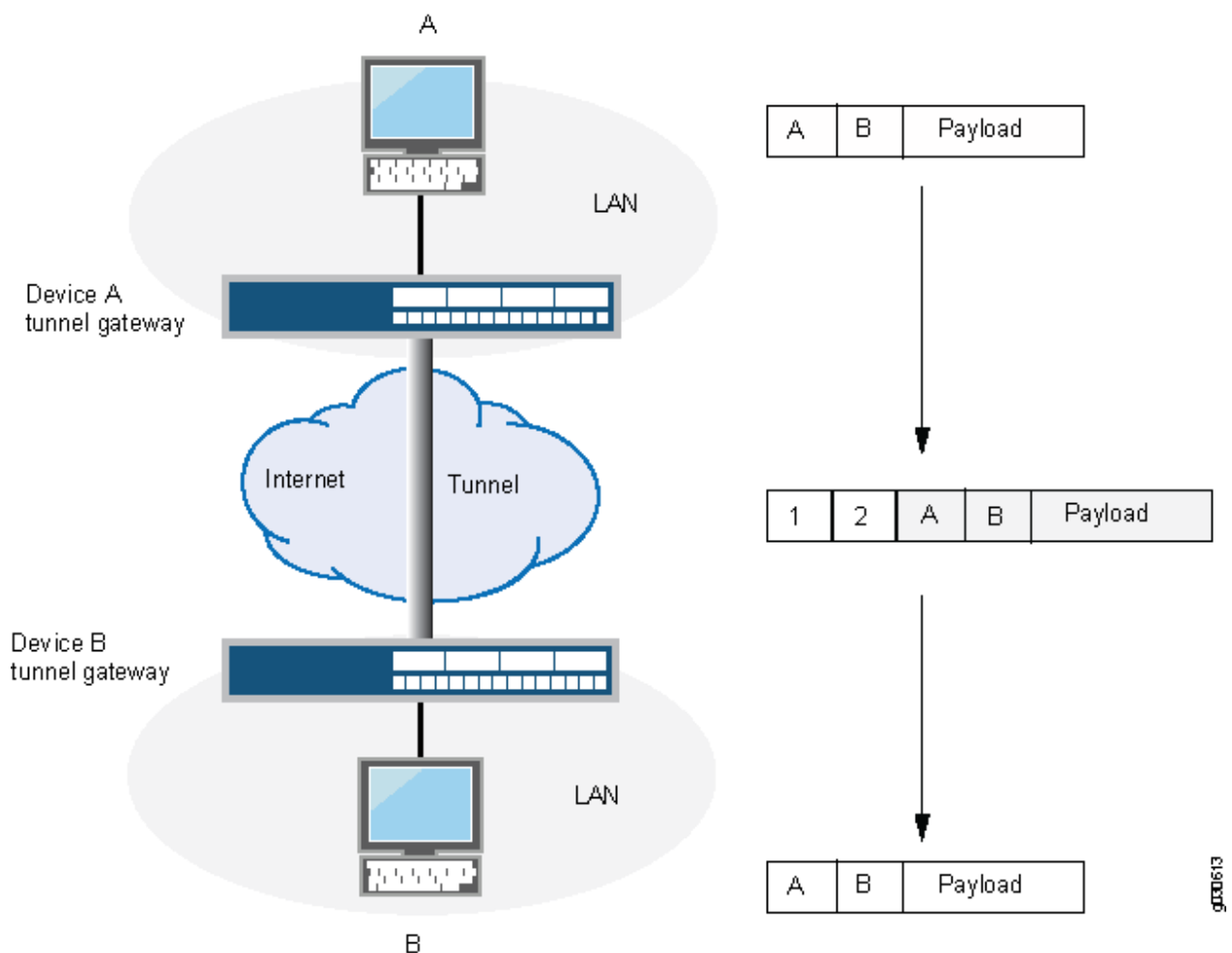


Рисунок 1.8 – Змінений заголовок у IPsec VPN Site-to-site

IPsec VPN працює на рівні мережі в моделі OSI і надає можливість віртуального доступу користувачів до всієї мережі, ніби вони знаходяться в ній фізично. Це дозволяє їм використовувати спільні файли, принтери та внутрішні програми. Натомість, SSL VPN сконцентрований на забезпеченні доступу до конкретних програм або сервісів на рівні додатків.

Одна з особливостей IPsec VPN - це його комплексний контроль над мережевим трафіком за допомогою списків контролю доступу (ACL) та політик маршрутизації. Адміністратори систем можуть встановлювати конкретні правила і регламенти для регулювання доступу до певних ресурсів для окремих користувачів або груп. З іншого боку, SSL VPN зазвичай надає обмежений контроль доступу, який часто визначається політиками на рівні додатків.

IPsec VPN відрізняється тим, що воно може створювати безпечні з'єднання між мережевими пристроями, такими як маршрутизатори, мережеві брандмауери та шлюзи, забезпечуючи захищений зв'язок між різними місцями або мережами. За своєю природою SSL VPN призначений головним чином для віддаленого доступу користувачів, а не для встановлення з'єднань між пристроями.

Важливо відзначити, що як IPsec VPN, так і SSL VPN мають свої унікальні переваги і відповідають різним сценаріям використання. Вибір між ними залежить від таких факторів, як вимоги до безпеки, мережева інфраструктура, сумісність і конкретні потреби користувачів у доступі.

### **1.5 Високопродуктивне запобігання загрозам Contend-ID у Palo Alto Networks Firewall**

В корпоративних мережах поширені програми, які можуть уникнути виявлення. Поширені методи включають динамічну зміну портів, повторне використання інших портів, емуляцію інших програм або тунелювання всередині SSL. Використання невидимих програм не залишилося непоміченим з боку злоумисників, оскільки вони все більше використовують ці невидимі програми для транспортування загроз поза межами брандмауера. Механізм

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 30   |

Content-ID поєднує єдиний формат підпису загроз, пошук за потоком даних і комплексну базу даних URL з елементами видимості програм, щоб виявляти та блокувати широкий спектр загроз, контролювати веб-серфінг, що не стосується роботи, та обмежувати несанкціоновану передачу файлів та даних.

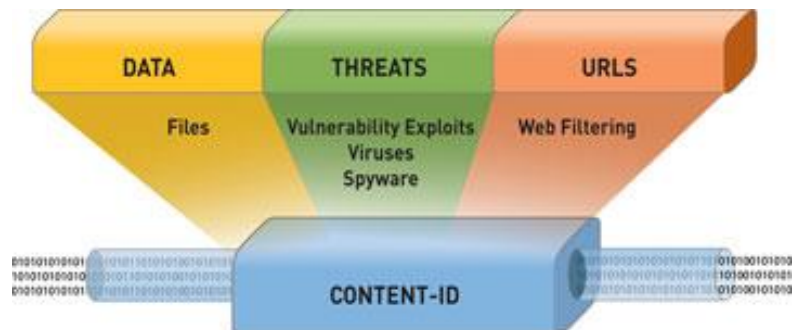


Рисунок 1.9 – Засоби, які входять у Content-ID

Content-ID надає механізм запобігання загрозам у реальному часі, поєднаний з комплексною базою даних URL та елементами ідентифікації програм, щоб:

- Обмежувати несанкціоновану передачу даних та файлів.
- Виявляти та блокувати використання вразливостей, шкідливих програм та комунікацій шкідливого програмного забезпечення.
- Контролювати несанкціоноване переглядання веб-сторінок.

Видимість та контроль застосунків (App-ID), разом із перевіркою вмісту, забезпечує ІТ-команду повною контролем над потоком даних застосунків та пов'язаним контентом.[2]

Водночас, якщо відповідні профілі безпеки були увімкнені в правилах безпеки, механізм Content-ID застосовуватиме політику фільтрації URL та постійно, паралельно скануватиме сеанс на наявність загроз, таких як використання вразливостей, інфікування вірусами або червами, підозрілі запити DNS, підписи командно-контрольного (C&C або C2) сервера, атаки DoS, сканування портів, некоректні протоколи або шаблони даних, що відповідають викраденню конфіденційної інформації. Виконується збірка TCP-пакетів та дефрагментації IP для запобігання методам ухилення на рівні пакетів:

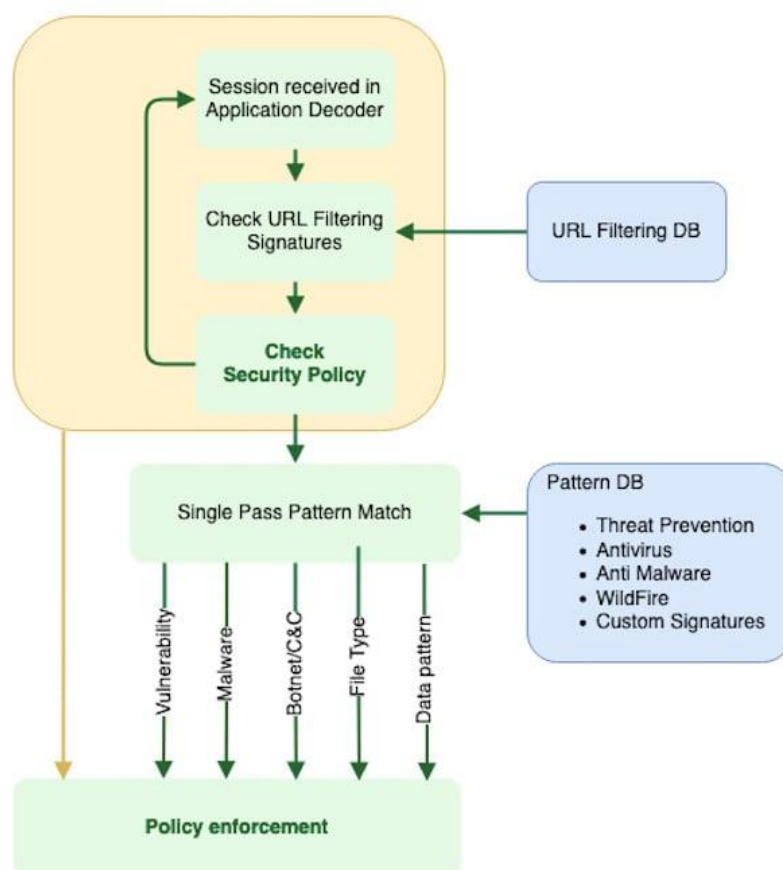


Рисунок 1.10 – Робота механізму Content-ID разом з іншими інструментами

Все це відбувається паралельно, оскільки апаратне та програмне забезпечення були розроблені таким чином, щоб кожен пакет одночасно оброблявся декодером App-ID та двигуном Content-ID на основі потоків, кожен з них у власному чіпі або через окремий процес в віртуальній машині (VM). Ця конструкція зменшує затримку порівняно з послідовною обробкою, що включення додаткових профілів безпеки не призводить до експоненціального збільшення витрат на продуктивність, як у інших брандмауерах та системах захисту від вторгнень (IPS).

### ***Threat Prevention***

Palo Alto Networks Content-ID займається викликами завдяки унікальним можливостям запобігання загроз, які не зустрічаються в інших рішеннях забезпечення безпеки. По-перше, брандмауер нового покоління видаляє методи, які використовують загрози для приховування від безпекових заходів, шляхом повного аналізу всього трафіку на всіх портах, незалежно від методів ухилення,

тунелювання або обхідних технік. Просто кажучи, жодне рішення запобігання загроз не буде ефективним, якщо воно не має видимості до трафіку, а лише Palo Alto Networks забезпечує таку видимість шляхом ідентифікації та контролю всього трафіку.

- Декодери застосунків: Content-ID використовує сотні декодерів застосунків та протоколів в App-ID для пошуку загроз, прихованих у потоках даних застосунків. Це дозволяє брандмауеру виявляти та запобігати загрозам, які тунелюються всередині схвалених застосунків, які пройшли би повз традиційні рішення IPS або проксі-сервери.

- Розшифрування SSL: З кожним днем все більше мережевого трафіку за замовчуванням шифрується за допомогою SSL. Це може забезпечити певний захист користувачам, але також може надати зловмисникам зашифрований канал для поширення шкідливих програм та вразливостей. Palo Alto Networks гарантує видимість, надаючи організаціям з можливістю, відповідно до політики, детально переглядати SSL-трафік на основі застосунку або категорії URL.

- Контроль обхідних технологій: Зловмисники все частіше використовують проксі-сервери та анонізатори для приховування від традиційних засобів мережевої безпеки. Palo Alto Networks надає можливість тісно контролювати ці технології та обмежувати їх на користь схвалених користувачів, одночасно блокуючи неприпустимі зв'язки, які можуть бути використані зловмисниками.

- Єдиноформатні загрози: Замість використання окремих сканерів та сигнатур для кожного виду загрози, Content-ID використовує єдиноформатний механізм виявлення та блокування широкого спектру шкідливих програм, шпигунського ПЗ та вразливостей за один прохід.

По-друге, Palo Alto Networks об'єднує декілька дисциплін безпеки в один контекст та один двигун запобігання загрозам. Цей контекст дозволяє командам безпеки легко бачити поза окремими подіями безпеки та розпізнавати повну картину загрози. Менеджери з безпеки тепер можуть бачити взаємозв'язки між застосунками, вразливостями, шкідливими програмами, URL-адресами, DNS-

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 33   |

запитами, аномальною мережевою поведінкою та забезпечувати передбачувану продуктивність, аналізуючи трафік один раз, замість поступового сканування декількома механізмами.[2]

### ***Інтегрований IPS i Anti-Malware***

Content-ID надає повністю інтегрований захист від використання вразливостей, шкідливих програм та трафіку, що генерується керуванням командами із зловживаннями. Як і у всіх аналізах Palo Alto Networks, запобігання загрозам застосовується у повному контексті застосунку та протоколу - по всьому трафіку та портам - для забезпечення виявлення та блокування загроз, незважаючи на спроби уникнення. Технології запобігання загрозам Palo Alto Networks включають:

- IPS - Функціональність IPS блокує використання вразливостей, переповнення буфера, атаки DoS та скани портів. Додаткові можливості, такі як блокування недійсних або неправильно сформованих пакетів, дефрагментація IP та збірка TCP, захищають вас від методів уникнення та замутнення, використовуваних зловмисниками.

- Мережевий антивірус на основі потоків - Palo Alto Networks підтримує базу даних з більш ніж 15 мільйонами зразків шкідливих програм. Кожен день ми аналізуємо ще 50 000 зразків. Шкідливі програми виявляються поточним двигуном, який блокує їх в режимі реального часу з високою швидкістю. Виявлення шкідливих програм доступне для різних протоколів, включаючи HTTP, SMTP, IMAP, POP3, FTP та SMB.

- Антишпигунство - Крім контролю вірусів і шкідливих програм, Content-ID блокує шпигунське програмне забезпечення та комунікацію шкідливих програм, включаючи:

- Комунікацію з ботнетами
- Перехоплення браузера
- Рекламне ПЗ
- Метод backdoor
- Кейлогери

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 34   |

- Крадіжку даних
- Мережеві черви
- Трафік підключення через піринг

Антишпигунське програмне забезпечення також пасивно аналізує запити DNS для виявлення унікальних шаблонів ботнетів. Це розкриває заражених користувачів та запобігає виходу даних з вашої корпорації.

### ***URL Filtering***

Повністю інтегрована база даних фільтрації URL дозволяє легше та ефективніше застосовувати політики для перегляду веб-сторінок, що доповнює політику з видимістю та контролем застосунків, яку надають брандмауери нового покоління на основі правил. Є можливість прив'язати видимість та контроль за фільтрацією URL до конкретних користувачів за допомогою прозорої інтеграції зі службами директорії підприємства, такими як Active Directory, LDAP та eDirectory. Ще більше інформації щодо фільтрації URL можна отримати, створюючи настроювані звіти та аналізуючи журнали.[2]

- Безпечно дозволяє використання вебу за допомогою тих самих механізмів контролю політик, які застосовуються до застосунків - дозволити, дозволити та сканувати, застосувати QoS, блокувати та інше.
- Зменшує випадки потрапляння у систему шкідливого програмного забезпечення, блокуючи доступ до відомих сайтів, що поширюють шкідливе програмне забезпечення та фішинг.[9]
- Створює білі списки (дозволити), чорні списки (блокувати) або налаштовує власних категорій та бази даних.
- Сприяє та допомагає налаштуванню політик розшифрування SSL. Наприклад, "не розшифровувати трафік до сайтів фінансових послуг", але "розшифровувати трафік до блогів".

### ***File and Data Filtering***

Засоби фільтрації даних в Content-ID дозволяють впроваджувати політики, що зменшують ризики, пов'язані з передачею несанкціонованих файлів та даних.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 35   |

- Блокування файлів за типом: Контролює потік різних типів файлів, проникаючи глибоко в тіло пакета, щоб визначити тип файлу (на відміну від перегляду лише розширення файлу).
- Фільтрація даних: Контролює передачу чутливих даних, таких як номери соціального страхування та кредитних карток, в змісті або вкладених додатків.
- Контроль функції передачі файлів: Контролює функцію передачі файлів у межах окремого застосунку, дозволяючи використання застосунку із запобіганням небажаної вхідної або вихідної передачі файлів.

