Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)
Кафедра Інформатики
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

ДОСЛІДЖЕННЯ ТА ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ
(тема)

Виконав:
студент 2 курсу, групи ІНФм-23-1
Босенко А.М.
(прізвище, ініціали)

Спеціальності 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

Керівник доц. Тітова О.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Кобилін О.А.
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)

Кафедра Інформатики
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Босенку Артему Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження та застосування технологій забезпечення безпеки мережевої інфраструктури

затверджена наказом по університету від 25 листопада 2024 року № 1246Ст

2. Термін подання студентом роботи до екзаменаційної комісії 30 грудня 2024 р.

3. Вихідні дані до роботи науково-методична та науково-технічна література, матеріали конференцій та форумів, дані інтернет-мережі, документація використаних інструментів.

4. Перелік питань, що потрібно опрацювати в роботі

1. Огляд методів забезпечення безпеки мережевої інфраструктури.
2. Дослідження моделей для налаштування безпеки брандмауера.
3. Реалізація правил та політик безпеки брандмауера для забезпечення безпеки мережевої інфраструктури.
4. Тестування налаштованих правил та політик безпеки брандмауера.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) актуальність проблеми забезпечення безпеки мережевої інфраструктури, постановка задачі, тестові налаштування правил безпеки брандмауера.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу	25.11.2024	
2	Аналіз завдання, підбір літератури	26.11.24-29.11.24	
3	Аналіз літератури з досліджуваної проблеми	01.12.24-04.12.24	
4	Аналіз платформ для роботи з брандмауерами	05.12.24-06.12.24	
5	Конфігурація правил безпеки брандмауера	09.12.24-14.12.24	
6	Програмна реалізація	16.12.24-20.12.24	
7	Оформлення пояснювальної записки	21.12.24-30.12.24	
8	Перевірка на плагіат	03.01.2024	
9	Рецензування	05.01.2024	
10	Підготовка презентації та доповіді	06.01.2024	
11	Занесення роботи в електронний архів	07.01.2025	
12	Попередній захист кваліфікаційної роботи	07.01.2025	

Дата видачі завдання 25 листопада 2024 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Тітова О.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ/ABSTRACT

Пояснювальна записка до кваліфікаційної роботи: 68 с., 5 табл., 33 рис., 40 джерел.

МЕРЕЖЕВА ІНФРАСТРУКТУРА, FIREWALL , FMC, FIREPOWER MANAGEMENT CENTER, CISCO, DDoS-АТАКИ, НАЛАШТУВАННЯ БЕЗПЕКИ МЕРЕЖІ.

Об’єктом роботи є правила та політики безпеки брандмауера для мережевої інфраструктури.

Метою роботи є налаштування правил та політик брандмауера за допомогою платформи FMC для забезпечення безпеки мережевої інфраструктури.

У ході роботи основну увагу приділено використанню та налаштуванню брандмауера, як основного чинника забезпечення безпеки мережі. Для цього було використано продукт Firepower Management Center (FMC), для ефективного налаштування безпеки. Досліджено вплив кібератак на мережеву інфраструктуру та способи їх нейтралізації за допомогою сучасних засобів захисту, на прикладі FMC.

У результаті роботи здійснено налаштування правил безпеки брандмауера та проаналізовано події, які були згенеровані на основі обробки трафіку згідно з налаштованими правилами.

NETWORK INFRASTRUCTURE, FIREWALL, FMC, FIREPOWER MANAGEMENT CENTER, CISCO, DDoS-ATTACKS, NETWORK SECURITY SETTINGS

The object of the work is the firewall security rules and policies for the network infrastructure.

The purpose of the work is to configure firewall rules and policies using the FMC platform to ensure the security of the network infrastructure.

During the work, the main attention is paid to the use and configuration of the firewall as the main factor in ensuring the security of the network. For this, the Firepower Management Center (FMC) product was used to effectively configure security. The impact of DDoS-attacks on the network infrastructure and ways to neutralize them with the help of modern means of protection are investigated, using the example of FMC.

As a result of the work, got configured firewall security rules and analyzed events, generated based on traffic processing according to the configured rules.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

FMC – Firewall Management Center

FTD – Firepower Threat Defense

Firewall (мережевий екран, брандмауер) – це загальна назва фізичних пристроїв чи програмних застосунків, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором правил безпеки

VPN (virtual private network) – це технологія, яка дає змогу створювати віртуальні захищені мережі поверх інших мереж із нижчим рівнем довіри.

Access Policy – політики забезпечення доступу до брандмауера

Prefilter Policy – політика попередньої фільтрації трафіку

Decryption Policy – політика розшифрування та обробки трафіку

Identity Policy – політика перевірки авторизації та автентифікації клієнта на основі трафіку

ВСТУП

Брандмауери у сучасному світі мають деяку особливість, яка базується на багатофункціональності інструментів для ефективного захисту приватних мережевих інфраструктур. Ці інструменти забезпечують захист на рівні пакетів та на рівні додатків. Саме це дозволяє дуже зручно керувати трафіком та запобігати загрозам. Безпека мережевої інфраструктури базується на двох факторах: правильний вибір брандмауера та його налаштування [1]. Це мінімізує ризики небажаного доступу до мережі та забезпечує конфіденційність та цілісність приватних даних.

Реалізація брандмауерів відбувається на двох рівнях: на апаратному та програмному. Слід зазначити, що це дозволяє мати велику кількість функціональних можливостей залежно від типу та рівня безпеки [2].

Наступним чинником забезпечення безпеки мережевої інфраструктури є правила фільтрації трафіку, які ґрунтуються на параметрах запитів до локальної мережі. Основними параметрами є:

– IP-адреса за якою може бути дозволено або заборонено трафік. Це може бути або конкретне значення IP-адреси, або діапазон IP-адрес;

– правила можуть бути налаштовані на основі номерів портів, що використовуються для різних протоколів. Наприклад, порт 80 зазвичай використовується для HTTP, а порт 443 для HTTPS;

– правила можуть також базуватися на типах протоколів, таких як TCP, UDP або ICMP [3]. Завдяки цьому є можливість налаштовувати брандмауер для обробки конкретних типів трафіку.

Актуальність дослідження полягає у важливості підтримки безпеки мережевої інфраструктури у сучасному світі, з дотриманням актуальних практик та протоколів безпеки. Необхідно поширювати навички налаштування правил та політик безпеки серед спеціалістів для збільшення протидії небажаним вторгненням у приватну мережу.

1 ОГЛЯД ОСНОВНИХ ЗАСОБІВ НАЛАШТУВАННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

1.1 Основні відомості про брандмауери та їх види

Брандмауер або фаєрвол – це загальна назва фізичних пристроїв чи програмних застосунків, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором правил безпеки [4]. Він є одним з основних засобів забезпечення безпеки сучасних мережевих інфраструктур. Брандмауер виконує роль захисного бар'єра (екрана) між внутрішньою мережею, що може належати організації, установі або приватній особі, та зовнішнім середовищем, яке можна назвати загальною інтернет мережею [5]. Головним завданням брандмауера є контроль і фільтрація вхідного та вихідного мережевого трафіку за допомогою правил, які можна задати використовуючи відповідні застосунки [6].

Важливість безпеки комп'ютерних мереж з'явилась ще з початку використання з'єднаних між собою групи пристроїв і дедалі зростає. А безпека цих мереж забезпечується такими інструментами як брандмауери. Розвиток цих технологій дозволяє створювати гнучкі і ефективні рішення, здатні запобігати несанкціонованому та неправомірному доступу до мереж, блокувати шкідливий трафік, а також контролювати використання мережевих ресурсів [7].

Особливість сучасних брандмауерів полягає у наявності багатофункціональних інструментів, які здатні ефективно захищати мережеву інфраструктуру організацій і користувачів. Вони забезпечують як базовий захист на рівні пакетів, так і складний захист на рівні додатків, що дозволяє гнучко керувати трафіком та запобігати загрозам [8]. Правильний вибір брандмауера та його налаштування є невід'ємними складовими безпеки мереж, що дозволяє уникнути ризиків неправомірного доступу, зберегти

конфіденційність та цілісність приватних даних, та забезпечити зручну та безперебійну роботу служб для налаштування мережевих інфраструктур [9].

Брандмауери можуть бути реалізовані як на апаратному, так і на програмному рівні і мати різноманітні функціональні можливості залежно від типу та рівня безпеки [10].

1.1.1 Апаратні брандмауери

Фізичні пристрої, які зазвичай розміщуються на межі мережі та контролюють вхідний і вихідний трафік між зовнішньою мережею інтернет та внутрішньою локальною мережею пристроїв – називаються апаратними брандмауерами. Цей вид брандмауерів здатний обробляти великі обсяги трафіку з дуже швидко, за рахунок встановлених потужних процесорів та спеціальних апаратних прискорювачів, встановлених в середину фізичного пристрою.

Наявність апаратного брандмауера більш притаманно великим корпораціям для забезпечення безпеки великої внутрішньої мережевою інфраструктури. Через це недоліком апаратного брандмауера є висока вартість самого фізичного пристрою, а також його встановлення та підтримка роботи [11, 12].

Прикладом апаратного брандмауеру є Cisco ASA (Adaptive Security Appliance). Цей пристрій є одним із найбільш популярних апаратних брандмауерів. Він надає рішення для захисту мережі з великим набором функціоналу, бо поєднує у собі безпосередньо функції брандмауера, VPN (virtual private network), систему запобіганню вторгнень (IPS) та антивірусного захисту. Також, цей пристрій користувачі обирають через легкість інтеграції та налаштування Cisco ASA з іншими пристроями для роботи мережі від компанії Cisco. Також, додатковим чинником

використання Cisco ASA є широкий набір правил безпеки (security policies) для різних пристроїв, з якими проведена інтеграція [13, 14].

1.1.2 Програмні брандмауери

Програми, а в деяких випадках компоненти операційної системи, які встановлюються безпосередньо на комп’ютерах або серверах – називаються програмними брандмауерами. Цей вид брандмауерів контролюють трафік на рівні окремих незалежних пристроїв.

Основною перевагою програмних брандмауерів є гнучкість у налаштуванні та легкість у використанні. Вони є ідеальними для персонального використання, а також можуть бути використані для захисту пристроїв, що мають обмежений доступ до корпоративної мережі. Водночас, програмні брандмауери здатні впливати на продуктивність пристрою. Внаслідок використання обчислювальних потужностей процесору та оперативної пам’яті комп’ютера, на якому використовується програмний брандмауер, може виникнути проблема зниження продуктивності пристрою.

Прикладом програмного брандмауеру є Windows Defender Firewall [15]. Це вбудований брандмауер для операційних систем Windows, який призначений для контролю вхідного та вихідного трафіку комп’ютеру з встановленою операційною системою, зазначеною вище.

Окрім налаштування правил безпеки пристрою, Windows Defender Firewall також має інструменти для інтеграції з іншими компонентами забезпечення безпеки комп’ютера, такими як антивірус та захист від загроз. Windows Defender Firewall також надає можливість фільтрації трафіку для окремих програм.

1.1.3 Хмарні брандмауери

Важливим елементом сучасних мережевих інфраструктур є хмарні брандмауери, ще відомі під назвою брандмауери як сервіс (Firewall as a Service, FWaaS). Важливість цього типу брандмауери особливо підкреслюється в умовах зростання популярності хмарних технологій [16]. Вони забезпечують захист мережевих ресурсів і даних, які розміщені в хмарах, а також управління трафіком, що проходить через мережу інтернет.

Хмарні брандмауери не потребують фізичного обладнання і через це знижуються витрати на організацію інфраструктури забезпечення безпеки. Також вагомою перевагою хмарних брандмауерів є висока доступність, оскільки вони можуть бути розгорнуті у декількох дата-центрах, що забезпечує надійний захист та швидкий доступ до ресурсів, даних та трафіку. Через високу доступність підкреслюється легкість у масштабуванні хмарних брандмауерів, для забезпечення безпеки великої кількості користувачів.

Прикладом хмарного брандмауеру є WAF (Web Application Firewall) від компанії Amazon. Цей брандмауер працює тільки у середовищі AWS (Amazon Web Services) та пропонує зручний вебзастосунок для налаштування безпеки додатків, які були розгорнуті в AWS, для запобігання шкідливих запитів та DDoS-атак.

1.2 Базові відомості про налаштування правил брандмауера

Найбільш важливим етапом в забезпеченні безпеки мережевої інфраструктури є налаштування правил брандмауера, оскільки правильно сформовані правила дозволяють ефективно та швидко фільтрувати трафік мережі, блокуючи несанкціоновані запити. Однак, налаштування брандмауера вимагає розуміння мережевих технологій та потенційних ризиків [17].

Розрізняють три основні принципи налаштування та роботи з правилами брандмауера:

– принцип найменших привілеїв (PoLP) – користувачі та пристрої можуть мати лише обмежені права для виконання лише цільового завдання. Це дозволяє пропускати лише аутентифіковані запити до локальної мережі;

– розділення мережі на окремі локальні сегменти для кращого контролю доступу до внутрішніх ресурсів;

– правила брандмауера мають регулярно перевірятись та оновлюватись для відображення змін у локальній мережі під нові загрози.

В першу чергу процес налаштування правил безпеки розпочинається з оцінки вимог до безпеки організації. Цей підготовчий етап є важливим для визначення, які ресурси або вебзастосунки потрібно захистити, які користувачі мають доступ, визначити їх ролі та права доступу, а також які типи трафіку можуть бути небезпечними. Наступним кроком є створення базових правил [18, 19].

При налаштуванні правил важливо визначити їх пріоритетність. Правила брандмауера зазвичай обробляються за порядком їх створення або відповідно до заданих пріоритетів, тому важливо правильно налаштувати їх, щоб уникнути конфліктів між різними правилами. Розглянемо основні види правил брандмауера.

1.2.1 Правила фільтрації трафіку

Правила фільтрації трафіку є важливою частиною брандмауера. Вони повинні базуватись на параметрах запитів які надсилають запит до локальної мережі. Основними параметрами є:

– IP-адреса за якою може бути дозволено або заборонено трафік. Це може бути або конкретне значення IP-адреси, або діапазон IP-адрес. Завдяки

цьому адміністратор контролює пристрої, які можуть під’єднуватись до мережі;

– правила можуть бути налаштовані на основі номерів портів, що використовуються для різних протоколів. Наприклад, порт 80 зазвичай використовується для HTTP, а порт 443 для HTTPS. Адміністратори можуть заблокувати доступ по певним портам, щоб запобігти несанкціонованому доступу до мережі;

– правила можуть також базуватися на типах протоколів, таких як TCP, UDP або ICMP. Завдяки цьому є можливість налаштовувати брандмауер для обробки конкретних типів трафіку [20, 21].

Приклад правил фільтрації трафіку наведено в таблиці 1.1.

Таблиця 1.1 – Приклад правил фільтрації трафіку

Пріоритет	IP-адреса джерела	IP-адреса призначення	Протокол	Порт	Дія	Опис
1	192.168.1.10	0.0.0.0/0	TCP	80	Allow	Дозволяє трафік по HTTP з внутрішнього IP-адресу.
3	203.0.113.5	0.0.0.0/0	ANY	ANY	Block	Блокує трафік з відомої IP-адреси.
2	0.0.0.0/0	192.168.1.0	TCP	443	Allow	Дозволяє трафік по HTTPS до внутрішньої мережі.

1.2.2 Правила NAT

Правила NAT (Network Address Translation) використовуються для перетворення IP-адрес запитів, що проходять через брандмауер. Завдяки цьому приватні IP-адреси, які використовуються в локальній мережі, перетворюються на публічні IP-адреси для доступу до загальної мережі інтернет. Розділяють 2 типи NAT: статичний (призначена одна публічної IP-адреси для однієї приватної) та динамічний (використовується набір публічних IP-адрес для відображення приватних адрес) [22]. Приклад правил NAT наведено на таблиці 1.2.

Таблиця 1.2 – Приклад правил NAT

Пріоритет	IP-адреса внутрішня	IP-адреса зовнішня	Тип NAT	Опис
1	192.168.1.10	203.0.113.10	Статичний	Призначає публічну IP-адресу для доступу в інтернет.
2	192.168.1.0/24	203.0.113.0/24	Динамічний	Дозволяє приватним адресам виходити в інтернет через пул публічних адрес.

1.2.3 Правила для VPN

VPN (Virtual Private Network) дозволяє користувачам з’єднуватися з віддаленими ресурсами (вебсервер, вебзастосунок і т. д.) через зашифровані тунелі, задля забезпечення конфіденційності та безпеки даних. Тому правила для VPN забезпечують захист трафіку, що проходить через віртуальні

приватні мережі. Для використання VPN користувач має бути аутентифікованим, а дані, які передає або отримує користувач, мають бути зашифровані. Приклад правил VPN наведено на таблиці 1.3.

Таблиця 1.3 – Приклад правил VPN

Пріоритет	Протокол	Порт	Дія	Опис
1	UDP	500	Allow	Дозволяє VPN-трафік для підключення до корпоративної мережі.
2	TCP	80	Block	Блокує трафік, якщо він не проходить через VPN.

1.2.4 Правила на основі контенту

Для аналізу змісту даних, які передаються в приватну мережу, застосовуються правила на основі контенту. Вони дозволяють або блокують трафік залежно від розширення файлу (наприклад .exe), вмісту файлу та URL з якого завантажується файл.

Таблиця 1.4 – Приклад правил на основі контенту

Пріоритет	**URL**	**Тип файлу**	**Дія**	**Опис**
1	**2**	**3**	**4**	**5**
1	ALL	*.exe	Block	Блокує завантаження виконуваних файлів.

Продовження таблиці 1.4

1	2	3	4	5
2	www.tiktok.com	ALL	Block	Блокує доступ до соціальних мереж.

1.3 Огляд застосунків для налаштування безпеки мережевої інфраструктури

1.3.1 Cisco FMC (Firewall Management Center)

Cisco FMC є централізованою платформою для управління брандмауерами мережі Cisco комплектуючих, які пов’язані у одну систему [23]. Ця платформа призначена для побудови комплексної системи захисту, яка підходить для середніх і великих організацій з потребами багаторівневого підходу до управління безпекою та захисту даних. FMC надає можливість централізованого управління правил і завдяки цьому дозволяє створювати, тестувати та застосовувати правила брандмауера для великої кількості пристроїв, таким чином забезпечуючи узгодженість мережевої інфраструктури [24].

Для зручного аналізу трафіку Cisco FMC дає можливість відстежувати події та активність у мережеві в режимі реального часу. Завдяки цьому з’являється можливість оперативно реагувати на підозрілі події у мережі.

Великою перевагою Cisco FMC є можливість інтеграції з іншими продуктами компанії та створення гнучкої можливості налаштування та управління безпекою мережевої інфраструктури.

1.3.2 pfSense

pfSense — це платформа з відкритим програмним кодом, яка працює як брандмауер і маршрутизатор (поєднує дві або більше мереж та дозволяє

передавати дані між ними). Здебільшого, ця платформа підходить для малих, середніх підприємств та задля особистого використання завдяки доступності, гнучкості та підтримці великої кількості мережевих функцій та гнучкому налаштуванню.

