ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія забезпечення мережевої безпеки на базі Cisco»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Вадим САЙЧУК
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
САЙЧУК Вадим
(прізвище, ім'я)

Керівник д.т.н., професор ГАЙДУР Галина,
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

ACL – Access Control Lists

ACE – Access Control Entries

ACI – Application Centric Infrastructure

BYOD – Bring-Your-Own-Device

CASB – Cloud Access Security Broker

CSP – Cloud Service Provider

DMZs – Demilitarized Zones

DNS – Domain Name System

IaaS – Infrastructure as a Service

IOS – Internetwork Operating System

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

NAC – Network Access Control

NGFW – Next-Generation Firewall

SDN Software Defined Network

SDP – Software Defined Perimeter

SIEM – Security Information and Event Monitoring

SSE –Security Service Edge

TIC – Trusted Internet Connections

VPN – Virtual Private Network

WFA – Work-From-Anywhere

ВСТУП

Актуальність дослідження. У сучасному цифровому світі забезпечення мережевої безпеки є критично важливим для стабільного функціонування організацій, державних установ і бізнесу в цілому. Технології кіберзагроз розвиваються та удосконалюються з шаленою швидкістю, що ставить під загрозу конфіденційність, доступність і цілісність даних. У цьому контексті, наявність надійних і ефективних рішень для забезпечення безпеки мережі стає невід'ємною частиною інформаційної інфраструктури кожної організації.

Однією з провідних компаній у сфері мережевої безпеки є Cisco Systems, що пропонує широкий спектр технологій та інструментів для захисту мереж від різноманітних загроз. Технології Cisco мають велике значення як для великих корпорацій, так і для малих і середніх підприємств, оскільки вони надають комплексний підхід до захисту корпоративних мереж і систем. Відтак, дослідження технологій забезпечення мережевої безпеки на базі Cisco є надзвичайно актуальним з кількох причин.

Зростання кіберзагроз і складність атак. Незважаючи на численні досягнення в галузі інформаційних технологій, кіберзлочинці постійно вдосконалюють свої методи атаки, використовуючи складні техніки, як-от фішинг, атаки на рівні додатків, DDoS-атаки, шкідливі програми, атаки на кінцеві точки, тощо. Це вимагає застосування новітніх технологій для виявлення та запобігання таким загрозам.

Збільшення значення мережевої безпеки в умовах цифрової трансформації. У епоху цифровізації підприємства все більше покладаються на інтернет, хмарні сервіси та мобільні технології, що збільшує поверхню атаки і створює нові виклики для забезпечення безпеки. Ці зміни вимагають оновлення методів і інструментів захисту, адже традиційні підходи не завжди можуть ефективно справлятися з новими загрозами.

Сучасні рішення безпеки повинні бути інтегрованими і автоматизованими для ефективного моніторингу та реагування на інциденти. Рішення на базі Cisco

дозволяють зібрати інформацію з різних джерел, автоматично реагувати на загрози і зменшувати час, необхідний для виявлення та усунення інцидентів.

Дослідження технологій забезпечення мережевої безпеки на базі Cisco є надзвичайно актуальним у сучасних умовах, коли кіберзагрози постійно еволюціонують, а вимоги до безпеки стають все більш жорсткими. Cisco надає потужні, масштабовані і інтегровані рішення, які дозволяють ефективно захищати корпоративні мережі від загроз і відповідати сучасним вимогам безпеки. Ця тема є важливою для тих, хто працює в сфері інформаційної безпеки, оскільки технології Cisco допомагають зберігати стабільність і захищеність цифрової інфраструктури в умовах зростаючих викликів.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології забезпечення мережевої безпеки на базі Cisco.

Об'єкт дослідження – забезпечення мережевої безпеки організації.

Предмет дослідження – технологія забезпечення мережевої безпеки організації на базі Cisco Secure Firewall Management Center.

Мета роботи – розробити порядок застосування технології забезпечення мережевої безпеки для роботи працівників організації та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми забезпечення мережевої безпеки для організації;

проаналізувати підходи до забезпечення мережевої безпеки організації;

проаналізувати існуючі рішення із забезпечення мережевої безпеки організації;

проаналізувати методи та засоби забезпечення мережевої безпеки організації на базі Cisco Secure Firewall Management Center;

розкрити порядок реалізації технології забезпечення мережевої безпеки для організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз

експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології забезпечення мережевої безпеки для безпечної роботи працівників організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1. Аналіз необхідності забезпечення мережевої безпеки

Проаналізувавши дані з мережі Інтернет та переглянувши статистику щодо атак, несанкціонованого доступу та кіберзлочинності варіюється залежно від регіону, організації та часу. Проте загалом спостерігаються декілька основних тенденцій у цій сфері, зокрема:

1. Загальна кількість кібератак.

За даними різних досліджень, кожен день відбувається мільйони кібератак (рис.1.1).

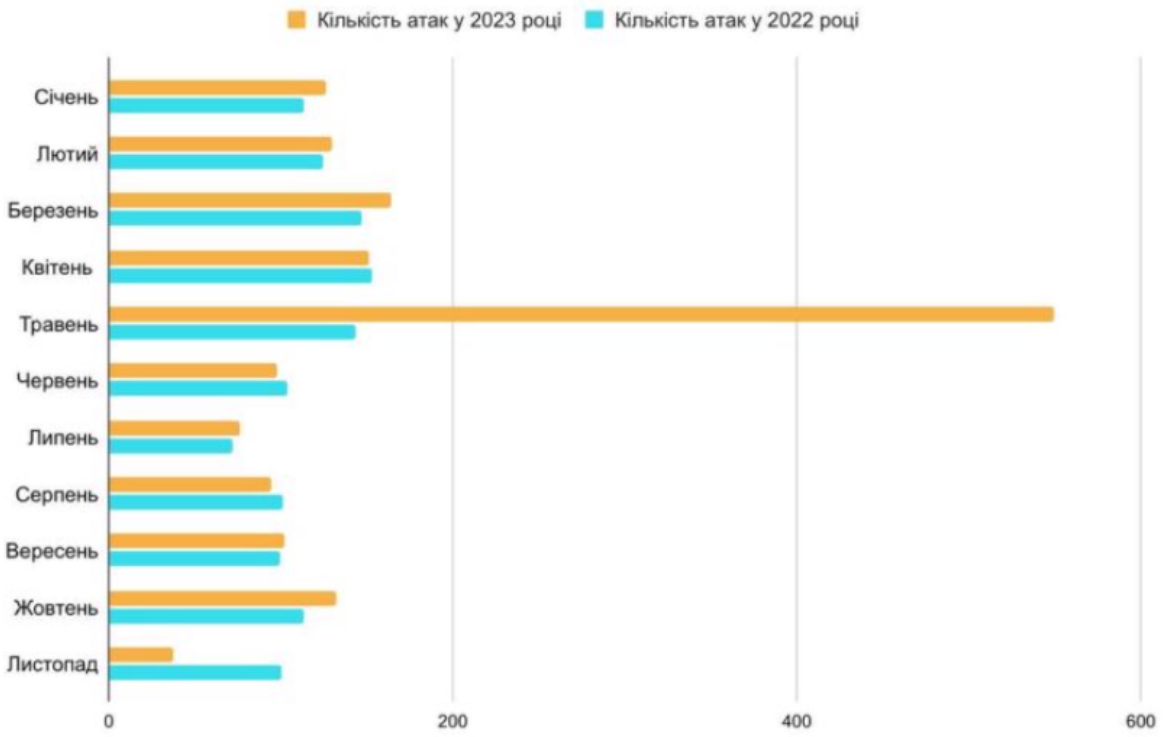

Рис.1.1. Статистика кібератак у мільйонах за 2022-2023 років

Згідно з даними Cybersecurity Ventures, глобальні витрати на кібербезпеку у 2024 році можуть досягти $267 млрд, а кількість атак збільшуватиметься на 15-20% щороку.

Офіційна статистика зазвичай показує, що кібернапади здійснюються з

використанням різних методів, серед яких найбільш популярні — фішинг, зловмисне програмне забезпечення, атакі типу DDoS, та неёсанкціонований доступ до систем.

2. Фішинг та соціальна інженерія.

Фішинг є однією з найбільш поширених форм кіберзлочинів. За даними Anti-Phishing Working Group (APWG), кількість фішингових атак збільшилась на 20-30% у порівнянні з попередніми роками (рис.1.2).

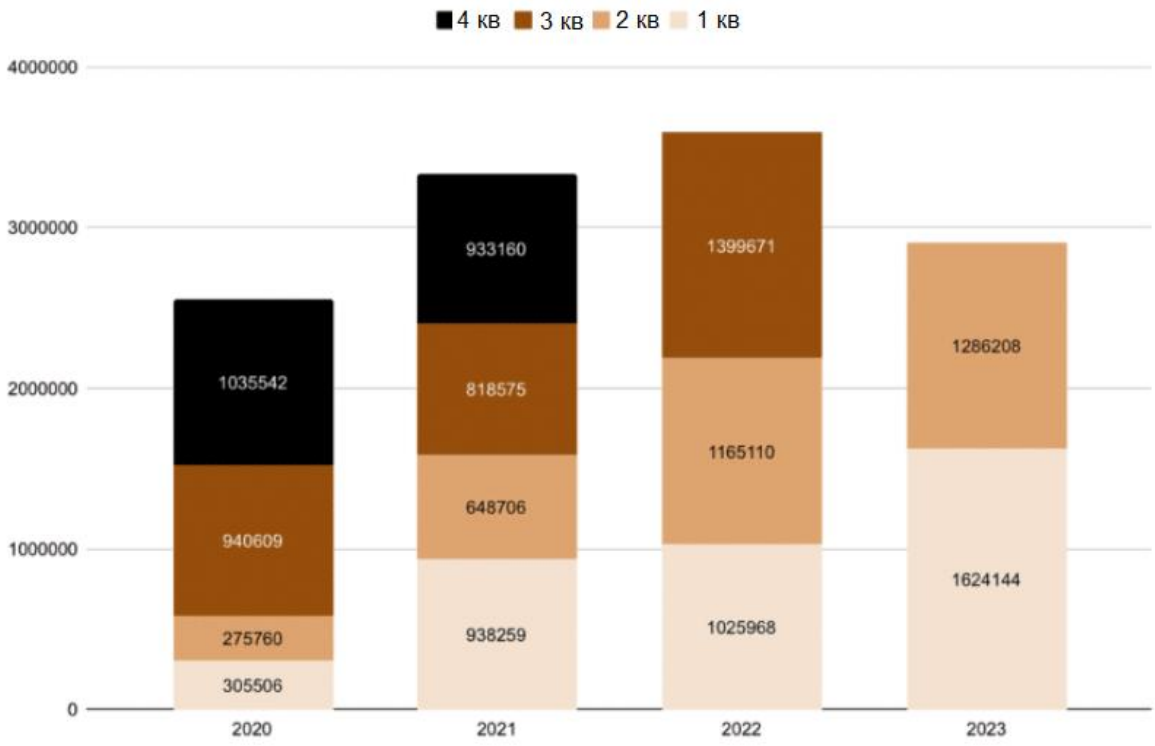

Рис.1.2. Кількість фішингових атак по кварталам за 2020-2023 років

Кіберзлочинці використовують фішингові електронні листи або вебсайти, щоб обдурити користувачів і змусити їх передати конфіденційну інформацію, як-от паролі, дані карток або доступ до облікових записів.

3. Атаки на підприємства та урядові установи.

Рансомвар (вимагачі) — ще один поширений вид атак. За даними Cybersecurity Ventures, щорічно збитки від атак з використанням програм-вимагачів зростають на 30%, і у 2024 році ці збитки можуть перевищити $20 млрд (рис.1.3).

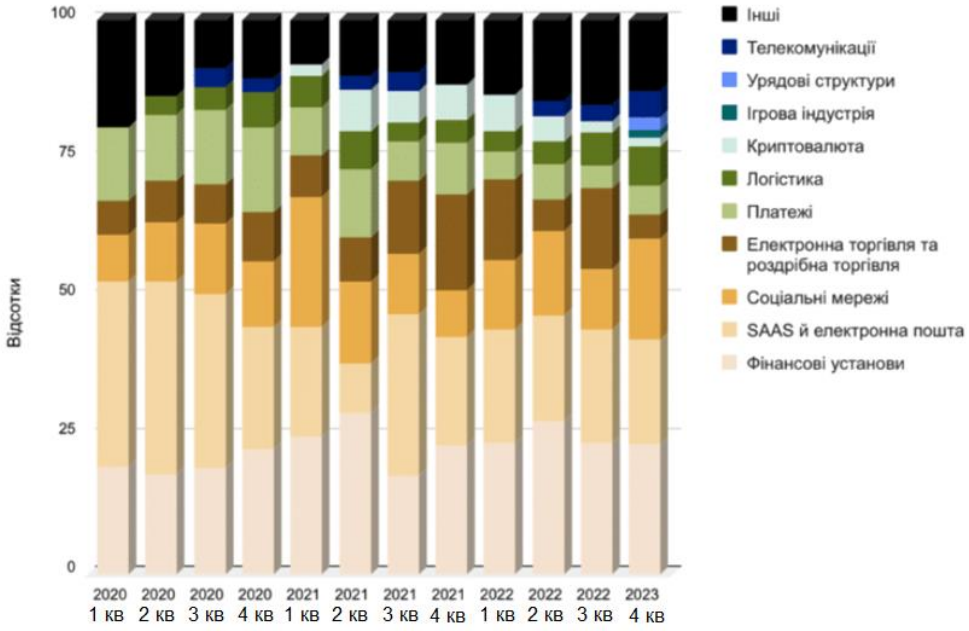

Рис.1.3. Кількість у відсотках кібератак по кварталам за 2020-2023 років

Згідно з дослідженнями, близько 60-70% атак спрямовані на малий та середній бізнес, хоча великі корпорації та урядові установи також не застраховані від подібних інцидентів.

4. Зловмисне програмне забезпечення (Malware).

Зловмисне програмне забезпечення — це ще одна значна проблема. У 2023 році дослідження компанії McAfee показало, що було зафіксовано понад 0,5 мільярда випадків зараження шкідливим ПЗ (рис.1.4).

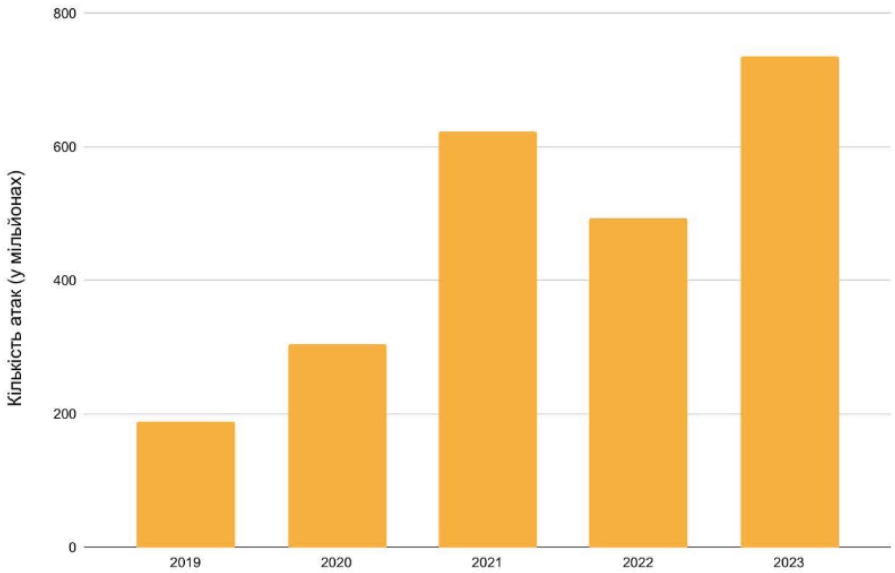

Рис.1.4. Кількість атак зловмисним ПЗ за 2019-2023 роки

Часто використовуються трояни, віруси, черви, а також складні багаторівневі шкідливі програми, що можуть маскуватися під легітимне ПЗ або інфікувати комп'ютери через вразливості в програмному забезпеченні.