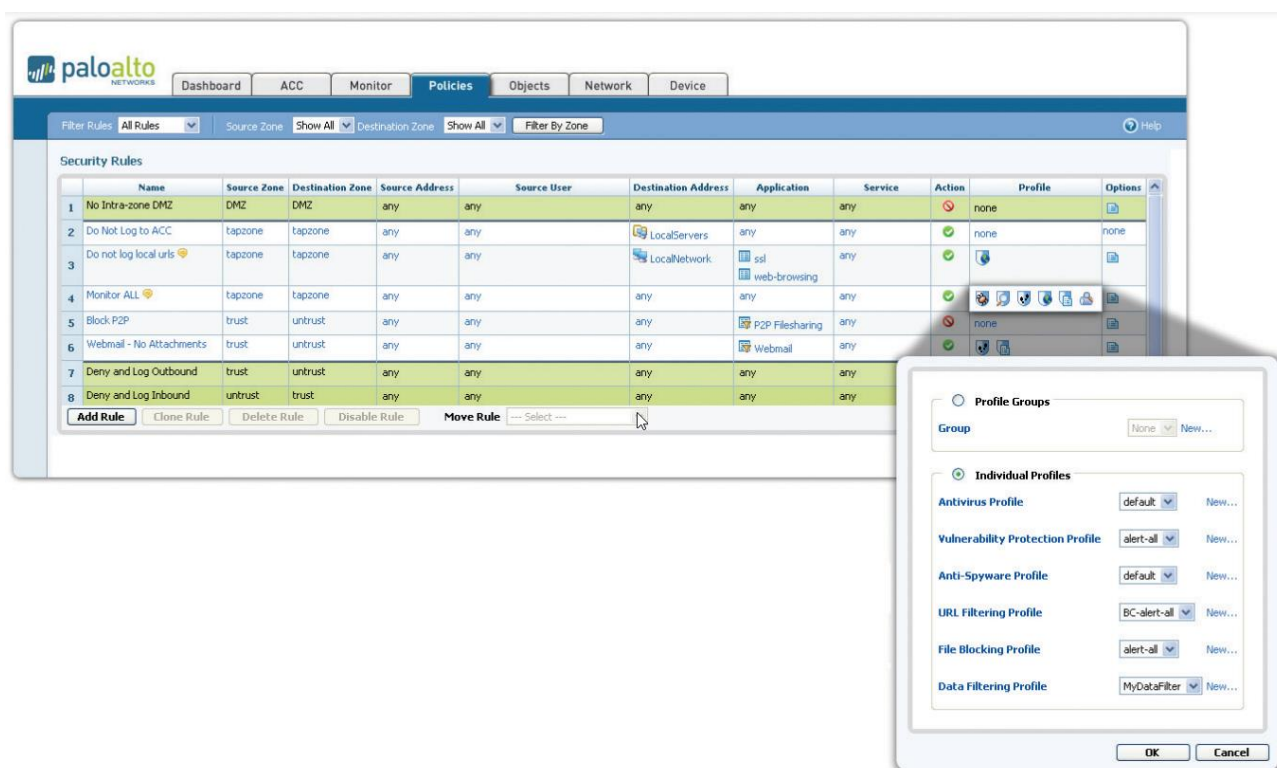


Рисунок 1.11 - Content-ID активується на основі правил за допомогою окремих або групових профілів, що сприяє політико-орієнтованому контролю над вмістом, що перетинає мережу

## Висновки до першого розділу

В цьому розділі розглянуто основні принципи побудови корпоративних мереж і описано різні типи корпоративних мереж, які використовуються в сучасних компаніях. Проаналізовано роботу та можливості мережевих екранів. Порівняно декілька сучасних брандмауерів нового покоління, таких як Barracuda

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 36   |

Firewall, Cisco ASA NGFW та Palo Alto Firewall. Кожен виробник ставить на перший план зручність використання своїх рішень, тому брандмауери надають інтуїтивно зрозумілі інструменти. Але Palo Alto відомий своєю високою масштабованістю, що дозволяє в майбутньому розширювати мережу та додавати нові об'єкти, не впливаючи на продуктивність.

Було досліджено застосування технології IPSec VPN у корпоративних мережах і порівняно її з SSL VPN забезпечення безпеки і приватності. Вони мають свої унікальні переваги і відповідають різним сценаріям використання. IPSec VPN хоч і має досить маленьку гнучкість, але через простоту налаштувань підходить більше.

Були описана технологія запобігання загрозам Content-ID, яка використовуються у брандмауерах Palo Alto Networks Firewall для захисту від загроз. Було пояснено її функції та роль у запобіганні компрометації мережі та захисту від шпигунського програмного забезпечення.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 37   |

## РОЗДІЛ 2 ПРОЄКТУВАННЯ АРХІТЕКТУРИ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ IPSEC VPN ТА МЕРЕЖЕВОГО ЕКРАНУВАННЯ

### 2.1. Аналіз створення та проектування захищеної мережі організації

На сьогоднішній день мережеві інтегратори реалізують проекти, керуючись власним розумінням ефективної організації роботи, і кожна компанія має свою унікальну методологію проектування. Однак, базуючись на західному досвіді, можна виділити загальні етапи реалізації мережевих проектів.

Перший етап - аналіз вимог. На цьому етапі визначаються основні бізнес-цілі підприємства, які повинні бути досягнуті проектом. Ці цілі можуть включати зменшення циклів виробництва, поліпшення ефективності обробки замовлень або підвищення продуктивності завдяки кращій співпраці співробітників. На цьому етапі проводиться дослідження подібних систем, їх аналіз і розгляд успішних досвідів для можливої інтеграції.

Другий етап - розробка технічної моделі. Технічна модель надає загальний опис комп'ютерного обладнання, необхідного для досягнення цілей, викладених у бізнес-моделі. Здійснюється інвентаризація наявного обладнання та встановлення вимог до нової системи, з урахуванням поглядів мережевих менеджерів та користувачів. На цьому етапі оцінюється сумісність наявного обладнання з новою системою, без зазначення конкретних брендів або моделей.

Третій етап - встановлення та налаштування системи. Здійснюється координація поставок від субпідрядників, управління завданнями налаштування, встановлення та налаштування обладнання, а також організація навчання персоналу.

Корпоративні мережі включають спеціалізовані програмні системи або комплекси, які відповідають потребам підприємств. Такі системи можуть включати автоматизацію проектування, управління технічним процесом, банківські системи, медичні діагностичні системи та інші.

У процесі роботи використовуються вищепоставлені програмні програми, але їх успішність залежить від роботи всіх інших підсистем в мережі.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 38   |

Корпоративні мережі охоплюють різні комп'ютери з різними конфігураціями. Можливості локальних мереж визначаються характеристиками комп'ютерів.

Після вибору технічної моделі важливо оцінити, наскільки вона відповідає вимогам виробництва. Проводиться перегляд бізнес-моделі і порівняння з технічними рішеннями. Вирівнювання між ними має важливе значення.

Наприклад, якщо потрібна висока мобільність співробітників, технічна модель повинна передбачати швидке і безперервне підключення та відключення робочих станцій.

Після забезпечення відповідності технічної моделі вимогам створюється фізична модель, яка надає детальний опис мережі, включаючи компоненти, їх кількості, розташування та взаємозв'язки.

Стосовно серверів, доступ до них може бути безкоштовним, дозволяючи користувачам отримувати ресурси веб-сервера без автентифікації за допомогою імені користувача та пароля. FTP-сервери та поштові сервери приймають пошту від подібних серверів. Проте, не можна гарантувати, що разом з поштою не буде доставлено шкідливий код або хтось не намагатиметься отримати несанкціонований доступ до мережі організації.

Якщо зловмиснику вдається отримати доступ принаймні до одного комп'ютера у локальній мережі, це дає йому можливість отримати паролі навіть до рівня адміністратора. Це відкриває доступ до всієї інформації, обмін якої та зберігання якої відбувається у мережі. Зловмисник також може змінювати паролі доступу таким чином, що бази даних стають недоступними або непридатними для використання. Ще одним ризиком є можливість отримання доступу до веб-сервера, який може бути використаний для запуску DoS-атак і призводити до порушення функціональності всіх внутрішніх ресурсів корпорації [6].

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 39   |

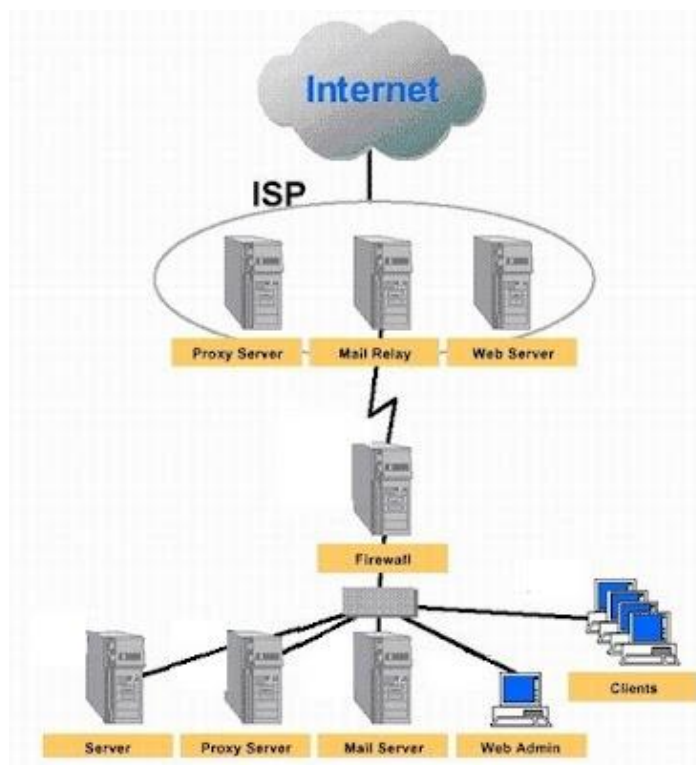


Рисунок 2.1 – Стандартна структура мережі невеликої компанії

При розробці архітектури корпоративної мережі з використанням зон і віртуальних локальних мереж (VLAN) необхідно провести детальне планування та налаштування інфраструктури мережі з метою забезпечення безпеки, масштабованості та ефективної передачі даних всередині організації.

Перший крок полягає у визначенні конкретних потреб і вимог організації під час проектування архітектури мережі. Це включає ідентифікацію відділів або груп користувачів, використовуваних сервісів та додатків, а також встановлення необхідного рівня безпеки.

Розбиття на зони дозволяє фізично або логічно розділити мережу на окремі сегменти, які можна керувати незалежно один від одного. Ці зони можуть бути налаштовані для різних цілей, таких як різні відділи, фізичні розташування або рівні безпеки. Кожна зона може мати власні мережеві пристрої, такі як комутатори і маршрутизатори, а також IP-підмережі. Наприклад, можна виділити зону "Центри обробки даних", "Маркетингу" або "Дослідний відділ".

Після визначення зон можна призначити IP-підмережі для кожної зони. Це дозволить контролювати комунікацію між зонами та встановлювати правила

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 40   |

доступу. Наприклад, IP-підмережа 200.168.10.0/24 може бути використана для зони "Центр обробки даних", а 10.0.2.0/24 - для "Маркетингу" і т.д.

VLAN - це логічні групи пристроїв у мережі, які можуть спілкуватися один з одним незалежно від фізичного розташування. Використання VLAN дозволяє поліпшити безпеку, масштабованість та керованість мережі. Комутатори можуть бути налаштовані для створення VLAN, а порти можуть бути призначені для підключення пристроїв до певних VLAN. Наприклад, можна створити VLAN "Гостьова мережа", "VoIP" або "Довідкова служба".

Після створення зон і VLAN можна призначити мережеві ресурси, такі як пропускну здатність, мережеві пристрої та сервіси, залежно від потреб організації. Це дозволить настроїти розподіл ресурсів, наприклад, виділити більше пропускну здатності для важливих зон або VLAN, що обробляють великі обсяги даних.

Це загальні вказівки та приклади корпоративної мережевої архітектури з використанням зон і VLAN. Фактична структура мережі буде залежати від унікальних потреб та розміру організації.

## **2.2 Розробка топології комп'ютерної мережі**

Ідея "ієрархії" має паралелі з динамікою, яку можна знайти у структурі сім'ї. Ієрархічний порядок дозволяє класифікувати об'єкти на різні рівні, вказуючи на зв'язки між конкретними об'єктами та завданнями, які вони виконують. Ієрархія служить для організації складних моделей та призначення різних ролей членам сім'ї.

Концепція ієрархії також знаходить застосування у дизайні мережі. Важливо класифікувати компоненти мережі на ієрархічні рівні залежно від їх функціональності. Зазвичай, після аналізу конкретного ієрархічного рівня, можна не звертати увагу на функції інших рівнів.

Сучасні мережі є складними через різноманітні конфігурації, протоколи та технології, що використовуються. Щоб створити керовану модель, яка охоплює всі компоненти, ієрархія стає цінним інструментом. Крім того, вона допомагає

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 41   |

визначити характерні особливості кожного ієрархічного рівня. Ієрархічна модель Cisco сприяє створенню, експлуатації та підтримці масштабованих, ефективних та надійних єдинообрахункових мереж. Cisco ідентифікувала три ієрархічні рівні, кожен з яких відведений певним мережевим операціям.[6]

У межах цієї моделі визначені наступні три рівні.

**Ядро мережі.** Цей рівень є основою мережі і забезпечує надійний та швидкий обмін великими обсягами трафіку. Його основне завдання - швидке перемикання трафіку. На рівні ядра трафік розподіляється між кількома користувачами, а користувацькі дані обробляються на розподільному рівні, що може призвести до додаткових запитів до рівня ядра.

**Рівень розподілу.** Також відомий як "рівень робочої групи", він розташовується між рівнями ядра та доступу. Рівень розподілу виконує маршрутизацію, фільтрацію та надає доступ до регіональних мереж. Він також визначає правила доступу до пакетів на рівень ядра, коли це необхідно. Основні цілі на рівні розподілу включають визначення найоптимальнішого підходу до обробки службових запитів. Після визначення оптимального шляху доступу на рівні розподілу запит пересилається на рівень ядра, де швидкий транспорт до призначеної служби здійснюється. Рівень розподілу встановлює політики мережі та надає гнучкі описи роботи мережі. Основні функції, які виконуються на рівні розподілу, включають:

- Перерозподіл маршрутів у протоколах маршрутизації, включаючи статичні маршрути.
- Розробка систем безпеки та політик мережі, таких як налаштування брандмауера та переклад адрес.
- Маршрутизація VLAN та інші функції, які підтримують робочі групи.
- Створення мультикастових та широкомовних доменів.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 42   |

- Розробка або впровадження інструментів, аналогічних спискам доступу, механізмам фільтрації або керуванню пакетами вхідного/вихідного потоку.

**Рівень доступу.** Цей рівень спрямований на керування робочими групами та користувачами під час доступу до ресурсів у єдинообрахунковій мережі. Для забезпечення плавної та безперебійної роботи більшість необхідних мережевих ресурсів повинні бути доступними користувачам мережі на місці. Перенаправлення трафіку до віддалених служб відбувається на рівні доступу. Рівень доступу вирішує такі завдання:

- Сегментація.
- Встановлення зв'язку між робочими групами та рівнем розподілу.
- Постійний контроль доступу та накладення політик через рівень розподілу.

Важливо уникати виконання функцій, що є характерними для ядра та рівня розподілу, на самому рівні розподілу.

Нижче представлена загальна структура корпоративної мережі:

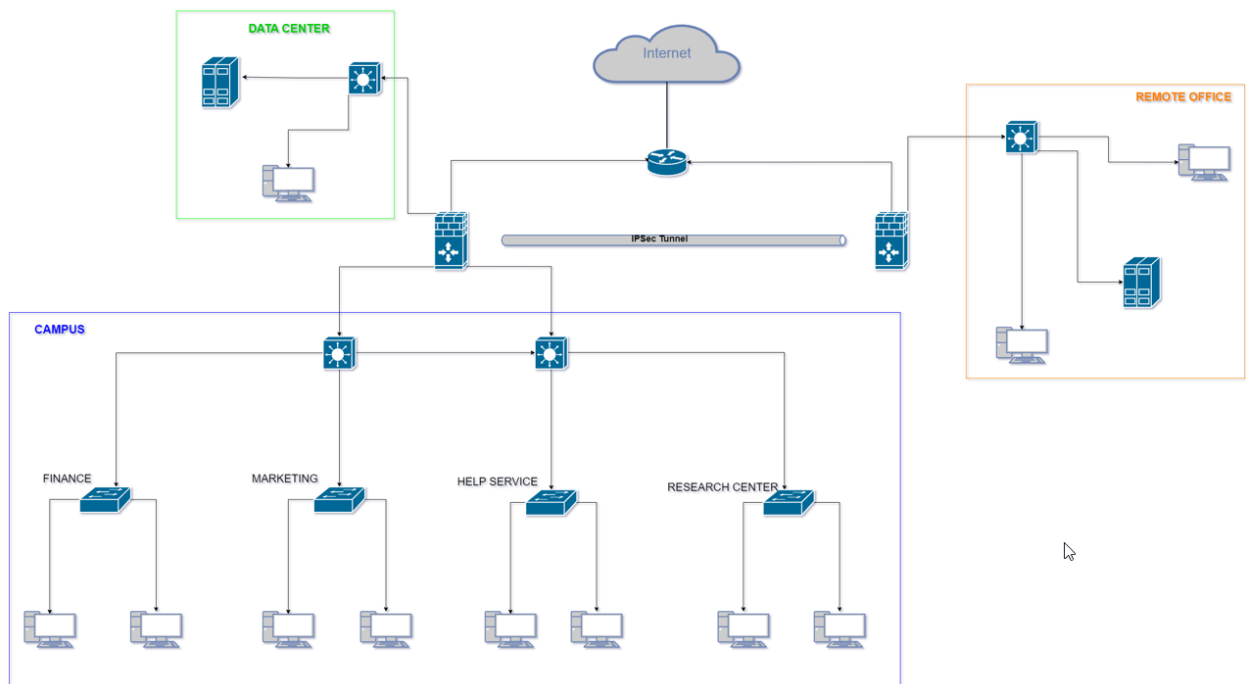


Рисунок 2.2 - Структурна схема корпоративної мережі організації

Мережа корпоративного містечка складається з рівня доступу, розподілу та ядра. Центр обробки даних складається з комутатора Cisco рівня 3 і сервера. Конструкція DC дуже спрощена, оскільки рівні мережі стиснуті до одного комутатора рівня 3. На відміну від мережі кампусу, метою є показати конфігурацію служб, що працюють на Server, замість того, щоб обговорювати повний дизайн DC. Брандмауер Palo Alto Networks Firewall компанії підключено до Інтернету за допомогою Інтернет-провайдера (ISP) та з'єднує мережу кампусу, центр обробки даних і по IPSec тунелю підтримує зв'язок з віддаленим офісом. У віддаленому офісі інший брандмауер Palo Alto приймає цей трафік на себе. Він також захищає віддалену мережу від несанкційного доступу. Підприємство підключено до маршрутизатора ISP через мережевий екран підприємства.