Платформа pfSense підтримує сучасні протоколи для налаштування VPN: OpenVPN, IPSec, PPTP. Завдяки цьому при використанні платформи є інструмент для конфігурації приватної мережі для забезпечення безпеки даних. Ще одним плюсом є автоматичний розподіл трафіку між декількома мережевими інтерфейсами для збільшення пропускної спроможності мережевої інфраструктури [25].

Також беззаперечною перевагою pfSense є відкритий програмний код, що робить цю платформу безкоштовною для користувачів та має підтримку функціоналу від великої спільноти.

1.3.3 FortiGate

Для середній та великих організацій був розроблений брандмауер нового покоління FortiGate. Він включає в себе функції мережевої безпеки та високу продуктивність, що в свою чергу дозволяє захищати мережеву інфраструктуру від комплексних загроз, такі як кібератаки. Це стало можливим через наявність інтегрованої системи запобігань вторгненням.

Так само як і pfSense, FortiGate має розвинену систему для налаштування VPN локальної мережі, користувачі відзначають високу продуктивність роботи VPN цієї платформи. Також, перевагою FortiGate є можливість швидкої обробки великих масивів даних. Цей аспект є критичним для великих компаній. Як і обидва конкурента (Cisco FMC та pfSense), FortiGate має інтуїтивно-зрозумілий інтерфейс, що спрощує налаштування та підтримку безпеки мережевої інфраструктури.

1.4 Порівняльний аналіз зручності та доступності між застосунками для налаштування безпеки мережевої інфраструктури

У даному розділі складено порівняльну характеристику у вигляді таблиці трьох найбільш популярних платформ для налаштування безпеки мережевої інфраструктури: Cisco FMC, pfSense, FortiGate [26].

Критеріями для порівняння є: тип, ліцензування, вартість, середня кількість користувачів, інтерфейс користувача, функціонал, масштабованість, складність налаштування. Порівняльна характеристика платформ показана на таблиці 1.5.

Таблиця 1.5 - Порівняльна характеристика платформ по критеріям

Критерій	**Cisco FMC**	**pfSense**	**FortiGate**
1	**2**	**3**	**4**
Тип	Централізована система управління брандмауерами (Cisco ASA та FTD)	Програмний брандмауер, розгортається як віртуальний пристрій	Комплексне рішення для безпеки мережі
Ліцензування	Комерційне	Безкоштовне	Комерційне
Вартість ($, долар США)	1000 – 10000	Безкоштовно (наявні платні версії з додатковими функціями)	500 – 2000
Середня кількість користувачів	До 2000	До 500	До 1000
Інтерфейс користувача	Веб-інтерфейс	Веб-інтерфейс	Веб-інтерфейс та консоль CLI

Продовження таблиці 1.5

1	2	3	4
Функціонал	Централізоване управління брандмауерами, політики безпеки, VPN, звітність	Брандмауер, VPN, балансування навантаження	Брандмауер, IPS, VPN, звітність, контроль додатків
Масштабованість	Висока, підтримує централізоване управління великою кількістю пристроїв	Висока для своїх категорій, підтримує кластеризацію	Висока, адаптивне масштабування для середніх і великих мереж
Складність налаштування	Висока, вимагає досвіду роботи з Cisco продуктами	Середня	Середня

На основі аналізу існуючих застосунків для налаштування безпеки мережі, для подальшого дослідження було обрано Cisco FMC. Завдяки підтримці найбільшої кількості користувачів та наявності звітності ця платформа є найкращим варіантом для налаштування правил брандмауера.

1.5 Постановка задачі дослідження

Таким чином, дослідження технологій, застосунків та підходів налаштування безпеки мережевої інфраструктури є актуальним завданням в сфері забезпечення безпеки комп’ютерних мереж. Тому ставиться завдання

застосування інструментів та сучасних підходів налаштування правил брандмауера для забезпечення безпеки мережевої інфраструктури.

Об’єктом дослідження є безпека комп’ютерної мережі, яка під’єднана до глобальної мережі інтернет.

Метою дослідження є налаштування безпеки мережевої інфраструктури, за допомогою застосунку FMC (Firewall Management Center), та аналіз трафіку, який надходить у локальну мережу.

Для досягнення мети необхідно вирішити такі завдання:

– провести аналіз існуючих платформ для налаштування безпеки мережевої інфраструктури;

– ознайомитися з моделями для налаштування правил брандмауера на платформі Cisco FMC;

– реалізувати налаштування правил брандмауера для фільтрації трафіку на платформі Cisco FMC;

– проаналізувати результат обробки трафіку за створеними правилами брандмауера за допомогою інтегрованої звітності Cisco FMC.

2 ДОСЛІДЖЕННЯ МОДЕЛЕЙ ДЛЯ НАЛАШТУВАННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ У ЗАСТОСУНКУ FMC

2.1 Дослідження та аналіз застосунку FMC як інструмент налаштування правил безпеки брандмауера

Cisco Firewall Management Center був розроблений як ключовий компонент забезпечення безпеки екосистеми мережеві пристроїв Cisco для управління брандмауерами та іншими системами захисту [27, 28]. Історія створення продукту почалася в 2013 році, коли Cisco придбала компанію Sourcefire, яка відома розробками в галузі мережевої безпеки, зокрема створенням IPS-систем (систем запобігання вторгненням) [29]. У свій час Sourcefire стала головною компанією у розробці інноваційних рішень, прикладом є система запобігання вторгненням Snort. Ця система стала широко використовуватися в сфері кібербезпеки завдяки таким особливостям як: надійність, відкритий код системи та здатність адаптуватися до нових загроз. Тільки придбання Sourcefire дозволило Cisco отримати доступ до інноваційних технологій та дало можливість інтегрувати їх у власні продукти. Завдяки цьому важливому кроку відкрилась можливість створення та розвитку FMC.

Особливістю продукту FMC стало централізоване управління усіма пристроями безпеки Cisco в корпоративних мережах. Єдина платформа керування дозволяє значно оптимізувати процеси забезпечення безпеки. Використовуючи FMC можна відстежувати мережевий трафік, створювати і застосовувати політики безпеки, а також отримувати аналітику про загрози в реальному часі. Ця можливість стала великим нововведенням та була втілена у життя завдяки інтеграції з продуктом Cisco Talos. Він включає в себе аналітичу команду з кібербезпеки, яка відповідає за моніторинг нових загроз та розробку алгоритмів для їх блокування. Компанія Cisco продовжує

удосконалювати FMC шляхом додавання нових функцій та покращення здатності обробляти трафік і аналізувати загрози [30].

Cisco FMC надає можливість створення гнучких правил фільтрації трафіку. Користувачі можуть визначати ці правила при конфігурації політик безпеки, а саме такими параметрами, як IP-адреси, протоколи та порти, що дозволяє забезпечувати високий рівень захисту мережевої інфраструктури. Крім того, платформа підтримує створення таких складних сутностей як політики, які охоплюють як вхідний, так і вихідний трафік, що дає змогу краще адаптувати захист до специфічних потреб мережі.

На сьогоднішній день, Cisco FMC є лідером серед потужних інструментів для забезпечення мережевої безпеки у корпоративних середовищах. FMC став важливою складовою екосистеми Cisco, спрямованою на підвищення рівня кіберзахисту та адаптацію до нових викликів у сфері інформаційної безпеки [31]. Це стало можливим завдяки забезпеченню комплексного захисту від загроз та централізованому управлінню політиками безпеки. FMC дозволяє налаштувати та керувати VPN-з’єднаннями, забезпечуючи захист віддаленого доступу роботи корпоративних мереж. Захист від загроз і інтегрований IPS є важливими складовими безпеки FMC. Завдяки цій функції платформа може виявляти й блокувати потенційні загрози в режимі реального часу (рис. 2.1).

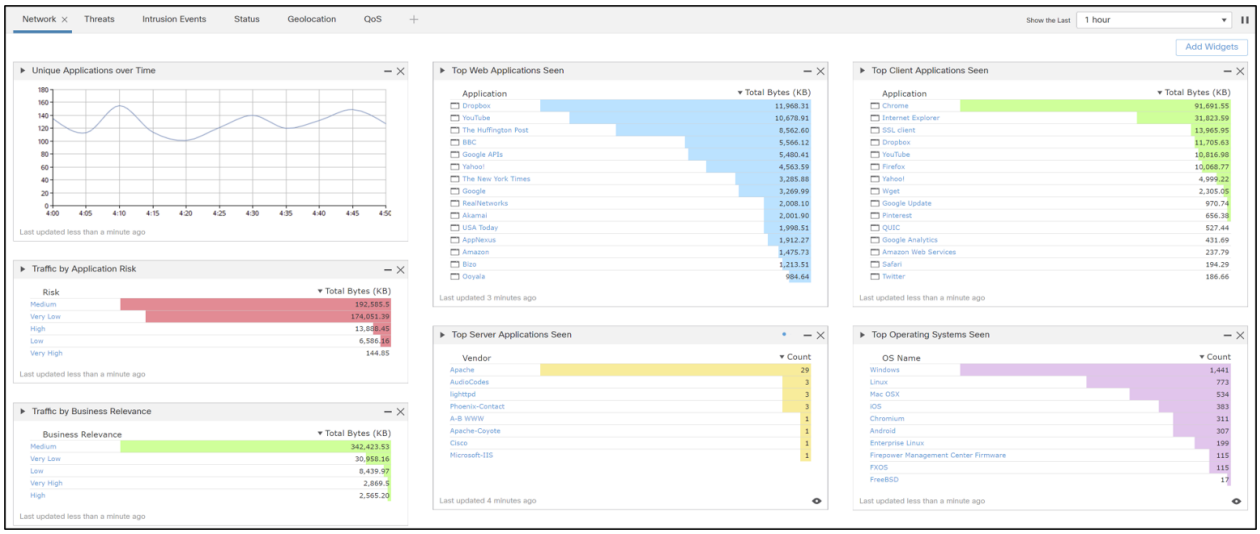


Рисунок 2.1 – Сторінка для аналізу трафіку та подій у застосунку FMC

Завдяки своїм широким можливостям, включаючи централізоване управління, гнучке налаштування політик і автоматизовану безпеку, Cisco FMC є ефективним рішенням для великих підприємств, які потребують потужних засобів захисту мережі. Високий рівень аналітики та адаптивність роблять FMC лідером серед рішень з управління мережевою безпекою, однак цей інструмент оптимальний для середніх та великих компаній із складною інфраструктурою та великими вимогами до захисту.

2.2 Огляд сутностей призначених для налаштування правил безпеки брандмауера

Для того аби перейти до етапу налаштування правил безпеки брандмауера для забезпечення безпеки мережевої інфраструктури, потрібно ознайомитись з базовими моделями. Тільки використовуючи ці моделі можна зручно та швидко налаштувати обмеження для вхідного або вихідного трафіку корпоративної мережі.

Основною моделлю, яка відповідає за отримання або відправку трафіку корпоративної мережі є Firepower Threat Defense (FTD) [32, 33]. Вона включає в себе функції традиційного брандмауера, правила для якого необхідно налаштувати. Отже, всі інші моделі представляють з себе правила обробки трафіку, які мають застосовуватися для FTD.

Cisco Firepower Threat Defense в рамках Firepower Management Center забезпечує централізоване керування та контроль над усіма аспектами безпеки мережевої інфраструктури. FMC дозволяє користувачам налаштовувати та управляти правилами безпеки, за допомогою іншої моделі Access Control Policy, здійснювати контроль трафіку та переглядати аналітику загроз на всіх пристроях з FTD, що під’єднані до мережі. Таким чином, у такій взаємодії FTD діє як захисний екран корпоративної мережі, а FMC — як інтерфейс управління правилами безпеки та аналізу трафіку FTD.

Лістинг 2.1 Спрощена модель відображення сутності FTD:

```
FirepowerThreatDefense {
    name: string,
    description: string,
    model: string,
    version: string,
    licenses: Array<string>,
    acp: AccessControlPolicy,
    interfaces: Array<{
        name: string,
        description: string,
        type: SubInterface | RedundantInterface | VTI Interface | Loopback,
        macAddress: string,
        ipAddress: string
    }>
}
```

Основним інструментом для управління правилами безпеки брандмауера, які визначають дії, що мають відбутися під час аналізу трафіку на основі певних критеріїв (IP-адреса, порт, протокол) є Access Control Policy. Прикладом застосування цієї політики безпеки є налаштування контролю доступу таким чином, щоб блокувати увесь трафік від ненадійних зовнішніх мереж, або обмежити доступ до окремих вебзастосунків чи вебсерверів для окремої корпоративної мережі.

Лістинг 2.2 Спрощена модель відображення сутності Access Control Policy:

```
AccessControlPolicy {
    name: string,
```

description: string,

lastModified: string,

defaultAction: BlockTraffic | IntrusionPrevention | NetworkDiskovery,

rules: Array< AccessControlPolicyRule>

}

Access Control Policy включає в себе налаштування інших політик: Prefilter Policy, Decryption Policy та Identity Policy. Це зроблено для того, щоб відокремити різні зони відповідальності аналізу трафіку. У свою чергу Access Control Policy виступає у ролі контейнера, який агрегує в собі правила з дочірніх політик, а також додає свої специфічні правила обробки та контролю трафіку. Загальний вигляд обробки потоку трафіку показано на рисунку 2.2.

Рисунок 2.2 – Перебіг обробки трафіку (де Packets – це пакет даних трафіку)

Складовою частиною Access Control Policy є Access Control Policy Rule, яка визначає дії, націлені на певний тип трафіку. Визначення типу трафіку відбувається за допомогою критеріїв фільтрації трафіку. Порядок правил важливий, оскільки кожне вони обробляються послідовно. У момент, коли трафік відповідає правилу відбувається дія, зазначена у правилі, а подальша перевірка припиняється.

Лістинг 2.3 Спрощена модель відображення сутності Access Control Policy Rule:

AccessControlPolicyRule {

name: string,

action: Allow | Block | Trust | Monitor,

sourceNetworks: Array<Network>,

sourceZones: Array<string>,
destinationNetworks: Array<Network>,
destinationPorts: Array<Port>,
destinationZones: Array<string>,
comments: string
}

Для визначення базових правил швидкої обробки трафіку, ще до етапу детального аналізу, використовується Prefilter Policy (політика попередньої фільтрації). Це перший етап обробки трафіку з мережі. Використання цього етапу може прискорити продуктивність мережевої інфраструктури. Найбільша різниця продуктивності використання цієї політики виявляється на великих обсягах даних, які проходять через брандмауер.

Лістинг 2.4 Спрощена модель відображення сутності Prefilter Policy:

PrefilterPolicy {
name: string,
description: string,
lastModified: string,
modifiedBy: string,
domain: string,
rules: Array< PrefilterPolicyRule >
}

Основною метою Prefilter Policy є спрощення фільтрації трафіку шляхом застосування певних правил (Prefilter Policy Rule) до певного типу даних, наприклад, дозволяючи або блокуючи доступ трафіку до корпоративної мережі, не відправляючи їх на детальний аналіз системою запобіганню вторгненням (IPS) або іншими сервісами детальної перевірки трафіку.

Лістинг 2.5 Спрощена модель відображення сутності Prefilter Policy Rule:

```
PrefilterPolicyRule {
    name: string,
    action: Analyze | Block | FastPath,
    sourceNetworks: Array<Network>,
    sourcePorts: Array<Port>,
    destinationNetworks: Array<Network>,
    destinationPorts: Array<Port>
}
```

Для обробки зашифрованого трафіку (SSL/TLS протокол) використовується модель Decryption Policy. Розшифровка трафіку надає брандмауеру можливість аналізувати зашифрований трафік, виявляти потенційні загрози і контролювати доступ на основі контенту, який зазвичай прихований за допомогою шифруванню контенту.

Лістинг 2.6 Спрощена модель відображення сутності Decryption Policy:

```
DecryptionPolicy {
    name: string,
    description: string,
    lastModified: string,
    modifiedBy: string,
    rules: Array<DecryptionPolicyRule>
}
```

За допомогою окремих правил, представлених моделлю Decryption Policy Rule, до трафіку можуть застосовуватися наступні дії:

– Decrypt-Resign (розшифровування трафіку для аналізу та подальшого підписання за допомогою сертифіката Internal Certificate);

– Decrypt-Known key (розшифровування трафіку для аналізу без подальшого підписання сертифікатом);

– Do not decrypt (розшифрування трафіку не відбувається, прикладом є трафік з банківських вебзастосунків).

Лістинг 2.7 Спрощена модель відображення сутності Decryption Policy Rule:

```
DecryptionPolicyRule {
    name: string,
    action: Decrypt-Resign | Decrypt-Knownkey | DoNotDecrypt,
    sourceZones: Array<string>,
    sourceNetwoks: Array<Network>,
    sourcePorts: Array<Port>,
    destinationZones: Array<string>,
    destinationNetwoks: Array<Network>,
    destinationPorts: Array<Port>,
    certificates: Array<InternalCa | InternalCsr | InternalCertificate>,
}
```

Для контролю доступу та застосування правил безпеки на основі інформації про користувача, або цілої групи користувачів, існує політика Identity Policy в FMC.

Користувач має можливість отримати більш детальну інформацію, на основі трафіку, про того, хто намагається отримати доступ до корпоративної мережі. Це зроблено задля забезпечення контролю доступу на рівні ідентифікації клієнта, що збільшує точність та ефективність безпеки мережевої інфраструктури. Також. Це дозволяє користувачам FMC застосовувати індивідуальні правила безпеки корпоративної мережі.

Лістинг 2.8 Спрощена модель відображення сутності Identity Policy:

```
IdentityPolicy {
    name: string,
    description: string,
    domain: string,
    status: string,
    lastModified: string,
    rules: Array<IdentityPolicyRule>
}
```

За допомогою окремих правил політики Identity Policy, представлених моделлю Identity Policy Rule, можна налаштовувати окремі випадки обробки даних відправника трафіку. Цей механізм обробки працює завдяки сутності Realm, як частини Identity Policy Rule. В цьому випадку Realm відповідає за ідентифікацію відправника за допомогою домену бази ідентифікації (наприклад Active Directory). Також, модель Realm контролює процес автентифікації користувачів, виконуючи запити до сторонніх сервісів автентифікації. Це допомагає визначити та підтвердити, що користувач має права доступу до необхідної корпоративної мережі.

Лістинг 2.9 Спрощена модель відображення сутності Identity Policy Rule:

```
IdentityPolicyRule {
    name: string,
    action: PassiveAuthentication | ActiveAuthentication | NoAuthentication,
    sourceZones: Array<string>,
    sourceNetwoks: Array<Network>,
    sourcePorts: Array<Port>,
    destinationZones: Array<string>,
```

```
    destinationNetwoks: Array<Network>,
    destinationPorts: Array<Port>,
    realm: {
        name: string,
        description: string,
        type: Local | LDAP | AzureAd,
        domain: string,
        value: string,
        enabled: boolean
    }
}
```

Модель Network дозволяє користувачам FMC визначити конкретні IP-адреси, або діапазони адрес, мережі, підмережі, хости або групи мереж для застосування під час створення правил безпеки брандмауера в політиках контролю доступу, безпеки і моніторингу. У свою чергу, це дозволяє чітко ідентифікувати, структурувати і управляти підконтрольними сегментами мережевої інфраструктури.