5. Атаки на системи та мережі.

Несанкціонований доступ до комп'ютерних систем — це також велика проблема. За статистикою, більше ніж 40% компаній у всьому світі зазнають атак на свої мережі або бази даних щорічно (рис.1.5, рис.1.6).

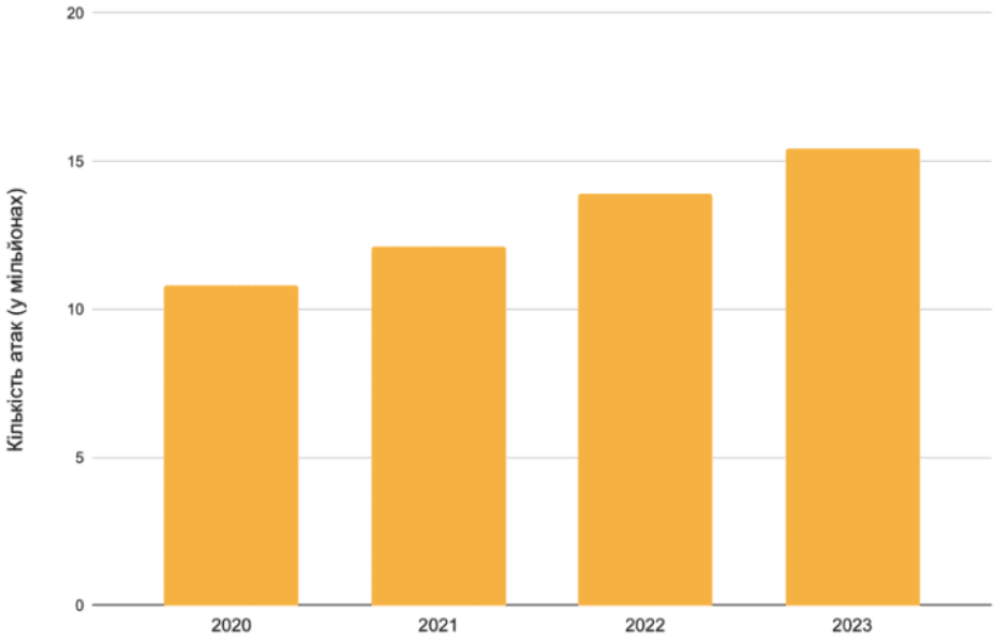

Рис.1.5. Кількість DDoS-атак за 2020-2023 роки

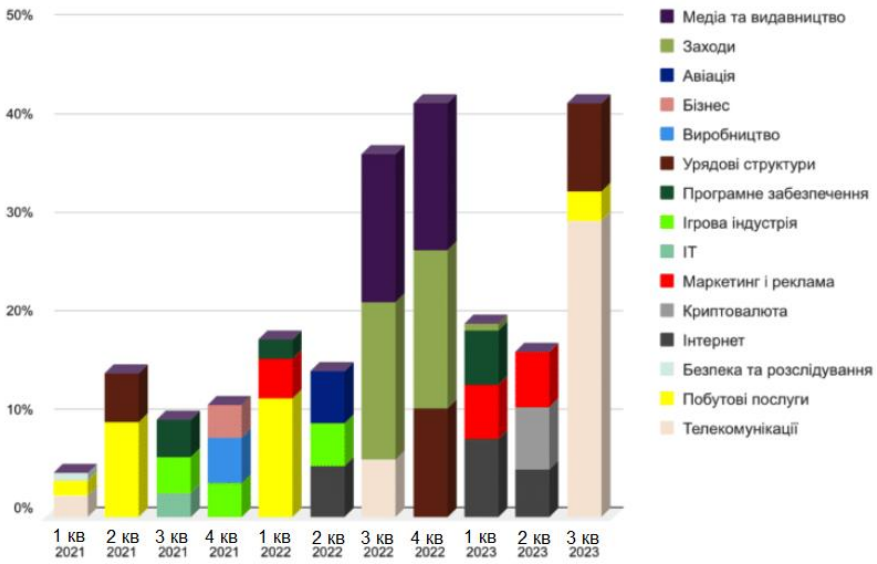

Рис.1.6. Галузі, що були найбільш атакованими DDoS по кварталах 2021-2023 років

Зловмисники можуть використовувати уразливості в мережевій інфраструктурі або несанкціоновані пристрої для проникнення в системи.

6. Призначення атак.

За даними досліджень Check Point Research, найбільші жертвами кібератак — це США, Китай, Індія, а також деякі країни Європи. Проте є тенденція до збільшення атак на країн, що розвиваються, оскільки там часто недостатньо розвинута кібербезпека (рис.1.7).

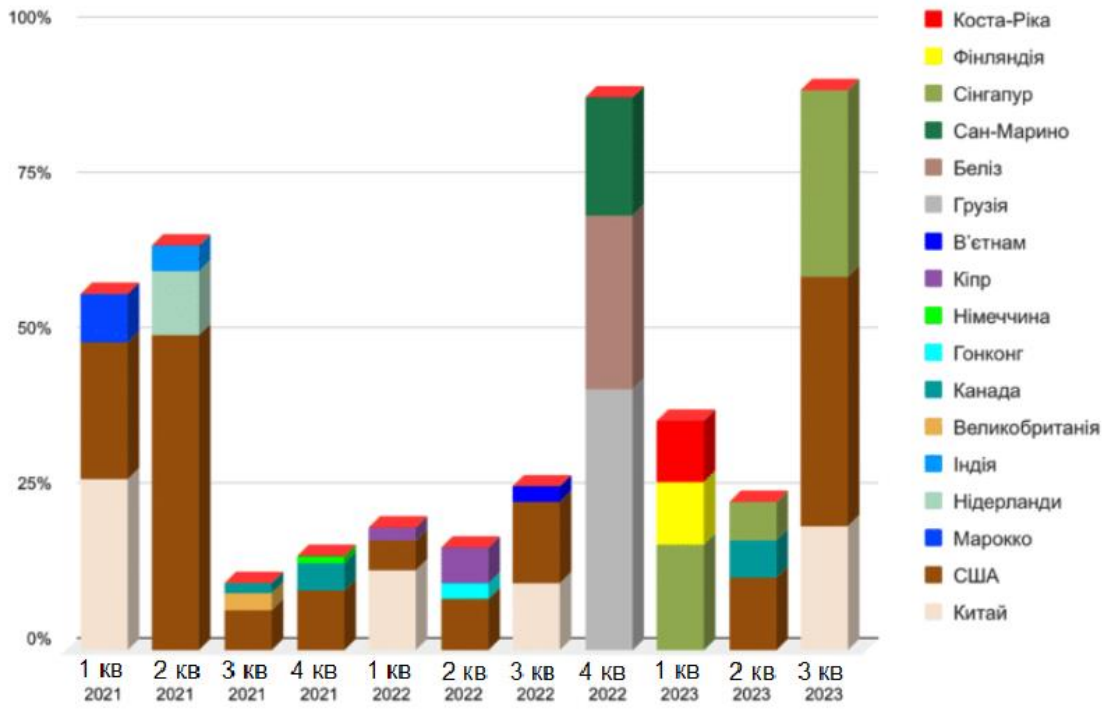

Рис.1.7. Країни, що були найбільш атакованими DDoS за квартали 2021-2023 років

7. Роль штучного інтелекту в атаках.

Існує тенденція до використання штучного інтелекту (ШІ) для автоматизації атак. Це дає змогу зловмисникам більш ефективно створювати фішингові кампанії, пошук вразливих систем або навіть здійснювати атаки на бази даних.

Як реагують на загрози

Сучасні технології захисту включають AI для виявлення аномалій, хмарні рішення для моніторингу та аналізу трафіку, а також мультифакторну аутентифікацію (MFA) для запобігання несанкціонованому доступу.

Зростає популярність інтегрованих систем безпеки, що поєднують в собі різні інструменти для боротьби з атаками, таких як антивірусні програми, системи моніторингу мереж та системи управління інцидентами безпеки.

Це лише частина статистичних даних щодо кіберзагроз. Кібербезпека продовжує бути важливою сферою для всіх видів організацій, адже атаки можуть призвести до серйозних фінансових втрат, репутаційних пошкоджень та витоку конфіденційної інформації.

У зв’язку з вище наведеним все більше організацій витрачають значні кошти на мережеву безпеку. Дослідження технологій забезпечення мережевої безпеки охоплює різноманітні аспекти, включаючи захист обладнання, програмного забезпечення, методи захисту даних, протидію кібератакам, управління ризиками та компетентності персоналу. Основні ключові напрями на котрі потрібну в першу чергу звертати увагу, це:

Firewall (Фаєрвол, мережевий екран) – комплекс апаратних та програмних засобів, що здійснює контроль трафіку (мережевих пакетів) між внутрішньою мережею та зовнішніми джерелами (Інтернет) за встановленими правилами, не пропускаючи (фільтруючи) пакети, що не відповідають критеріям конфігурації мережі (рис.1.8). В сучасному світі для корпоративних мереж Firewall не є панацеєю від усіх загроз, але при грамотному його налаштуванні буде закрита низка мережевих загроз.

Рис.1.8. Принцип роботи Firewall

В свою чергу фаєрволи можуть використовуватись для обмежених задач на різних рівнях:

- Мережевому – фільтрація на основі мережевих адрес, для направлення трафіку у необхідну мережу або до потрібного IP адреса (сервера),

- Сеансовому – відстеження сеанси між додатками, відфільтровуючи пакети, які не відповідають специфікації TCP/IP,
- Рівень додатків – відстеження на підставі аналізу даних програми.

Системи виявлення та запобігання вторгнення (IDS/IPS) (рис.1.9). IDS – програмний або апаратний засіб для виявлення фактів несанкціонованого доступу до мережі, або управляння нею IPS – програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у разі їх виявлення.

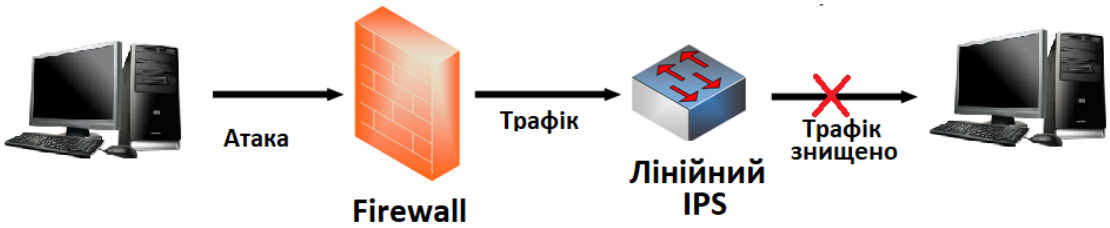

Рис.1.9. Система запобігання вторгнення

VPN (віртуальні приватні мережі) – використовується для забезпечення безпечного з'єднання між віддаленими користувачами та корпоративними мережами. VPN поділяється на підключення типу: «точка-точка» логічне з’єднання, яке працює поверх приватних або публічних мереж; «мережа-мережа» з’єднання, яке дозволяє організувати підключення між мережами віддалених офісів.

Шифрування даних – використовуються криптографічні методи для захисту даних під час передачі, що запобігає їх перехопленню.

Аудит безпеки – регулярна перевірка мережевої інфраструктури на наявність вразливостей та загроз, щоб у подальшому проводити заходи для їх зменшення.

Керування доступом – використання методів аутентифікації (наприклад, багатофакторна аутентифікація) для контролю доступу до систем, комп’ютерів та інших інформаційних ресурсів.

Захист від DDoS-атак – впровадження технологій для виявлення та блокування розподілених атак на відмову в обслуговуванні.

Системи управління інформацією та подіями безпеки (SIEM) (рис.1.10) – це сучасна технологія кіберзахисту, яка об’єднала у собі компоненти збору, обробки, аналізу подій безпеки, виявлення загроз у реального часі, аналіз та управління ризиками безпеки, проведення розслідувань інцидентів.

Рис.1.10. Системи управління інформацією та подіями безпеки (SIEM)

Навчання та підвищення обізнаності – регулярне навчання співробітників щодо основ мережевої безпеки для зменшення ризиків, пов'язаних з людським фактором.

Кожен з цих напрямків має свої особливості та застосування, і їх інтеграція є важливою для забезпечення комплексного підходу до мережевої безпеки.

1.2. Аналіз підходів до забезпечення мережевої безпеки

Проаналізувавши основні підходи до забезпечення мережевої безпеки можна зробити висновок про різноманітні методи та стратегії, що застосовуються для захисту інформаційних систем від загроз. Ось кілька основних підходів:

Периметровий захист або ще його називають *периметральний міжмережевий екран* – цей підхід слугує як надійний бар’єр, який фокусується на захисті зовнішніх меж мережі організації від зовнішніх загроз та несанкціонованого доступу. Для досягнення поставленої цілі застосовується фаєрволи, системи виявлення та запобігання вторгненням (IDS/IPS), щоб контролювати вхідний та вихідний трафік. Основна мета – зупинити атаки на стадії

їх виникнення за допомогою складних наборів заздалегідь визначених правил безпеки.

Захист на рівні мережі – цей підхід передбачає використання технологій, таких як VPN, VLAN та сегментація мережі на підмережі, щоб обмежити доступ до чутливих даних та систем. Це дозволяє зменшити ризик внутрішніх загроз і забезпечити безпечний доступ до ресурсів.

Контроль доступу – це метод перевірки користувача за допомогою аутентифікації та авторизації для контролю, хто має доступ до систем і даних. Це може бути реалізовано через паролі, біометрію або багатофакторну аутентифікацію. Застосування політик «мінімальних привілеїв» дозволяє обмежити доступ лише до необхідних ресурсів.

Криптографія - шифрування даних вважається важливим інструментом для забезпечення конфіденційності та цілісності інформації. Використання протоколів шифрування, таких як TLS/SSL для захисту передавання даних, є стандартною практикою захисту інформації.

Оцінка ризиків та реакція на інциденти – регулярний аналіз вразливостей та оцінка ризиків допомагають ідентифікувати потенційні загрози та слабкі місця в системах, що дозволяє вчасно вжити заходів для їх усунення, а також планувати реалізацію заходів у разі виникнення кібератак.

Навчання та підвищення обізнаності персоналу – людський фактор, як показала практика, є однією з найбільш поширених проблем для мережевої безпеки. Регулярне навчання співробітників щодо найкращих практик безпеки може суттєво знизити ризики, пов’язані з фішингом та іншими атаками соціальної інженерії.

Інтеграція технологій – сучасний підхід до забезпечення безпеки вимагає інтеграції різних технологій, таких як SIEM системи, для збору та аналізу даних з різних джерел. Це дозволяє виявляти та реагувати на загрози в реальному часі.

Отже, комбінування цих та інших підходів створює багатошарову стратегію забезпечення мережевої безпеки, яка є необхідною для захисту інформаційних систем та ресурсів у сучасному цифровому середовищі. Використання

інтегрованих рішень та постійне вдосконалення політик безпеки дозволяє адаптуватися до загроз, що змінюються.

1.3. Аналіз існуючих рішень із забезпечення мережевої безпеки

Аналіз існуючих рішень із забезпечення мережевої безпеки охоплює різні технології та програмні продукти, які використовуються для захисту інформаційних систем та ресурсів від загроз. Ось огляд ключових категорій для вирішення питань мережевої безпеки:

- Апаратні та програмні фаєрволи. До найбільш поширених можна віднести: Cisco ASA, Fortinet FortiGate, Palo Alto Networks.

Основна функціональність – контроль трафіку, блокування несанкціонованого доступу, гнучкість в налаштуваннях політик.