#### DC-DATA CENTER

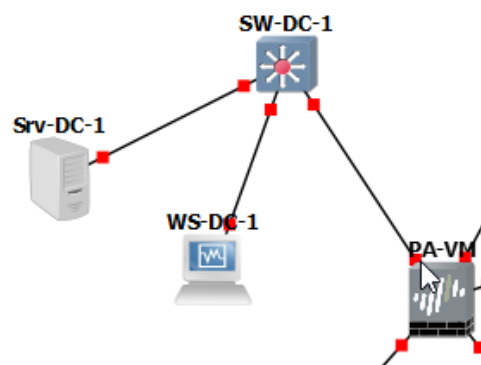


Рисунок 2.3 – Підмережа Data Center підключена до граничного Palo Alto

DC складається з трьох пристроїв – SRV-191-1, комутатора SW-DC-1 та робочої станції адміністратора WS-DC-1. Звичайно, мережа з одним комутатором і сервером далека від будь-якої відомої конструкції мережі DC. Як правило, сучасні горизонтально масштабовані великогабаритні DC 3-го рівня складаються з тисяч серверів, підключених до комутаторів Top of Rack (ToR) L3, і вони дотримуються листової та хребтової конструкції. DC такого розміру навряд чи можна емулювати на одному ПК. З цієї причини я надаю лише конфігурацію комутатора Cisco L3, який розташований у нашому DC.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 44   |

Перемикач SW-DC-1 підключає Windows Server до мережі DC. Конфігурація таких служб, як з'єднання Syslog-ng, Active Directory, Netflow, які працюють на сервері, пояснюється більш детально пізніше.

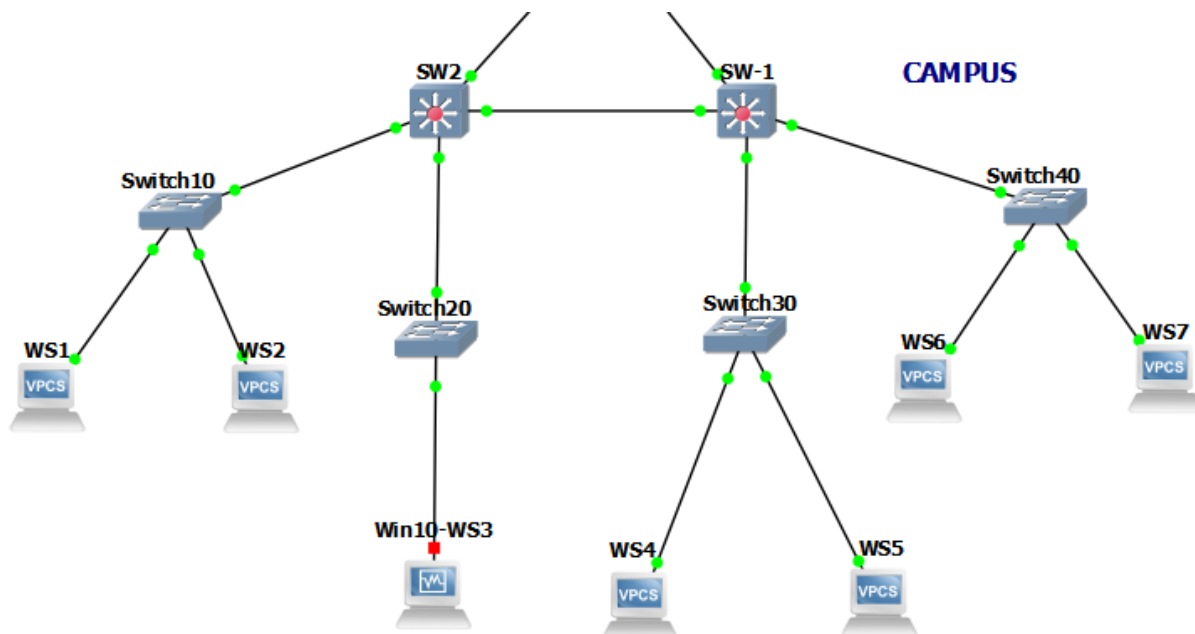


Рисунок 2.4 - Підмережа Campus з чотирма відділами

Розподіл в мережі кампусу перемикає маршрут трафіку між кінцевими користувачами VLAN, і вони підключають мережу нижчого рівня до основного рівня. Інтерфейси рівня 3 (маршрутизовані) з'єднують 4 комутатори розподілу і з брандмауером Core. Інтерфейси до рівня доступу є рівнем 2 (порти комутаторів). Протокол маршрутизації OSPF працює на розподільних комутаторах, тому між розподільним і основним рівнем існує лише зв'язок ІЗ.

Одним з найважливіших етапів під час проектування топології є розробка схеми адресації мережі для уникнення дублікатів адрес та можливих проблем в функціонуванні мережі.

Під час розробки схеми адресації, увагу було звернено в першу чергу на оптимальну кількість IP-адрес, не забуваючи про можливість розширення поточних мереж.

Налаштований інтерфейс WAN з IP мережою 172.31.104.0/28 з одної сторони, та з іншої сторони 173.31.104.0/28 аналогічно.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 45   |

Існує високошвидкісний тунель для зв'язку з віддаленим офісом по IPsec VPN. Його мережа 172.16.4.0/30, яка в майбутньому може контролюватись та перевірятись на загрози чи швидкість передачі пакетів.

Більш детального огляду потребує розрахунок IP-адрес локальних мереж. Результати розрахунків подано у вигляді таблиць 2.1 – 2.5.

Таблиця 2.1 – Адресація підмережі Finance 10

| Призначення                 | IP-адреса                   |
|-----------------------------|-----------------------------|
| Адреса мережі               | 192.168.10.0                |
| Маска мережі                | 255.255.255.0 /24           |
| Інвертована маска           | 0.0.0.255                   |
| Мінімальна адреса           | 192.168.10.1                |
| Максимальна адреса          | 192.168.10.254              |
| Широкомовна адреса          | 192.168.10.255              |
| Шлюз по замовчуванню        | 192.168.10.1                |
| Діапазон статичних адрес    | 192.168.10.0 - 192.168.10.4 |
| Діапазон адрес майбутніх ПК | DHCP                        |

Таблиця 2.2 – Адресація підмережі Marketing 20

| Призначення                 | IP-адреса                   |
|-----------------------------|-----------------------------|
| Адреса мережі               | 192.168.20.0                |
| Маска мережі                | 255.255.255.0 /24           |
| Інвертована маска           | 0.0.0.255                   |
| Мінімальна адреса           | 192.168.20.1                |
| Максимальна адреса          | 192.168.20.254              |
| Широкомовна адреса          | 192.168.20.255              |
| Шлюз по замовчуванню        | 192.168.20.1                |
| Діапазон статичних адрес    | 192.168.20.0 - 192.168.20.4 |
| Діапазон адрес майбутніх ПК | DHCP                        |

Таблиця 2.3 – Адресація підмережі Help Service 30

| Призначення                 | IP-адреса                   |
|-----------------------------|-----------------------------|
| Адреса мережі               | 192.168.30.0                |
| Маска мережі                | 255.255.255.0 /24           |
| Інвертована маска           | 0.0.0.255                   |
| Мінімальна адреса           | 192.168.30.1                |
| Максимальна адреса          | 192.168.30.254              |
| Широкомовна адреса          | 192.168.30.255              |
| Шлюз по замовчуванню        | 192.168.30.1                |
| Діапазон статичних адрес    | 192.168.30.0 - 192.168.30.4 |
| Діапазон адрес майбутніх ПК | DHCP                        |

Таблиця 2.4 – Адресація підмережі Research center 40

| Призначення                 | IP-адреса                   |
|-----------------------------|-----------------------------|
| Адреса мережі               | 192.168.40.0                |
| Маска мережі                | 255.255.255.0 /24           |
| Інвертована маска           | 0.0.0.255                   |
| Мінімальна адреса           | 192.168.40.1                |
| Максимальна адреса          | 192.168.40.254              |
| Широкомовна адреса          | 192.168.40.255              |
| Шлюз по замовчуванню        | 192.168.40.1                |
| Діапазон статичних адрес    | 192.168.40.0 – 192.168.40.4 |
| Діапазон адрес майбутніх ПК | DHCP                        |

Таблиця 2.5 – Адресація підмережі DC

| Призначення       | IP-адреса           |
|-------------------|---------------------|
| Адреса мережі     | 200.168.10.0        |
| Маска мережі      | 255.255.255.240 /28 |
| Інвертована маска | 0.0.0.15            |

Продовження таблиці 2.5 – Адресація підмережі DC

|                             |                             |
|-----------------------------|-----------------------------|
| Мінімальна адреса           | 200.168.10.1                |
| Максимальна адреса          | 200.168.10.14               |
| Широкомовна адреса          | 200.168.10.15               |
| Шлюз по замовчуванню        | 200.168.10.1                |
| Діапазон статичних адрес    | 200.168.10.1 - 200.168.10.3 |
| Діапазон адрес майбутніх ПК | DHCP                        |

Таблиця 2.6 – Адресація підмережі Remote Office

| Призначення                 | IP-адреса             |
|-----------------------------|-----------------------|
| Адреса мережі               | 120.5.5.0             |
| Маска мережі                | 255.255.255.128 /25   |
| Інвертована маска           | 0.0.0.127             |
| Мінімальна адреса           | 120.5.5.1             |
| Максимальна адреса          | 120.5.5.126           |
| Широкомовна адреса          | 120.5.5.127           |
| Шлюз по замовчуванню        | 120.5.5.1             |
| Діапазон статичних адрес    | 120.5.5.1 - 120.5.5.2 |
| Діапазон адрес майбутніх ПК | DHCP                  |

### 2.3 Програмне забезпечення для проектування GNS3 (Graphical Network Simulator 3)

GNS3 - безкоштовний графічний симулятор мережі, що дозволяє створювати віртуальні мережі з маршрутизаторів і віртуальних машин. Цей інструмент є надійним для навчання та тестування, підтримує більшість платформ і особливо підходить для створення лабораторій на робочих станціях.

За допомогою GNS3 можна розробляти складні проекти з використанням маршрутизаторів Cisco, Cisco ASA, Juniper та серверів, що працюють під управлінням мережевих операційних систем. У випадках, коли доступ до

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 48   |

фізичного обладнання обмежений, GNS3 може виконувати функції повноцінної лабораторії. Крім того, лабораторні роботи, проведені в GNS3, можуть доповнювати практичне навчання, яке відбувається у фізичних лабораторіях, особливо для студентів, які готуються до сертифікаційних іспитів CCNA/CCNP і CCIE.

Один з недоліків цього програмного забезпечення полягає у обмежених можливостях повноцінної симуляції комутаторів Layer 2 Cisco. Це обмеження не буде виправлено в майбутніх версіях через фундаментальні різниці між апаратними платформами маршрутизаторів і комутаторів. Однак цю обмеженість можна частково подолати за допомогою мережевого модуля NM-16ESW. Хоча список команд може трохи відрізнятись при використанні NM-16ESW порівняно з реальними комутаторами Cisco, він все ще виконує свою основну функцію сприяння процесу навчання.[18]

GNS3 не включає в себе образи PIX/IOS/ASA/IPS/JunOS, оскільки вони належать комерційним продуктам відповідних компаній і не мають прямого зв'язку з проектом GNS3. Проте, отримання необхідного образу тепер не є проблемою.

Однією з найцікавіших можливостей GNS3 є підключення розробленої мережевої топології до реальної мережі, що надає унікальну можливість тестувати будь-який проект у практичних умовах, не використовуючи фізичне обладнання.

Використання програми Wireshark дозволяє моніторити трафік у розробленій мережевій топології і надає додаткову інформацію для кращого розуміння вивчених технологій. Наразі доступні версії GNS3 для MS Windows XP і Windows 7-11+, Linux, а також macOS. Основною перевагою GNS3 є його легкість та зручність у створенні проектів для проведення лабораторних робіт. Встановлення програми не вимагає значного початкового налаштування і може бути завершено всього за кілька хвилин.[18]

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 49   |

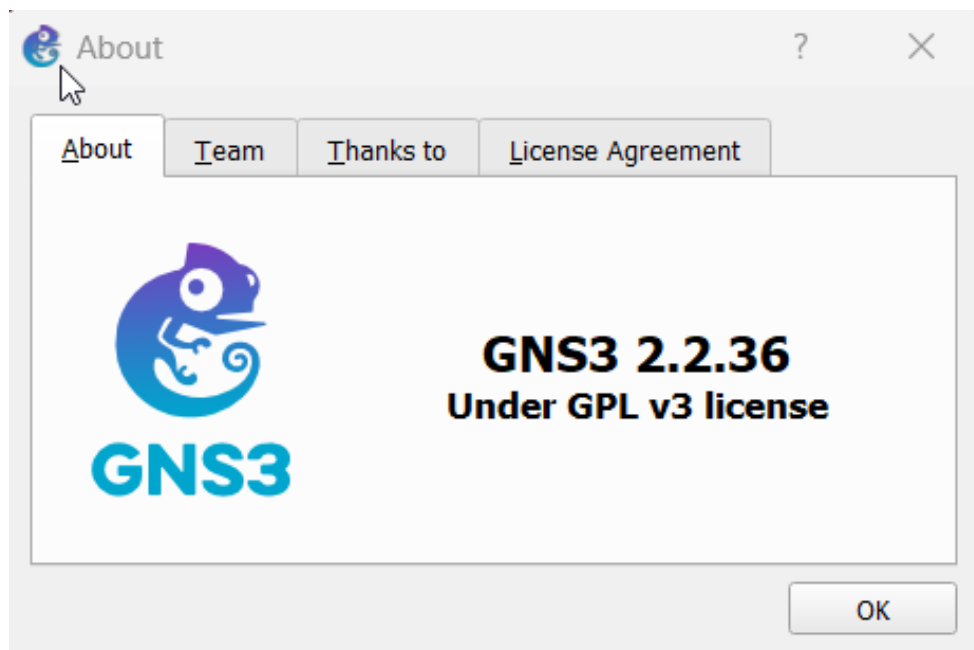


Рисунок 2.5 Graphical Network Simulator 3

### Висновки до другого розділу

В розділі було проаналізовано етапи створення корпоративних мереж для підприємства. Зазначено рекомендації щодо архітектури та захисту із виходом в мережу Інтернет, і керуванням трафіку з нього.

Крім того, було розглянуто розробку топології комп'ютерної мережі, що відповідає вимогам організації. Враховуючи потреби організації, було запропоновано оптимальну топологію мережі, яка включає різні типи мережевих пристроїв та забезпечує ефективний обмін даними між внутрішніми департаментами. Також досліджено швидку взаємодію з віддаленим офісом, до якого буде застосована технологія IPSec VPN для безпечного з'єднання.

Було вирішено використовувати програмне забезпечення GNS3 для виконання симуляції мережі. GNS3 надає можливість моделювання та тестування різних мережевих конфігурацій без реального обладнання. Це дозволить перевірити працездатність та ефективність розробленої топології мережі до її впровадження.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 50   |

## РОЗДІЛ 3 АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОРПОРАТИВНОЇ МЕРЕЖІ, РОЗРОБКА ТА ДОСЛІДЖЕННЯ РОБОТИ ЗАХИЩЕНОЇ МЕРЕЖІ

### 3.1 Вибір обладнання для організації роботи мережі

Мережеве устаткування складається з основних пристроїв, необхідних для операцій комп'ютерної мережі, таких як маршрутизатори, комутатори, концентратори, патч-панелі та інші компоненти. Зазвичай, виокремлюють активне та пасивне мережеве устаткування.

Коли ми згадуємо про "активне мережеве устаткування", маємо на увазі певні "інтелектуальні" можливості, які характерні для мережевих пристроїв, таких як маршрутизатори, комутатори та подібні пристрої.

В даній кваліфікаційній роботі необхідно обрати брандмауер, комутатори та маршрутизатор.

При виборі комутаторів 3 рівня потрібно врахувати такі параметри: наявність необхідної кількості портів витої пари, підтримка технологій FastEthernet, підтримка протоколів маршрутизації, захисту та прикладного рівня. З урахуванням вище описаних умов, я обрав брандмауери серії Palo Alto Networks. Сімейства моделей брандмауерів наступного покоління включають Palo Alto Networks серії PA-4000 і PA-2000, а також нещодавно випущений PA-500 з пропускнуою здатністю від 250 Мбіт/с до 10 Гбіт/с. Брандмауери наступного покоління Palo Alto Networks побудовані на потужній мережевій основі, пропонують знайомий інтерфейс керування політиками та пропонують безпрецедентні функції для вашої інфраструктури безпеки.[9]

Брандмауери нового покоління Palo Alto Networks PA-1400 серії ML-Powered, що включають PA-1420 і PA-1410, розроблені для забезпечення безпечного підключення для філій організацій, а також підприємств середнього розміру.