Використання Network моделі набагато спрощує створення об’єктів для визначення мереж та хостів. Саме це допомагає уникнути ручного введення IP-адрес для кожного правила політик і забезпечує їх швидке створення та легку підтримку.

У підсумку, Network є основним інструментом для структурування, управління та моніторингу мережевих політик безпеки в складних мережевих інфраструктурах, які контролюються за допомогою FMC.

Лістинг 2.10 Спрощена модель відображення сутності Network:

```
Network {
    name: string,
    description: string,
```

type: Group | Network

value: string

}

Модель Port – це об’єкт або група об’єктів, що представляють номери або діапазон номерів портів, які використовуються для ідентифікації та контролю різних типів трафіку. Завдяки цьому, користувачі FMC мають можливість налаштовувати правила безпеки на основі портів, які трафік використовує для з’єднання з корпоративною мережею.

Port надає можливість створювати об’єкти портів для конкретних протоколів, наприклад HTTP (порт 80), HTTPS (порт 443), FTP (порт 21), SSH (порт 22). Це спрощує і стандартизує правила та політики безпеки, адже користувач FMC може створювати правила для контролю доступу на основі портів, без необхідності багаторазового введення номері портів.

Лістинг 2.11 Спрощена модель відображення сутності Port:

Port {

name: string,

description: string,

type: Group | Port

protocol: TCP | UDP | ICMP | IPv6ICMP

value: string

}

Для забезпечення можливості генерації сертифікатів, які використовуються під час конфігурації SSL/TLS з’єднань на етапі створення Decryption Policy, платформа FMC має вбудовану функціональність Internal Certificate Authority (Internal CA). Це дозволяє FMC створювати, підписувати та керувати сертифікатами для захищених з’єднань і аутентифікації пристроїв.

Основною особливістю моделі Internal CA є надання можливості користувачам FMC створювати розвинену ієрархію довірених центрів сертифікації всередині корпоративної мережі, за допомогою генерації сертифікатів для внутрішніх користувачів і пристроїв без необхідності звернення до зовнішніх центрів сертифікації.

Лістинг 2.12 Спрощена модель відображення сутності Internal CA:

```
InternalCa {
    name: string,
    countryName: string,
    state: string,
    locality: string,
    organization: string,
    department: string,
    commonName: string
}
```

В результаті успішного створення Internal CA, користувач FMC має змогу створити, або підписати вже наявні, сертифікати, які представлені у вигляді моделі Internal Certificate. Сертифікат, створений за допмогою Internal CA, використовується для забезпечення захищених з’єднань між внутрішніми компонентами і пристроями мережевої інфраструктури.

Лістинг 2.13 Спрощена модель відображення сутності Internal Certificate:

```
InternalCertificate {
    name: string,
    certificateData: string,
    certificateString: string
}
```

2.3 Огляд сутностей призначених для відстеження трафіку по мережі

У випадку успішного налаштування правил та політик безпеки брандмауера, користувачу необхідно застосувати ці зміни для брандмауера. Для цього в рамках Firewall Management Center використовується спеціальний процес розміщення оновлених налаштувань на Firepower Threat Defense під назвою Deploy.

Під час цього процесу на першому етапі відбувається перевірка узгодженності нових змін (так як деякі зміни можуть конфліктувати між собою). У випадку відсутності цієї перевірки стабільність роботи брандмауера буде погіршена.

Після цього, якщо зміни узгодженні, оновлені налаштування будуть відправлені на відповідні пристрої (FTDs). Під час цього FMC синхронізує нові правила на пристроях в режимі реального часу. Це гарантує, що оновлені налаштування починають діяти негайно або відповідно до визначеного плану.

Для забезпечення роботи процесу Deploy, користувач має змогу відслідковувати статус роботи за допомогою моделі Deploy Item.

Лістинг 2.14 Спрощена модель відображення сутності Deploy Item:

```
DeployItem {
    device: FirepowerThreatDefense,
    modifiedBy: string,
    inspectInterruption: Progress | Done,
    group: string,
    lastDeployTime: srting,
    status: Progress | Info | Warning | Error  | Success
}
```

Після успішно завершеного процесу Deploy користувач Cisco Firewall Management Center має змогу перевірити роботу створених, або оновлених, правил та політик безпеки брандмауера. Результат обробки трафіку зберігається у форматі подій (events) на платформі FMC. Головною моделлю для відображення подій, які генеруються під час з'єднання до корпоративної мережі через Firepower Threat Defense, є Connection Event.

Connection Event - це пріоритетний компонент для аналізу результату обробки трафіку, бо він забезпечує відображення даних клієнтів і контроль над мережею. Це дозволяє користувачам FMC виявляти потенційні загрози або аномалії в трафіку. Дані з моделі Connection Event можуть бути використані для формування звітів, налаштування тригерів безпеки або систем запобіганню вторгнень, а також оптимізації правил та політик брандмауера для забезпечення кращої безпеки мережевої інфраструктури.

Лістинг 2.15 Спрощена модель відображення сутності Connection Event:

```
ConnectionEvent {
    firstPacket: string,
    lastPacket: string,
    action: Allow | Block | Trust | Monitor,
    reason: string,
    initiatorIp: string,
    responderIp: string,
    sourcePort: Por,t
    destinationPort: Port,
    client: ICMP | NETBIOS | IGMP
    application: string
    device: FirepowerThreatDefense
}
```

Модель Intrusion Event відображає події, в яких було виявлено потенційні загрози для мережевої інфраструктури, або кібератаки націлені на мережу. Події моделі Intrusion Event генеруються у випадку коли система запобігання вторгненням (IPS) виявляє трафік, що відповідає правилам виявлення загроз внаслідок аналізу трафіку на наявність поведінкових ознак злоякісного трафіку. Важлива особливість Intrusion Event полягає у викладенні детальної та вичерпної інформації про небезпеку, оскільки ця модель включає в себе додаткову інформацію про тип загрози та серйозність інциденту. Таким чином, користувач FMC може швидко провести аналіз та зреагувати на загрозу мережі.

Лістинг 2.16 Спрощена модель відображення сутності Intrusion Event:

```
IntrusionEvent {
    message: string,
    priority: Low | Medium | High | Critical,
    classification: string,
    count: number
}
```

У свою чергу модель Unified Event включає в себе всі можливі типи подій, які можуть генеруватись в процесі обробки трафіку, у мінімізованому форматі. У тому числі і ті, що були описані вище.

Ця модель надає можливість відобразити більшу кількість загальної інформації про події. Ще однією перевагою цієї моделі є можливість фільтрації подій за великою кількістю параметрів, що робить взаємодію дуже зручною з боку користувача FMC (рис. 2.3).

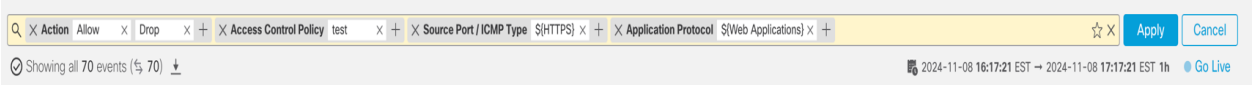


Рисунок 2.3 – Можливість фільтрації подій за окремими параметрами

Внаслідок цього, Unified Event є більш сучасною моделлю для відображення подій, однак, при необхідності більш детального аналізу Connection Event та Intrusion Event краще звернутись до відповідних моделей.

Лістинг 2.17 Спрощена модель відображення сутності Unified Event:

```
UnifiedEvent {
    time: string,
    type: Connection | File | Intrusion | Malware | Secure,
    action: Alert | Allow | Block | Detect | Drop | Monitor | Reject,
    reason: string,
    sourceIp: string,
    sourcePort: Port,
    destinationIp: string,
    destinationPort: Port,
    acpRule: AccessControlPolicyRule,
    acp: AccessControlPolicy,
    device: FirepowerThreatDefense
}
```

3 РЕАЛІЗАЦІЯ НАЛАШТУВАНЬ ПРАВИЛ БЕЗПЕКИ БРАНДМАУЕРА ЗА ДОПОМОГОЮ FMC

3.1 Налаштування базових правил та політик безпеки брандмауера

У рамках кваліфікаційної роботи було досліджено правила та політики безпеки для налаштування брандмауера, за допомогою платформи FMC. Для реалізації цих налаштувань потрібно скористатися візуальним інтерфейсом користувача платформи Firewall Management Center. Ця платформа була обрана виходячи з висновків під час аналізу доступних інструментів для налаштування брандмауера у першому розділі кваліфікаційної роботи.

Варто зазначити, що налаштовувати правила безпеки брандмауера можна також використовуючи консольний інтерфейс. До моменту створення візуального інтерфейсу FMC саме консольний вигляд був пріоритетним вибором користувачів. При порівнянні цих двох видів інтерфейсів користувача більш зручним способом налаштування правил та політик безпеки є візуальне відображення у вебзастосунку завдяки наочному та зрозумілому формату моделей. Це дозволяє швидко проводити аналіз правил та орієнтуватися серед великої кількості політик безпеки у складних системах налаштування. До створення вебзастосунку, користувач мав налаштовувати правила безпеки брандмауера тільки за допомогою тексту, тобто без зручних моделей для відображення правил та політик безпеки і це, в свою чергу, породжувало дуплікацію тексту у складних конфігураціях.

Окрім можливості зручного та зрозумілого відображення правил безпеки брандмауера, візуальний інтерфейс вебзастосунку має інтерактивні елементи (наприклад модальні діалогу, меню, підказки), які у свою чергу роблять процес створення, налаштування та підтримки політик безпеки простим та без необхідності запам’ятовувати складні команди для налаштування цих же правил безпеки брандмауера у консольному вигляді.

Головним недоліком консольного вигляду інтерфейсу користувача є неможливість перегляду аналітичних даних та звітів подій, як результат обробки трафіку. Саме тому переважна частина користувачів FMC обирає візуальне відображення інтерфейсу для налаштування правил безпеки брандмауеру. Для подальшого дослідження забезпечення безпеки мережевої інфраструктури було обрано саме вебзастосунок FMC.

Перед початком налаштування правил безпеки брандмауера користувач має пройти процес авторизації, для того щоб підтвердити що він саме спеціаліст (адміністратор) з підтримки безпеки мережевої інфраструктури. Це гарантує доступ до конфігурацій тільки довіреним особам. Приклад вигляду сторінки для авторизації користувача FMC наведено на рисунку 3.1.

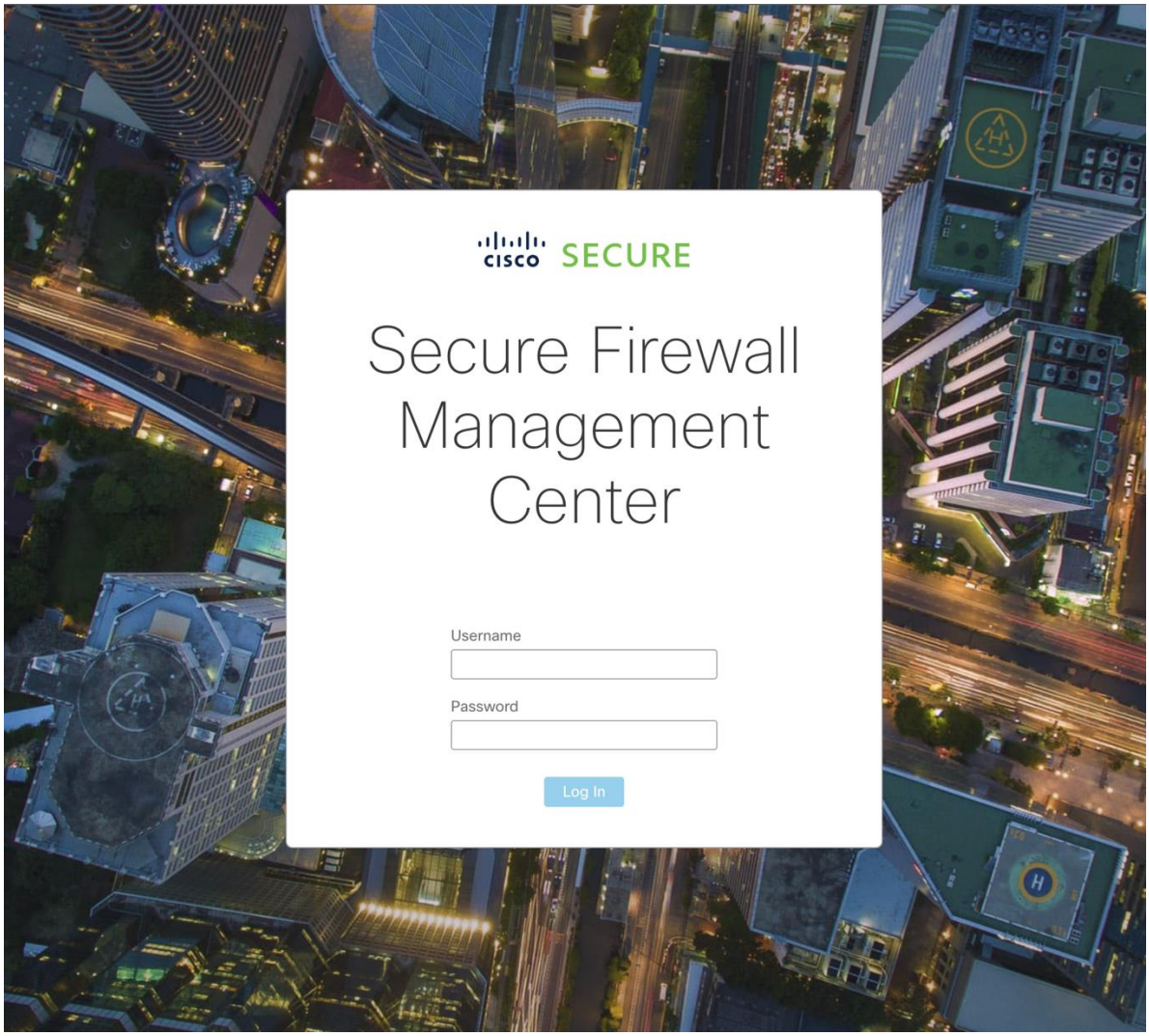


Рисунок 3.1 – Початкова сторінка для авторизації користувача FMC

Після успішної авторизації користувач має доступ до налаштування правил та політик брандмауера. Для зручної навігації в межах вебзастосунку користувачу запропоновано використовувати спеціальне меню у верхній частині застосунку (рис. 3.2). Для того аби перейти на будь-яку сторінку користувач має обрати одну із категорій: Overview, Analysis, Policies, Devices, Objects, Integration. Після цього користувач отримає випадаюче меню, за допомогою якого буде можливість перейти на сторінку представлення необхідної моделі за допомогою кліку на потрібний заголовок.

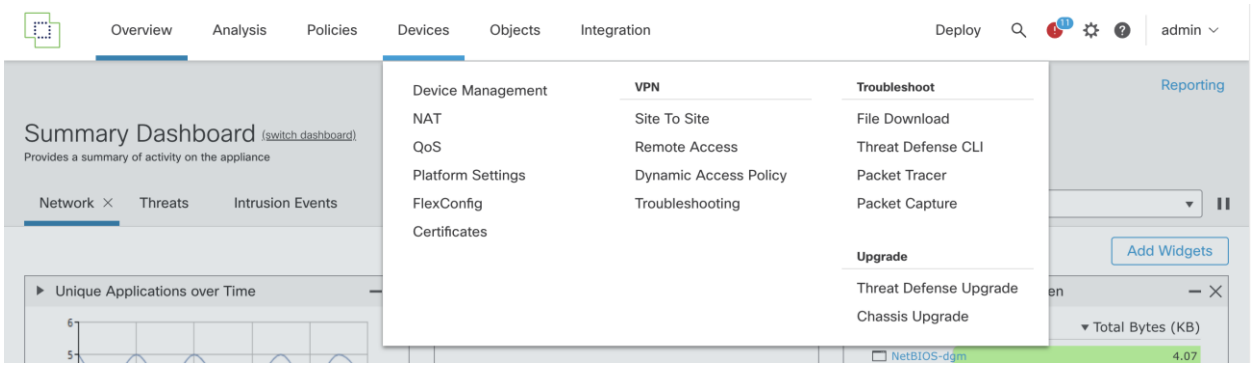


Рисунок 3.2 – Меню для навігації користувача по FMC

Слід зазначити, що FMC не підтримує українську мову, як можливу мову для застосунку. Базовою мовою застосунку є англійська, проте користувач може обрати одну із запропонованих мов, яку підтримує FMC, використавши для цього відповідну сторінку (рис. 3.3).

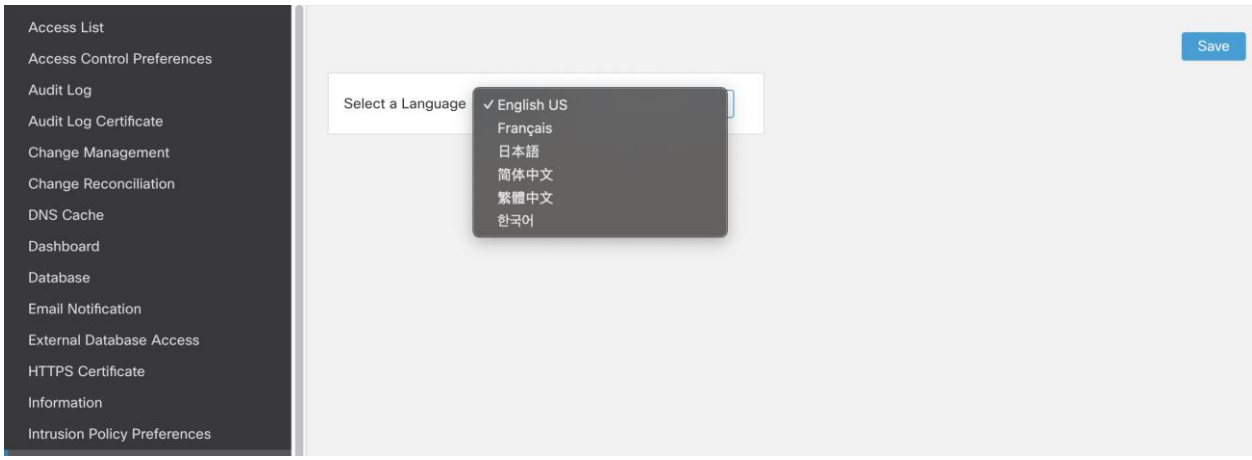


Рисунок 3.3 – Вигляд сторінки для перемикання мови застосунку

Для початку налаштування правил безпеки брандмауера користувач має додати Firepower Threat Defense (FTD). За результатами дослідження цієї моделі у розділі 2, вона відображає фаєрвол, доступ до якого необхідно налаштувати. Це можна зробити за допомогою модального діалогу (рис. 3.4).