- Системи виявлення та запобігання вторгнення (IDS/IPS). До найбільш поширених можна віднести: Snort, Suricata, Cisco Firepower.

Основні переваги – виявлення загроз у реальному часі, можливість реагування на атаки.

- Рішення для захисту кінцевих пристроїв – антивірусні програми, рішення для управління мобільними пристроями (MDM). До найбільш поширених можна віднести: Trellix Endpoint Security, Symantec Endpoint Protection, McAfee, CrowdStrike.

Переваги: Захист від шкідливого ПО, контроль за пристроями, що підключаються до мережі.

- Віртуальні приватні мережі (VPN). Найбільш популярними є OpenVPN, Cisco AnyConnect, NordVPN, які забезпечують захищене з'єднання для віддалених працівників, шифрування трафіку.

- Системи управління інформацією та подіями безпеки (SIEM). До найбільш поширених можна віднести: Splunk, IBM QRadar, LogRhythm.

Переваги: Центральний збір та аналіз логів, виявлення загроз, звітність.

- Шифрування даних на рівні файлів, дисків, баз даних. До них

відносяться VeraCrypt, BitLocker, AWS KMS. Забезпечують захист чутливих даних, забезпечення конфіденційності.

- Аудит та управління вразливостями. Найбільш популярними програмними продуктами є Nessus, Qualys, Rapid7, які забезпечують регулярну перевірку на вразливості та надають рекомендації щодо їх усунення.

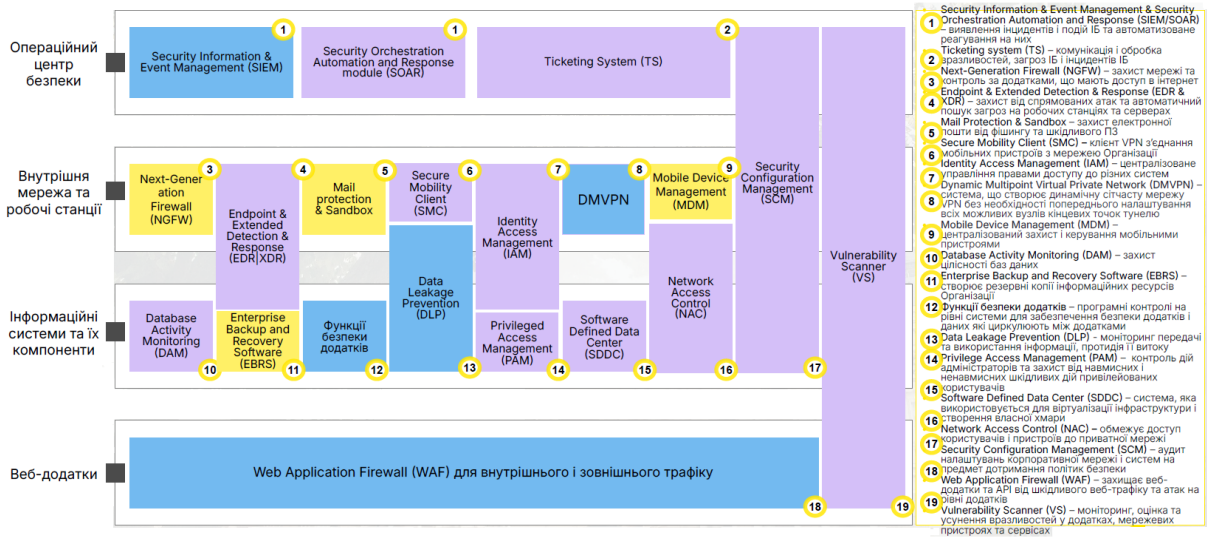

Рис.1.11. Ідеальна схема мережевої безпеки

Компанія Cisco Systems пропонує на базі Cisco Firepower архітектурне рішення, яке може об’єднати більшість систем захисту для забезпечення мережевої безпеки в організаціях.

Висновки до розділу 1

Сучасні рішення для забезпечення мережевої безпеки відрізняються за своєю функціональністю та спрямованістю. Їх інтеграція дозволяє створити багатошарову архітектуру безпеки, що відповідає специфічним потребам організацій і допомагає протистояти різноманітним загрозам у динамічному середовищі кібербезпеки. Сучасні системи забезпечення мережевої безпеки корпоративної мережі підприємства дають можливість обрати найбільш вдалий та дієвий спосіб захисту інформації, яка підходить для мережі організації. Враховуючи вище сказане, власник мережі має можливість обрати, відповідно до

свого бюджету, необхідні механізми захисту починаючи від антивірусного ПЗ, закінчуючи системами виявлення та запобігання вторгненням. Кінцевою метою є розробка комплексної системи захисту інформації, яка забезпечить надійний захист інформації в мережі.

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ НА БАЗІ CISCO FIREPOWER

2.1. Варіанти архітектурних рішень застосування Cisco Firepower

Cisco Firepower пропонує кілька архітектурних рішень для забезпечення мережевої безпеки в організаціях. Ось кілька варіантів архітектурних рішень для застосування Cisco Firepower:

1. Периметральна архітектура

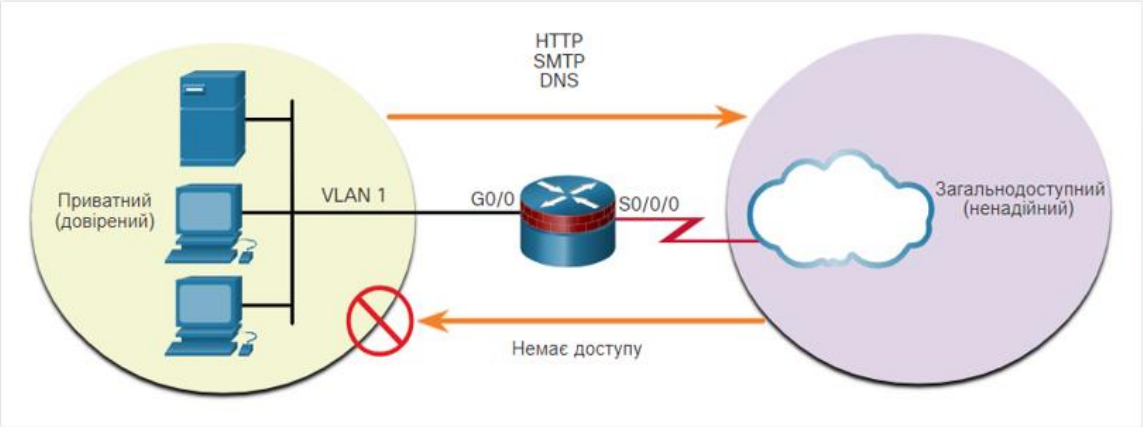

Рис.2.1. Схема периметральної архітектури корпоративної мережі

Cisco Firepower розміщується на межі мережі (мереж), між внутрішньою та зовнішньою (наприклад, Інтернет) мережею. Основними функціями даного методу є:

- захист від зовнішніх (внутрішніх) загроз;
- контроль доступу до внутрішніх (зовнішніх) ресурсів.
- моніторинг трафіку та виявлення загроз.

Даний метод використовується в нашій компанії і доволі добре себе зарекомендував. Периментральна архітектура обробляє великий обсяг трафікі з Інтернету та має гарний функціонал по контролю доступу до ресурсів.

2. Внутрішня сегментація

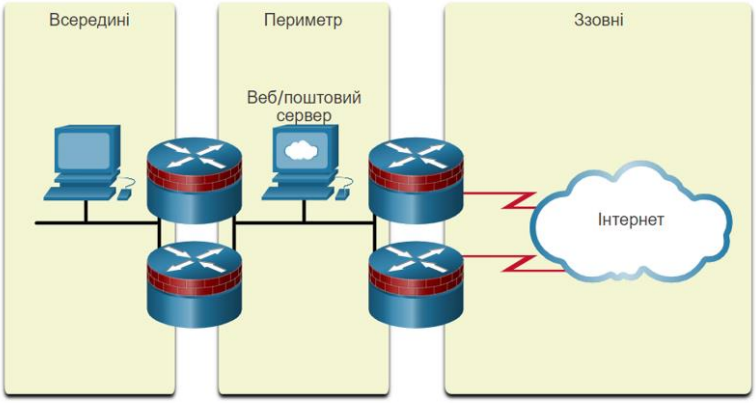

Рис.2.2. Сегментація корпоративної мережі

Firepower використовується для сегментації мережі всередині організації, контролюючи трафік між різними VLAN або сегментами.

Функції сегментації:

- забезпечує додатковий рівень безпеки між внутрішніми ресурсами.
- запобігає розповсюдженню загроз між сегментами.
- Можливість застосування політик безпеки для різних сегментів.

Застосовується для чутливої інформації, яку використовують різні відділи з різними вимогами безпеки.

3. Архітектура з декількома демілітаризованими зонами (DMZ)

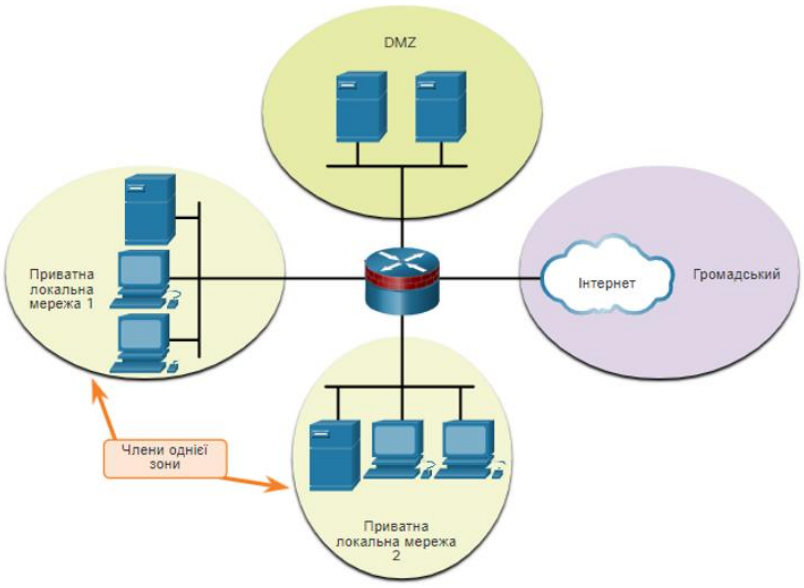

Рис.2.3. Архітектура демілітаризованих зон корпоративної мережі

Використання Cisco Firepower для захисту демілітаризованих зон DMZ, яка містить публічно доступні сервіси (веб-сервери, поштові сервери).

Основна функція:

- контроль доступу до ресурсів DMZ з Інтернету.
- моніторинг трафіку між DMZ та внутрішньою мережею.
- захист від атак на публічні сервіси.

Підходить для компаній, які надають послуги або інформацію через Інтернет.

4. Гібридна архітектура

Поєднання периметрального захисту та внутрішньої сегментації, з використанням Cisco Firepower для всіх точок доступу.

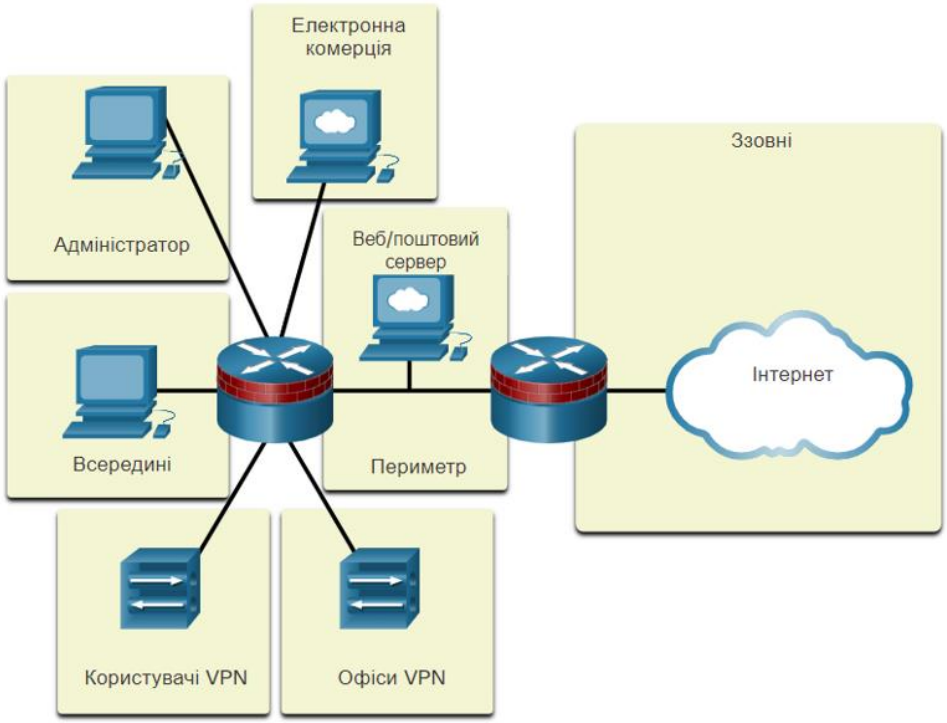

Рис.2.4. Гібридна архітектура корпоративної мережі

Забезпечує функції:

- комплексний захист усіх рівнів мережі.
- можливість адаптації до різних загроз на різних етапах.
- централізоване управління через Firepower Management Center (FMC).

Найбільш гнучка система для захисту мережі.

5. Cloud Security Architecture

Використання Cisco Firepower для захисту гібридних або повністю хмарних середовищ.

Функції:

- захист хмарних додатків та даних.
- моніторинг трафіку між локальними і хмарними ресурсами.
- інтеграція з іншими службами Cisco для забезпечення безпеки в хмарі.

Підходить для компаній, які активно використовують хмарні технології.

Висновок

Cisco Firepower може бути адаптований до різних архітектурних рішень в залежності від потреб бізнесу та специфіки роботи. Кожен з варіантів забезпечує різний рівень безпеки та контролю, що дозволяє організаціям ефективно захищати свої ресурси від загроз.

2.2. Призначення та основні функціональні рішення Cisco Firepower

Для реалізації проектів забезпечення мережевої безпеки можливе використання обладнання провідних світових виробників, що пропонують свої методики побудови систем безпеки.

Компанія Cisco Systems пропонує найбільш повний спектр обладнання та рішень для забезпечення мережевої безпеки:

- обладнання доступу;
- міжмережеві екрани;
- VPN-концентратори;
- мережеві сенсори виявлення вторгнень (IDS);
- системи запобігання вторгнень (IPS);
- спеціалізоване програмне забезпечення для маршрутизаторів;
- клієнтське ПЗ - захист на рівні хоста або сервера;
- модулі забезпечення безпеки для комутаційних шасі;
- системи управління.