Серія пристроїв PA-1400 працює під управлінням ПЗ PAN-OS, яке є тим самим програмним забезпеченням, що використовується для управління мережами NGFW компанії Palo Alto Networks. PAN-OS проводить початкову

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 51   |

класифікацію усього потоку даних, включаючи програми, можливі загрози та контент. Потім він асоціює цей потік даних з відповідним користувачем, незалежно від його місцезнаходження або типу пристрою. Ці складові, а саме програми, контент та користувачі, є основою для створення політики безпеки вашого бізнесу. Такий підхід сприяє покращенню загального рівня безпеки і зменшенню часу реагування на інциденти.[9]



Рисунок 3.1 – Брандмауер Palo Alto Networks PA-1420

Основні особливості:

- Перший у світі NGFW з технологією ML
- Одинадцятиразовий лідер у Magic Quadrant Gartner для мережевих брандмауерів
- Лідер хвилі Forrester: брандмауери для підприємств, 4 квартал 2022 р
- Забезпечує передбачувану продуктивність із службами безпеки
- Спрощує розгортання великої кількості брандмауерів із додатковим Zero Touch Provisioning (ZTP)
- Вбудована підтримка веб-проксі в NGFW для спрощення та консолідації керування брандмауером і функціями проксі
- Підтримує централізоване адміністрування з керуванням безпекою мережі Panorama
- Розширює видимість і безпеку для всіх пристроїв, включаючи некеровані пристрої IoT, без необхідності розгортання додаткових датчиків
- Підтримує високу доступність з активним/активним і активним/пасивним режимами
- Максимізує інвестиції в безпеку та запобігає перебоям у роботі з AIOps

Я прийняв рішення вибрати тип маршрутизатора компанії Cisco 7200 серії, даний маршрутизатор повністю задовольняє вище описані умови, має усі

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 52   |

необхідні порти за рахунок встановлення модулів, підтримує усі необхідні протоколи та технології. Маршрутизатори Cisco 7200 – це обладнання провайдерського класу для інтернет-трафіку зі швидкістю до 2 мільйонів пакетів в секунду. Завдяки модульній архітектурі ці маршрутизатори дозволяють створювати масштабовані рішення, що відповідають різним вимогам до щільності, продуктивності та асортименту послуг, одночасно забезпечуючи захист інвестицій з урахуванням майбутнього розвитку мережі.

Пристрої Cisco 7200 серії підтримують великий вибір модулів розширення для створення різних конфігурацій, включаючи швидкісні модулі маршрутизації (NPE-G2 Network Processing Engine), модулі інтерфейсні PA та інші.

До переваг модульних маршрутизаторів Cisco 7200 серії можна віднести апаратну підтримку VPN-шифрування (VPN Services Adapter), підтримка інтерфейсів від DS0 до OC-3, а також Fast Ethernet, Gigabit Ethernet, Packet over SONET, надлишковість та стійкість до відмов. Також, маршрутизатори Cisco 7200 серії підтримують QoS (quality of service), MPLS, IPSec (до 5000 тунелів на шасі) та передача голосу, відео та даних.



Рисунок 3.2 – Маршрутизатор Cisco 7206VXR/NPE-G1

Спільно з чіпами Cisco 7200 NPE-G2 створюється мережева платформа, здатна не тільки швидко передавати дані, але й справлятися із завантаженістю на каналах передачі. У разі включається магістральна передача інформації, що допомагає відправити надлишок пакетів протягом короткого періоду. Якщо врахувати, скільки пакетів відправляється за секунду, можна зрозуміти, що це

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 53   |

продукт повністю виправдовує вкладені інвестиції. Залежно від складності проектів, адміністратор може сам підбирати прийнятний виконання завдань інтерфейс. Початковий рівень завдання використовуватиме інтерфейс DS 0, а в міру розвитку користувач сам повинен підбирати відповідний варіант роботи. Сімейство маршрутизаторів Series 7200 підтримує термінацію PPP та L 2 TP, а також 16 тисяч абонентських сесій.[9]

Технічні характеристики маршрутизатора подано у табл. 3.1.

Таблиця 3.1 – Характеристики маршрутизатора

|                                     |                                                        |
|-------------------------------------|--------------------------------------------------------|
| Виробник:                           | Cisco                                                  |
| Ідентифікатор продукту:             | 7206VXR/NPE-G1                                         |
| Опис продукту:                      | 7206VXR with NPE-G1 включає 3GigE/FE/E Ports and IP SW |
| Тип продукту:                       | Маршрутизатор                                          |
| Загальна кількість портів:          | 3                                                      |
| Кількість мережевих портів (RJ-45): | 3                                                      |
| Кількість слотів для розширення:    | 9                                                      |
| Тип слоту розширення:               | Порт-адаптер                                           |
| Мережева технологія:                | 10/100/1000Base-T                                      |
| Технологія Ethernet:                | Gigabit Ethernet                                       |
| Стандартна пам'ять:                 | 256 MB                                                 |
| Максимальна пам'ять:                | 1 GB                                                   |
| Технологія пам'яті:                 | SDRAM                                                  |
| Вхідна напруга:                     | 110 V AC                                               |
|                                     | 220 V AC                                               |
| Сумісна розмірність шафи:           | 3U                                                     |
| Форм-фактор:                        | Монтаж в шафу                                          |
| Висота:                             | 5.3"                                                   |
| Ширина:                             | 16.8"                                                  |
| Глибина:                            | 17"                                                    |
| Вага (приблизна):                   | 50 фунтів                                              |

Основним критерієм вибору моделей комутаторів є кількість портів. Також враховується швидкість передачі цих портів. У нашій мережі використовуються всі комутатори на 24 порти. Найбільш оптимальним є комутатор фірми Cisco, а саме Cisco Systems WS-C2960-24TT, рисунок 3.2.



Рисунок 3.3 – Cisco Systems WS-C2960-24TT

Компанія Cisco розробила мережеве обладнання, що підтримує передачу найпопулярніших типів інформації, в тому числі відео та голосу. Її продукти серії Catalyst 2960 Switch відповідають сучасним нормам і використовуються багатьма компаніями як засіб для передачі всіх типів інформації. Дане обладнання підтримує масштабування своїх функцій під безперервно зростаюче підприємство [10].

Комутатори Cisco Catalyst серії 2960 мають інтерфейс, простий для користувача. Для першого налаштування використовується пакет утиліт під назвою Cisco Network Assistant, воно допоможе налаштувати робоче середовище, зробить його більш продуктивним та швидкодіючим.

Cisco Catalyst 2960 можуть використовуватись в різних типах зв'язку, наприклад, як провідна мережа, так і бездротова, саме тому ці продукти отримали таке широке поширення.

Комутаторам серії Cisco 2960 надані свої обчислювальні можливості. Користувачеві в першу чергу необхідно вказати темпи, а також важливі пріоритети, тип передачі інформації і швидкість виконання всіх операцій. Звичайно, при виконанні складних завдань продуктивність даних комутаторів може скорочуватися, але за рахунок впроваджених технологій система швидко справляється з великим навантаженням.[11]

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 55   |

Комутатори Cisco Catalyst серії 2960 легко і надійно захищають робоче середовище. Користувачеві необхідно використовувати функцію доступу по пароллю, після чого проникнення з боку незареєстрованих користувачів буде виключено. Окрім цього, є функція відновлення (backup) інформації після позаштатних випадків.

Комутатори у цій лінійці продуктів мають кілька характеристик. Вони дозволяють регулювати швидкість передачі на кожному порту з точністю 64 Кбіт/с. Також вони підтримують об'єднання портів для створення швидких з'єднань між комутаторами та серверами. Більше того, можна встановити транкові з'єднання на кожному порту за допомогою тегів 802.1q.

Більшість комутаторів серії Cisco Catalyst 2960 не мають можливості маршрутизації. Але вони можуть фільтрувати трафік на основі інформації 3-го рівня (IP).

Крім цього, на рівні розподілу, маршрутизацією займаються багаторівневі комутатори Cisco Catalyst 3650 (рис. 3.4).



Рисунок 3.4 – Комутатор серії Cisco Catalyst 3650

Комутатори Cisco Catalyst 3650 є стековими пристроями, спеціально розробленими для злитого доступу. Вони мають фіксовану конфігурацію і вбудований контролер ASIC для бездротового зв'язку. Ці комутатори працюють на операційній системі IOS XE з модульною архітектурою. Аналогічні ASIC використовуються в платформах Catalyst 3850 та Supervisor 8-E для Catalyst 4500-E. Комутатори Cisco Catalyst 3650 забезпечують політики безпеки та якості обслуговування (QoS) як для проводового, так і для бездротового клієнтського трафіку. Вони також надають можливості моніторингу та оптимізації трафіку корпоративної мережі. Основні особливості моделей Catalyst 3650 включають фіксовану конфігурацію з 24 або 48 портами 10/100/1000 з підтримкою PoE+ (до 30 Вт на порт), вбудовані високошвидкісні канали: 4 x Gigabit Ethernet, 2 x 10

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 56   |

Gigabit Ethernet або 4 x 10 Gigabit Ethernet з можливістю використання трансиверів SFP і SFP+. Ці комутатори мають можливість підключення до 2-х резервних джерел живлення змінного струму різної потужності і оснащені 3 вентиляторами для охолодження. Крім того, Catalyst 3650 підтримує стекування StackWise, що дозволяє об'єднувати до 9 пристроїв в стек за допомогою додаткових модулів з пропускною здатністю 160 Гбіт/с. Він також має технологію Stateful Switch Over (SSO) і бездротову пропускну здатність 40 Гбіт/с на основі ASIC Unified Access Data Plane (UADP). Комутатори працюють на операційній системі IOS XE і підтримують до 25 точок доступу та 1000 бездротових клієнтів на один комутатор Catalyst 3650 або стек StackWise.

### 3.2 Налаштування обладнання мережі організації

Брандмауери Palo Alto Networks засновані на зоні. Для того, щоб трафік проходив, для розгортання потрібно впровадити зони безпеки. Ці зони діють як логічний спосіб групування фізичних і віртуальних інтерфейсів. Зони також потрібні для контролю та реєстрації трафіку, який проходить через інтерфейси. Інтерфейс має бути того самого типу, що й зона, якій він призначений (TAP, Virtual Wire, Layer 2 або Layer 3). Щоб пропускати трафік через інтерфейс, він повинен бути призначений зоні. Зоні може бути призначено кілька інтерфейсів одного типу, але інтерфейс може належати лише одній зоні.

Усі сеанси брандмауера визначаються зонами джерела та призначення. Правила можуть використовувати ці визначені зони, щоб дозволити або заборонити трафік, застосувати QoS або виконати NAT. Весь трафік може вільно проходити в межах зони, яка називається внутрішньозонним трафіком. Трафік між зонами (міжзоновий трафік) за замовчуванням заборонено. Трафік буде дозволений лише між зонами, якщо визначено правило безпеки, яке відповідає всім умовам сеансу. Для міжзонального трафіку правила політики безпеки мають посилатися на зону джерела та зону призначення (не інтерфейси), щоб дозволити або заборонити трафік.[9]

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 57   |

Існує три вимоги до налаштування інтерфейсів рівня 3 на брандмауері PAN:

- 1) Налаштувати зону безпеки (подібно до Cisco ZBF)
- 2) Налаштувати віртуальний маршрутизатор (подібний до Cisco VRF)
- 3) Налаштувати інтерфейс (прив'язати зону безпеки, віртуальний маршрутизатор і IP-адресу).

Щоб додати нову зону, потрібно клацнути «Додати» (із символом «+» нижче) > ввести назву зони > вибрати «Тип» у спадному меню (у цьому випадку — «Рівень 3»).

Я створив Inside, DC(Data Center), Outside, які є інтерфейсами рівня 3 і дозволять функціонувати маршрутизації та NAT. А також створив зону VPN, щоб помістити туди тунелі IPSec VPN та в майбутньому керувати трафіком, спостерігати за ним. У разі несправності, можна легко знайти, в чому проблема, та виправити помилку.

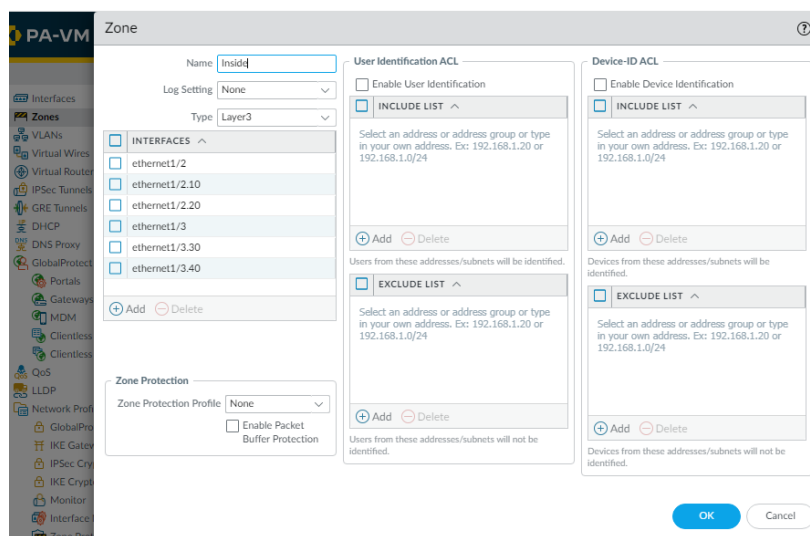


Рисунок 3.5 - Створення зони безпеки та додавання інтерфейсу до нього

PA-VM

DASHBOARD

MONITOR

POLICIES

OBJECTS

NETWORK

DEVICE

Commit

Interfaces

Zones

VLANs

Virtual Wires

Virtual Routers

IPSec Tunnels

GRE Tunnels

DHCP

DNS Proxy

GlobalProtect

Portals

Gateways

MDM

Clientless Ap

VPN

4 Items

|                          |         |        | INTERFACES /<br>VIRTUAL<br>SYSTEMS | ZONE<br>PROTECT...<br>PROFILE | PACKET<br>BUFFER<br>PROTECT... | LOG<br>SETTING | User-ID                             |                        |                        | Device-ID                |                        |                        |
|--------------------------|---------|--------|------------------------------------|-------------------------------|--------------------------------|----------------|-------------------------------------|------------------------|------------------------|--------------------------|------------------------|------------------------|
|                          | NAME    | TYPE   |                                    |                               |                                |                | ENABLED                             | INCLUDED<br>NETWORK... | EXCLUDED<br>NETWORK... | ENABLED                  | INCLUDED<br>NETWORK... | EXCLUDED<br>NETWORK... |
| <input type="checkbox"/> | DC      | layer3 | ethernet1/5                        |                               | <input type="checkbox"/>       |                | <input checked="" type="checkbox"/> | any                    | none                   | <input type="checkbox"/> | any                    | none                   |
| <input type="checkbox"/> | Inside  | layer3 | ethernet1/3                        |                               | <input type="checkbox"/>       |                | <input type="checkbox"/>            | any                    | none                   | <input type="checkbox"/> | any                    | none                   |
|                          |         |        | ethernet1/2                        |                               |                                |                |                                     |                        |                        |                          |                        |                        |
|                          |         |        | ethernet1/2.10                     |                               |                                |                |                                     |                        |                        |                          |                        |                        |
|                          |         |        | ethernet1/2.20                     |                               |                                |                |                                     |                        |                        |                          |                        |                        |
|                          |         |        | ethernet1/3.20                     |                               |                                |                |                                     |                        |                        |                          |                        |                        |
|                          |         |        | ethernet1/3.40                     |                               |                                |                |                                     |                        |                        |                          |                        |                        |
| <input type="checkbox"/> | Outside | layer3 | ethernet1/1                        |                               | <input type="checkbox"/>       |                | <input type="checkbox"/>            | any                    | none                   | <input type="checkbox"/> | any                    | none                   |
| <input type="checkbox"/> | VPN     | layer3 | tunnel                             |                               | <input type="checkbox"/>       |                | <input type="checkbox"/>            | any                    | none                   | <input type="checkbox"/> | any                    | none                   |

Рисунок 3.6 – Створені зони на брандмауері PA-VM

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 58   |

Також аналогічно було створено зони на віддаленому мережевому екрані Remote Office. Тут створена також зона VPN для зручності, а також присутні зони Remote та Outside.

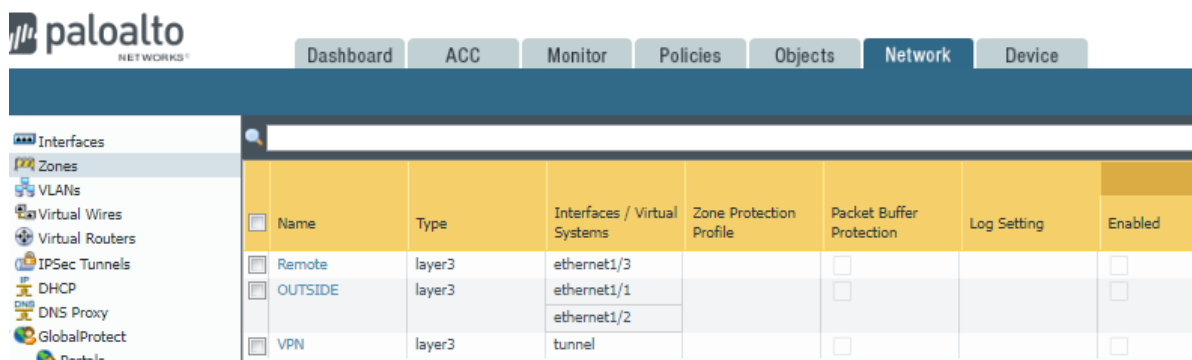


Рисунок 3.7 – Створені зони на брандмауері PA-VM-Remote

Щоб додати новий віртуальний маршрутизатор, потрібно перейти до Мережа > Віртуальні маршрутизатори > Додати > ввести назву віртуального маршрутизатора (у цьому випадку default).