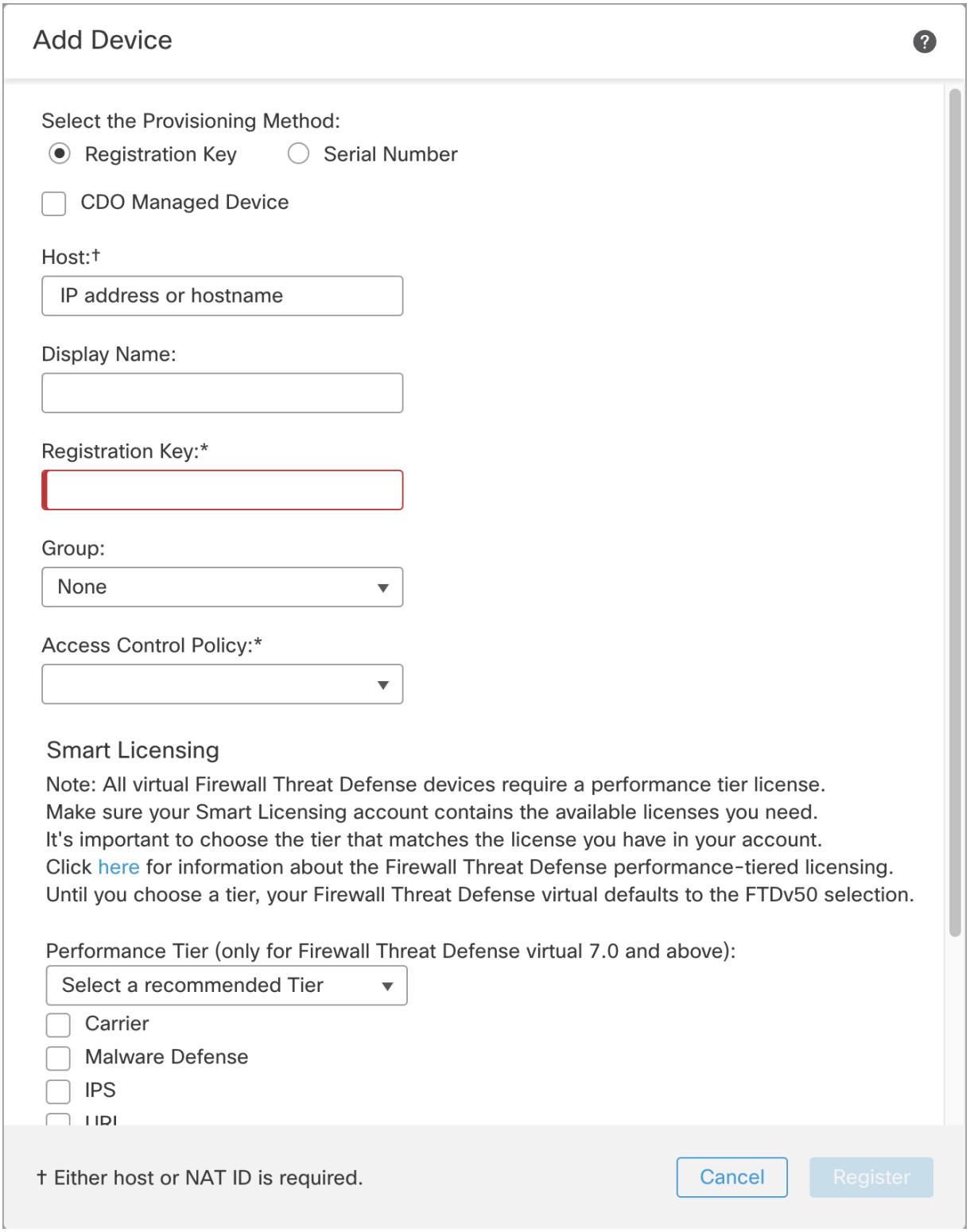


Рисунок 3.4 – Модальний діалог для додавання брандмауера до платформи FMC

Слід звернути увагу на такі поля як Host, Registration Key, Access Control Policy, бо ці поля є обов'язковими для заповнення. Host відповідає за IP-адресу пристрою брандмауера із системи Cisco, Registration Key – це спеціальний секретний ключ, який буде зазначено після покупки ліцензії для пристрою Cisco, Access Control Policy – це внутрішня модель FMC, яка відповідає за правила безпеки брандмауера (налаштування цієї моделі відбудеться далі у ході кваліфікаційної роботи).

Після успішного додавання FTD користувач отримає візуальне підтвердження у вигляді нового запису у загальній таблиці створених FTDs. Приклад доданого брандмауера з IP-адресою 172.16.0.100 наведено на рисунку 3.5.

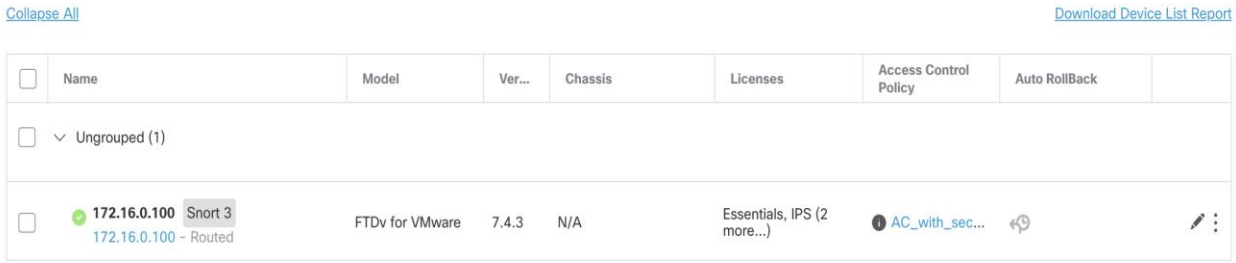


Рисунок 3.5 – Вигляд таблиці FTDs після додавання нового брандмауера

Основною моделлю яка включає в себе всі правила безпеки брандмауера є Access Control Policy. Вона відповідає за доступ трафіку до корпоративної мережі. За допомогою Access Control Policy Rule ця політика визначає дії, щодо певного трафіку. Визначення типу трафіку відбувається за допомогою критеріїв фільтрації трафіку, наприклад IP-адреса та порт. FMC має власну реалізацію для відображення цих двох критеріїв фільтрації.

Щоб створити Network та Port моделі користувач Firewall Management Center має скористатися відповідними діалогами (рис. 3.6, 3.7). Це зручний спосіб зазначити необхідні дані щоб фільтрувати трафік який надходить до корпоративної мережі. Ці створені моделі можуть перевикористовуватися між різними політиками або правилами безпеки брандмауера.

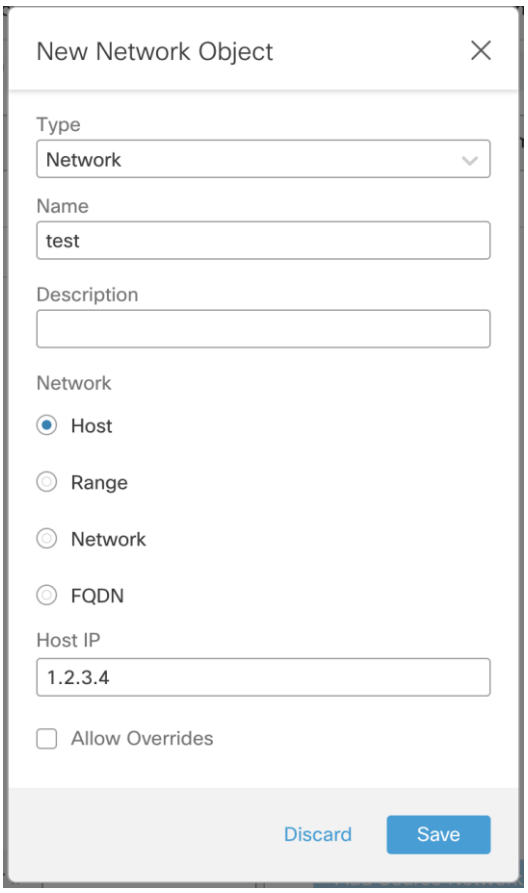


Рисунок 3.6 – Модальний діалог для створення моделі Network

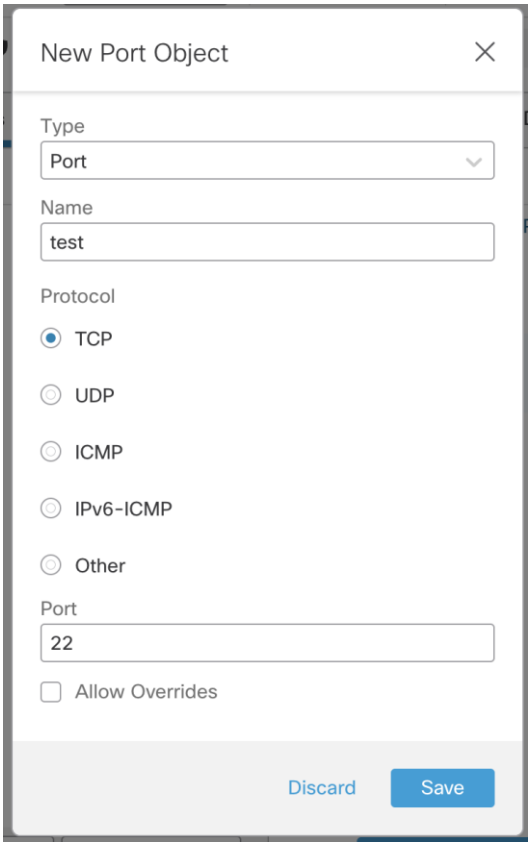


Рисунок 3.7 – Модальний діалог для створення моделі Port

Модель Access Control Policy Rule має включати в себе дію (action), яка має відбутися у випадку якщо трафік задовольняє критерії фільтрації. Кількість критеріїв фільтрації необмежена, але в той же час необхідно слідкувати за тим щоб не допустити конфлікту між декількома критеріями. При збереженні нового правила може з'явитись окремий модальний діалог, який сповістить користувача про проблему, у випадку конфліктної ситуації.

Обрані критерії фільтрації будуть моментально відображені у модальному діалозі для створення Access Control Policy Rule (рис. 3.8). У рамках кваліфікаційної роботи, критеріями фільтрації трафіку є моделі Network та Port, створені на попередньому етапі за допомогою відповідних модальних діалогів. Source Network представляє собою IP-адресу 1.2.3.4, Destination Network – 2.3.4.5, Source Port має значення 22 (ssh з'єднання), Destination Port – 433 (HTTPS з'єднання) [34].

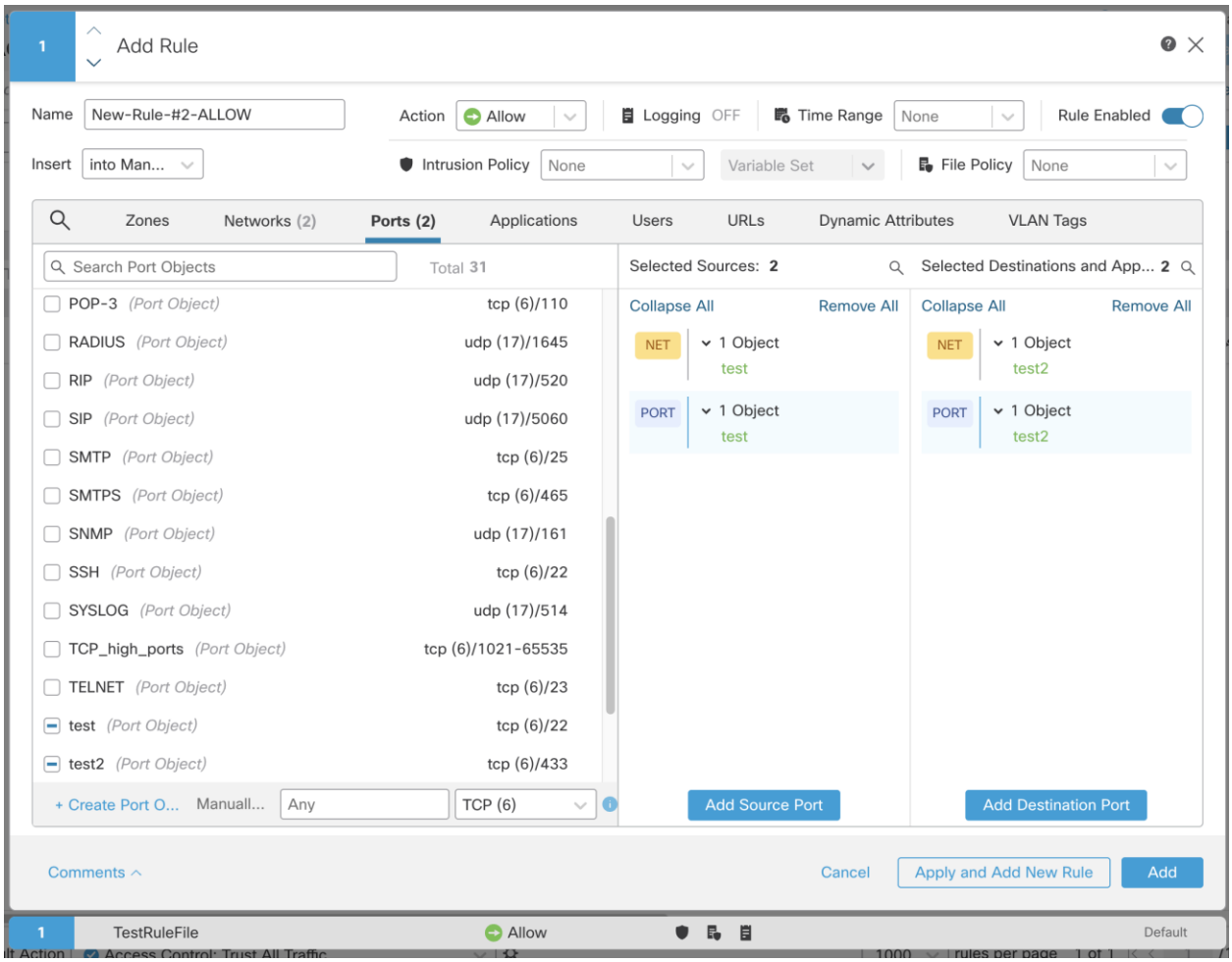


Рисунок 3.8 – Модальний діалог для створення Access Control Policy Rule

В результаті успішного створення моделі Access Control Policy Rule було додано новий запис у таблицю правил політики безпеки доступу до брандмауера (рис. 3.9). У таблиці відображено дію, у наведеному прикладі трафіку буде дозволено доступ до корпоративної мережі, та критерії фільтрації трафіку розділені глобальними колонками Source та Destination.

Під таблицею правил політики безпеки доступу зазначено поле Default Action. Це означає, що на випадок відсутності створених правил буде застосовано зазначено певну дію. На наведеному прикладі, увесь трафік вважається безпечним та буде дозволено доступ до мережі.

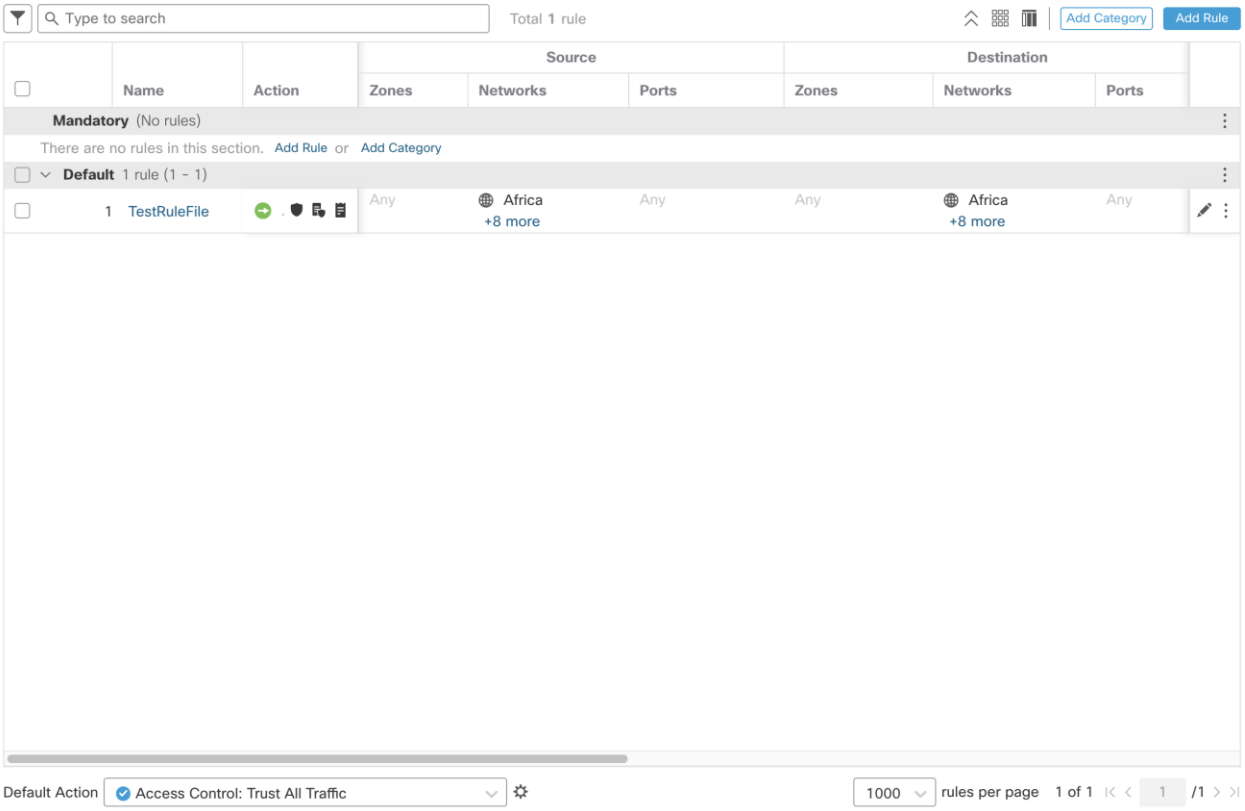


Рисунок 3.9 – Вигляд таблиці Access Policy Rules після створення правила

Access Control Policy включає в себе ще три типи політик: Prefilter Policy, Decryption Policy, Identity Policy. Першою складовою є політика попередньої фільтрації (Prefilter Policy). Важливим призначенням цієї політики є спрощення перевірки та аналізу трафіку шляхом застосування зазначених правил (Prefilter Policy Rule) до певного типу даних, наприклад, дозволяючи або блокуючи доступ трафіку до корпоративної мережі.

Основною конфігурацією цього правила є визначення дії, яка буде застосовуватись відповідно до параметрів фільтрації. Серед можливих дій є Analyze, Block, Fastpath. У випадку вибору дії Analyze – трафік буде передано далі на обробку іншими політиками, щоб в подальшому допустити до корпоративної мережі. Block дія – не дозволяє трафіку потрапити до мережі, якщо були зазначені відповідні критерії до дії. Дія Fastpath дозволяє трафіку потрапити до брандмауера без подальшої перевірки іншими політиками безпеки. Ці налаштування можна додати за допомогою відповідного модального діалогу (рис. 3.10).