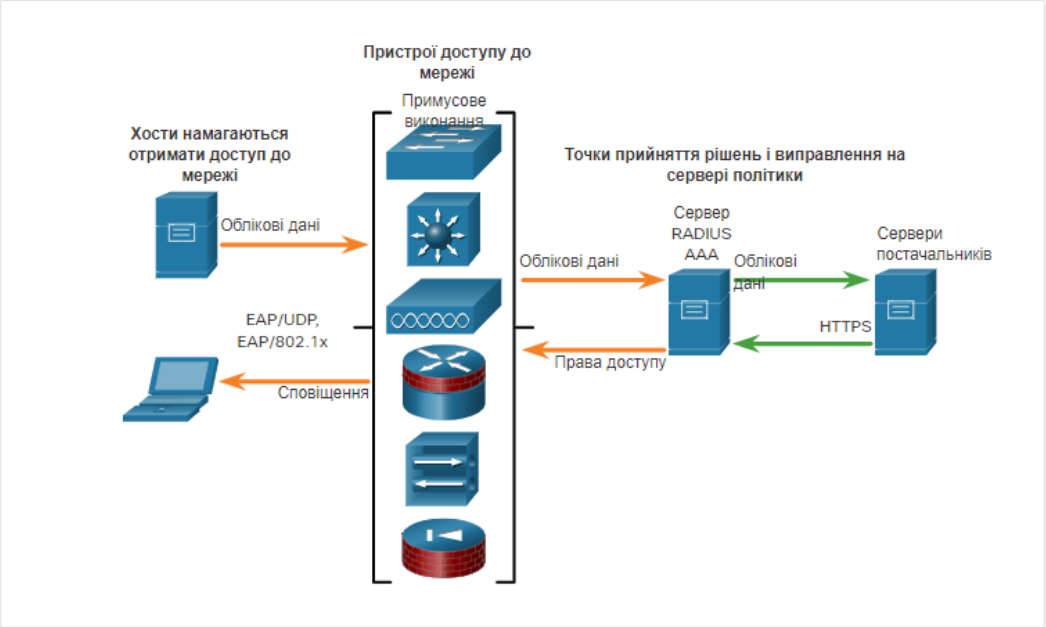

Рис.2.5. Пристрої доступу до мережі

Cisco Firepower — це рішення для мережевої безпеки, яке об'єднує функції між мережевих екранів, систем виявлення та запобігання вторгнень (IDS/IPS), а також розширених можливостей захисту від загроз. Основні призначення та функціональні рішення Cisco Firepower включають:

Призначення:

Захист мережі: Забезпечення безпеки мережевих з'єднань та захист від зовнішніх загроз.

Моніторинг та аналіз трафіку: Відстеження мережевої активності для виявлення аномалій та потенційних атак.

Управління загрозами: Виявлення, аналіз та нейтралізація шкідливих дій у реальному часі.

Основні функціональні рішення:

Міжмережевий екран (Firewall): Контроль доступу до мережі на основі політик безпеки, що визначають, який трафік дозволено або заблоковано.

Система виявлення та запобігання вторгнення (IDS/IPS): Виявлення та блокування шкідливих дій і вторгнень на ранніх стадіях.

Контроль додатків: Виявлення та управління трафіком різних додатків для

підвищення безпеки та продуктивності.

Антивірусний захист: Вбудовані функції для виявлення та блокування шкідливих програм.

Захист від шкідливих URL: Блокування доступу до відомих шкідливих веб-сайтів та контенту.

Аналітика та звітність: Інструменти для моніторингу безпеки, аналізу подій та генерації звітів для адміністрації.

Інтеграція з іншими рішеннями Cisco: Легке інтегрування з іншими продуктами Cisco для комплексного управління безпекою.

Ці функції допомагають організаціям забезпечити всебічний захист від численних загроз і зберегти цілісність мережі.

2.3. Основні компоненти загальної архітектури Cisco Firepower

Основні компоненти архітектури Cisco Firepower включають:

Cisco Firepower Threat Defense (FTD):

Це інтегроване рішення, яке об'єднує функції між мережевого екрану (firewall) та системи виявлення та запобігання вторгнень (IDS/IPS). FTD забезпечує контроль доступу, аналіз трафіку, захист від загроз та управління безпекою.

Cisco Firepower Management Center (FMC):

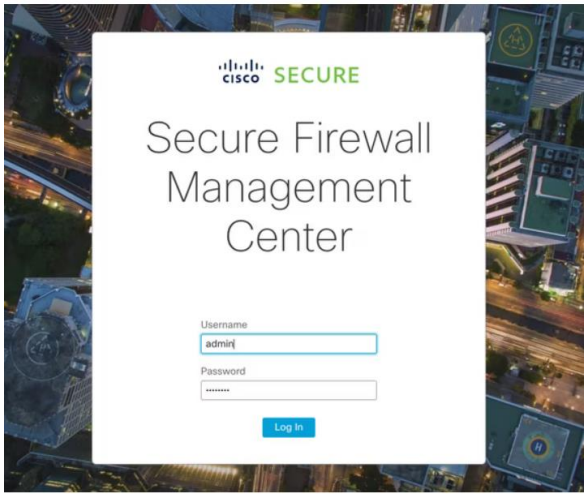

Рис.2.6. Cisco Secure Firewall Management Center

Централізований інтерфейс управління для налаштування та моніторингу пристроїв Firepower. FMC дозволяє адміністраторам розробляти політики безпеки, аналізувати події безпеки, генерувати звіти та управляти оновленнями.

Cisco Firepower Devices:

Це фізичні або віртуальні пристрої, що реалізують функції FTD. Вони можуть бути розгорнуті в різних середовищах: на периметрі мережі, в дата-центрах або в хмарах.

Threat Intelligence:

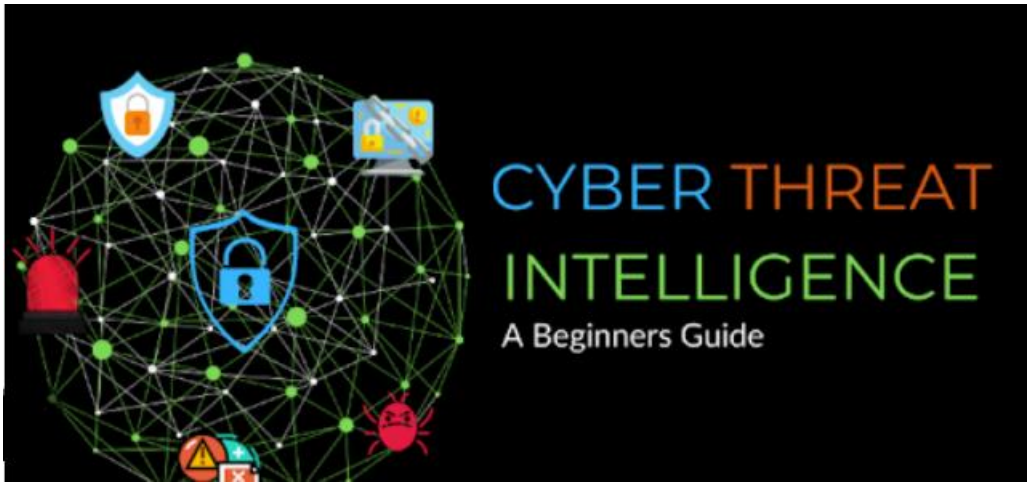

Рис.2.7. Cisco Threat Intelligence

Cisco використовує власні бази даних загроз і аналітику, щоб забезпечити актуальну інформацію про шкідливі дії та вразливості. Це дозволяє FTD швидко реагувати на нові загрози.

Integration with Other Cisco Products:

Cisco Firepower може інтегруватися з іншими продуктами Cisco, такими як Cisco Identity Services Engine (ISE) для покращення контролю доступу, а також з рішеннями для управління безпекою та аналітики.

Cloud-Based Services:

Використання хмарних сервісів для розширення функцій захисту, включаючи доступ до глобальних даних про загрози та автоматизовані реагування на інциденти.

Security Automation and Orchestration:

Cisco Firepower підтримує автоматизацію та оркестрацію процесів безпеки для швидшого реагування на загрози та спрощення управління безпекою.

Рис.2.8. Оркестрація від Cisco

Ці компоненти працюють разом, забезпечуючи багатошарову архітектуру безпеки, що дозволяє організаціям захищати свої мережі від різноманітних загроз.

2.4. Порядок функціонування рішення Cisco Firepower

Порядок функціонування рішення Cisco Firepower можна описати через кілька основних етапів:

1. Моніторинг трафіку:

Cisco Firepower розпочинає свою роботу з моніторингу всього мережевого трафіку, проходячи через міжмережевий екран (firewall). Це включає аналіз заголовків пакетів та вмісту даних.

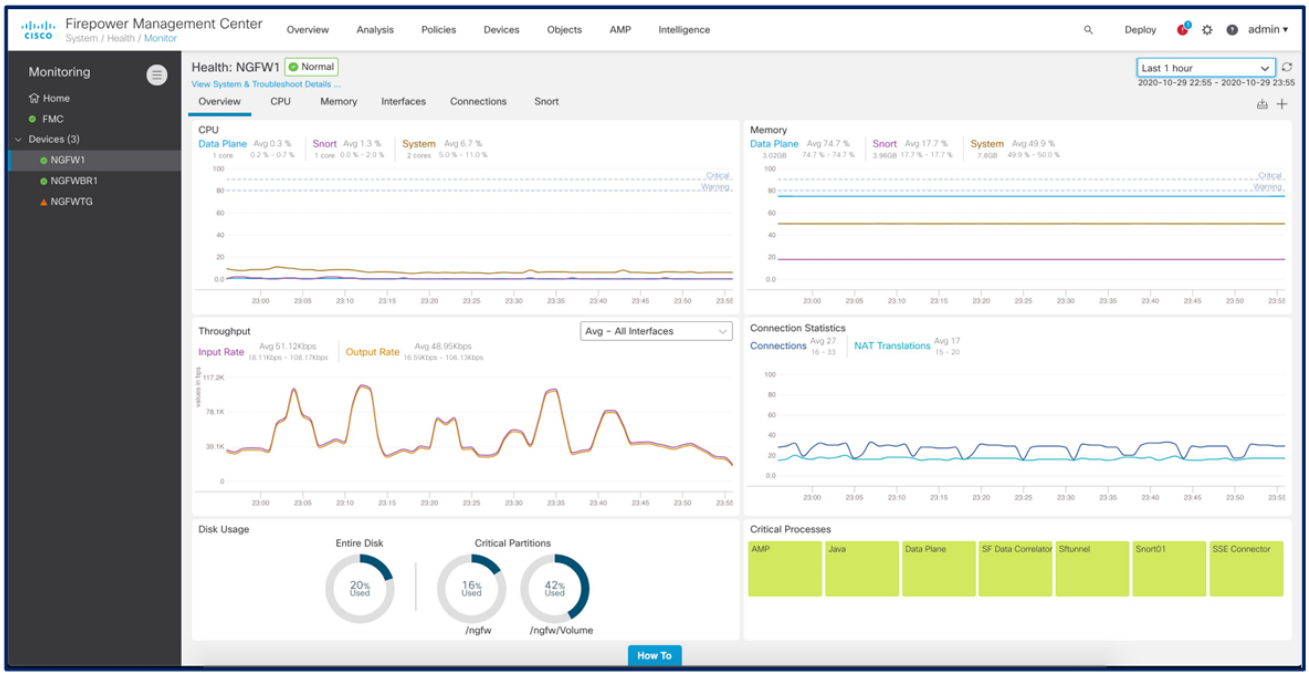

Рис.2.9. Моніторинг трафіку

2. Аналіз трафіку:

Трафік підлягає глибокому аналізу (Deep Packet Inspection), де Firepower перевіряє наявність шкідливих кодів, вразливостей та аномалій, використовуючи вбудовані механізми IDS/IPS.

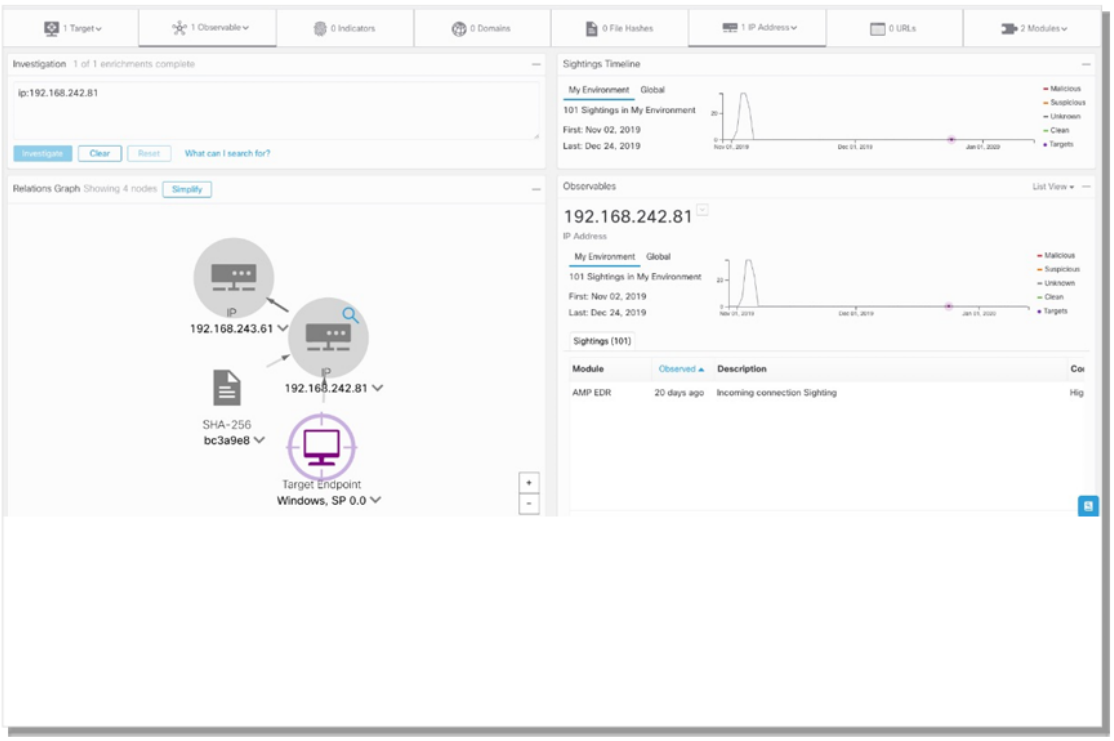

Рис.2.10. Аналіз трафіку

3. Визначення політик безпеки:

На базі політик безпеки, налаштованих в Cisco Firepower Management Center (FMC), система приймає рішення про те, які дії виконати з трафіком — дозволити, заблокувати або перевірити його.

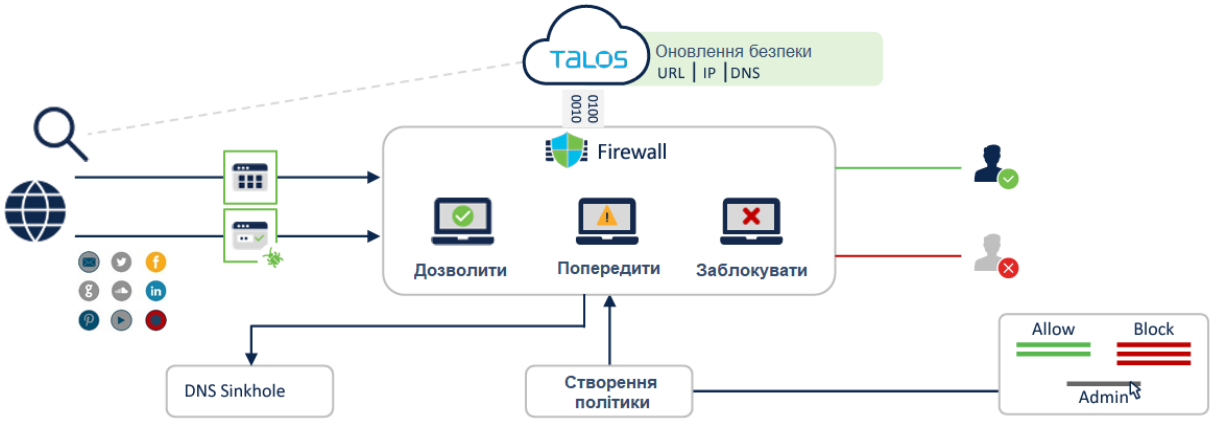

Рис.2.11. Визначення політик безпеки в Cisco

4. Інтеграція з Threat Intelligence:

Cisco Firepower отримує дані з бази даних загроз, що дозволяє йому виявляти відомі шкідливі адреси, домени та IP-адреси, підвищуючи ефективність захисту.