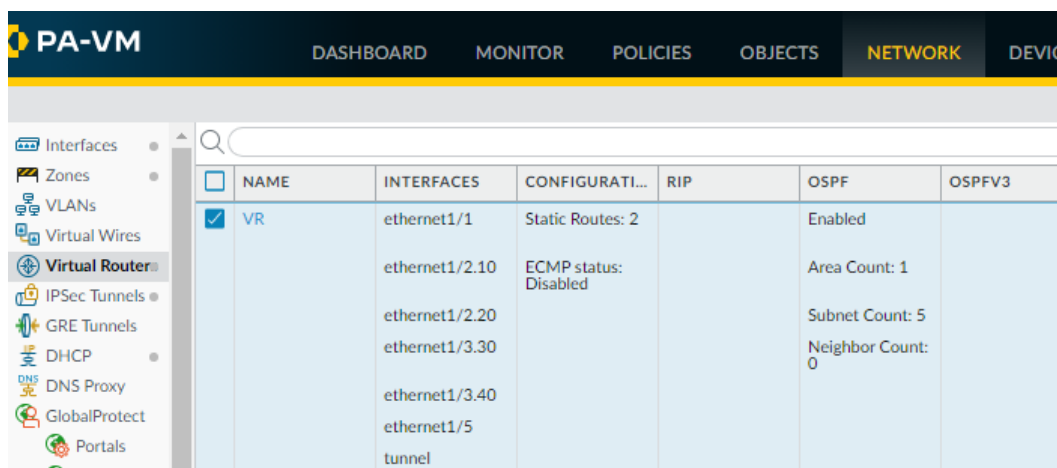


Рисунок 3.8 – Створення віртуального маршрутизатора з відповідними протоколами

Щоб налаштувати інтерфейси рівня 3 на брандмауері PAN на основі топології, потрібно перейти до Мережа > Інтерфейси > натиснути ethernet1/1 (Outside). Вибрати Рівень 3 у розділі Тип інтерфейсу. Вибрати Outside, створений раніше в зоні безпеки.

Перейти на вкладку IPv4 > вибрати «Статичний» > поставити прапорець «IP» > ввести IP-адресу/маску мережі (у цьому випадку 172.31.104.2/28) >

натиснути ОК. Також можна змінити параметри швидкості та дуплексу на вкладці Додатково. Я просто залишаю параметри за замовчуванням (авто).

| INTERFACE      | INTERFACE TYPE | MANAGEMENT PROFILE | LINK STATE | IP ADDRESS      | VIRTUAL ROUTER | TAG      | VLAN / WIRE |
|----------------|----------------|--------------------|------------|-----------------|----------------|----------|-------------|
| ethernet1/1    | Layer3         | Access-allow       |            | 172.31.104.2/28 | VR             | Untagged | none        |
| ethernet1/2    | Layer3         |                    |            | none            | none           | Untagged | none        |
| ethernet1/2.10 | Layer3         | MGMT-ALLOW         |            | 192.168.10.1/24 | VR             | 10       | none        |
| ethernet1/2.20 | Layer3         | MGMT-ALLOW         |            | 192.168.20.1/24 | VR             | 20       | none        |
| ethernet1/3    | Layer3         |                    |            | none            | none           | Untagged | none        |
| ethernet1/3.30 | Layer3         | MGMT-ALLOW         |            | 192.168.30.1/24 | VR             | 30       | none        |
| ethernet1/3.40 | Layer3         | MGMT-ALLOW         |            | 192.168.40.1/24 | VR             | 40       | none        |
| ethernet1/4    |                |                    |            | none            | none           | Untagged | none        |
| ethernet1/5    | Layer3         | MGMT-ALLOW         |            | 200.168.10.1/28 | VR             | Untagged | none        |

Рисунок 3.9 – Налаштування інтерфейсів Layer 3 на PA Firewall

На інших також було налаштовано IP-адресацію та розподілено мережу на підмережі. Для кожної підмережі своя власна IP-адреса. Після цього доцільним є налагодити маршрутизацію між підмережами, щоб було можливим здійснити зв'язок між пристроями різних підмереж. Для цього було обрано протокол динамічної маршрутизації OSPF.

OSPF, що означає Open Shortest Path First, є протоколом маршрутизації, який використовує технологію стану каналу та алгоритм Дейкстри для визначення найкоротшого шляху між вузлами мережі.

Деякі переваги OSPF включають:

- Швидка збіжність порівняно з протоколами маршрутизації на основі відстані-вектора.
- Сумісність з масками підмережі змінної довжини (VLSM).

- Ефективне використання пропускну́ї здатності за допомогою побудови дерева найкоротших шляхів.

Налагодження протоколу OSPF на обладнанні (на інших пристроях налаштування проводяться аналогічно):

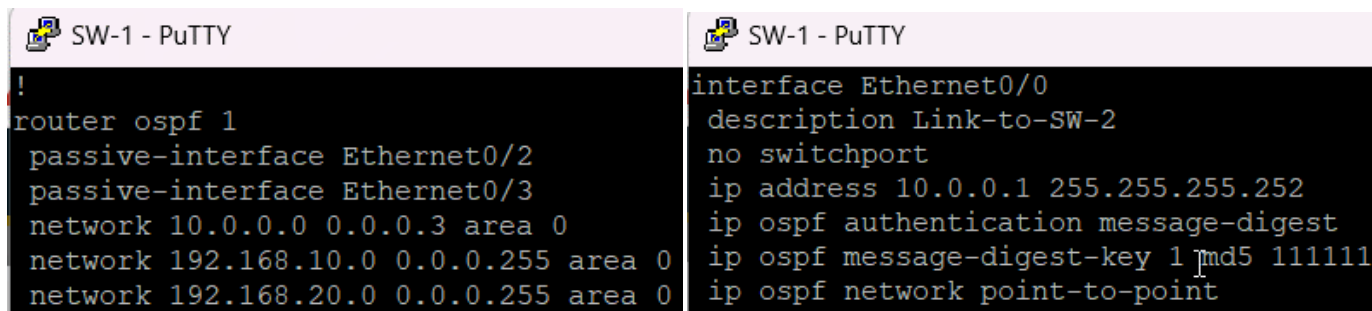


Рисунок 3.10 – Налаштування протоколу OSPF

Оскільки мережеві екрани з'єднують різні підмережі, на них також налаштовано динамічну маршрутизацію всіх підключених пристроїв. Це здійснюється у створеному віртуальному маршрутизаторі.

Щоб налаштувати OSPF на брандмауері PAN, потрібно перейти до Мережа > Віртуальні маршрутизатори > натиснути власний віртуальний маршрутизатор (у цьому випадку VR) > OSPF. Ввести ідентифікатор зони в десятковій формі з крапками (як адреса IPv4) 0.0.0.0 > залишити Тип за замовчуванням (Тип області) як Звичайний.

Після цього перейти на вкладку «Діапазон» > натиснути «Додати» > ввести мережу/nm, які братимуть участь у маршрутизації OSPF.

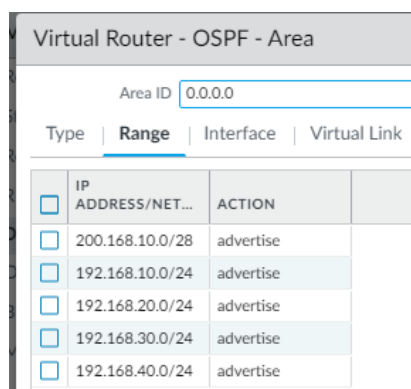


Рисунок 3.11 – Додані мережі для маршрутизації на PAN (аналогічно на Remote PAN)

Перейти на вкладку «Інтерфейс» > клацнути «Додати» > вибрати інтерфейс, який братиме участь у OSPF Area 0 > залишити тип посилення за замовчуванням як Broadcast та інші таймери OSPF та інші показники.

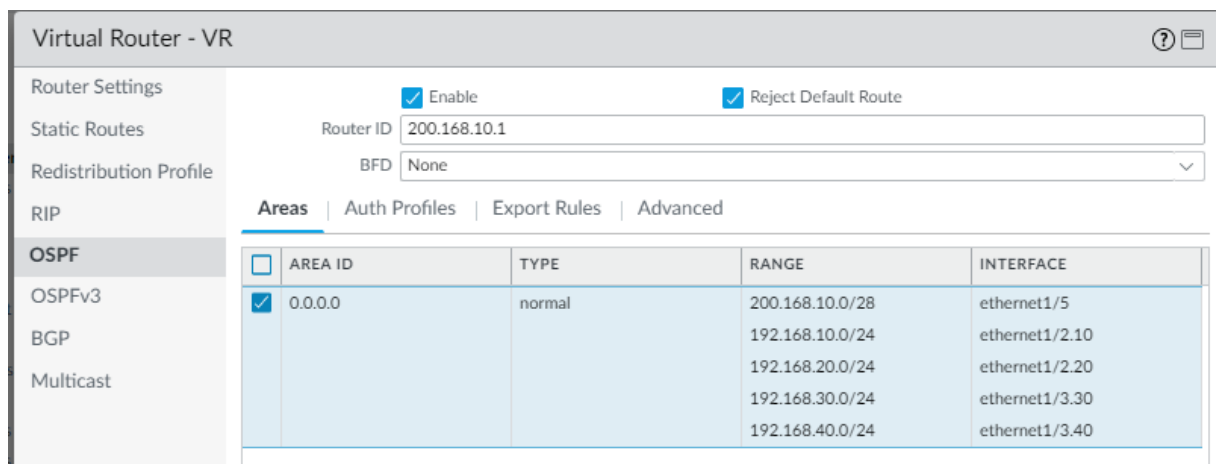


Рисунок 3.12 – Налаштовані інтерфейси для протоколу OSPF

Для налаштування тунелю IPsec VPN, одна з перших речей, які можна зробити після переговорів зі своїм партнером або вирішивши для себе, чи можливо керувати обома пунктами, це підготувати профілі Crypto.

Переходимо на вкладку мережі та додаємо новий профіль у профілі IPsec Crypto та IKE Crypto:

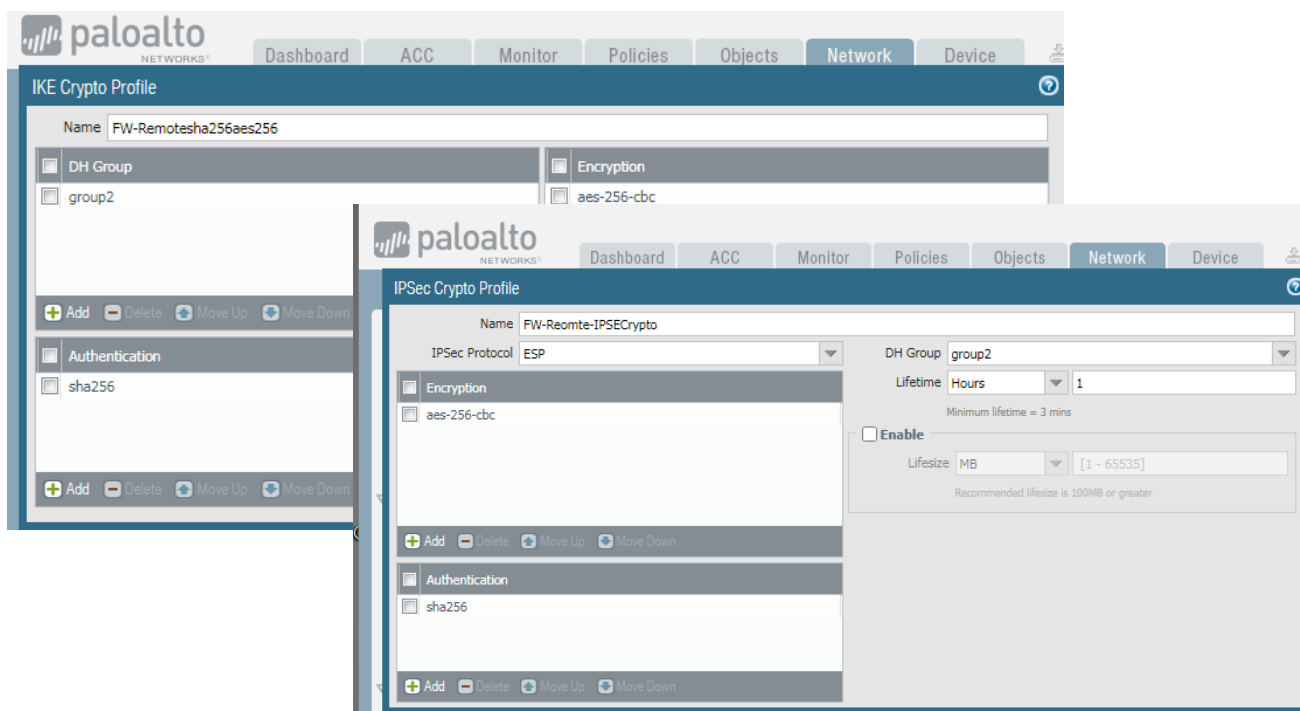


Рисунок 3.13 – Профілі IKE Crypto та IPsec Crypto

Далі потрібно буде створити одноранговий об'єкт, який представлятиме віддалений шлюз, і властивості IKE, спільні з цим шлюзом, щоб дозволити узгодження IPSec. Переходимо до профілів IKE Gateways на вкладці «Мережа» та створюємо новий об'єкт IKE Gateway.

Рисунок 3.14 – Створення нового об'єкту IKE Gateway

Далі потрібно буде створити інтерфейс тунелю: переходимо до Інтерфейси та відкриваємо вкладку Тунель. Створюємо новий інтерфейс, який буде служити віртуальним інтерфейсом для віртуальної приватної мережі. Також цей інтерфейс розміщуємо у зоні VPN для контроль доступу.

Рисунок 3.15 – Створення інтерфейсу тунелю

Після налаштування інтерфейсу можна переходити до створення фази 2 VPN-тунелю. Переходимо до меню тунелів IPsec і створюємо новий тунель IPsec.

Рисунок 3.16 – Створений IPsec тунель на одному з PAN

Також до віртуального маршрутизатора потрібно буде додати маршрути, щоб забезпечити пересилання трафіку між локальною та віддаленою мережею. Заодно тут створено маршрут до інтернет-провайдера із виходом у мережу Інтернет.

| Virtual Router - VR      |         |                 |             |            |              |                |        |      |             |
|--------------------------|---------|-----------------|-------------|------------|--------------|----------------|--------|------|-------------|
| Static Routes            |         |                 |             |            |              |                |        |      |             |
| IPv4                     |         |                 |             |            |              |                |        |      |             |
| 6 items                  |         |                 |             |            |              |                |        |      |             |
|                          | Name    | Destination     | Interface   | Next Hop   |              | Admin Distance | Metric | BFD  | Route Table |
|                          |         |                 |             | Type       | Value        |                |        |      |             |
| <input type="checkbox"/> | Remote  | 200.168.10.0/28 | tunnel      |            |              | default        | 10     | None | unicast     |
| <input type="checkbox"/> | Remote1 | 192.168.10.0/24 | tunnel      |            |              | default        | 10     | None | unicast     |
| <input type="checkbox"/> | Remote2 | 192.168.20.0/24 | tunnel      |            |              | default        | 10     | None | unicast     |
| <input type="checkbox"/> | Remote3 | 192.168.30.0/24 | tunnel      |            |              | default        | 10     | None | unicast     |
| <input type="checkbox"/> | Remote4 | 192.168.40.0/24 | tunnel      |            |              | default        | 10     | None | unicast     |
| <input type="checkbox"/> | Route   | 0.0.0.0/0       | ethernet1/1 | ip-address | 173.31.104.1 | default        | 10     | None | unicast     |

```
ISP

interface FastEthernet0/0
ip address dhcp
ip nat outside
ip virtual-reassembly
duplex half
!
interface FastEthernet1/0
description LINK-TO-PAVM
ip address 172.31.104.1 255.255.255.240
ip virtual-reassembly
duplex half
!
interface FastEthernet2/0
description LINK-TO-PA-REMOTE
ip address 173.31.104.1 255.255.255.240
ip virtual-reassembly
duplex half
```

Рисунок 3.17 – Маршрути для пересилання трафіку та IP-адресація на ISP

Щоб дозволити трафік між обома сайтами, необхідно створити політику безпеки між локальною зоною безпеки та зоною безпеки тунелю VPN

| Name             | Tags | Type      | Zone    | Address | User | HTTP Profile | Zone    | Address | Application | Service          | Action |
|------------------|------|-----------|---------|---------|------|--------------|---------|---------|-------------|------------------|--------|
| Allow-to-Outside | none | universal | Remote  | any     | any  | any          | OUTSIDE | any     | any         | any              | Allow  |
| VPN              | none | universal | Remote  | any     | any  | any          | VPN     | any     | any         | any              | Allow  |
| allow-ipsec      | none | universal | OUTSIDE | any     | any  | any          | OUTSIDE | any     | ike         | application-d... | Allow  |
| PING             | none | universal | OUTSIDE | any     | any  | any          | OUTSIDE | any     | icmp        | application-d... | Allow  |

Рисунок 3.18 – Політики безпеки для тунелю VPN та між іншими зонами

Обидва кінці налаштовано, VPN-тунель встановлено, значки на тунелях IPSec стали зеленими:

| Name           | Status      | Type     | IKE Gateway/Satellite |                 |              |          | Tunnel Interface |                  |                |               |        |
|----------------|-------------|----------|-----------------------|-----------------|--------------|----------|------------------|------------------|----------------|---------------|--------|
|                |             |          | Interface             | Local IP        | Peer IP      | Status   | Interface        | Virtual Router   | Virtual System | Security Zone | Status |
| FW-RemoteIP... | Tunnel Info | Auto Key | ethernet1/1           | 173.31.104.2/28 | 172.31.104.2 | IKE Info | tunnel           | VR (Show Routes) | vsys1          | VPN           |        |

| NAME        | STATUS      | TYPE     | IKE Gateway/Satellite |                |              |          | Tunnel Interface |                  |                |               |        |
|-------------|-------------|----------|-----------------------|----------------|--------------|----------|------------------|------------------|----------------|---------------|--------|
|             |             |          | INTERFA...            | LOCAL IP       | PEER ADDRESS | STATUS   | INTERFA...       | VIRTUAL ROUTER   | VIRTUAL SYSTEM | SECURITY ZONE | STATUS |
| FW-VM-IPSec | Tunnel Info | Auto Key | ethernet...           | 172.31.104.... | 173.31.1...  | IKE Info | tunnel           | VR (Show Routes) | vsys1          | VPN           |        |

Рисунок 3.19 – Працюючі IPSec VPN тунелі

Операційна система Windows Server вкрай популярна в корпоративному сегменті, хоча більшість рядових користувачів асоціюють Windows виключно з версією для персональних комп'ютерів. Залежно від завдань і необхідної до

підтримки інфраструктури зараз в експлуатації компаній знаходяться відразу кілька версій Windows Server, починаючи з Windows Server 2003 і закінчуючи останньою версією - Windows Server 2019.