Саме використання дій Block та Fastpath дозволяє оптимізувати процес обробки трафіку та відчути це на великому об’єму даних.

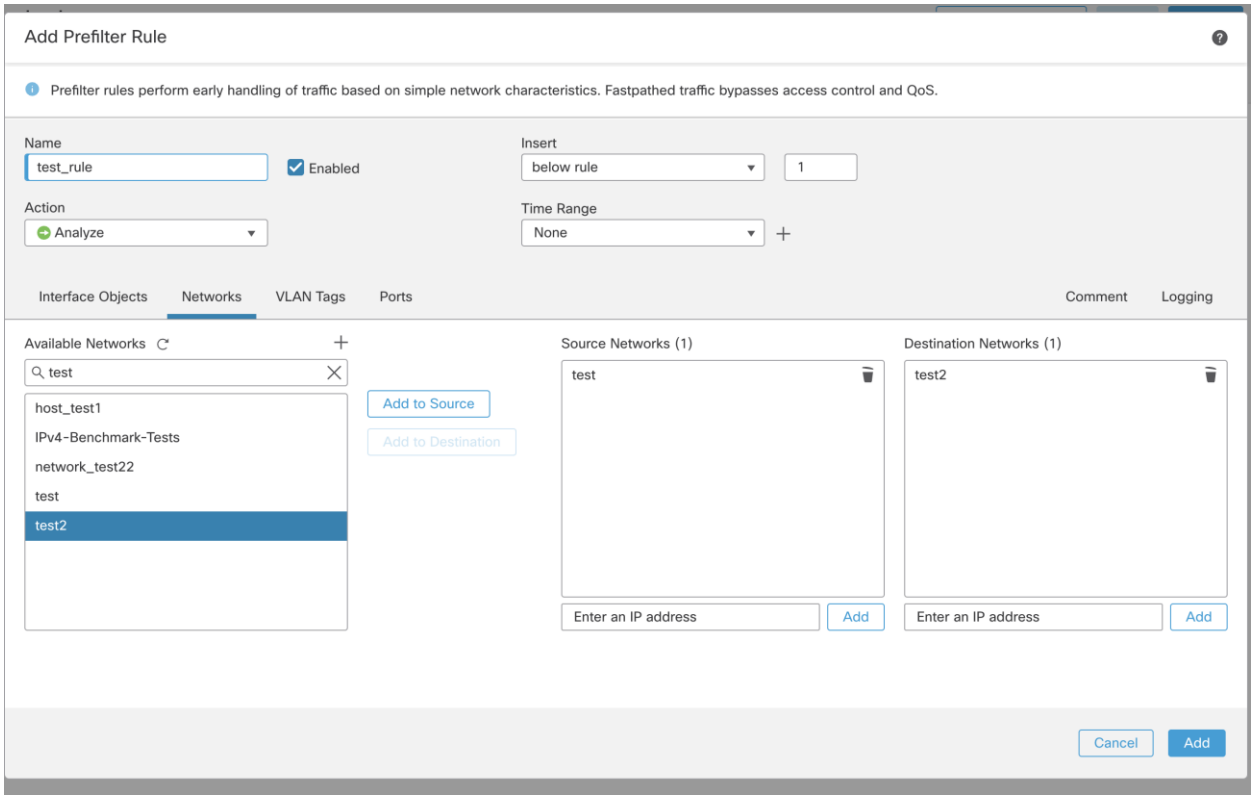


Рисунок 3.10 – Модальний діалог для створення Prefilter Policy Rule

У випадку успішно створеної моделі Prefilter Policy Rule відповідні зміни будуть відображені у таблиці правил (рис. 3.11). Нове створене правило буде першим записом у таблиці правил за замовчуванням, що

гарантує високий пріоритет серед інших правил попередньої фільтрації трафіку. У рамках кваліфікаційної роботи було створено правило з назвою test_rule та дією Analyze, для того щоб перевірити роботу наступних політик.

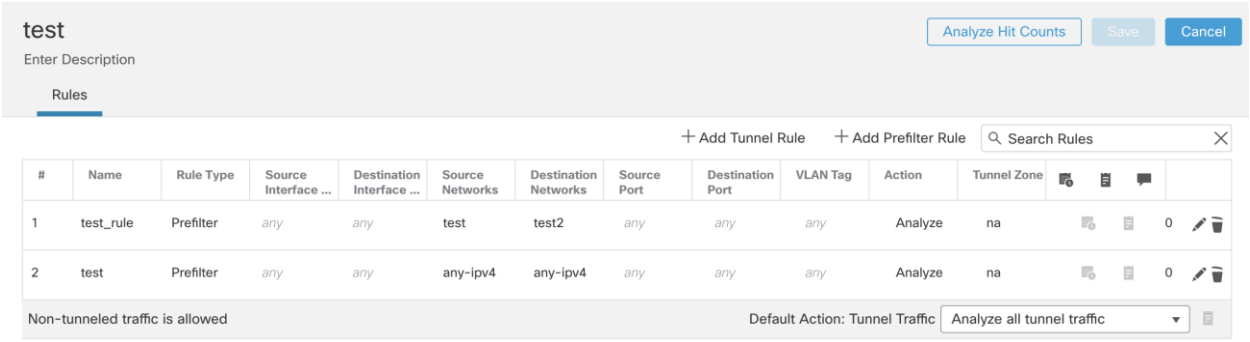


Рисунок 3.11 – Вигляд таблиці Prefilter Policy Rules після створення правила

У випадку якщо трафік відповідає критеріям правила попередньої фільтрації з дією Analyze обробка трафіку буде проводитись політикою розшифрування даних (Decryption Policy). Розшифровка трафіку дозволяє аналізувати зашифрований трафік, який у багатьох випадках прихований за допомогою різних методів шифрування контенту. Також розшифровка трафіку надає можливість брандмауеру контролювати доступ на основі контенту та виявляти потенційні загрози.

У процесі конфігурації політики розшифрування даних важливу роль відіграють моделі які допомагають з процесом розкриття вмісту трафіку: Internal CA та Internal Certificate. Роль моделі Internal CA в рамках Firewall Managenent Center полягає у тому, щоб видавати сертифікати, які необхідні для інспекції зашифрованого трафіку, що намагається отримати доступ до корпоративної мережі.

Суть роботи моделі Internal CA може бути описана наступним чином: центр сертифікації видає сертифікат, FMC може використовувати його для реалізації розшифровки SSL/TLS трафіку за допомогою технології man-in-the-middle (MITM). У цьому процесі FMC отримує зашифрований трафік, розшифровує його для перевірки. У випадку успішно пройденої перевірки,

FMC повторно шифрує трафік, використовуючи сертифікат, який був виданий Internal CA, та після цього передає трафік на подальшу перевірку. Внаслідок цього, користувач Firewall Management Center може вловити потенційно небезпечний трафік і при цьому не порушувати порядок проведення обробки трафіку.

Для створення моделі Internal CA існує відповідний діалог, де необхідно зазначити такі параметри як: Country Name (індекс країни), State (область), City (місто), Organization (назва організації для якої генерується Internal CA), Organization Unit (скорочена назва організації), Common Name (публічне ім’я). Приклад модального діалогу наведено на рисунку 3.12.

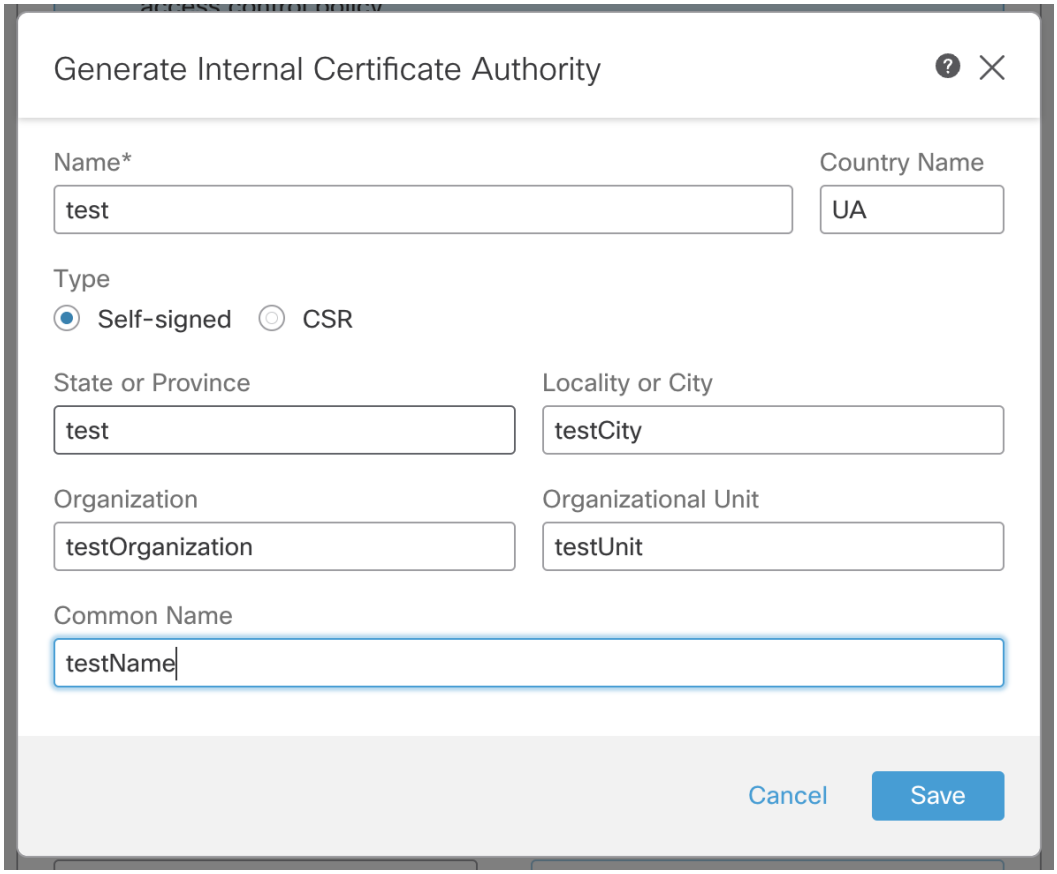


Рисунок 3.12 – Модальний діалог для створення Internal CA

У результаті успішного створення моделі Internal CA відразу буде показаний інший модальний діалог з розширеною інформацією, яка необхідна для можливості створення та підписання сертифікатів (рис. 3.13).

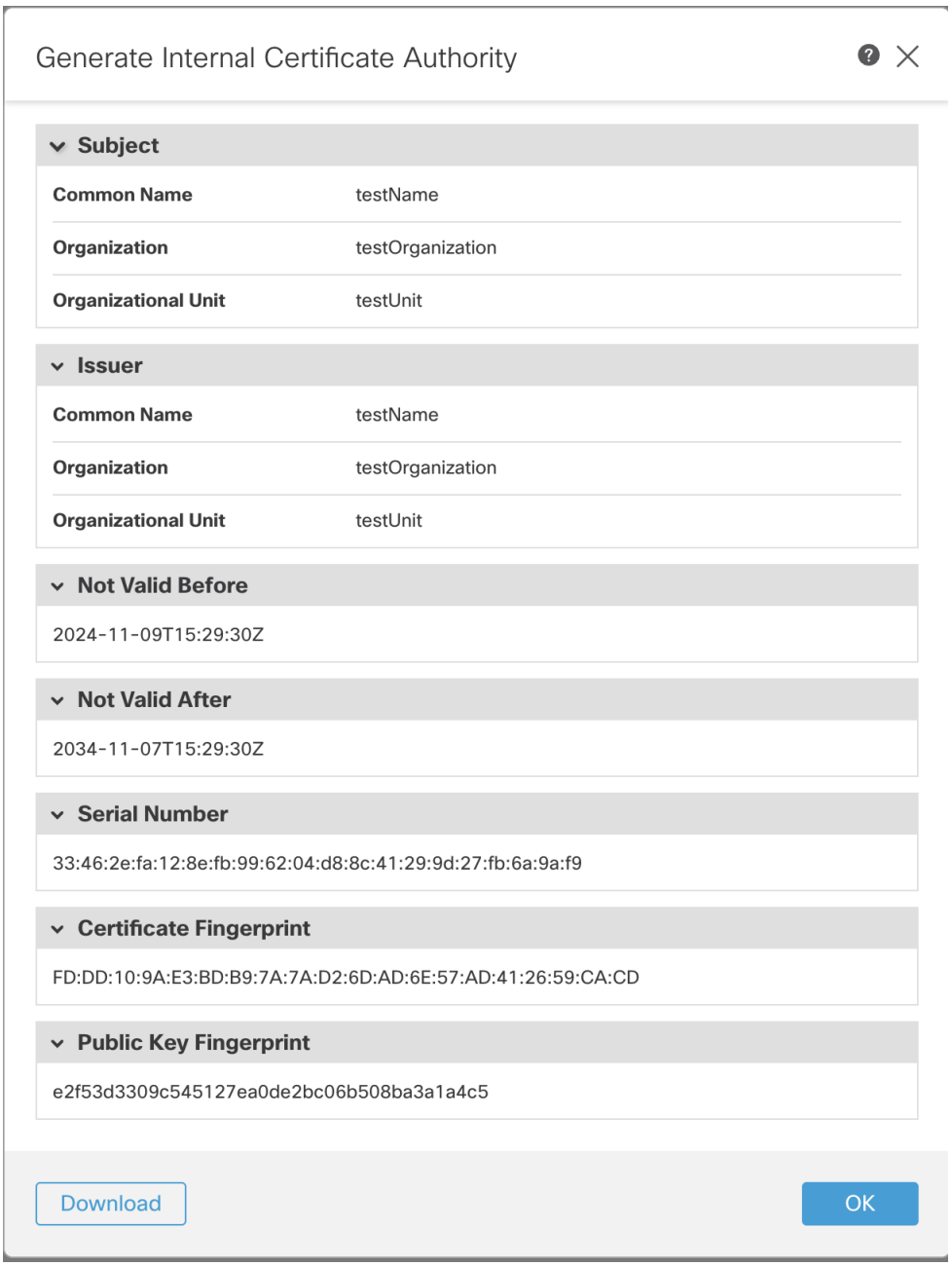


Рисунок 3.13 – Модальний діалог для відображення даних створеного Internal CA

Варто зазначити, що використання лише Internal CA не принесе бажаного результату в процесі налаштування безпеки мережевої інфраструктури. Для повного контролю над процесом аналізу зашифрованого трафіку необхідно використовувати модель Internal Certificate. Центр сертифікації (Internal CA) підписує та видає сертифікати, які використовуються у FMC. За допомогою сторонніх ресурсів є можливість згенерувати дані сертифікату та секретний ключ, який допомагає шифрувати

оброблений трафік. Після цього, використовуючи згенеровані дані можна додати нову модель Internal Certificate (рис. 3.14).

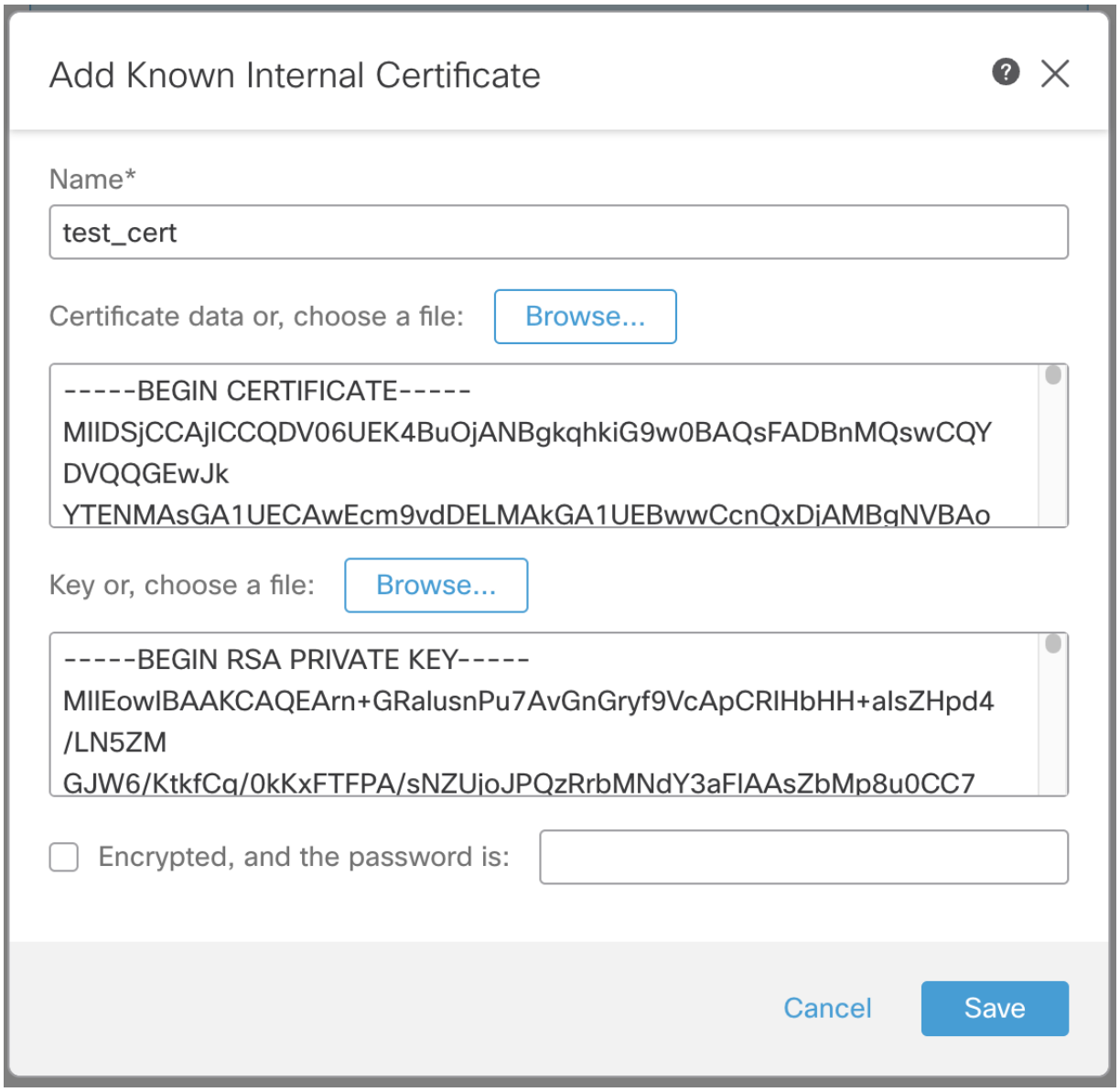


Рисунок 3.14 – Модальний діалог для створення моделі Internal Certificate

Завдяки використанню Internal Certificate користувачі мають можливість налаштовувати політику розшифровки даних з підтримкою довіри до трафіку. Це забезпечується завдяки тому, що сертифікат, який підписаний Internal CA, розпізнається пристроями в мережі як надійний.