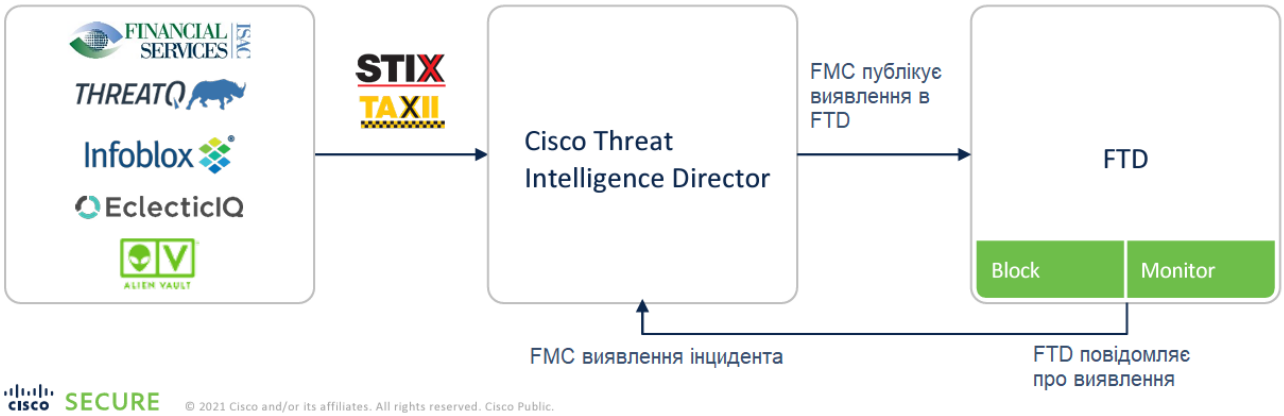

Рис.2.12. Cisco Threat Intelligence

5. Реакція на загрози:

У разі виявлення загрози Firepower може автоматично заблокувати трафік, згенерувати оповіщення, або надіслати інформацію про інцидент в FMC для

подальшого аналізу.

6. Аналіз і звітність:

FMC забезпечує централізований моніторинг подій безпеки, дозволяючи адміністраторам переглядати журнали, генерувати звіти і аналізувати тренди безпеки для виявлення потенційних загроз.

7. Адаптація та оновлення:

Система постійно адаптується до нових загроз, отримуючи оновлення від Cisco та інших джерел, що дозволяє зберігати високу ефективність захисту.

8. Автоматизація та оркестрація:

Cisco Firepower підтримує автоматизовані реагування на інциденти та інтеграцію з іншими рішеннями безпеки для поліпшення управління загрозами.

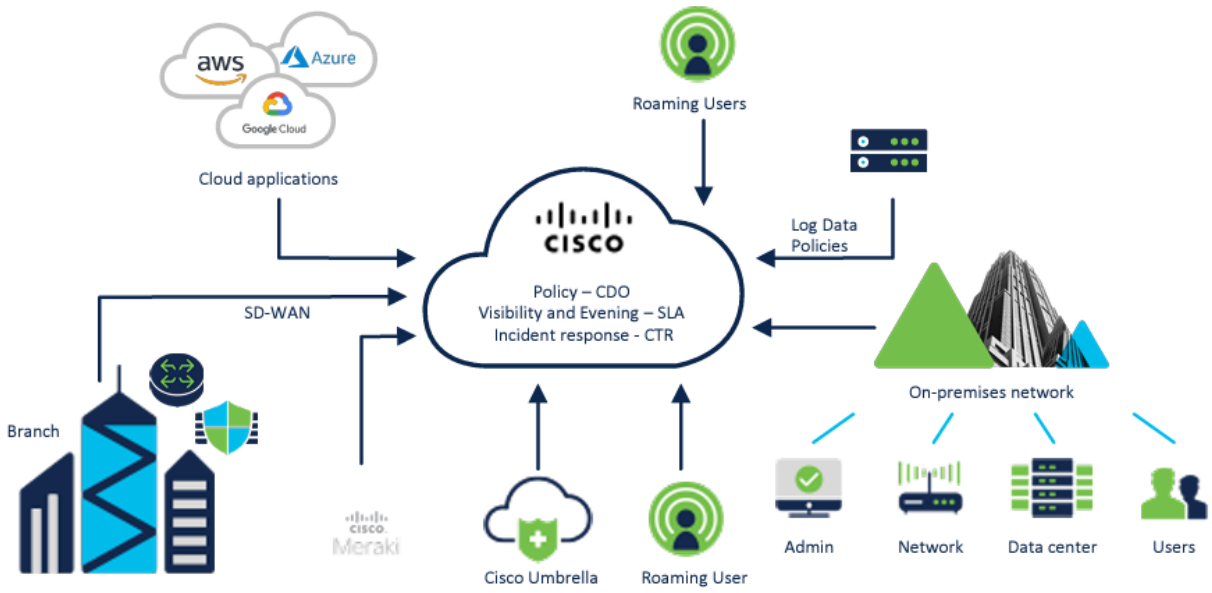

Рис.2.13. Автоматизація управління

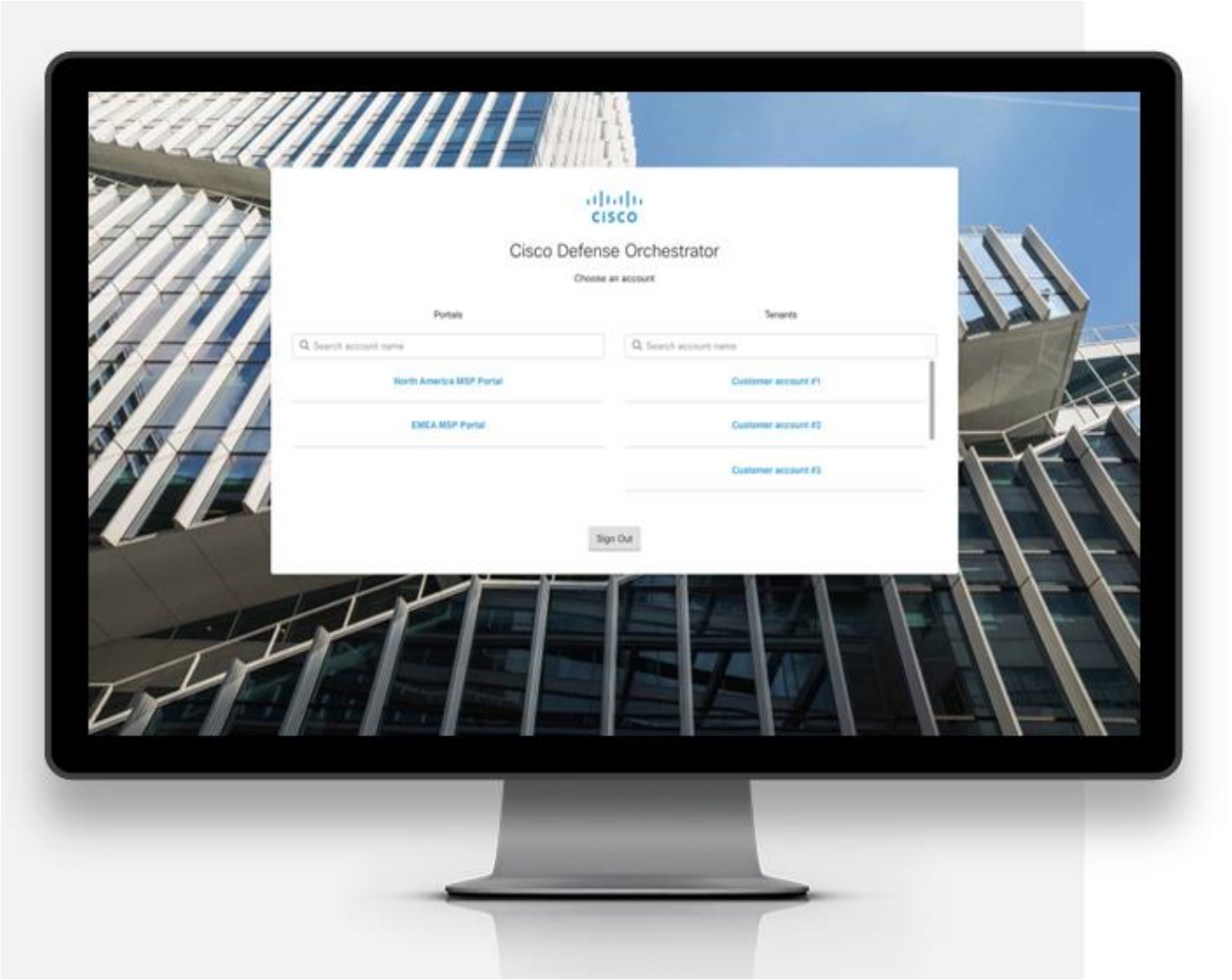

Рис.2.14. Cisco оркестрація

Цей порядок функціонування забезпечує комплексний підхід до захисту мережі, дозволяючи організаціям виявляти та нейтралізувати загрози в реальному часі.

Висновки до розділу 2

Cisco Firepower є одним з найсучасніших і потужних рішень для забезпечення мережевої безпеки. Його багатофункціональність, включаючи захист від вторгнень, аналіз поведінки трафіку, забезпечення шифрування та захист від шкідливого ПЗ, робить його ефективним інструментом для великих організацій та підприємств, що потребують високого рівня безпеки. Однак для досягнення

найкращих результатів важливо мати досвідчених фахівців та розуміти специфіку налаштування і підтримки цієї системи.

Завдяки своїм можливостям і гнучкості, Cisco Firepower є важливим елементом для комплексного забезпечення безпеки мереж, що підвищує надійність і захищеність інформаційних систем організацій у боротьбі з сучасними кіберзагрозами.

3. ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ НА БАЗІ CISCO НА ПРИКЛАДІ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

3.1. Приклад топології проектування архітектури Cisco Firepower мережі організації.

Проектування архітектури Cisco Firepower для мережі організації може включати кілька ключових компонентів, щоб забезпечити безпеку, управління та моніторинг мережевого трафіку. Для правильної розробки проекта мережі, необхідно проаналізувати усі дані, які є в наявності у замовника, задачі, які будуть виконуватись в даній мережі та потрібний рівень безпеки, щоб розуміти план дій у часі при розгортані мережі. Розглянемо на прикладі топологію мережі організації:

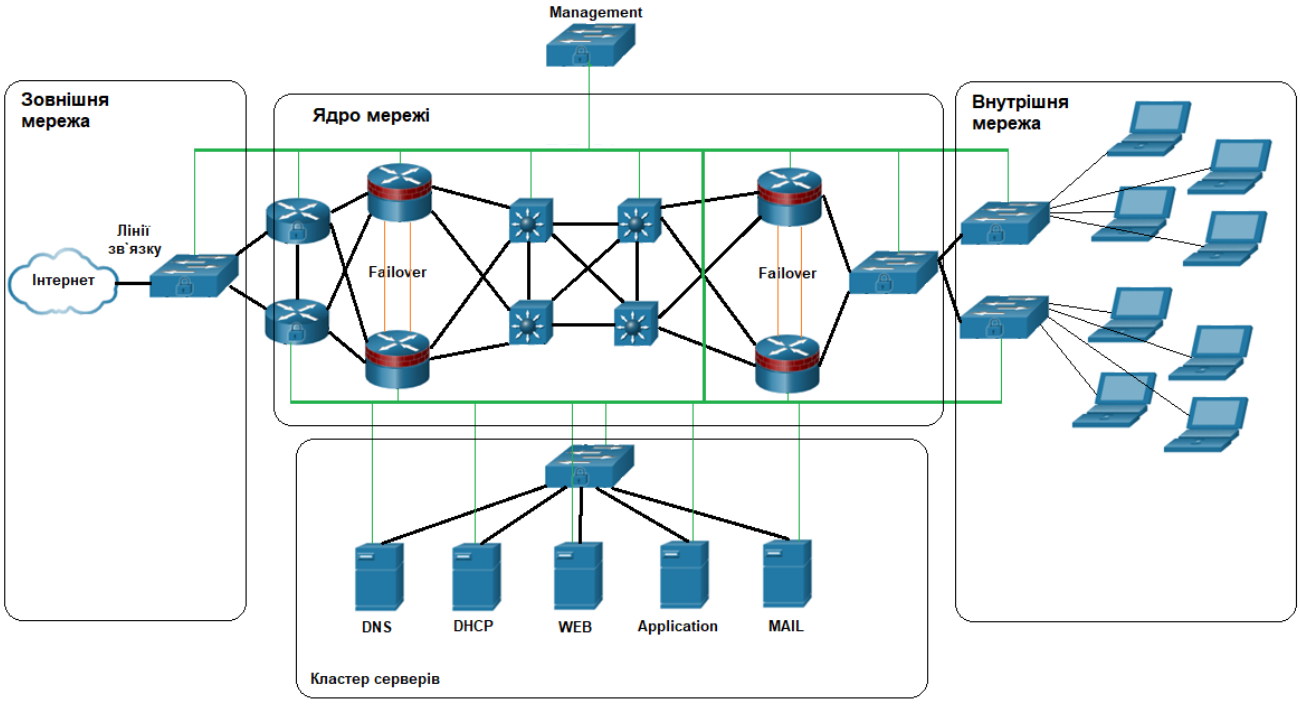

Рис.3.1. Схема корпоративної мережі організації

Як видно з топології (рис.3.1), мережа розділена на чотири частини у яких є свої задачі та призначення, розглянемо детальніше:

- **Основні три демілітаризовані зони (DMZ)**:

1) Кластер серверів, доступні з зовнішньої мережі (наприклад, WEB-сервери, MAIL сервери) так і з внутрішньою мережею (DNS та DHCP сервери, Application – сервери додатків та MAIL сервери). Основна задача даного кластера заключається в обробці інформації, її збережені та забезпечення доступу до даної інформацією усіх користувачів.

2) Внутрішня мережа – об’єднує усі кінцеві пристрої локальної мережі (робочі станції (персональні комп’ютери, ноутбуки), принтери, сканери, камери, мобільні пристрої). Розподільчі комутатори - які забезпечують зв'язок між кінцевими пристроями та маршрутизаторами. Забезпечує зв'язок з кластером серверів так і доступом до всесвітньої мережі Інтернет.

3) Зовнішня мережа – об’єднує лінії зв’язку, які заходять з мережі Інтернет. Забезпечує зв'язок користувачів, які знаходяться віддалено, до інформаційних ресурсів організації.

- **Ядро мережі** — це головна частина архітектури, яка забезпечує високу продуктивність, надійність і управління трафіком. В контексті Cisco Firepower, ядро включає:

1) Маршрутизатори – виконують маршрутизацію між різними сегментами мережі та забезпечують з'єднання з зовнішньою мережею. Включають функції маршрутизації та QoS (Quality of Service) для оптимізації трафіку.

2) Комутатори – використовуються для зв’язку між пристроями всередині локальної мережі. Підтримують VLAN для сегментації трафіку та покращення безпеки.

3) Cisco Firepower (FTD): встановлюється в ядро зі сторони зовнішньої мережі (Інтернет) так і з внутрішньої мережі, для контролю трафіку, моніторингу загроз і реалізації політик безпеки. Здійснює аналіз трафіку в реальному часі та реагує на виявлені загрози.

4) Системи управління - Firepower Management Center (FMC): забезпечує централізоване управління всіма пристроями Cisco Firepower, спрощує

налаштування політик безпеки та аналізу трафіку. Потоки трафіку розділяються на: внутрішній трафік - проходить через ядро мережі, де здійснюється контроль та моніторинг та зовнішній трафік - аналізується та контролюється через Cisco Firepower, щоб захистити внутрішні ресурси.

Основні функції ядра мережі:

- Маршрутизація: оптимізація шляхів передачі даних між сегментами.
- Безпека: захист від зовнішніх і внутрішніх загроз за допомогою Firepower.
- Моніторинг: аналіз трафіку та виявлення аномалій.
- Надійність: резервування і відновлення для забезпечення безперервної роботи мережі.