Active Directory, як контролер домену працюватиме під управлінням Windows Server 2019, основна його задачі – це збереження даних каталогів і управління взаємодією користувача та домену, такі як процеси авторизації користувача в системі і перевірка автентичності користувача у каталогах домену.[17]

Контролер домену Active Directory (AD) складається із служб:

- Directory Services – служба організації бази даних каталогів.
- Certification Services – служба роботи із сертифікатами відповідності.
- Lightweight Directory Services – служба, створена для опрацювання додаткових екземплярів баз даних.
- Federations Services – служба налаштування довірчих відносин між організаціями у Active Directory.[16]

Встановлення Active Directory:

1) Встановлення і розгортання служб налаштовується за допомогою Server Manager та Add Roles and Features. У розділі "Полі сервера" (Server Roles) вибрати Доменні служби Active Directory (Active Directory Domain Services). Після цього буде запропоновано додати додаткові функції.

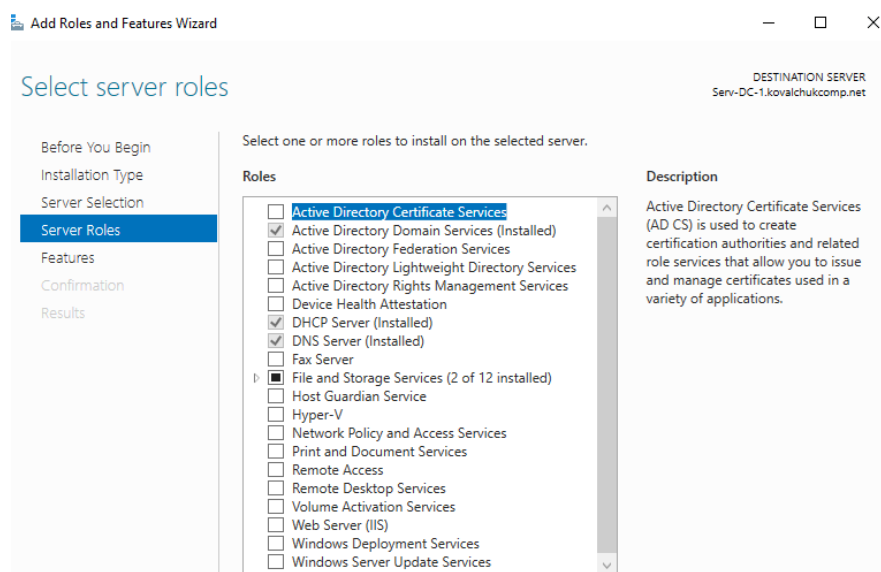


Рисунок 3.20 – Ініціалізація сценарію встановлення і налаштування AD

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 66   |

2) Виконується перевірка даних для встановлення нового лісу в AD. Після встановлення конфігурацій сервер перезавантажиться з встановленими службами. Домен підприємства має назву: kovalchukcomp.net

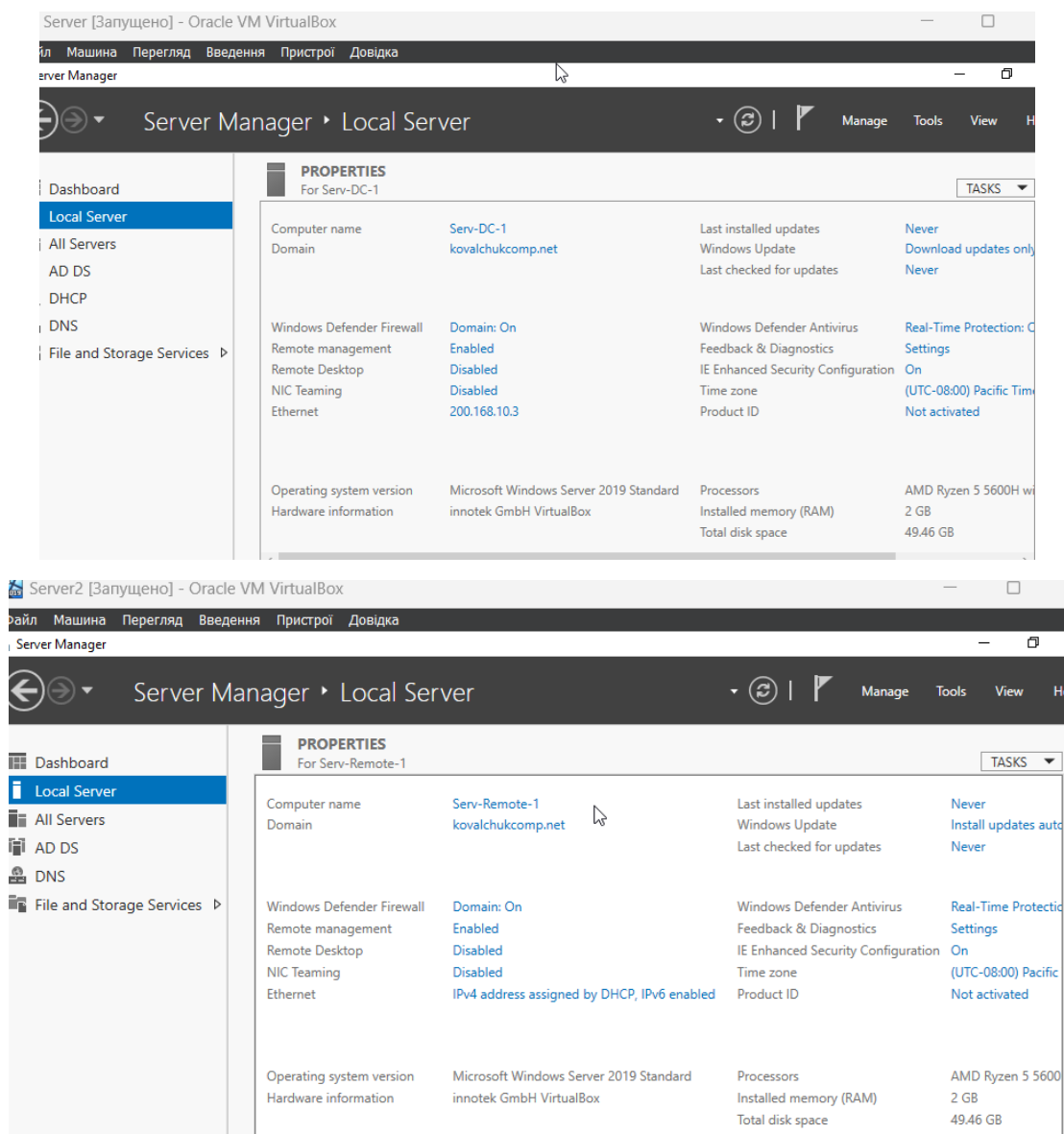


Рисунок 3.21 – Інформація про домен налаштований на 2 контролерах

В нашій мережі організації 1 контролер поєднаний з другим, який знаходиться у віддаленому офісі. Він з'єднаний між першим контролером в зоні Дата центру та налаштований на реплікацію з ним.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 67   |

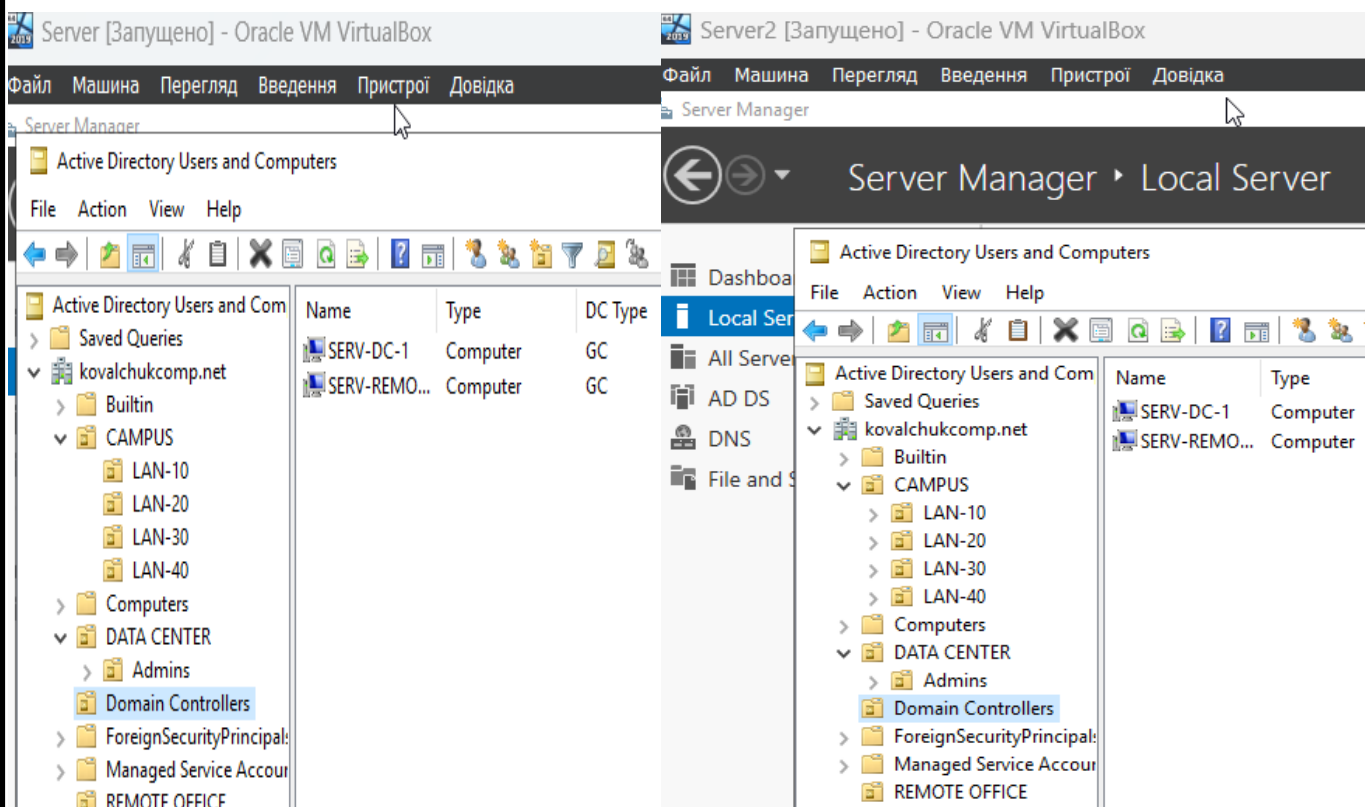


Рисунок 3.22 – Перший контролер домену SRV-DC-1 та другий контролер Srv-Remote-1 з тією ж структурою домену

### 3.3 Додавання правил безпеки на основі технології Content-ID та власних сигнатур

Брандмауер Palo Alto Networks підтримує спеціальні сигнатури вразливостей за допомогою механізму загроз брандмауера. Підтримуються власні шаблони регулярних виразів, щоб виявити використання вразливостей. Отримані шаблони вразливостей стають доступними для використання в усіх профілях безпеки вразливостей. Брандмауер шукає користувальницькі шаблони в мережевому трафіку та виконує вказану дію для використання вразливості.

Спочатку додаємо спеціальний об'єкт уразливості на вкладці «Об'єкти» > «Користувальцькі об'єкти» > «Уразливість», як показано на рисунку 3.24.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 68   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

Рисунок 3.24 – Додавання об’єкта уразливості, яка може статися  
У наступному вікні ми вкажемо збіг підпису.

Оператор: визначає тип умови, яка має бути істинною, щоб настроюваний підпис відповідав трафіку. Ми шукатимемо відповідність шаблону "Chrome/" у полі контексту "http-req-headers", як показано на рисунку 3.25.

Рисунок 3.25 – Додавання шаблону сигнатури, яка буде буде помічена

Якщо зробити захоплення пакета під час перегляду за допомогою веб-переглядача Chrome, видно такий збіг шаблону в захопленні, тому і шаблоні вказуємо ту частину, щоб дізнатись про такого користувача:

Щоб увімкнути власний підпис, переходимо до профілю захисту від вразливостей. Відредагуємо свій профіль і на вкладці «Винятки» знаходимо ідентифікатор загрози. Коли профіль додано до політик безпеки, з'являється відповідний значок профілю захисту:

| ENAB...                  | ID    | THREAT NAME   | IP ADDRESS EXEMPTI... | RULE                 | CVE | HOST   | CATEGORY | SEVERI... | ACTION          | PACKET CAPTURE |
|--------------------------|-------|---------------|-----------------------|----------------------|-----|--------|----------|-----------|-----------------|----------------|
| <input type="checkbox"/> | 41... | 404_Not_Found |                       | simple-client-medium |     | client |          | medium    | default (alert) | disable        |
| <input type="checkbox"/> | 41... | ChromeTraffic |                       | simple-client-high   |     | client |          | high      | default (alert) | disable        |

Рисунок 3.26 – Застосування сигнатури в профіль та додавання її до політик безпеки

Також було створено правило захисту від вразливостей різних рівнів, яке вже налаштовані автоматично на мережевому екрану Palo Alto Networks, та застосовано його до політик безпеки із зовнішньої зони до зони довіри (рис. 3.27).

Rule Name: Vuln\_Rule

Threat Name: any

Used to match any signature containing the entered text as part of the signature name

Action: Alert

Packet Capture: single-packet

Host Type: any

Category: any

Severity: ☒ any (All severities), ☐ critical, ☐ high, ☐ medium, ☐ low, ☐ informational

☒ Any, ☐ CVE, ☐ VENDOR ID

Рисунок 3.27 – Правило захисту від зовнішніх небезпечних вразливостей

Цей спеціальний підпис може використовуватися для ідентифікації хостів Windows XP на основі активності їх веб-додатків. Він шукає в заголовках запитів HTTP поле User-Agent, яке містить рядок ідентифікатора платформи Windows. Стандартною дією цього підпису є сповіщення. Однак це можна легко замінити

на використання дії «скидання» або «скидання клієнта», щоб заблокувати хостам Windows XP використання веб-програм через платформу безпеки Palo Alto Networks.

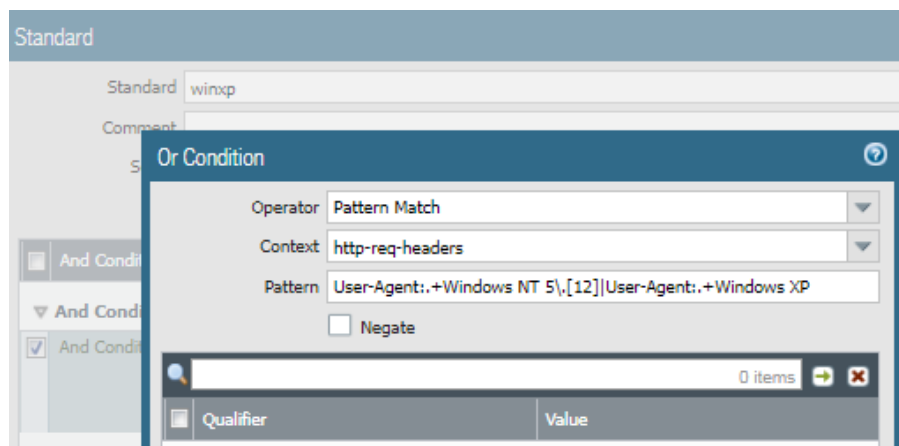


Рисунок 3.28 – Підпис на ідентифікацію застарілої версії Windows XP в мережі

Створено спеціальний звіт, який підсумовуватиме унікальні адреси джерел, які викликали цю сигнатуру вразливості (рис. 3.29).

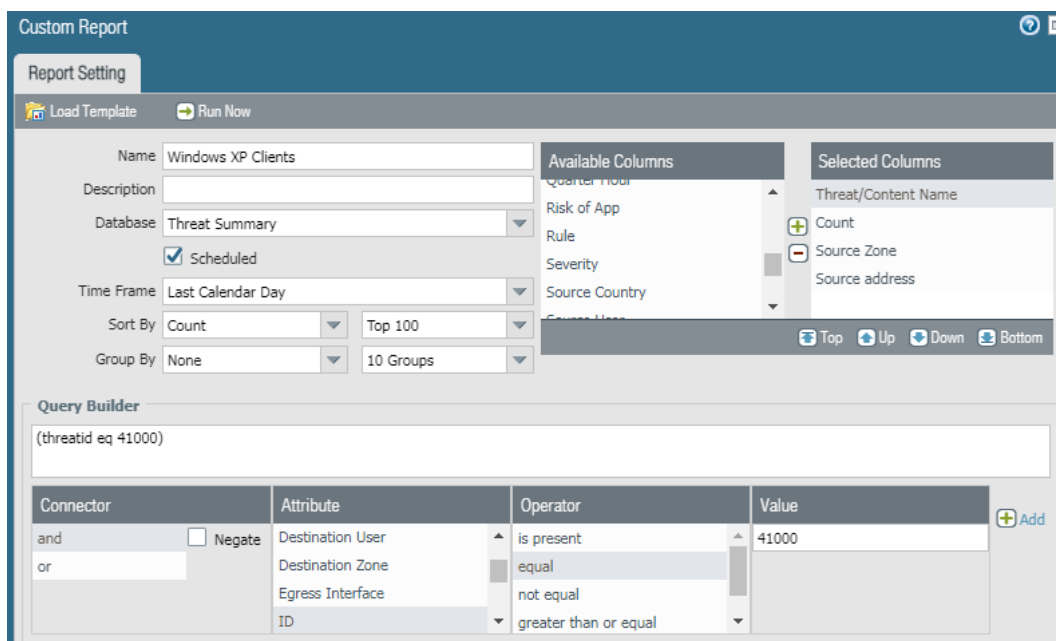


Рисунок 3.29 – Сформований звіт на підсумок користувачів Windows XP

Інше також створено та налаштовано власний профіль блокування файлів.