Обидві моделі можуть бути опціонально використані в процесі створення політики розшифрування даних для конфігурування обробки

вхідного та вихідного трафіку. Для забезпечення цієї необхідності FMC надає можливість використовувати дві вкладки: Outbound Connections та Inbound Connections (рис. 3.15). На першій вкладці можна зазначити центр сертифікації, який буде шифрувати трафік для подальшої обробки. На другій вкладці необхідно зазначити створений Internal Certificate для розшифрування трафіку, який надходить в мережу.

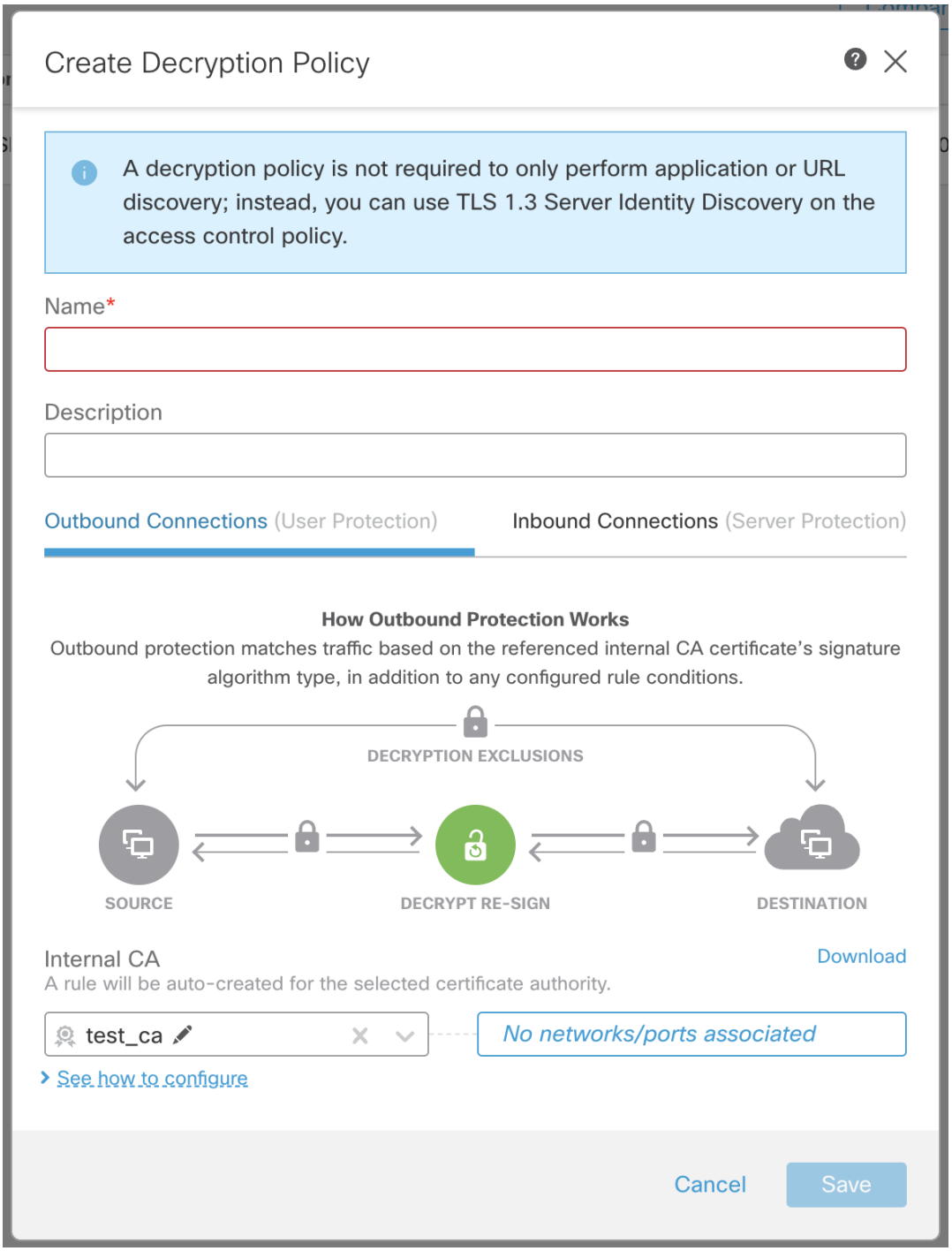


Рисунок 3.15 – Модальний діалог для створення моделі Decryption Policy

У рамках роботи над кваліфікаційною роботи було додано моделі Internal CA та Internal Certificate та застосовано їх для створення моделі Decryption Policy [35]. Унаслідок цього, після збереження налаштувань цієї моделі було автоматично створено два правила політики розшифрування даних (рис. 3.16). Слід зазначити, якщо користувач не зазначить Internal CA та Internal Certificate, то таблиця правил буде порожня.

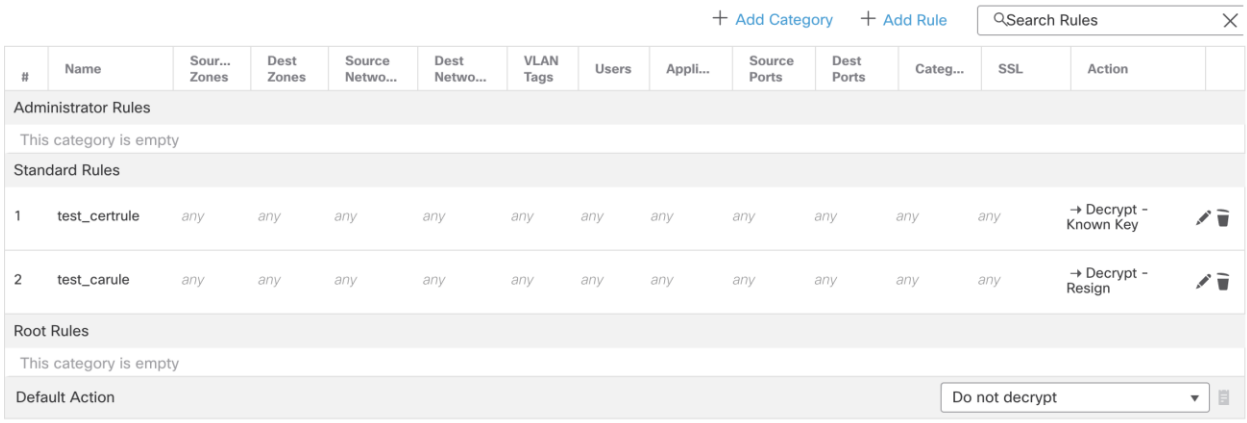


Рисунок 3.16 – Приклад таблиці Decryption Policy Rules із автоматично згенерованими правилами

Для того щоб додати необхідні правили політики розшифрування даних можна використати відповідний модальний діалог, приклад якого наведено на рисунку 3.17. Цей діалог має широкий набір налаштувань для фільтрації трафіку. У випадку, якщо трафік задовольняє цим критеріям, буде застосована дія, яка була зазначена у правилі (Decrypt-Resign, Decrypt-Known key, Do not decrypt).

Розглянемо дію Do not decrypt – вона дозволяє не розшифровувати трафік взагалі, таким чином підтверджуючи повну довіру до адресанта. У свою чергу дія Decrypt-Resign дозволяє розшифровування трафіку для аналізу та подальшого підписання за допомогою сертифіката Internal Certificate. Дія Decrypt-Known Key схожа на приклад вище, але розшифровування трафіку для аналізу відбувається без подальшого підписання сертифікатом.

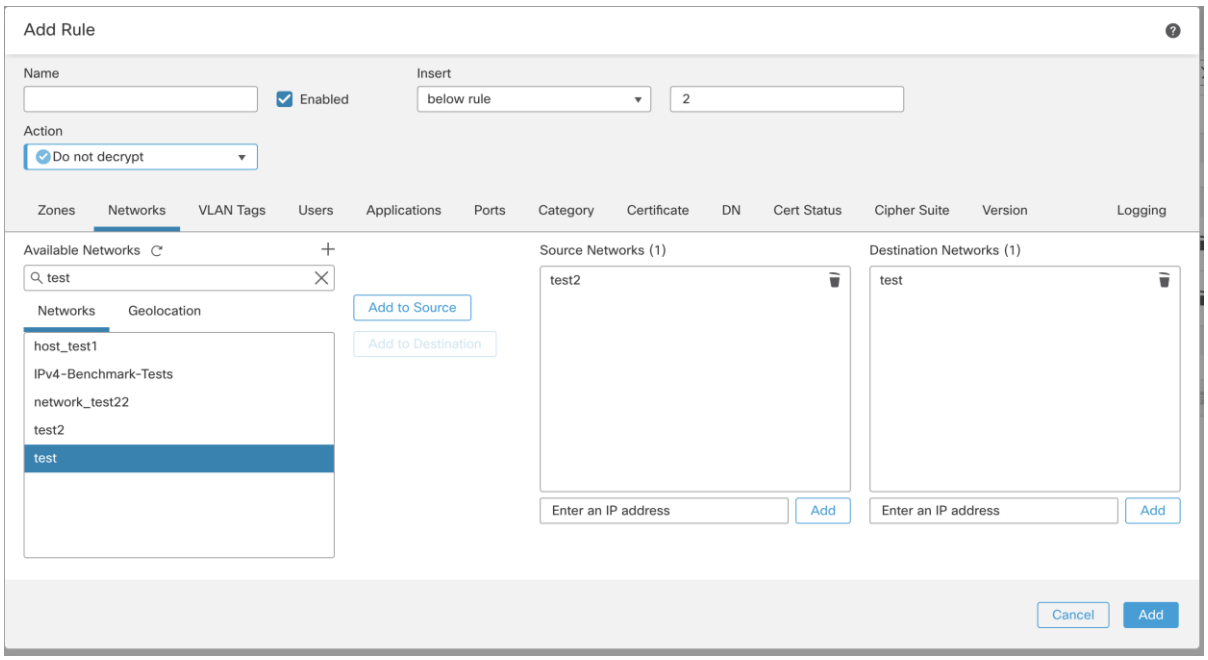


Рисунок 3.17 – Модальний діалог для створення моделі Decryption Policy Rule

Після успішного завершення налаштування політики розшифрування даних переходимо до налаштування правил політики ідентифікації користувачів (Identity Policy). За допомогою цих правил є можливість налаштовувати окремі випадки обробки даних відправника трафіку. Зробити це можна використавши модальний діалог для створення моделі (рис. 3.18).

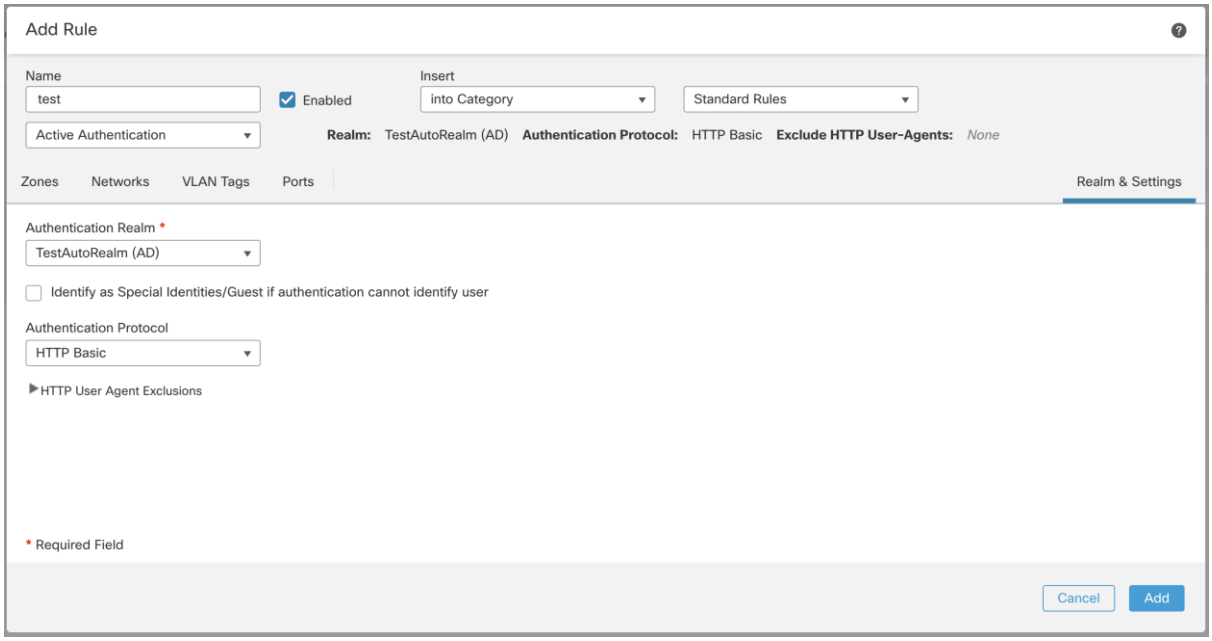


Рисунок 3.18 – Модальний діалог для створення моделі Identity Policy Rule

Механізм обробки даних відправника трафіку працює завдяки моделі Realm, яка є частиною правила політики ідентифікації користувачів. Ця модель представляє собою домен (простір ідентифікації), який FMC використовує для взаємодії з зовнішніми сервісами аутентифікації (Active Directory, LDAP, RADIUS, Azure AD). Це забезпечує доступ FMC до інформації про користувачів, зокрема їхні ролі, групи та права доступу для використання цієї інформації при застосуванні Identity Policy [36].

FMC дає можливість створити модель Realm за допомогою відповідного модального діалогу (рис. 3.19). Під час налаштування даних для моделі є можливість виконати перевірку з'єднання з зовнішнім сервісом аутентифікації.

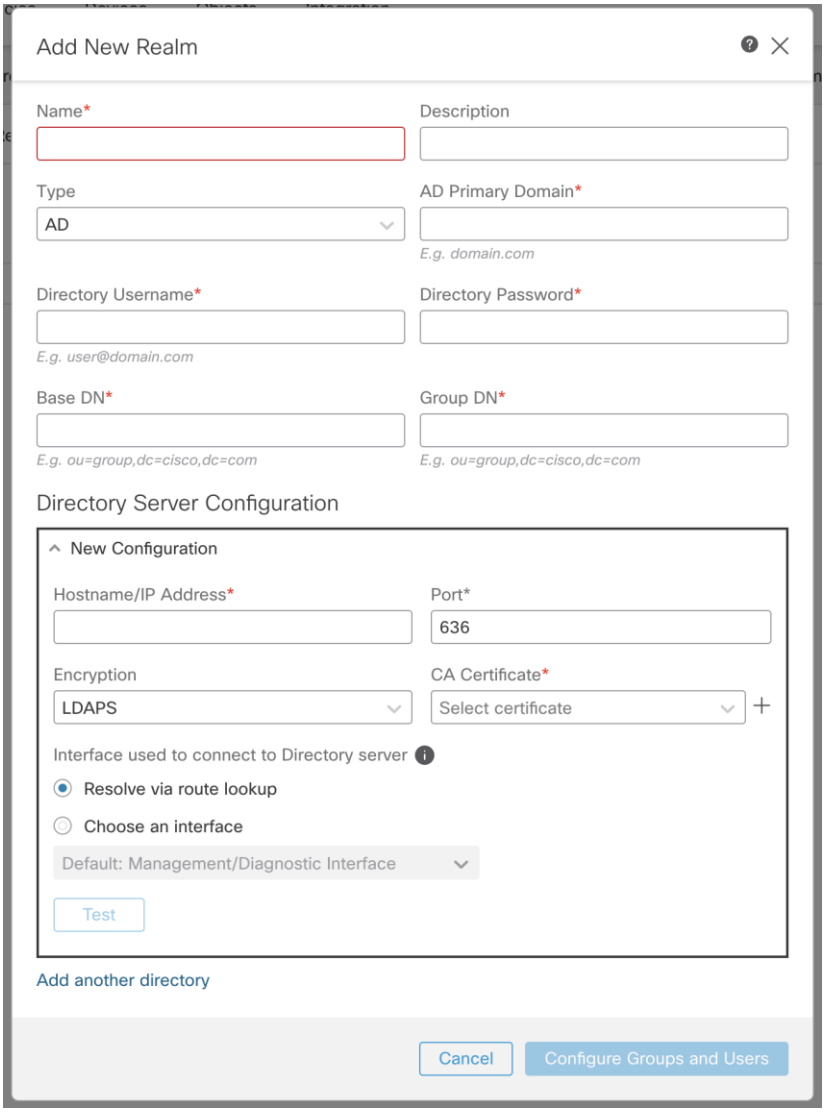


Рисунок 3.19 – Модальний діалог для створення моделі Realm

У результаті налаштування політики ідентифікації користувача була створена модель Identity Policy Rule, яка фільтрує трафік шляхом перевірки аутентифікації користувача до домену movies.cisco.com (рис. 3.20).

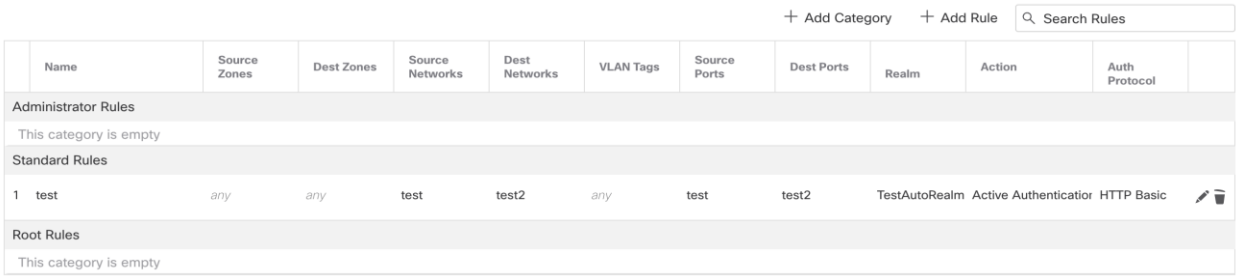


Рисунок 3.20 – Вигляд таблиці після створення моделі Identity Policy Rule

Для того щоб всі створені правила та політики безпеки могли бути застосовані, необхідно перейти на сторінку редагування Access Control Policy Rule. Після переходу на сторінку користувач може скористатись випадаючим меню на клік заголовку відповідної політики (рис. 3.21). У меню необхідно обрати створену модель, наприклад для Prefilter Policy це буде модель з назвою Default Prefilter Policy. У процесі роботи над кваліфікаційною роботою було оновлено налаштування усіх політик безпеки.