Ядро мережі є критично важливим для ефективної роботи організації, оскільки забезпечує стабільність, безпеку та швидкість передачі даних.

Ця топологія забезпечує багатошарову безпеку і дозволяє організації ефективно управляти мережевими загрозами.

Для підключення співробітників котрі знаходяться у віддалених офісах або працюють з доми використовуються топологія наведена на рис.3.2.

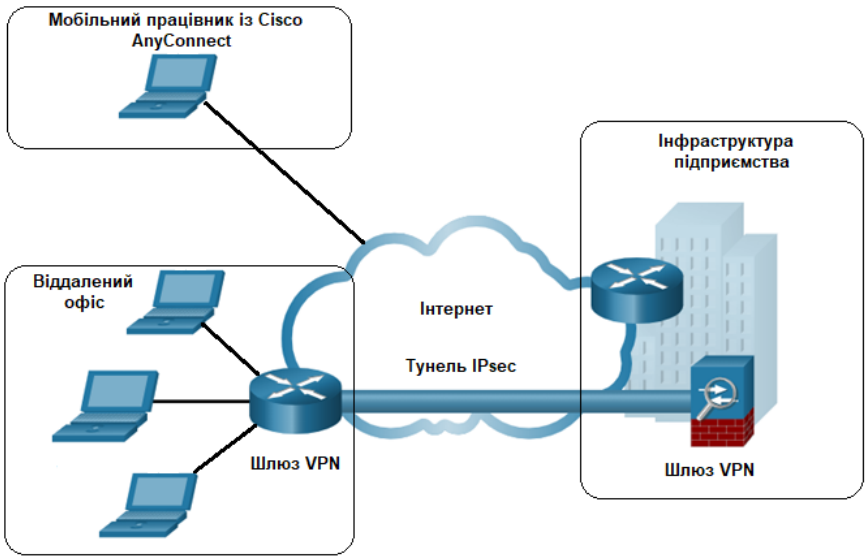

Рис.3.2. Схема підключення віддалених працівників до корпоративної мережі

Мобільні працівники підключаються за допомогою Cisco AnyConnect - це рішення для безпечного доступу до корпоративних мереж, яке забезпечує

віддаленим користувачам можливість підключення до мережі через VPN. Являється потужний інструмент для забезпечення безпечного віддаленого доступу, що підходить для сучасних вимог бізнесу до гнучкості та безпеки.

Віддалені офіси з’єднуються за допомогою шлюзу VPN, який налаштований з використанням тунелювання IPsec, включаючи шифрування та автентифікацію для доступу до ресурсів організації.

3.2. Технологія застосування рішення Cisco Firepower

Технологія застосування рішення Cisco Firepower заключається в грамотному налаштуванні обладнанні та постійному його моніторингу на вразливості.

Основне керування виконується за допомогою Cisco Secure Firewall Management Center.

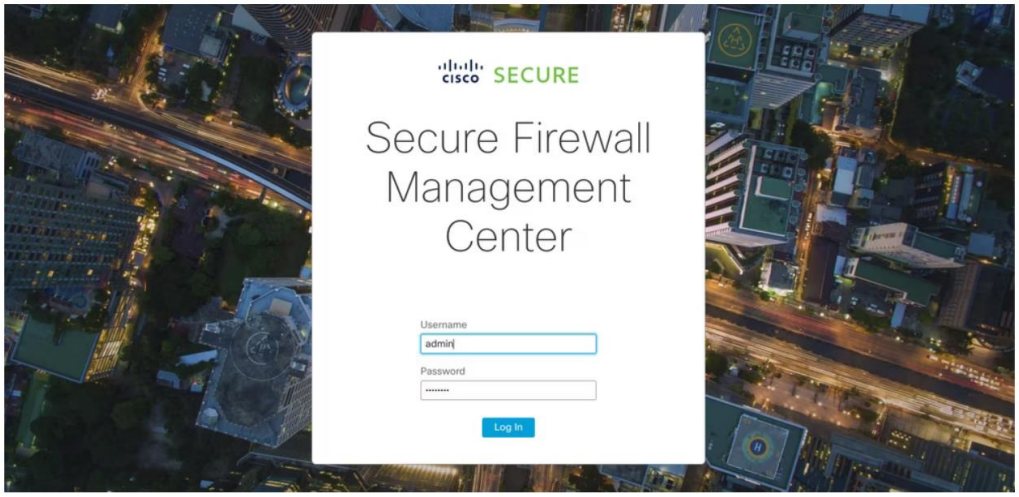

Рис.3.3. Cisco Secure Firewall Management Center

При вході в систему після авторизації ми потрапляємо на сторінку Summary Dashboard – вікно у якому показується стан мережі за останню годину, мережевий трафік та багато іншої корисної інформації. Дану сторінку можна налаштовувати під свої задачі та відображати ті звіти, які потрібно переглядати у першу чергу (рис.3.4).

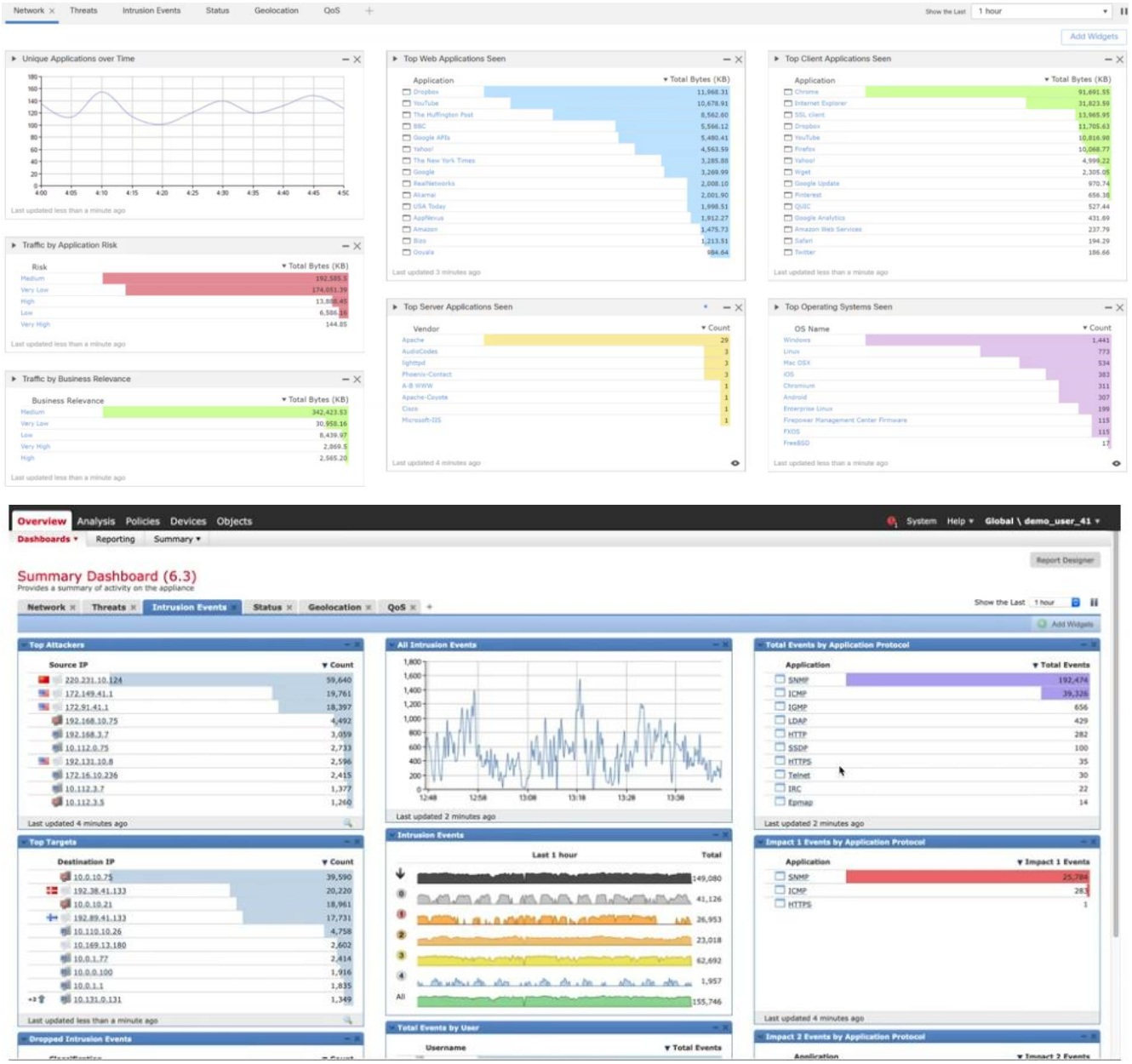

Рис.3.4. Cisco Secure Firewall Management Center – Summary Dashboard

Наступна вкладка Cisco Secure Firewall Management Center – Analysis. Аналітика по багатьом параметрам, яка постійно збирається в мережі (рис.3.5).

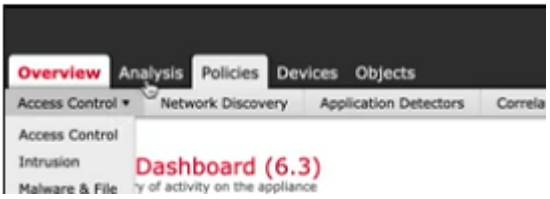

Рис.3.5. Cisco Secure Firewall Management Center – Analysis

На рисунку 3.6. зображена інформація відносно трафіку. Синім кольором лінії зображено загальний трафік в мережі та статистика по найбільш активним хостам в мережі (у вигляді стовпчастої діаграми) – відображаючи їхню IP-адресу. Червоним кольором відображається лінія подій, на котрі потрібно звернути увагу в першу чергу.

Рис.3.6. Аналітика трафіку та подій

Аналітика трафіку та подій зберігається на протязі одного року, для відображення періоду часу який потрібний для аналітики, необхідно у верхньому правому куті сторінки вибрати період, та натиснути кнопку RELOAD (перезагрузка) статистики (рис.3.7).

Рис.3.7. Період аналітики трафіку та подій

Наступним параметром аналітики є відображення Операційних систем (ОС) у вигляді кругової діаграми, які встановлені на хостах мережі. Контроль активності користувачів відповідно до правил також відображається у круговій діаграмі у вигляді дозволеного та заблокованого трафіку, статистику по найбільш активним користувачам (рис.3.8).

Рис.3.8. Аналітика по операційним системам та контролю трафіку

Важливим параметром аналітики трафіку в мережі – є інформація по протоколам, якими проходить трафік. Як видно з рисунка 3.9, найбільш важливим протоколом для вразливості залишається SNMP, тому що великий ризик потрапляння шкідливого програмного забезпечення відбувається через хости користувачів.

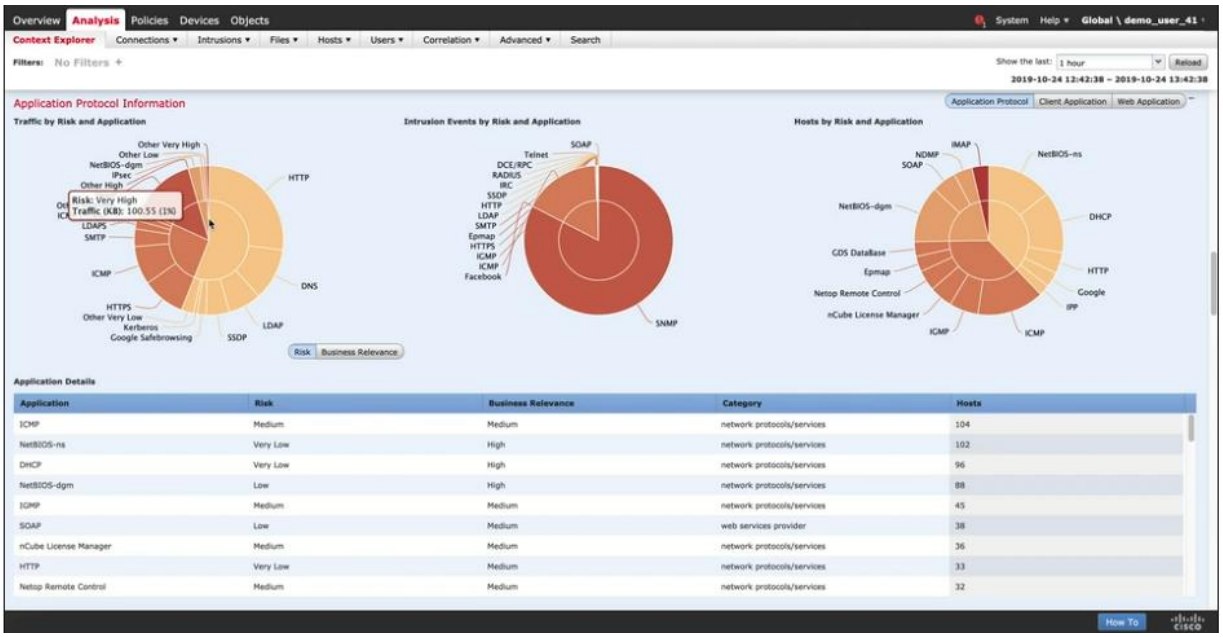

Рис.3.9. Аналітика по протоколами зв’язку

Інформація про клієнтські програми за допомогою яких користувачі отримують доступ до інформації та Веб-ресурсів мережі та які ризики можуть нести ті чи інші з’єднання (рис.3.10).

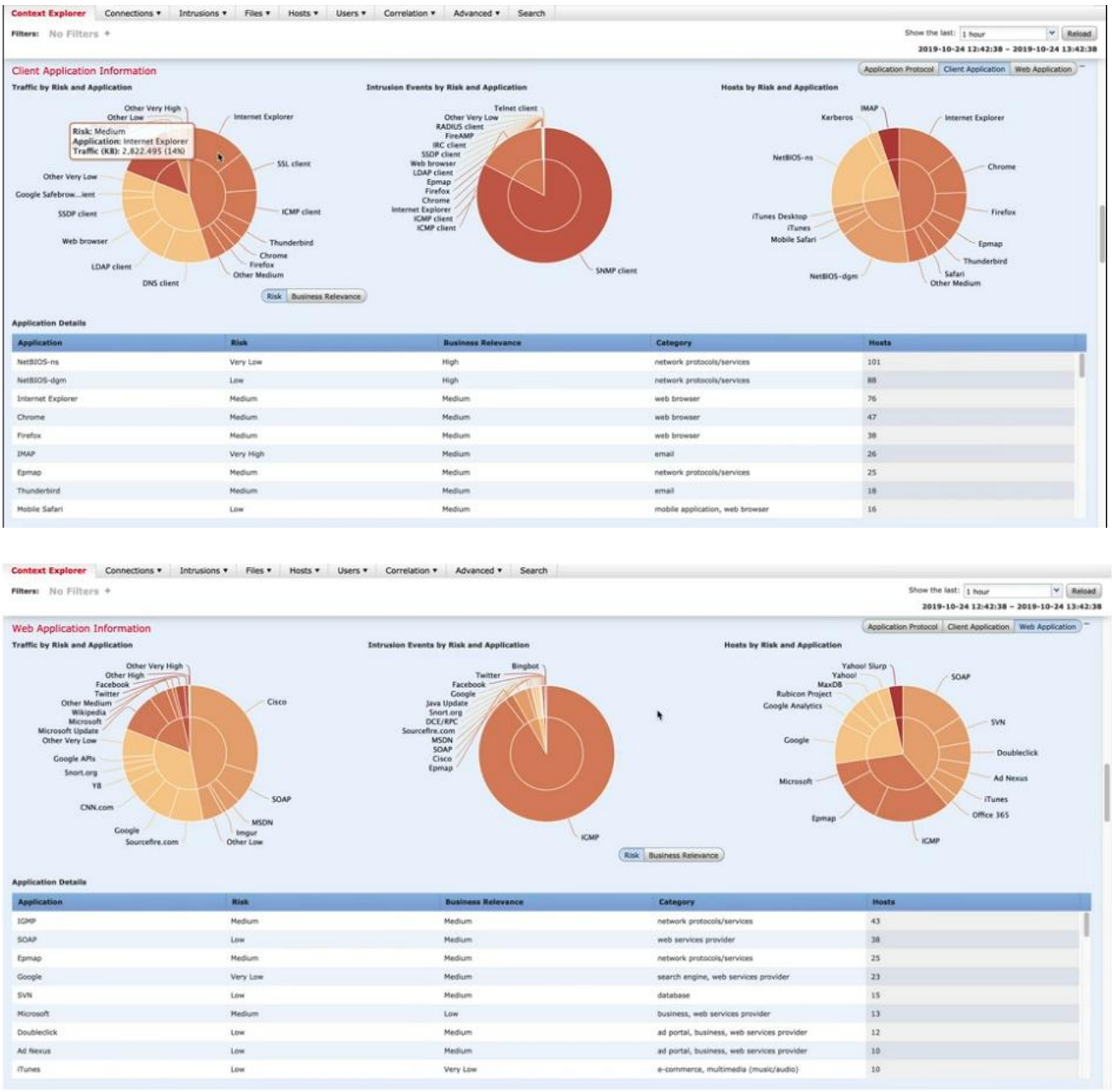

Рис.3.10. Аналітика по клієнтським програмам

На наступному рисунку (рис 3.11) відображається інформація про вторгнення в корпоративну мережу організації. Основні показники, які відображаються в даній аналітиці є головні хости атаки, хости в мережі на які йде максимальна атака та демілітаризовані зони на які припадає максимальна кількість атак.