Для прикладу будуть блокуватись файли у форматі PDF, які можуть бути завантажені з мережі або завантажені іншому користувачі чи хостингу. Дію вибрано «продовжити», щоб користувач не зміг відразу завантажити файл, а тільки після власного продовження.

**File Blocking Profile** ?

Name

Description

1 item → ×

| <input type="checkbox"/>            | NAME | APPLICATIONS | FILE TYPES | DIRECTION | ACTION   |
|-------------------------------------|------|--------------|------------|-----------|----------|
| <input checked="" type="checkbox"/> | PDF  | any          | pdf        | both      | continue |

Рисунок 3.30 – Профіль File Blocking

Також було створено для майбутнього захисту мережі власний підпис загрози з підписів Snort. Розглянуто відомий північнокорейський троян: Volgmer хакерів HIDDEN COBRA. За допомогою комплексних процесів перевірки цього шпигунського ПЗ, зафіксовано правило Snort після аналізу цієї перевірки:

```
alert tcp any any -> any any (msg:"Malformed_UA"; content:"User-Agent: Mozillar/"; depth:500; sid:99999999;)[13]
```

На основі цього правила створено власний підпис, щоб запобігти проникненню загрози в нашу мережу і сповістити про це.

**PA-VM** DASHBOARD MONITOR POLICIES **OBJECTS** NETWORK DEVICE

**Standard** ?

Standard

Comment

Scope ☒ Transaction ☐ Session

☒ Ordered Condition Match

| <input type="checkbox"/> | AND CONDITION   | CONDITIONS     | OPERATOR      | VALUE                 | CONTEXT          | QUALIFIER | NEGATE                   |
|--------------------------|-----------------|----------------|---------------|-----------------------|------------------|-----------|--------------------------|
| And Condition 1          |                 |                |               |                       |                  |           |                          |
| <input type="checkbox"/> | And Condition 1 | Or Condition 1 | pattern-match | User-Agent: Mozillar/ | http-req-headers |           | <input type="checkbox"/> |

Рисунок 3.31 – Власна сигнатура за виявлення шпигунського ПЗ

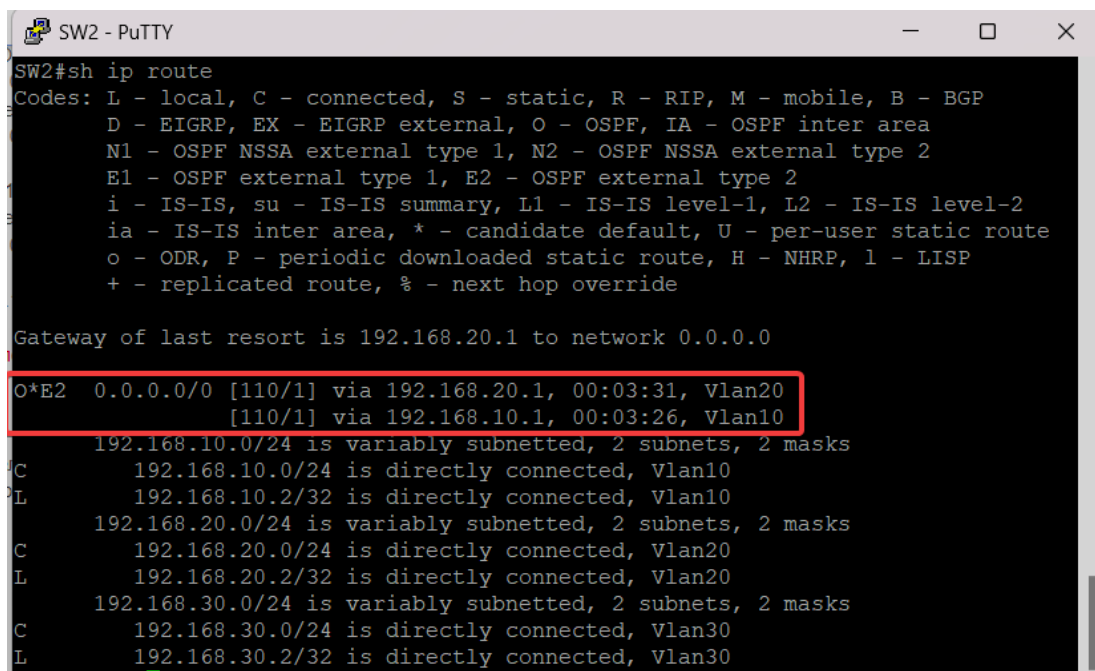
Шаблон «User-Agent: Mozillar/» із підпису snort використовується з контекстом «http-req-headers» для створення спеціального підпису. Об'єкт Sruware доданий до профілю захисту від шпигунського ПЗ та закріплено до політик безпеки.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 72   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

### 3.4 Перевірка працездатності мережі та тестування виконаних налаштувань

Для перевірки працездатності розробленої мережі необхідно протестувати передачу пакетів даних, провести пінгування між окремими пристроями. Також перевірити працездатність політик брандмауера та зв'язку між зонами. Результати перевірки працездатності наведені на рисунках нижче.

Перевірка відображення таблиці маршрутизації отриманої від брандмауера PAN:

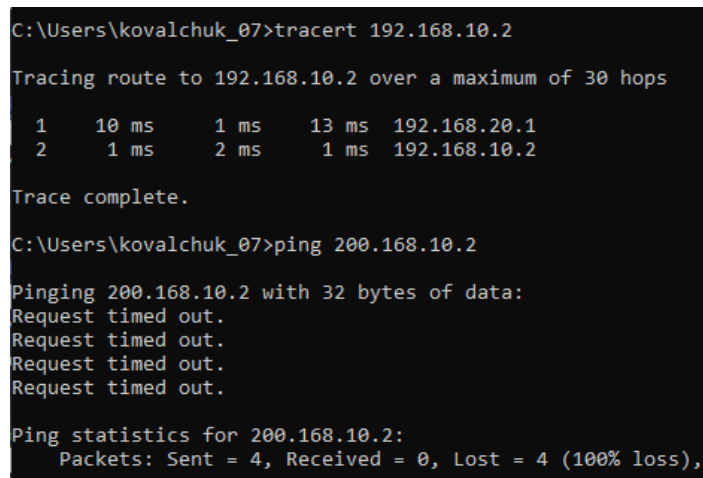


```
SW2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.20.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 192.168.20.1, 00:03:31, Vlan20
      [110/1] via 192.168.10.1, 00:03:26, Vlan10
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.0/24 is directly connected, Vlan10
L      192.168.10.2/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.20.0/24 is directly connected, Vlan20
L      192.168.20.2/32 is directly connected, Vlan20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.30.0/24 is directly connected, Vlan30
L      192.168.30.2/32 is directly connected, Vlan30
```

Перевірка зв'язку з іншою мережею Campus та Data Center:



```
C:\Users\kovalchuk_07>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops

  1    10 ms    1 ms    13 ms  192.168.20.1
  2     1 ms    2 ms    1 ms  192.168.10.2

Trace complete.

C:\Users\kovalchuk_07>ping 200.168.10.2

Pinging 200.168.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.168.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Під час перевірки зв'язку з DC, пінгування не відбувалося, тому що налаштована безпека на брандмауері PAN. Користувачі з Кампусу на мають прав зв'язуватись з основним центром, де є всі інші сервери.

Також з будівлі Data Center зв'язок можливий і зону Campus, на це дозвіл є:

```
*May 8 18:02:35.400: %OSPF-5-ADJCHG: Process 1, Nbr 200.168.10.1 on Vlan1000
om LOADING to FULL, Loading Done
SW-2-DC#
SW-2-DC#ping 192.168.20.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/15/30 ms
SW-2-DC#ping 200.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.168.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/42 ms
```

Перевірка передачі пакетів з віддаленого офісу до головного офісу організації:

```
SW-1-Remote - PuTTY
Success rate is 0 percent (0/5)
SW-1-Remote#trac
SW-1-Remote#tracert 200.168.10.2
Type escape sequence to abort.
Tracing the route to 200.168.10.2
VRF info: (vrf in name/id, vrf out name/id)
 0 120.5.5.1 8 msec 1 msec 2 msec
 1 172.16.4.1 13 msec 22 msec 20 msec
 2 200.168.10.2 45 msec 21 msec 20 msec
SW-1-Remote#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/20/21 ms
```

Після розгортання контролера Active Directory у зоні Data Center, можливе підключення робочих станцій до домену та аутентифікації користувачів у системі. Також це можливо і на віддаленому офісі від другого контролера завдяки реплікації (рис.3.32).

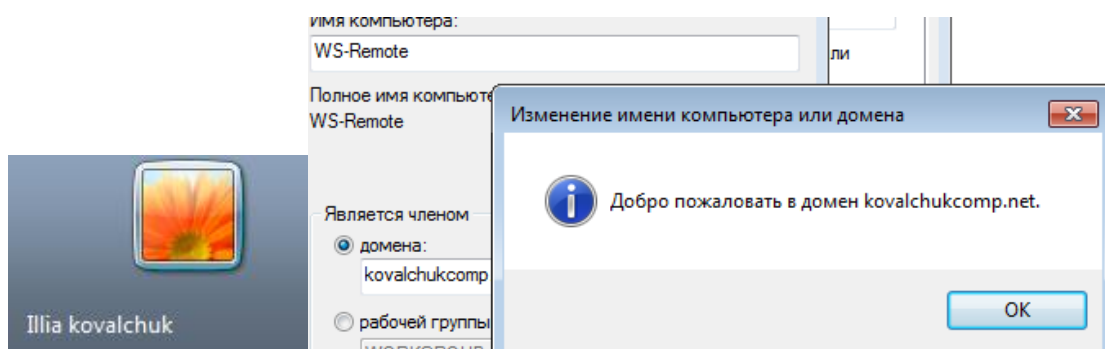


Рисунок 3.32 Перевірка підключення до домену робочої станції та вхід під створеним користувачем на контролері домену

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 74   |

Ми вже налаштували сервер NetFlow. Я використовую сервер SolarWinds Netflow. Потрібно виконати базову конфігурацію налаштування сервера Netflow. Після того, як ми все правильно налаштували, інтерфейси брандмауера будуть зображені у програмі Netflow.

Після цього можна перевірити програму/послуги, IP-адресу джерела та призначення та багато інших речей у своїй програмі Netflow.

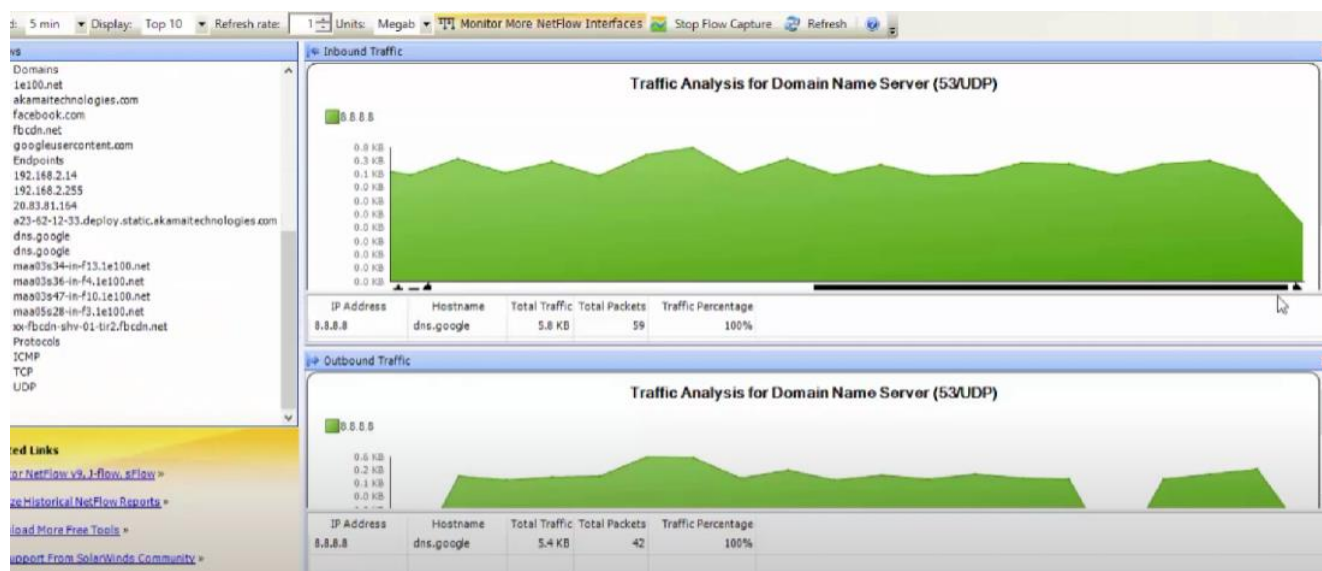


Рисунок 3.33 – Зображення різних функцій, графіків у програмі

Процес здійснення атаки від зовнішнього користувача на мережевий екран за допомогою утиліти nmap (рис. 3.34).