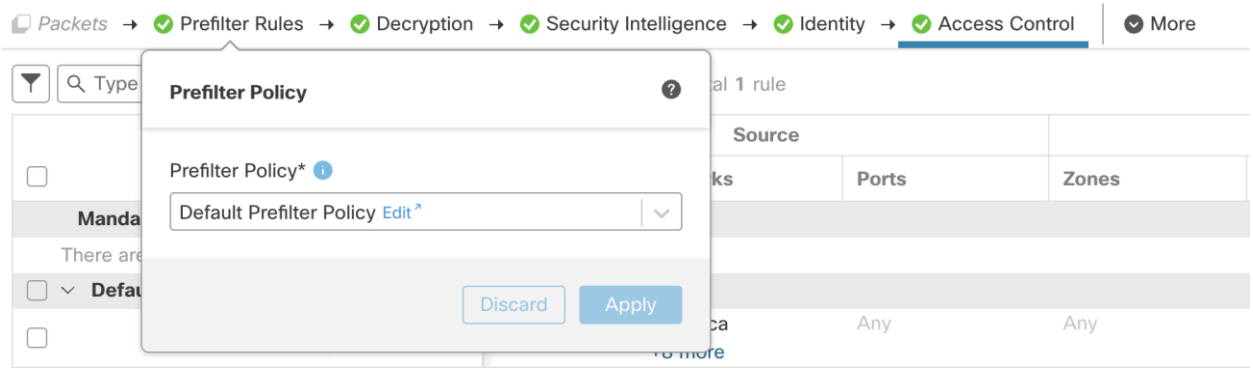


Рисунок 3.21 – Приклад вигляду випадаючого меню для моделі Prefilter Policy

Після цього процес налаштування правил та політик безпеки брандмауера вважається завершеним. Для застосування нових або змінених конфігурацій потрібно пройти процес Deployment.

3.2 Застосування створених правил та політик безпеки до брандмауера

Cisco Firepower Management Center підтримує процес Deployment, який є основним етапом для застосування змін та налаштувань правил політик для доданих до FMC пристроїв, таких як Firepower Threat Defense (FTD). Процес Deployment забезпечує синхронізацію локальних змін, які були зроблені за допомогою FMC, із мережевими пристроями. Це допомагає гарантувати відповідність нових налаштувань для вирішення реальних потребам безпеки мережевої інфраструктури.

Після внесення змін до політик та правил безпеки брандмауера, такі як правил політики доступу, правила політики розшифровки даних чи правилам політики ідентифікації користувачів, FMC зберігає ці налаштування локально. Для цього платформа використовує власні ресурси баз даних. У той же час, FMC позначає ці зміни як підготовлені до розгортання (рис.3.22). Це дозволяє користувачам платформи мати єдину точку для застосування всіх змін для полегшування моніторингу і контролю безпеки приватної мережі.

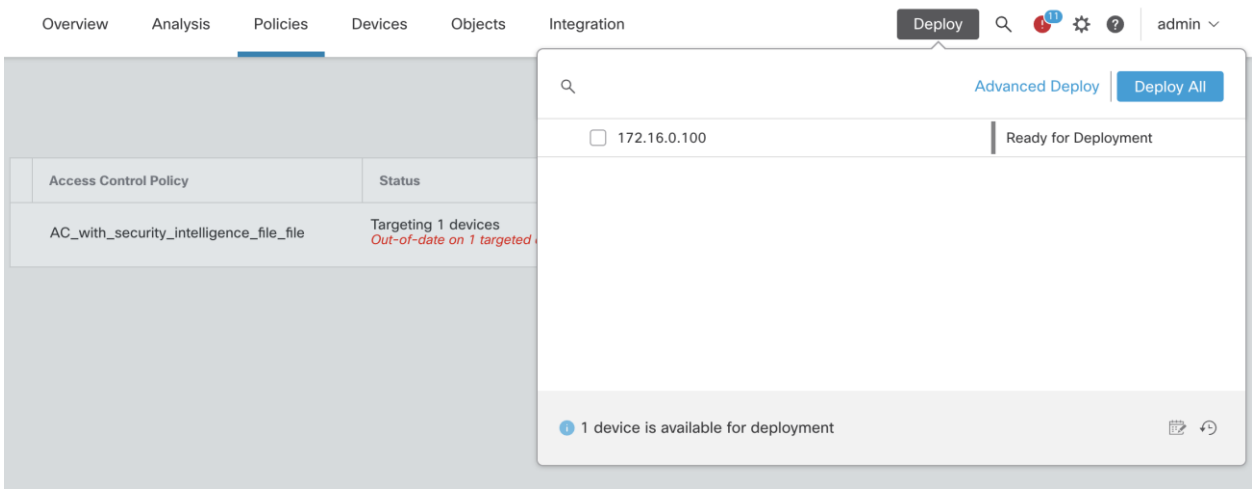


Рисунок 3.22 – Повідомлення про можливість розгортаннях змінених налаштувань

Перед початком застосування FMC здійснює ретельну перевірку конфігурацій, щоб уникнути можливих конфліктів або помилок у

налаштуваннях. Завдяки цій перевірці система автоматично ідентифікує будь-які потенційні проблеми, такі як суперечливі правила, некоректні посилання чи помилки синтаксису, що дозволяє знизити ризик порушень у роботі мережі.

У випадку виявлення що правила конфліктують між собою, користувачу FMC буде показано повідомлення для внесення коригувань, що знижує ризик помилок в роботі корпоративної мережі [37]. Такий багатоступеневий підхід до перевірки значно покращує надійність розгортання нових налаштувань.

Після підтвердження коректності конфігурацій користувач FMC починає процес розгортання, шляхом передачі налаштувань на обрані пристрої за допомогою захищеного каналу зв'язку. Після відправлення оновлень на FTD, відбувається етапи перевірки отриманих даних і застосування їх у таблиці правил доступу, профілі захисту від загроз, політики обробки трафіку та інші параметри для забезпечення безпеки мережевої інфраструктури. Варто зазначити, що FMC надає можливість моніторингу процесу розгортання змін на FTD за допомогою спеціального меню, в якому зазначено IP-адресу брандмауера, відсоток пройденого процесу з назвою етапу (рис. 3.23).

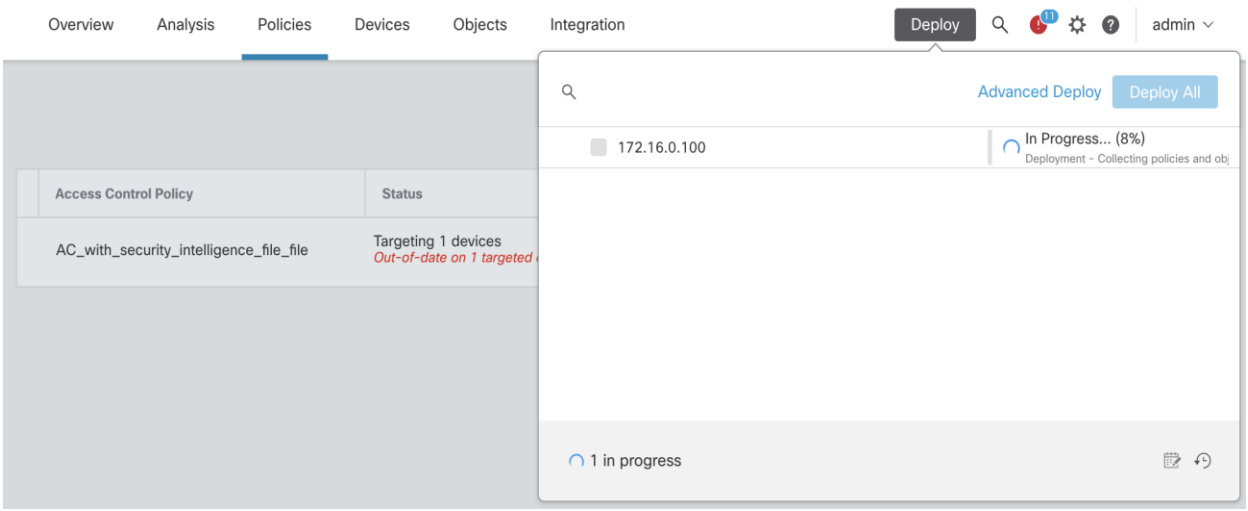


Рисунок 3.23 – Повідомлення про процес розгортаннях змінених налаштувань

Після завершення процесу Deployment, платформа FMC оновлює журнали подій і записи про історію зроблених змін для можливості аудиту. Користувач може відстежувати зміни та їх вплив на обробку трафіку.. Завдяки цьому процес Deployment гарантує надійне, безпечне і точне застосування оновлених налаштувань без перерв у захисті мережевої інфраструктури від потенційних загроз. Приклад повідомлення про успішне завершення процесу Deployment наведено на рисунку 3.24.

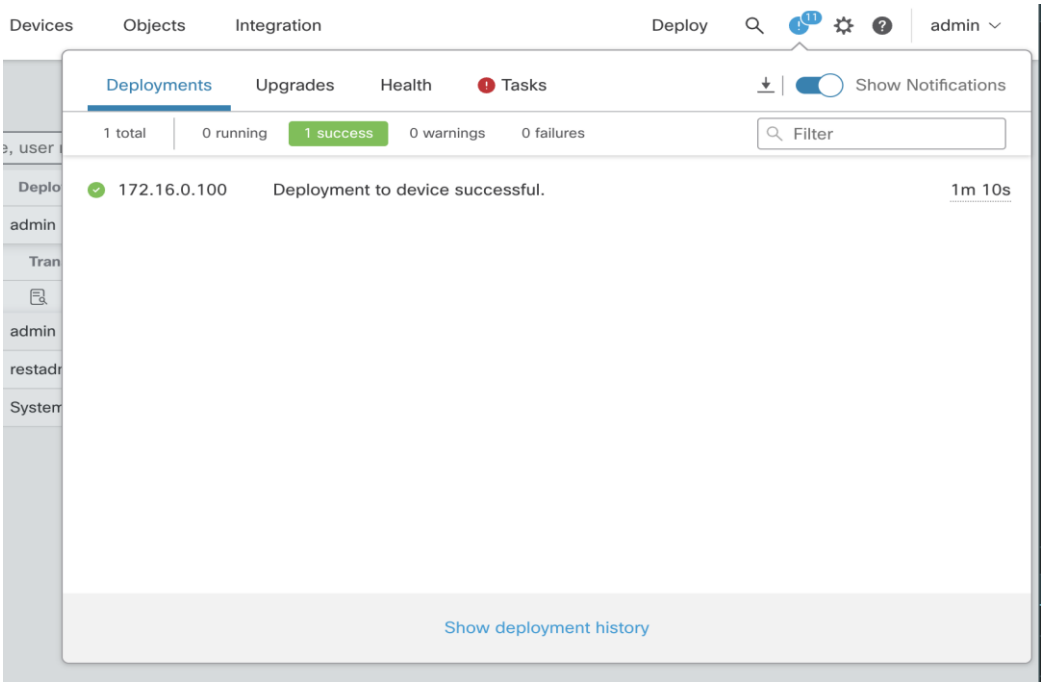


Рисунок 3.24 – Приклад повідомлення про успішне застосування змін

Також, FMC надає можливість перегляду історії завершених чи активних спроб застосування змін для FTD. Користувач має перейти на сторінку Deploy History та перегляду таблицю з записами (рис. 3.25)

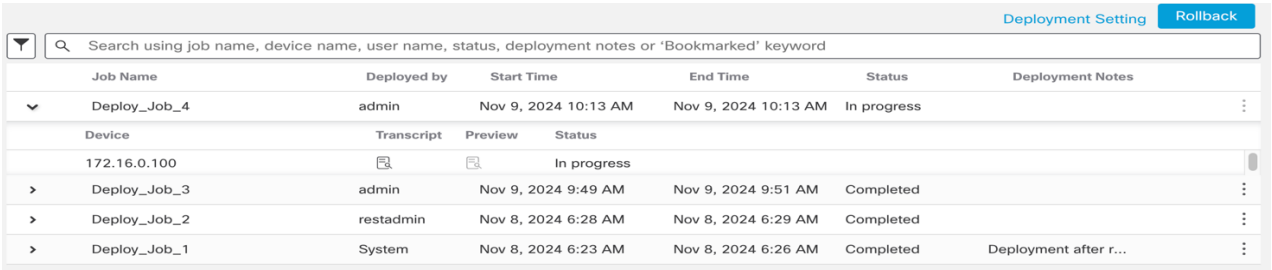


Рисунок 3.25 – Приклад таблиці з записами про спроби застування змін

3.3 Аналіз згенерованих подій на основі обробки трафіку

У результаті успішного застосування змінених конфігурацій для Firepower Threat Defense, користувач може одразу відстежувати та оновлені алгоритми обробки трафіку. У момент коли трафік намагатись потрапити на пристрій, спрацьовують правила та політики безпеки брандмауера. На основі застосованих конфігурацій застосовується дія, щодо цього трафіку. Після виконання дії, Firewall Management Center регіструє це шляхом створення моделі подія (event) [38].

Для представлення великої кількості записів подій про з’єднання, які проходять через створені пристрої (FTD), Cisco Firepower Management Center має модель Connection Event. Це важливий компонент для аналізу трафіку, оскільки головною метою є забезпечення відображення та контролю над мережею, дозволяючи користувачам виявляти потенційні загрози або аномалії в трафіку. Всі події Conection Event відображені у відповідній таблиці, яка надає всю необхідну інформацію про трафік (рис. 3.26).

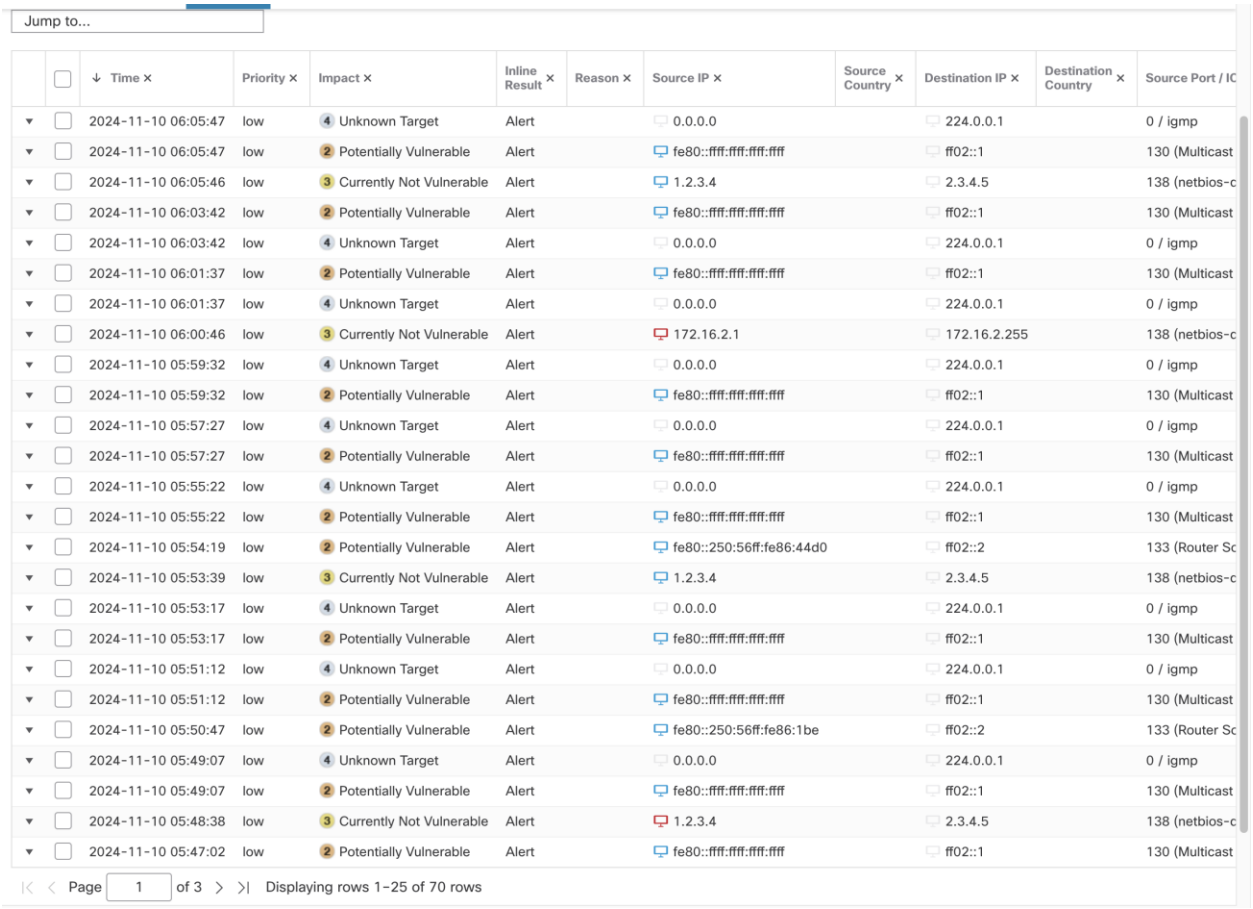
Jump to...

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type
2024-11-10 06:09:33		Allow		1.2.3.4		2.3.4.5		SZ_In	SZ_Out	22 (netbios-dgm) / udp
2024-11-10 06:09:21	2024-11-10 06:09:21	Allow		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:09:21		Allow		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:09:21		Allow		0.0.0.0		224.0.0.1		SZ_In	SZ_Out	0 / igmp
2024-11-10 06:09:13		Allow		1.2.3.4		2.3.4.5		SZ_Out	SZ_In	22 (netbios-dgm) / udp
2024-11-10 06:07:16	2024-11-10 06:07:16	Allow		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:07:16	2024-11-10 06:07:16	Allow		0.0.0.0		224.0.0.1		SZ_In	SZ_Out	0 / igmp
2024-11-10 06:07:16		Allow		0.0.0.0		224.0.0.1		SZ_In	SZ_Out	0 / igmp
2024-11-10 06:07:16		Block		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:05:11	2024-11-10 06:05:11	Allow		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:05:11	2024-11-10 06:05:11	Allow		0.0.0.0		224.0.0.1		SZ_In	SZ_Out	0 / igmp
2024-11-10 06:05:11		Allow		0.0.0.0		224.0.0.1		SZ_In	SZ_Out	0 / igmp
2024-11-10 06:05:11		Block		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:03:06	2024-11-10 06:03:06	Block		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:03:06	2024-11-10 06:03:06	Allow		0.0.0.0		224.0.0.1		SZ_In	SZ_Out	0 / igmp
2024-11-10 06:03:06		Allow		0.0.0.0		224.0.0.1		SZ_In	SZ_Out	0 / igmp
2024-11-10 06:03:06		Allow		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:01:01	2024-11-10 06:01:01	Allow		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 06:01:01	2024-11-10 06:01:01	Block		fe80::250:56ff:fe86:e6de		ff02::16		SZ_Out	SZ_In	143 (Multicast Listener Di
2024-11-10 06:01:01	2024-11-10 06:01:01	Allow		1.2.3.4		2.3.4.5		SZ_Out	SZ_In	0 / igmp
2024-11-10 06:01:01		Allow		fe80::250:56ff:fe86:e6de		ff02::16		SZ_Out	SZ_In	143 (Multicast Listener Di
2024-11-10 06:01:01		Allow		1.2.3.4		2.3.4.5		SZ_Out	SZ_In	22 / igmp
2024-11-10 06:01:01		Allow		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q
2024-11-10 05:58:56	2024-11-10 05:58:56	Allow		fe80::250:56ff:fe86:e6de		ff02::16		SZ_Out	SZ_In	143 (Multicast Listener Di
2024-11-10 05:58:56	2024-11-10 05:58:56	Allow		fe80::ffff:ffff:ffff:ffff		ff02::1		SZ_In	SZ_Out	130 (Multicast Listener Q

Page 1 of 6 Displaying rows 1–25 of 143 rows

Рисунок 3.26 – Приклад вигляду таблиці Connection Events

Інша модель, яка призначена для відображення подій з виявленими потенційними загрозами для корпоративної мережі, зафіксованими системою запобігання вторгненням (IPS), називається Intrusion Event. Основною особливість цієї моделі є аналіз трафіку для виявлення конкретних шаблонів, сигнатур та поведінкових ознак, які можуть вказувати на шкідливу активність. Приклад записів потенційно небезпечних подій представлено на рисунку 3.27. Таблиця Intrusion Events містить додаткову інформацію про тип загрози, серйозність інциденту, джерело та призначення атаки, а також рекомендації щодо пом'якшення загрози [39].