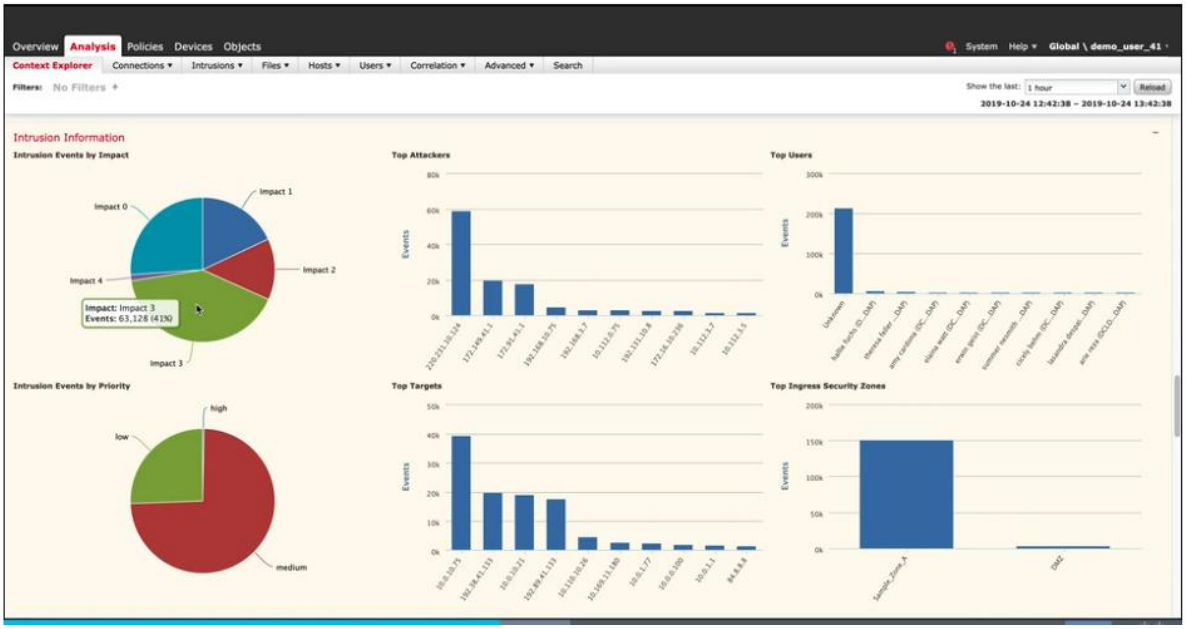

Рис.3.11. Інформація по вторгненням

На рисунку (рис 3.12) відображається інформація про країни з яких відбувається вторгнення в корпоративну мережу організації. Головними показники, які відображаються в даній аналітиці є хости (IP-адреси) атаки, за допомогою яких можна визначити точне місце розташування кіберзлочинця мережі Інтернет.

Рис.3.12. Інформація про країни з яких відбувається вторгненням

Наступна вкладка Cisco Secure Firewall Management Center – Policies. Політика безпеки – це одна з головних вкладок де відбуваються усі налаштування правил безпеки та параметри усіх ліній передачі даних (рис.3.13).

Рис.3.13. Вкладка політика безпеки

В даній вкладці відбуваються усі налаштування правил безпеки (рис.3.14-3.16). Правила можна поділити на групи, щоб легше було їх переглядати, так як на початку роботи з Фаєрволом правил мало і здається, що все добре, а переглянувши правила через кілька місяців ми помітимо, що правил буде кілька сотень, тому краще одразу при налаштуванні поміркувати і розробити основні групи куди в подальшому будуть додаватись нові правила.

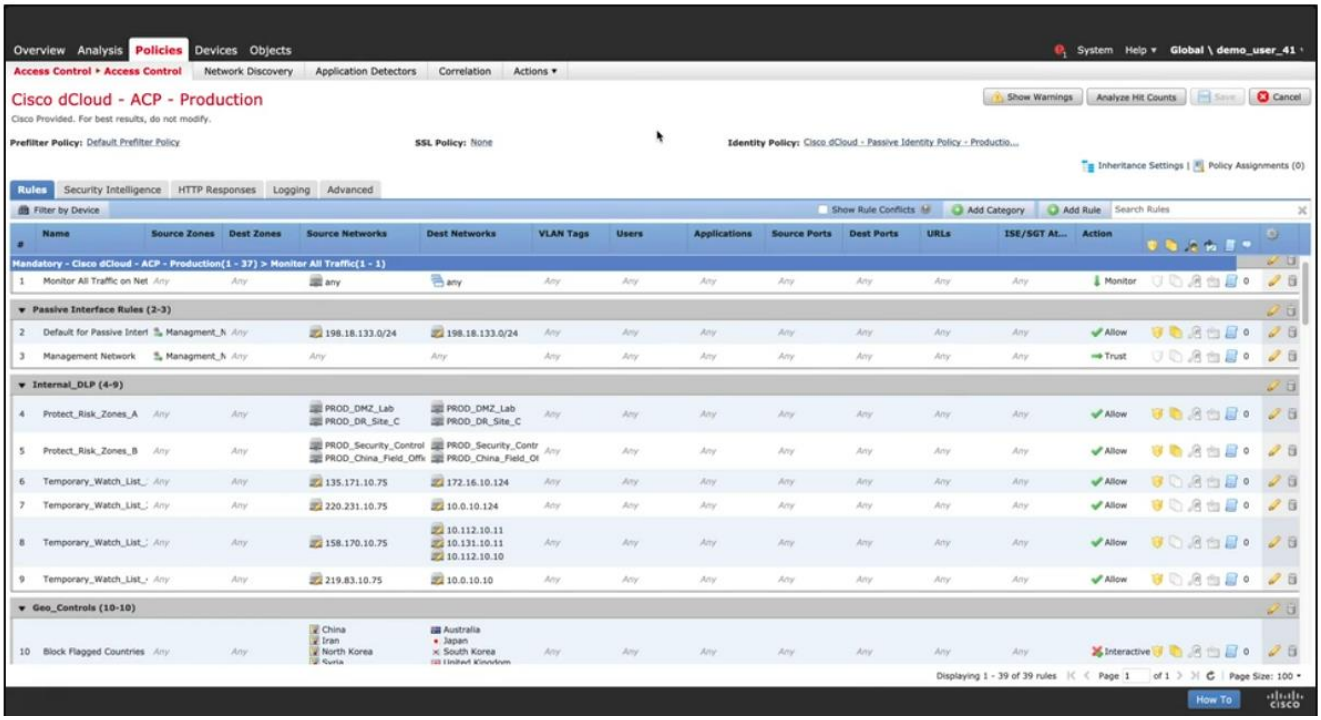

Рис.3.14. Правила політики безпеки

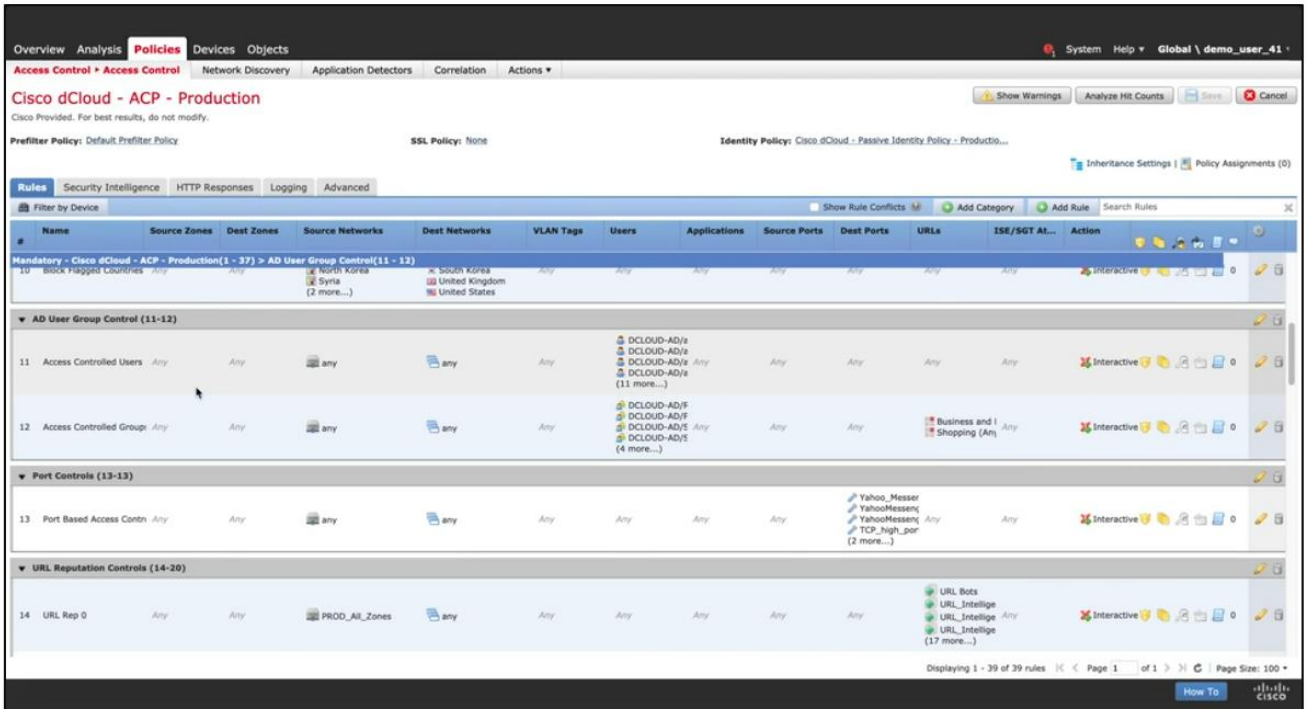

Рис.3.15. Правила політики безпеки

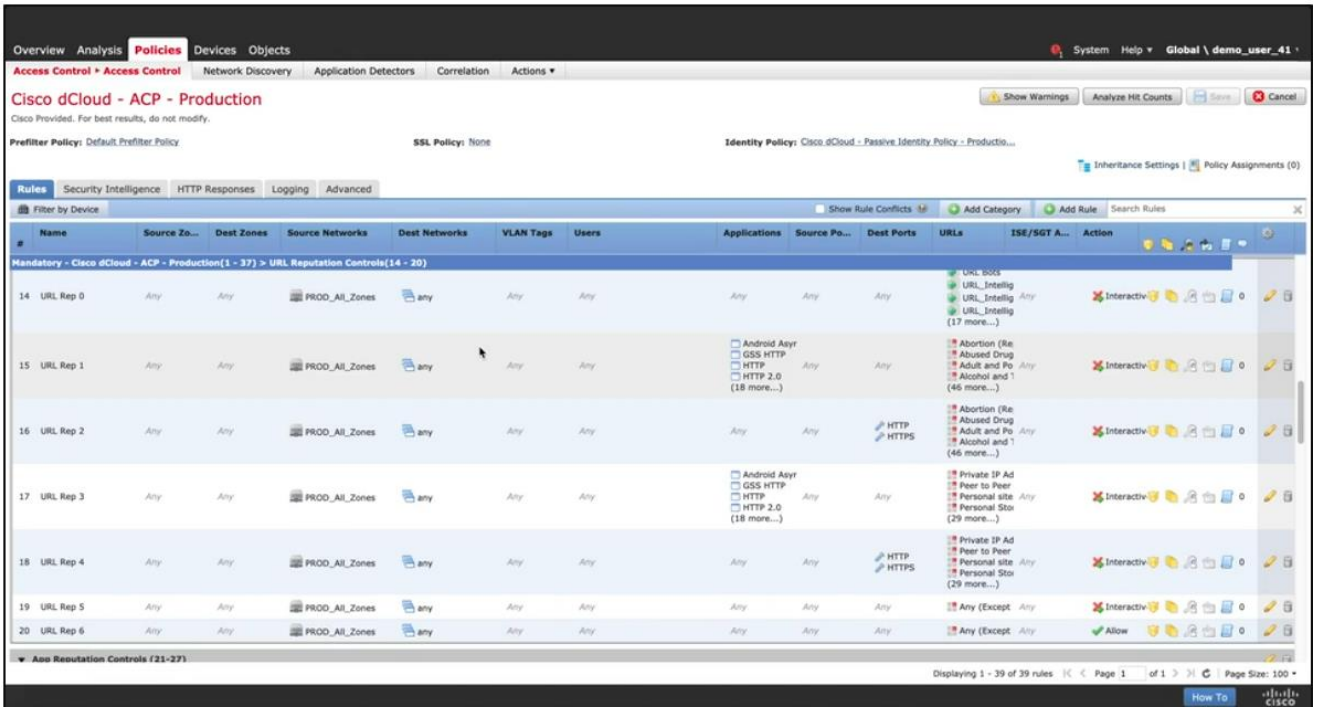

Рис.3.16. Правила політики безпеки

Наглядний приклад додавання нового правила безпеки з по крововим оглядом зображено на рисунках знизу. При натисканні кнопки “Add Rule” – додати правило, відкривається контекстне вікно для створення правила (рис.3.17).