```
(root@kali)-[/home/kali]
# nmap -v --script vuln 172.31.104.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-15 12:12 EDT
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:12
Completed NSE at 12:12, 10.00s elapsed
Initiating NSE at 12:12
Completed NSE at 12:12, 0.00s elapsed
Initiating Ping Scan at 12:12
Scanning 172.31.104.2 [4 ports]
Completed Ping Scan at 12:12, 0.05s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 12:12
Scanning 172.31.104.2 [1000 ports]
Discovered open port 22/tcp on 172.31.104.2
Discovered open port 443/tcp on 172.31.104.2
Discovered open port 80/tcp on 172.31.104.2
Discovered open port 23/tcp on 172.31.104.2
Increasing send delay for 172.31.104.2 from 0 to 5 due to 11 out of 17 droppe
```

Рисунок 3.34 – Атака з зовнішньої робочої станції зломисника

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 75   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

Детальна інформація про атаку відразу відображається на Palo Alto Networks (рис. 3.35).

| Detailed Log View                              |                       |                                   |
|------------------------------------------------|-----------------------|-----------------------------------|
| General                                        | Source                | Destination                       |
| Session ID 3380                                | Source User           | Destination User                  |
| Action alert                                   | Source 1.1.1.2        | Destination 172.31.104.2          |
| Host ID                                        | Source DAG            | Destination DAG                   |
| Application web-browsing                       | Country Australia     | Country 172.16.0.0-172.31.255.255 |
| Rule Outside-to-inside                         | Port 45778            | Port 80                           |
| Rule UUID 3d45e213-2f78-40b0-84d7-3e35ff1d7c66 | Zone Outside          | Zone Inside                       |
| Device SN                                      | Interface ethernet1/1 | Interface ethernet1/2.10          |
| IP Protocol tcp                                | NAT IP 1.1.1.2        | NAT IP 192.168.10.1               |
|                                                | NAT Port 45778        |                                   |

Рисунок 3.35 – Детальне логування здійсненого пакету

Також присутня інформація в журналі загроз на здійснення атаки. Вказана IP-адреса джерела, рішення, які використав зломисник та наш профіль захисту від вразливостей, який спрацював (рис. 3.36).

|   |   |                |               |         |                                                              |         |        |    |              |       |
|---|---|----------------|---------------|---------|--------------------------------------------------------------|---------|--------|----|--------------|-------|
| 🔍 | ⬇ | 06/15 09:14:16 | vulnerability | 1.1.1.2 | Nmap Scripting Engine Detection                              | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:16 | vulnerability | 1.1.1.2 | Apache Tomcat URLEncoding Directory Traversal Vulnerability  | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:16 | vulnerability | 1.1.1.2 | YAWS Unauthenticated Remote File Disclosure Vulnerability    | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:16 | vulnerability | 1.1.1.2 | Nmap Scripting Engine Detection                              | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:16 | vulnerability | 1.1.1.2 | Spring Cloud Config Server Directory Traversal Vulnerability | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:11 | vulnerability | 1.1.1.2 | HTTP /etc/passwd Access Attempt                              | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:11 | vulnerability | 1.1.1.2 | HTTP /etc/passwd Access Attempt                              | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:11 | vulnerability | 1.1.1.2 | HTTP Directory Traversal Request Attempt                     | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:11 | vulnerability | 1.1.1.2 | Nmap Scripting Engine Detection                              | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:11 | vulnerability | 1.1.1.2 | 404_Not_Found                                                | Outside | Inside | 80 | web-browsing | alert |
| 🔍 | ⬇ | 06/15 09:14:11 | vulnerability | 1.1.1.2 | Nmap Scripting Engine Detection                              | Outside | Inside | 80 | web-browsing | alert |

Рисунок 3.36 – Журнал загроз на брандмауері PAN

Перевірка іншого захисту від вразливості, який ми створили. В журналі загроз спостерігається активність використання ОС Windows XP на одній з робочих станцій. Наш профіль з власним підписом виявив це. Дія була вибрана, як Сповіщення адміністратору.

| Type          | Name                  | From Zone | To Zone       | Attacker        | Attacker Name | Victim         | To Port | Application  | Action | Severity      |
|---------------|-----------------------|-----------|---------------|-----------------|---------------|----------------|---------|--------------|--------|---------------|
| vulnerability | Windows XP User-Agent | home-zone | internet-zone | 192.168.150.109 |               | 64.233.171.95  | 80      | google-maps  | alert  | informational |
| vulnerability | Windows XP User-Agent | home-zone | internet-zone | 192.168.150.109 |               | 50.31.164.192  | 80      | new-relic    | alert  | informational |
| vulnerability | Windows XP User-Agent | home-zone | internet-zone | 192.168.150.109 |               | 192.33.31.101  | 80      | web-browsing | alert  | informational |
| vulnerability | Windows XP User-Agent | home-zone | internet-zone | 192.168.150.109 |               | 157.55.211.12  | 80      | web-browsing | alert  | informational |
| vulnerability | Windows XP User-Agent | home-zone | internet-zone | 192.168.150.109 |               | 54.230.18.117  | 80      | web-browsing | alert  | informational |
| vulnerability | Windows XP User-Agent | home-zone | internet-zone | 192.168.150.109 |               | 54.186.231.204 | 80      | web-browsing | alert  | informational |

Рисунок 3.37 – Журнал з виявленою ідентифікацією користувача Windows XP

Після цього перевіримо наш захист проти небажаних файлів, завантажених з мережі Інтернет. На рисунку 3.37 бачимо сповіщення про блокування файлу PDF (вказано в політиці) та з можливістю продовження його завантаження в мережу.

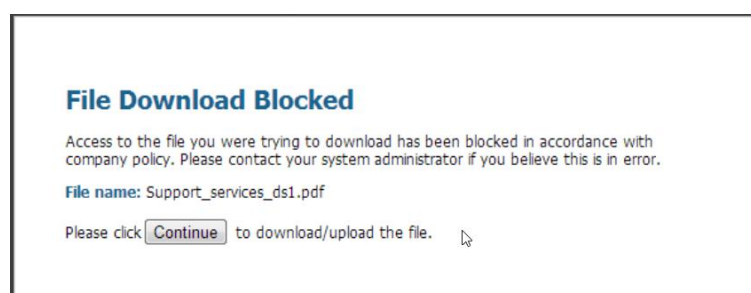


Рисунок 3.38– Блокування небажаних файлів

### Висновок до третього розділу

В результаті виконання третього розділу було здійснено відповідний аналіз та вибір обладнання, що найкраще відповідає потребам організації. Проведено налаштування обраного обладнання для забезпечення ефективної роботи мережі, вдалося реалізувати технологію IPSec VPN між двома мережевими екранами Palo Alto Networks та поєднати віддалений офіс з головним. Налаштовано також сервер на базі Active Directory для контролю користувачів та комфортної роботи.

Розроблено та впроваджено правила безпеки на основі профілів від вразливостей, небажаних файлів, шпигунського ПЗ та власних сигнатур для забезпечення захисту мережі від потенційних загроз.

Здійснено перевірку працездатності мережі та виконаних налаштувань, а також проведено відповідне тестування на виконання налагоджених систем захисту на мережевих екранах PAN.

Результати цих розділів будуть використовуватись для подальшого функціонування мережі організації та забезпечення її безперебійної роботи.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 77   |

## ВИСНОВКИ

У даній кваліфікаційній роботі бакалавра було проведено детальне дослідження та аналіз корпоративних мереж і їхньої безпеки. У першому розділі було розглянуто основні принципи побудови корпоративних мереж і порівняно декілька сучасних брандмауерів нового покоління. Встановлено, що Palo Alto Firewall є найбільш масштабованим рішенням, що дозволяє розширювати мережу без втрати продуктивності. Також було порівняно застосування технологій IPSec VPN і SSL VPN, виявлено їхні унікальні переваги і визначено, що IPSec VPN забезпечує більшу простоту налаштувань і відповідає більшим потребам.

У другому розділі було проведено аналіз етапів створення корпоративної мережі для підприємства, включаючи рекомендації щодо архітектури, захисту та керування трафіком. Була запропонована оптимальна топологія мережі, яка відповідає потребам організації та забезпечує ефективний обмін даними між внутрішніми департаментами. Для перевірки працездатності було використано програмне забезпечення GNS3, що дозволяє моделювати та тестувати мережеві конфігурації перед їх впровадженням.

У третьому розділі було здійснено аналіз і вибір обладнання, проведено його налаштування та реалізовано технологію IPSec VPN для безпечного з'єднання віддаленого офісу з головним. Було встановлено правила безпеки на основі профілів та розроблено власні сигнатури для захисту мережі від потенційних загроз. Проведено перевірку працездатності мережі та налаштувань, а також виконано тестування систем захисту на мережевих екранах.

Результати роботи полягають в тому, що розроблені рішення та проведені заходи забезпечують безперебійну та ефективну роботу корпоративної мережі організації. Ця кваліфікаційна робота може бути використана як практичний посібник для планування та реалізації корпоративних мереж з використанням сучасних технологій та засобів безпеки.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 78   |

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF), IETF, Request for Comments: 6020, Category: Standards, ISSN: 2070-1721.
2. Content-ID. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.paloguard.com/Content-ID.asp>.
3. NGFW. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.paloaltonetworks.com/network-security/next-generation-firewall-hardware>
4. Barracuda Firewall. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.gartner.com/reviews/market/networkfirewalls/vendor/barracuda/product/barracuda-cloudgen>
5. Cisco ASA. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.router-switch.com/cisco-firepower-ngfw.html>
6. Topology. [Електронний ресурс] – Режим доступу до ресурсу: <https://kremenetskyy.blogspot.com/2017/11/blog-post.html>
7. IPSec VPN. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-ipsec-vpn-overview.html>
8. Міжмережевий екран (МЕ). [Електронний ресурс] – Режим доступу до ресурсу: <https://sites.google.com/site/zahistlokalnoiemerezi/zahist/mizmerezevij-ekran>.
9. Palo Alto Networks Enterprise Firewall PA-1420. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.paloguard.com/Firewall-PA-1420.asp>
10. Навчальний курс CCNA Routing and Switching: Routing and Switching Essentials [Електронний ресурс] – Режим доступу: [www.netacad.com](http://www.netacad.com).
11. Cisco IOS VPN Configuration Guide, 2005. – 131 с.
12. The Complete Cisco VPN Configuration Guide By Richard Deal, 2005. – 1032с.

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 79   |

13. HIDDEN COBRA. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.us-cert.gov/ncas/alerts/TA17-318B>

14. VPN. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-does-a-vpn-work.html#~types-of-encrypted-vpns>

15. Віртуальні приватні мережі VPN. [Електронний ресурс] – Режим доступу до ресурсу: [https://www.ibm.com/support/knowledgecenter/ru/ssw\\_ibm\\_i\\_73/rzaja/rzajagetstart.html](https://www.ibm.com/support/knowledgecenter/ru/ssw_ibm_i_73/rzaja/rzajagetstart.html)

16. What Is LDAP? [Електронний ресурс]. – 2022. – Режим доступу: <https://jumpcloud.com/blog/what-is-ldap>

17. Active Directory Domain Services [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services>.

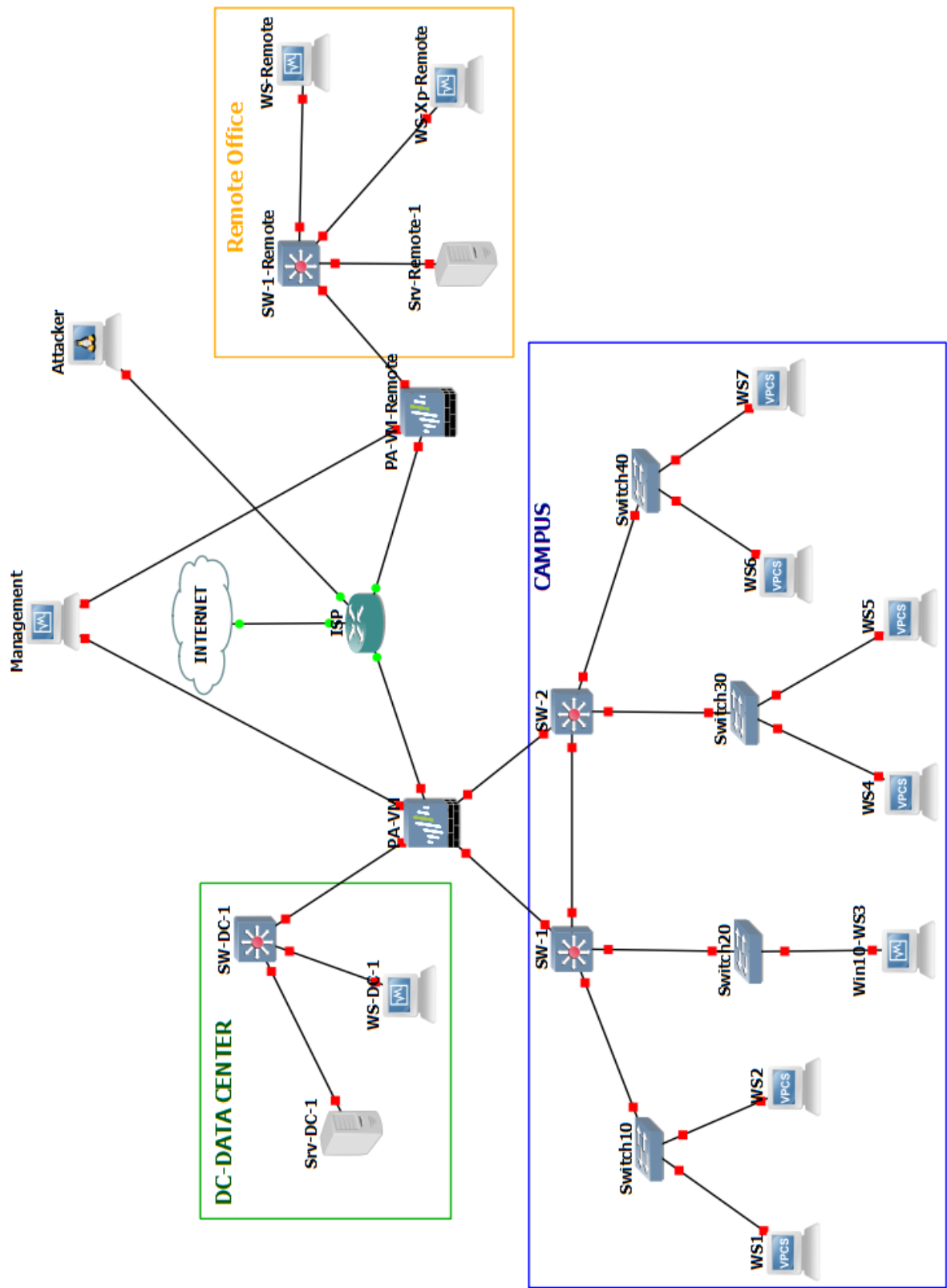
18. GNS3. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.gns3.com>

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 80   |

# ДОДАТКИ

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 81   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

Додаток А – Детальна схема побудованої мережі



## Додаток Б – Конфігураційні файли налаштованих пристроїв

```
hostname ISP
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
archive
  log config
  hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
  ip address dhcp
  ip nat outside
  ip virtual-reassembly
  duplex half
!
interface FastEthernet1/0
  description LINK-TO-PAVM
  ip address 172.31.104.1 255.255.255.240
  ip virtual-reassembly
  duplex half
!
interface FastEthernet2/0
  description LINK-TO-PA-REMOTE
  ip address 173.31.104.1 255.255.255.240
  ip virtual-reassembly
  duplex half
!
interface FastEthernet3/0
  ip address 1.1.1.1 255.255.255.0
  duplex half
!
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
control-plane
gatekeeper
shutdown
!
line con 0
  exec-timeout 0 0
  privilege level 15
```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 83   |

```

logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end
*****

hostname SW-DC-1
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport access vlan 1000
switchport mode access
!
interface Ethernet0/1
switchport access vlan 1000
switchport mode access
!
interface Ethernet0/2
switchport access vlan 1000
switchport mode access
!
interface Vlan1
no ip address
shutdown
!
interface Vlan1000
ip address 200.168.10.2 255.255.255.240

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 84   |

```

!
router ospf 1
 network 200.168.10.0 0.0.0.15 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 200.168.10.1
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
*****
hostname SW-1-Remote
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
no ip domain-lookup
no ipv6 cef
ipv6 multicast rpf use-bgp
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
interface Ethernet0/0
 switchport access vlan 5
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 5
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 5
 switchport mode access
 duplex auto

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 85   |

```

!
interface Ethernet0/3
  switchport access vlan 5
  switchport mode access
  duplex auto
!
interface Ethernet1/0
  duplex auto
!
interface Ethernet1/1
  duplex auto
!
interface Ethernet1/2
  duplex auto
!
interface Ethernet1/3
  duplex auto
!
interface Ethernet2/0
  duplex auto
!
interface Ethernet2/1
  duplex auto
!
interface Ethernet2/2
  duplex auto
!
interface Ethernet2/3
  duplex auto
!
interface Ethernet3/0
  duplex auto
!
interface Ethernet3/1
  duplex auto
!
interface Ethernet3/2
  duplex auto
!
interface Ethernet3/3
  duplex auto
!
interface Vlan1
  no ip address
!
interface Vlan5
  description Remote_Office
  ip address 120.5.5.2 255.255.255.128
router ospf 1
  passive-interface Ethernet0/1
  passive-interface Ethernet0/2

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 86   |

```

network 120.5.5.0 0.0.0.127 area 0
no ip http server
ip route 0.0.0.0 0.0.0.0 120.5.5.1
control-plane
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
end
*****
hostname SW-1
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Loopback0
  ip address 10.1.1.7 255.255.255.255
!
interface Ethernet0/0
  description Link-to-SW-2
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10,20,30,40
  switchport mode trunk
  duplex auto
!
interface Ethernet0/1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 10,20,30,40
  switchport mode trunk
  duplex auto
!

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 87   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

```

interface Ethernet0/2
  switchport access vlan 10
  switchport mode access
  duplex auto
!
interface Ethernet0/3
  switchport access vlan 20
  switchport mode access
  duplex auto
!
interface Ethernet1/0
  duplex auto
!
interface Ethernet1/1
  duplex auto
!
interface Ethernet1/2
  duplex auto
!
interface Ethernet1/3
  duplex auto
!
interface Ethernet2/0
  duplex auto
!
interface Ethernet2/1
  duplex auto
!
interface Ethernet2/2
  duplex auto
!
interface Ethernet2/3
  duplex auto
!
interface Ethernet3/0
  duplex auto
!
interface Ethernet3/1
  duplex auto
!
interface Ethernet3/2
  duplex auto
!
interface Ethernet3/3
  duplex auto
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan10

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 88   |

```

ip address 192.168.10.2 255.255.255.0
!
interface Vlan20
ip address 192.168.20.2 255.255.255.0
!
interface Vlan30
ip address 192.168.30.2 255.255.255.0
!
interface Vlan40
ip address 192.168.40.2 255.255.255.0
!
router ospf 1
passive-interface Ethernet0/2
passive-interface Ethernet0/3
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
no ip http server
ip route 0.0.0.0 0.0.0.0 192.168.10.1
ip route 0.0.0.0 0.0.0.0 192.168.20.1
control-plane
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
End
*****
hostname SW-2
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
no ip domain-lookup
ip cef
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
!
ip tcp synwait-time 5

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 89   |

```

!
interface Loopback0
 ip address 10.1.1.6 255.255.255.255
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 30
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 switchport access vlan 40
 switchport mode access
 duplex auto
!
interface Ethernet1/0
 switchport access vlan 200
 duplex auto
!
interface Ethernet1/1
 description Link-to-SW-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
interface Ethernet2/0
 duplex auto
!
interface Ethernet2/1
 duplex auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 duplex auto

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 90   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

```

!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!
interface Vlan1
    no ip address
    shutdown
!
interface Vlan10
    ip address 192.168.10.3 255.255.255.0
!
interface Vlan20
    ip address 192.168.20.3 255.255.255.0
!
interface Vlan30
    ip address 192.168.30.3 255.255.255.0
!
interface Vlan40
    ip address 192.168.40.3 255.255.255.0
!
interface Vlan200
    no ip address
!
router ospf 1
    passive-interface Ethernet0/2
    passive-interface Ethernet0/3
    network 192.168.10.0 0.0.0.255 area 0
    network 192.168.20.0 0.0.0.255 area 0
    network 192.168.30.0 0.0.0.255 area 0
    network 192.168.40.0 0.0.0.255 area 0
!
no ip http server
!
ip route 0.0.0.0 0.0.0.0 192.168.30.1
ip route 0.0.0.0 0.0.0.0 192.168.40.1
control-plane
line con 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line aux 0
    exec-timeout 0 0

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 91   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

```

privilege level 15
logging synchronous
line vty 0 4
login
End
*****
hostname Switch10
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
switchport access vlan 10
switchport mode access
!
interface Ethernet0/1
switchport access vlan 10
switchport mode access
!
interface Ethernet0/2
switchport access vlan 10
switchport mode access
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 92   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

```

!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan10
  description LAN-10-Finance
  ip address 192.168.10.4 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.2
!
control-plane
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
End
*****
hostname Switch20
!
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
ip cef
no ipv6 cef

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 93   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

```

spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
!
interface Ethernet0/0
    switchport access vlan 20
    switchport mode access
!
interface Ethernet0/1
    switchport access vlan 20
    switchport mode access
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
    no ip address
    shutdown
!
interface Vlan20
    description LAN-20-Marketing
    ip address 192.168.20.4 255.255.255.0
!
ip forward-protocol nd
!

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 94   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

```

no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.20.2
control-plane
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
End
*****
hostname Switch30
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
  switchport access vlan 30
  switchport mode access
!
interface Ethernet0/1
  switchport access vlan 30
  switchport mode access
!
interface Ethernet0/2
  switchport access vlan 30
  switchport mode access
!
interface Ethernet0/3
!
interface Ethernet1/0
!
```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 95   |

```

interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan30
  description LAN-30-Help
  ip address 192.168.30.4 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
control-plane
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
End
.....
hostname Switch40
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         |      |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         | 96   |

```

logging console discriminator EXCESS
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain-lookup
ip cef
no ipv6 cef
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
!
interface Ethernet0/0
    switchport access vlan 40
    switchport mode access
!
interface Ethernet0/1
    switchport access vlan 40
    switchport mode access
!
interface Ethernet0/2
    switchport access vlan 40
    switchport mode access
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
    no ip address

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 97   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |

```

shutdown
!
interface Vlan40
  description LAN-40-RESEARCH
  ip address 192.168.40.4 255.255.255.0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
end

```

|      |      |                |        |      |                         |      |
|------|------|----------------|--------|------|-------------------------|------|
|      |      | Ковальчук І.В. |        |      | КІК.КР.Б – 123 – 7 – ПЗ | Арк. |
|      |      | Головня О.С.   |        |      |                         | 98   |
| Змн. | Арк. | № докум.       | Підпис | Дата |                         |      |