Jump to...

Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP	Destination Country	Source Port / IC
2024-11-10 06:05:47	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 06:05:47	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 06:05:46	low	Currently Not Vulnerable	Alert		1.2.3.4		2.3.4.5		138 (netbios-c
2024-11-10 06:03:42	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 06:03:42	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 06:01:37	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 06:01:37	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 06:00:46	low	Currently Not Vulnerable	Alert		172.16.2.1		172.16.2.255		138 (netbios-c
2024-11-10 05:59:32	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 05:59:32	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 05:57:27	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 05:57:27	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 05:55:22	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 05:55:22	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 05:54:19	low	Potentially Vulnerable	Alert		fe80::250:56ff:fe86:44d0		ff02::2		133 (Router Sc
2024-11-10 05:53:39	low	Currently Not Vulnerable	Alert		1.2.3.4		2.3.4.5		138 (netbios-c
2024-11-10 05:53:17	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 05:53:17	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 05:51:12	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 05:51:12	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 05:50:47	low	Potentially Vulnerable	Alert		fe80::250:56ff:fe86:1be		ff02::2		133 (Router Sc
2024-11-10 05:49:07	low	Unknown Target	Alert		0.0.0.0		224.0.0.1		0 / igmp
2024-11-10 05:49:07	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast
2024-11-10 05:48:38	low	Currently Not Vulnerable	Alert		1.2.3.4		2.3.4.5		138 (netbios-c
2024-11-10 05:47:02	low	Potentially Vulnerable	Alert		fe80::ffff:ffff:ffff:ffff		ff02::1		130 (Multicast

Page 1 of 3 Displaying rows 1–25 of 70 rows

Рисунок 3.27 – Приклад вигляду таблиці Intrusion Events

Наступна модель Unified Event – це більш сучасна модель для відображення подій, яка об'єднує кілька типів мережевих подій і подій безпеки в єдиний універсальний формат. Завдяки уніфікуванню, Firewall Management Center може відображати і зберігати велику кількість інформації,

яка пов’язана з мережевим трафіком і загрозами. Ця інформація відображається у вигляді таблиці з довільним наповненням колонок і завдяки цьому процес аналізу та обробку даних стає комфортнішим для користувачів платформи FMC (рис. 3.28).

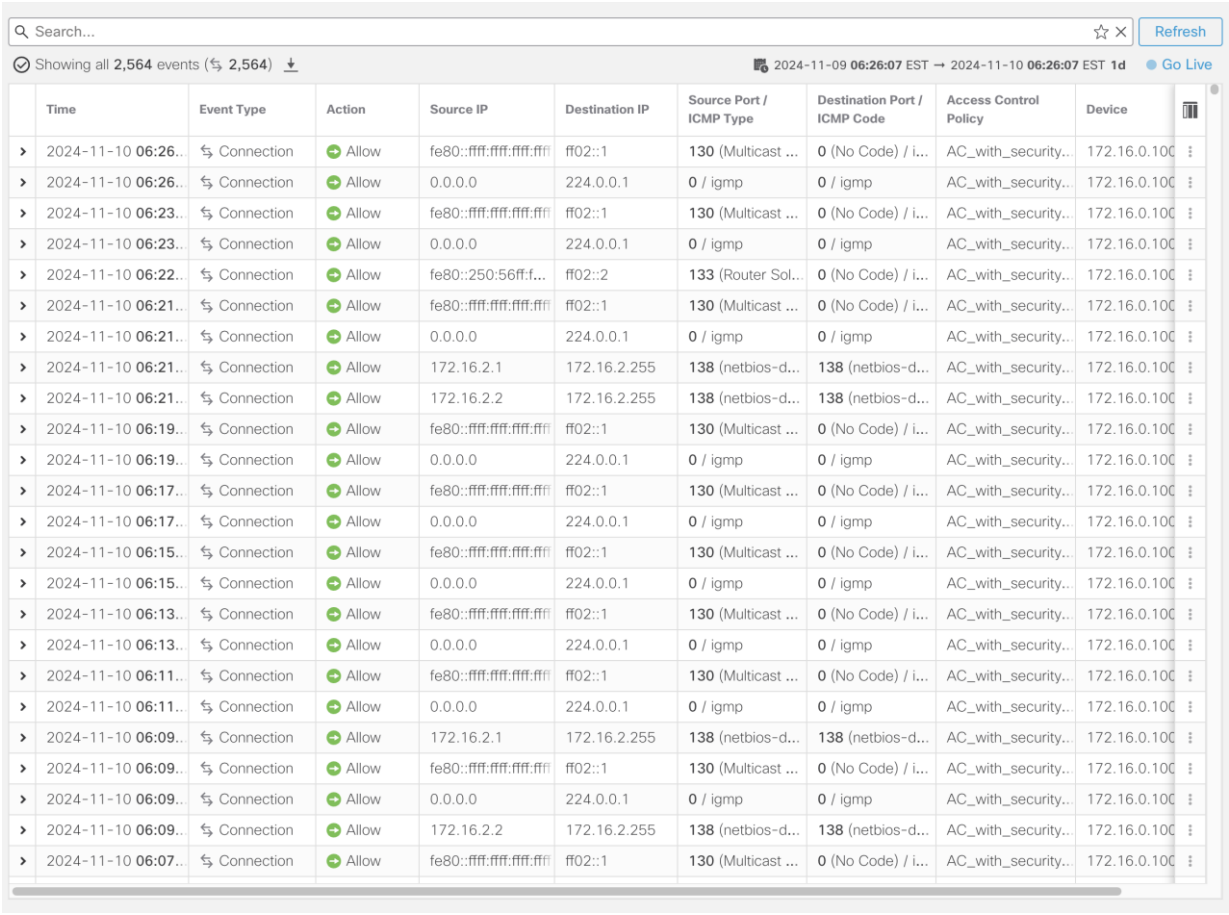


Рисунок 3.28 – Приклад вигляду таблиці Unified Events

Користувач FMC має можливість скористатись великим набором критерій фільтрацій відображених подій. Прикладом такого критерію є період часу, з який були зроблені записи подій під час аналізу трафіку. Для цього необхідно відкрити випадаюче меню над таблицею Unified Events виконавши клік на період часу, який був зазначений за замовчуванням. Коли меню відобразилось, користувач може використати заготовлені періоди часу, наприклад 5 хвилин, 30 хвилин, 1 година, 6 годин, 1 день, 2 тижні, 1 місяць. Також, у користувача є можливість зазначити необхідний період часу за допомогою календаря (рис. 3.29).

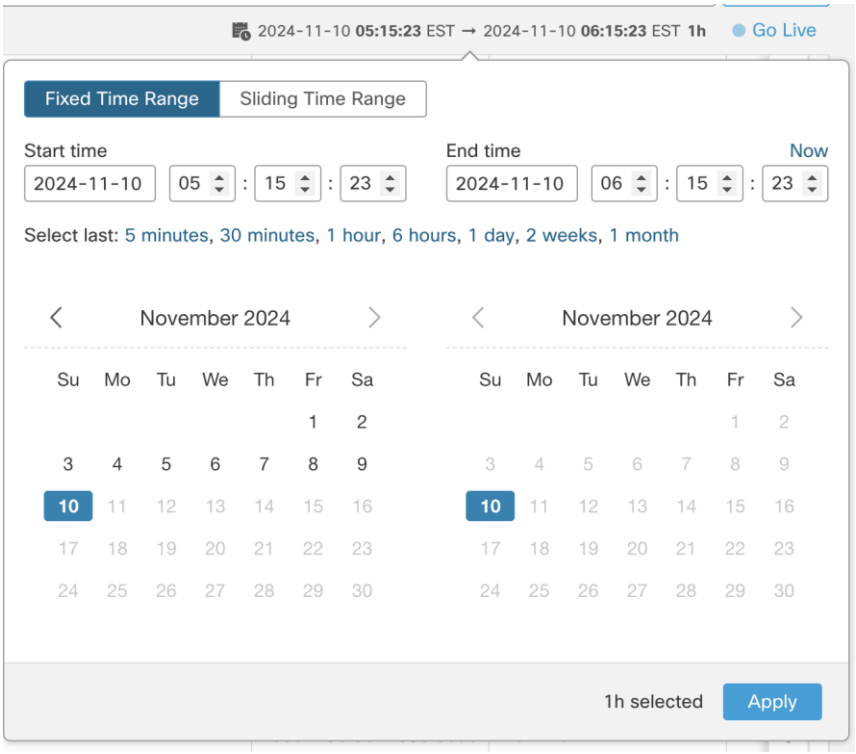


Рисунок 3.29 – Приклад вигляду випадаючого меню для фільтрації подій за певний період часу

Користувач Firewall Management Center також має можливість відстежувати трафік та згенеровані події, на основі обробки трафіку, в режимі реального часу. Для реалізації цього підходу необхідно скористатись кнопкою Go Live, яка розташована над таблицею Unified Events. Під час роботи цього режиму, користувач має змогу аналізувати щойно створені події, що допомагає покращити аналіз роботи правил та політик безпеки мережевої інфраструктури (рис. 3.30).

Рисунок 3.30 – Приклад вигляду таблиці Unified Events з подіями в режимі реального часу

ВИСНОВКИ

У рамках кваліфікаційної роботи були реалізовані та застосовані правила та політики безпеки брандмауера за допомогою моделей платформи Cisco Firewall Management Center. Головними перевагами обраної платформи є сучасний та інтуїтивно зрозумілий інтерфейс користувача для налаштування правил та політик безпеки, а також можливість централізованого аналізу результатів обробки трафіку за налаштованими правилами безпеки брандмауера.

Для цього були вирішені такі завдання:

– проаналізовано існуючі платформи для налаштування безпеки мережевої інфраструктури;

– вивчено наявні моделі на платформі Cisco FMC для налаштування правил безпеки брандмауера;

– реалізовано налаштування правил брандмауера для фільтрації трафіку на платформі Cisco FMC;

– проаналізовано результати обробки трафіку у вигляді подій у результаті обробки трафіку за створеними правилами брандмауера за допомогою інтегрованої звітності Cisco FMC.

Для налаштування верифікованого доступу до приватної мережі слід було б організувати VPN мережу з окремими тунелями для доступу до неї. У випадку надсилання трафіку від небажаного джерела – доступ до приватної мережі буде відхиллено.

Також у майбутньому необхідно налаштувати процес логування (запису) індивідуальних подій до журналу брандмауерів. У випадку наявності правильно налаштованого процесу логування, FMC дає можливість централізованого аналізу цих журналів на відповідній сторінці.

Результати дослідження апробовано у вигляді тез доповідей під час X Міжнародної науково-практичної конференції «Scientific trends in the development of science and education» [40].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Тітов С. В., & Тітова О. В. (2014). Інформаційно-освітнє середовище навчального закладу: розвиток засобів і способів комунікаційної й інформаційної взаємодії. Вісник Харківської державної академії культури, (43), 144-150.

2. Тітов С. В., & Тітова О. В. (2015). Оцінка юзабіліті освітніх сайтів: методи і технології. Вісник Харківської державної академії культури. Серія: Соціальні комунікації, (47), 127-134.

3. Путятін Є. П., Гороховатський В. О., & Матат О. О. (2006). Методи та алгоритми комп'ютерного зору: навч. посіб. Харків: ТОВ «Компанія СМІТ».

4. Lyashenko V., Kobylin O., & Ahmad M. A. (2014). General methodology for implementation of image normalization procedure using its wavelet transform. *International Journal of Science and Research (IJSR),* 3 (11), pp. 2870-2877.

5. Gorokhovatskyi V., Gorokhovatskyi O., Yevgenyi P., & Olena P. (2018, August). Quantization of the Space of Structural Image Features as a Way to Increase Recognition Performance. In *2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*, (pp. 464-467). IEEE.

6. Gorokhovatskyi V.O., Tvoroshenko I.S., and Peredrii O.O. (2020). Image classification method modification based on model of logic processing of bit description weights vector. *Telecommunications and Radio Engineering*, 1 (79), pp. 59-69. DOI: 10.1615/TelecomRadEng.v79.i1.60.

7. Daradkeh Y.I., Tvoroshenko I., Gorokhovatskyi V., Latiff L.A., and Ahmad N. (2021). Development of Effective Methods for Structural Image Recognition Using the Principles of Data Granulation and Apparatus of Fuzzy Logic. *IEEE Access, 9*, pp. 13417-13428.

8. Тітов С.В., Тітова О.В., Чорна О.С. (2022). Опис нескоротних наборів ознак в приблизних множинах з використанням систем числення. *Збірник наукових праць Харківського національного університету Повітряних Сил. № 1(71)*, с. 106-110.

9. Mashtalir S., Mashtalir V., & Stolbovyi M. (2018, August). Representative Based Clustering of Long Multivariate Sequences with Different Lengths. In *2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*, pp. 545-548.

10. 5 Ways to share data between applications. URL: https://medium.com/codex/sending-data-between-applications-e08fb0028a71 (дата звернення 11.11.2024)

11. Sitnikov D., Titova O., Minukhin S., Kovalenko A., Titov S. (2018). Informativity of Association Rules from the Viewpoint of Information Theory. Conference: *2018 IEEE International Scientific-Practical Conference Problems of Infocommunications*. Science and Technology.

12. Kobylin O., Vyskrebentseva S., & Petrova R. (2019). Обробка даних, що містять пропуски в задачах кластеризації. *Системи управління, навігації та зв'язку. Збірник наукових праць, 5(57).*

13. Опис Cisco ASA. URL: https://www.cisco.com/c/en/us/products /security/adaptive-security-appliance-asa-software/index.html (дата звернення 30.09.2024).

14. Cisco ASA розгорнута документація. URL: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-appliance-asa-software/data_sheet_c78-714849.html (дата звернення 30.09.2024).

15. Початок роботи та опис Microsoft Defender Firewall. URL: https://support.microsoft.com/en-us/topic/getting-started-with-microsoft-defender-9df0cb0f-4866-4433-9cbc-f83e5cf77693 (дата звернення 30.09.2024).

16. Firewall as a Service Fortifies State and Local Governments in the Cloud. URL: https://statetechmagazine.com/article/2024/06/firewall-as-a-service-perfcon (дата звернення 02.10.2024).

17. What Is Network Monitoring. URL: https://www.cisco.com/c/en_uk /solutions/automation/what-is-network-monitoring.html (дата звернення 08.10.2024).

18. Configure Network Rules: URL https://community.netwitness.com/t5 /netwitness-platform-online/configure-network-rules/ta-p/669142 (дата звернення 08.10.2024).

19. Network rules documentation. URL: https://docs.snowflake.com/en/user-guide/network-rules (дата звернення 12.10.2024).

20. Application layer protocols. URL: https://adacomputerscience.org /concepts/internet_application_layer (дата звернення 12.11.2024).

21. Protocols in Application Layer. URL: https://www.geeksforgeeks.org /protocols-application-layer/ (дата звернення 12.10.2024).

22. Configure Network Address Translation. URL: https://www.cisco.com/c /en/us/support/docs/ip/network-address-translation-nat/13772-12.html (дата звернення 14.10.2024).

23. Розгорнута документація про FMC. URL: https://www.cisco.com/c/en /us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html (дата звернення 18.10.2024).

24. Next-Generation Firewall (NGFW). URL: https://www.fortinet.com /products/next-generation-firewall (дата звернення 10.10.2024).

25. pfSense Detailed latest documentation. URL: https://docs.netgate.com /pfsense/en/latest/ (дата звернення 18.10.2024).

26. Best Network Monitoring Software Reviewed for 2024. URL: https://thectoclub.com/tools/best-network-monitoring-software/ (дата звернення 18.10.2024).

27. Cisco Systems history. URL: https://www.britannica.com/money/Cisco-Systems-Inc (дата звернення 18.10.2024).

28. Cisco Security White Papers. URL: https://sec.cloudapps.cisco.com/ security/center/whitePapers.x?i=43 (дата звернення 24.10.2024).

29. Cisco Acquires Cybersecurity Company Sourcefire. URL: https://techcrunch.com/2013/07/23/cisco-acquires-cybersecurity-company-sourcefire-for-2-7b/ (дата звернення 29.10.2024).

30. Cisco Secure Firewall Management Center Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html?dtid=osscdc000283 (дата звернення 06.11.2024).

31. Cisco Talos. URL: https://talosintelligence.com/ (дата звернення 06.11.2024).

32. Introduction to the Cisco Secure Firewall Threat Defense Virtual. URL: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/consolidated_ftdv_gsg/threat-defense-virtual-74-gsg/m-introduction-to-ftdv.html (дата звернення 06.11.2024).

33. Introduction to the Secure Firewall Management Center Virtual Appliance. URL: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcv/fpmc-virtual/fpmc-virtual-intro.html (дата звернення 06.11.2024).

34. Cisco Access Control Policy. URL: https://networkdirection.net/articles/firewalls/firepowermanagementcentre/fmcaccesscontrolpolicies/ (дата звернення 10.11.2024).

35. TLS/SSL Rules Best Practices. URL: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/ssl-rules/710/deploy-ssl-rules-with-examples_71/tls-ssl_rule_best_practices.html (дата звернення 10.11.2024)

36. Realms and Identity Policies. URL: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Identity_Policies_and_Realms.html (дата звернення 10.11.2024).

37. Security Policy Management. URL: https://www.skyboxsecurity.com/solutions/security-policy-management/ (дата звернення 10.11.2024).

38. Introduction To Cisco Stealthwatch. URL: https://tesrex.com/article/an-introduction-to-cisco-stealthwatch/ (дата звернення 11.11.2024).

39. Cisco FMC Increase Events Rows. URL: https://bluenetsec.com/cisco-fmc-increase-events-rows/ (дата звернення 12.11.2024).

40. Босенко А.М. (2024). Дослідження та застосування технологій забезпечення безпеки мережевої інфраструктури.. *Радіоелектроніка та молодь у XXI столітті: X Міжнародна науково-практична конференція «Scientific trends in the development of science and education»*. С. 235-236.