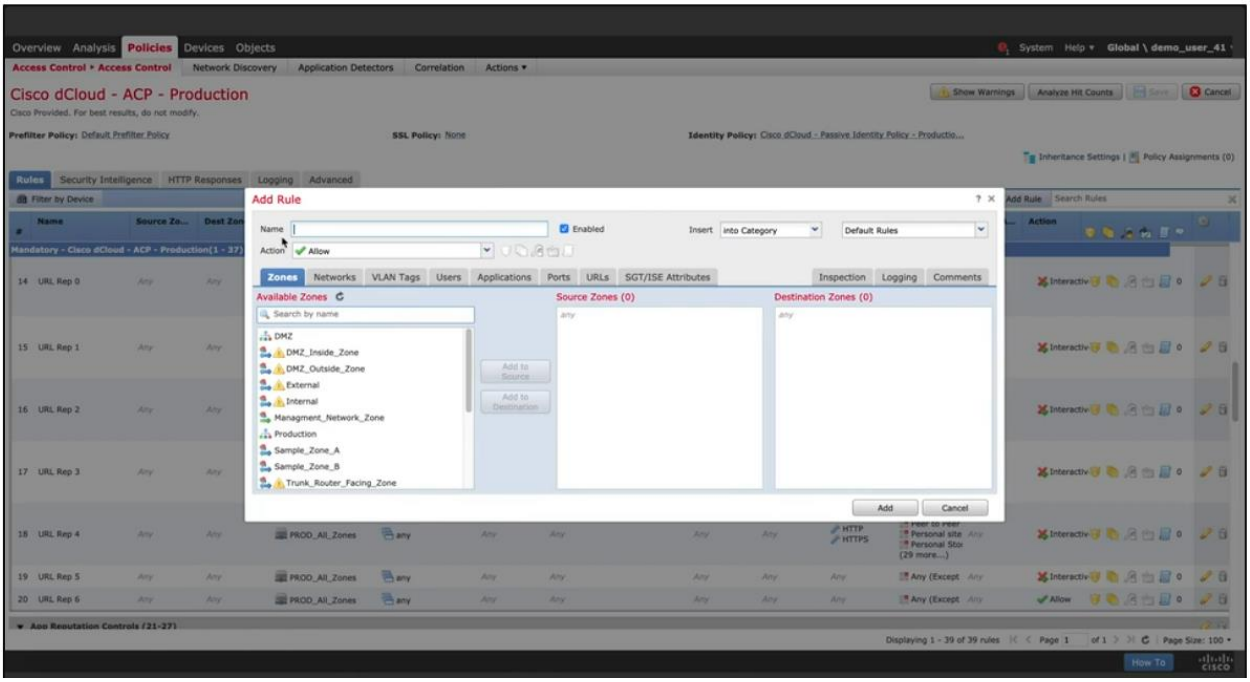

Рис.3.17. Додавання нового правила безпеки

В даному вікні (рис.3.18). створюється Ім’я (Name) нового правила, воно повинно коротко описувати призначення правила, для легшої аутентифікації їх у майбутньому. Справа від назви поле для ввімкнення правила (Enable). Також вибирається у яку групу його перемістити (Insert). В полі Дія (Action) вибираємо дію, яку виконувати над цим правило (дозволити, пропустити, моніторити, блокувати та ін.). В нижній частині відмічаємо зона джерела трафіку та кому призначено даний трафік.

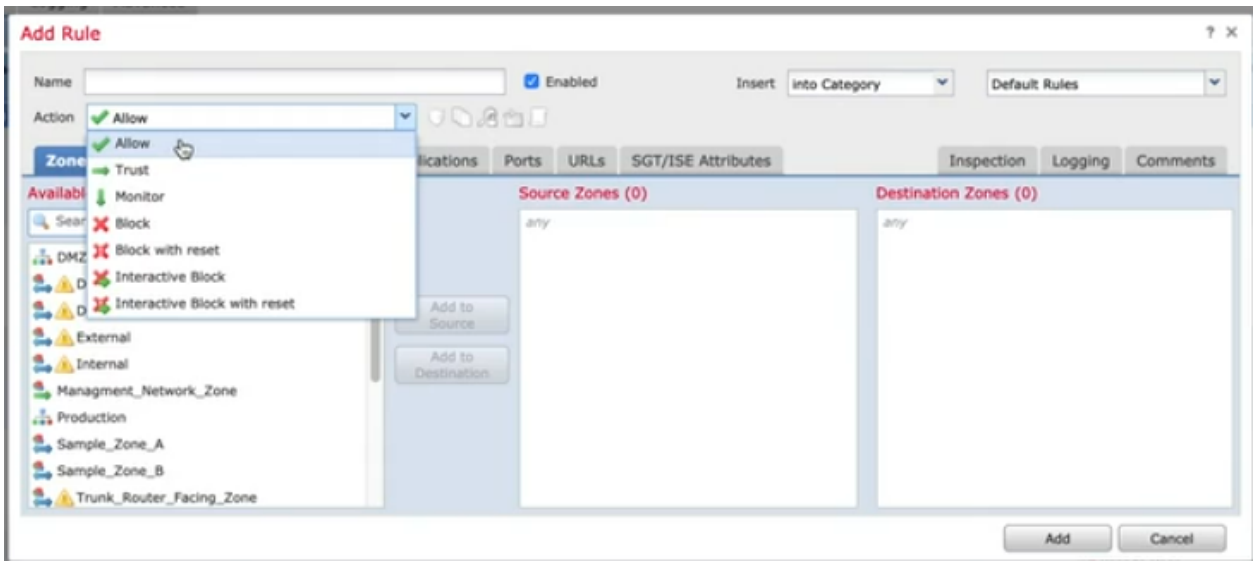

Рис.3.18. Назва правила безпеки та до яких зон воно застосовується

Наступник кроком у вкладці мережі (Networks) (рис.3.19) є можливість застосувати правило безпеки до усієї мережі, якщо це правило виконується для групи хостів. Це також дає змогу керувати безпекою пулом IP-адрес у підмережі визначивши діапазон адрес до яких застосовується дане правило. В наступній вкладці можна застосовувати правила для VLAN-мереж.

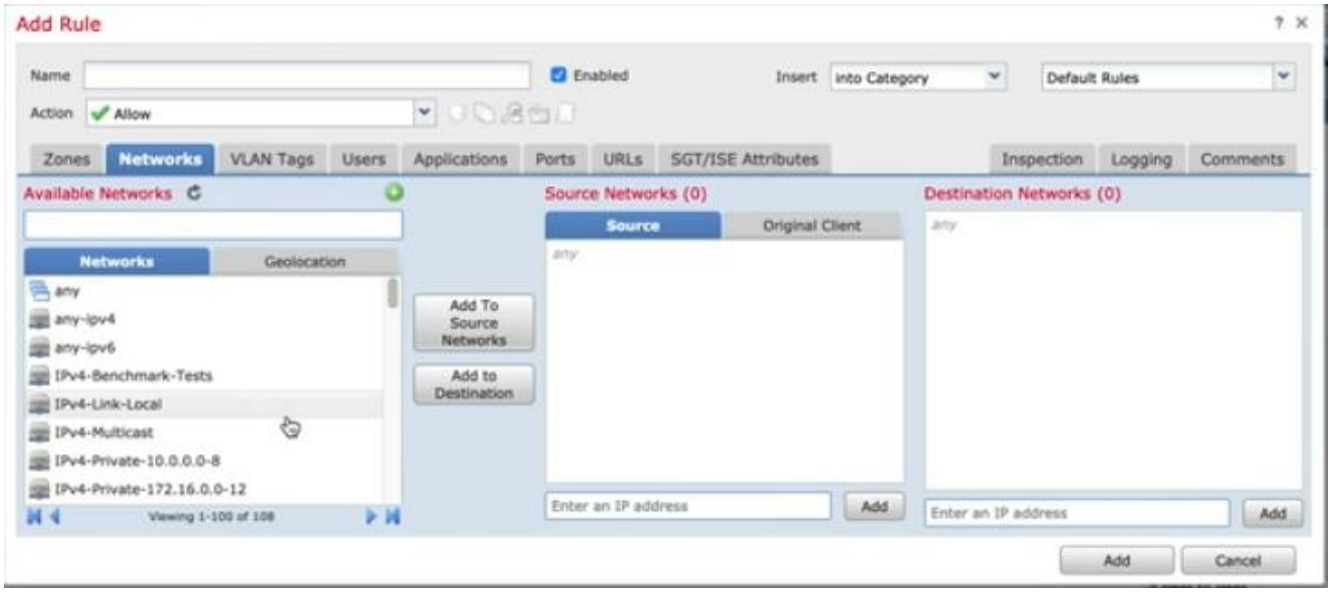

Рис.3.19. Правило безпеки, яке застосовується на цілу мережу

Наступник кроком у вкладці користувачі (Users) (рис.3.20) є можливість застосувати правило безпеки окремого до користувача або групи користувачів.

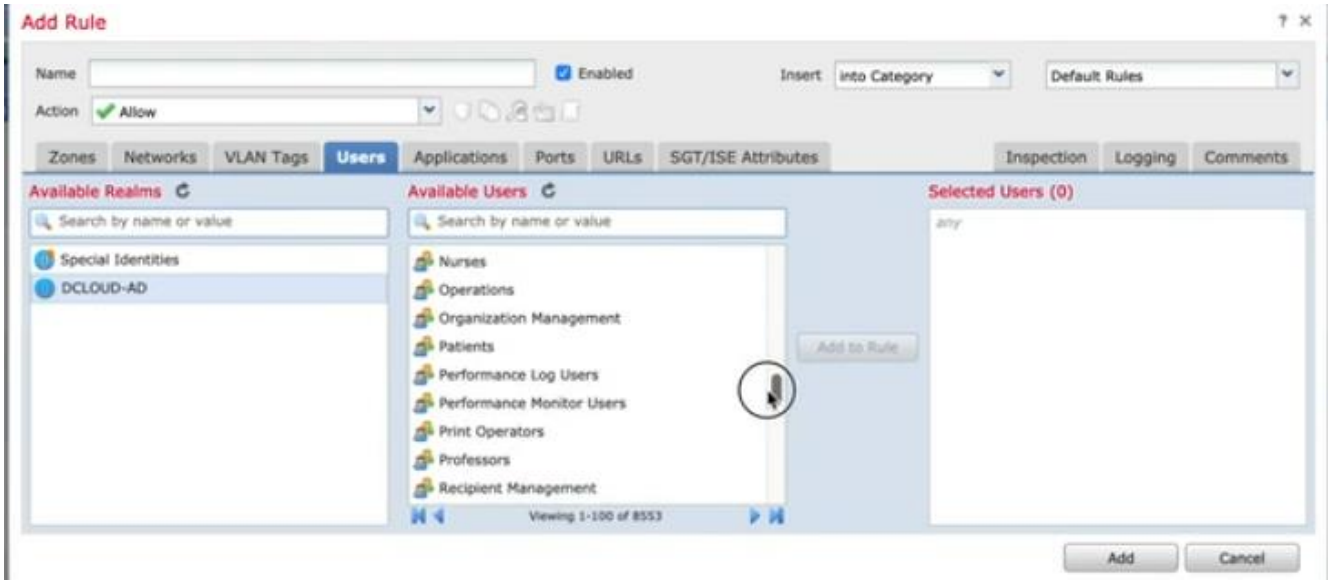

Рис.3.20. Правило безпеки, яке застосовується для користувача

Вкладка Застосунки (Applications) (рис.3.21) є можливість застосувати правило безпеки окремого для застосунків, надаючи чи забороняючи доступ до програм. Можливість контролю програм, які використовуються користувачі, забезпечуючи безпеку, якщо застосунок був скомпрометований.

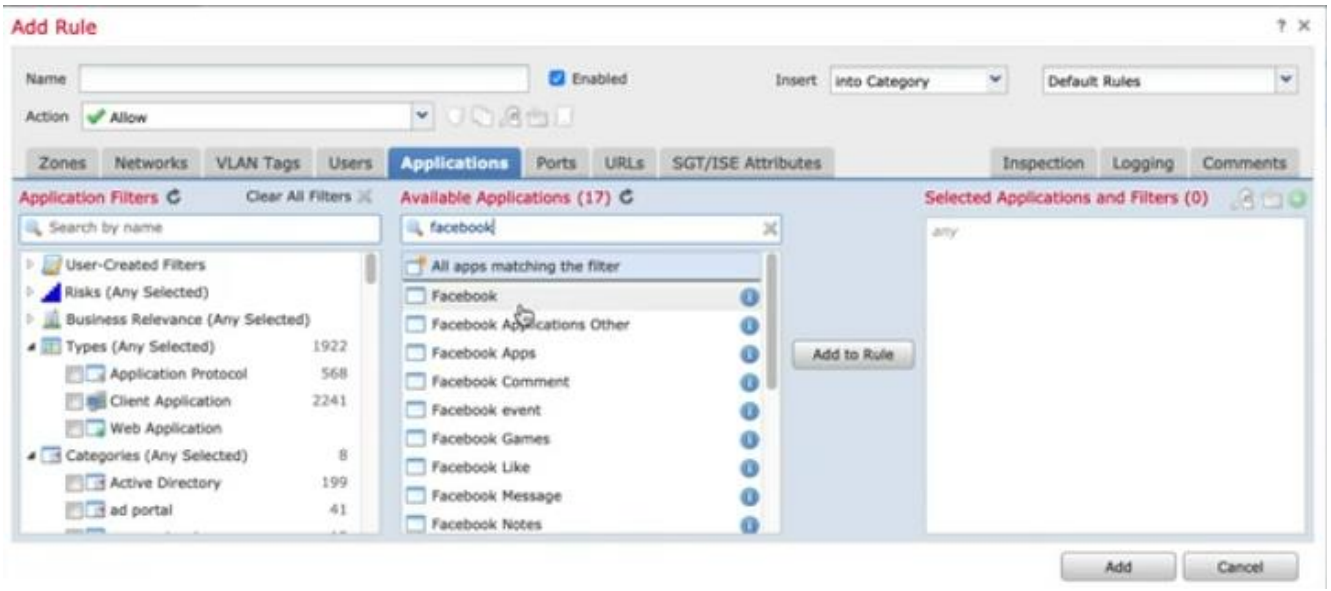

Рис.3.21. Правило безпеки, яке застосовується для застосунків

Вкладка Порти (Ports) (рис.3.22) є можливість застосувати правило безпеки окремого по портам, надаючи чи забороняючи доступ до програм по портам.

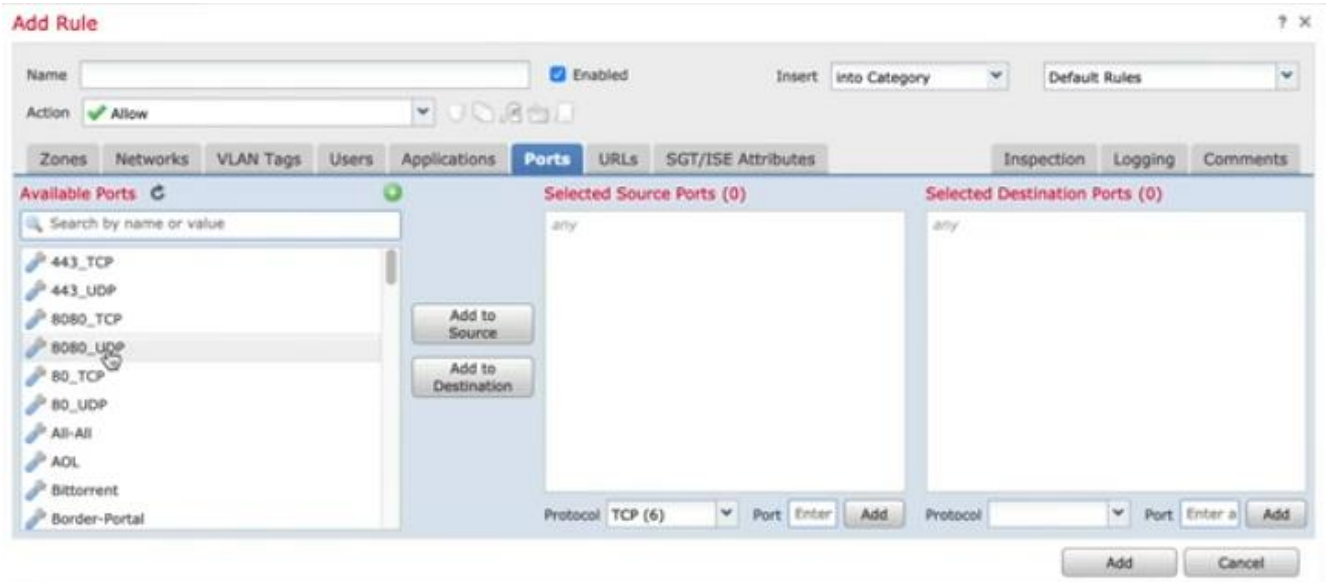

Рис.3.22. Правило безпеки, яке застосовується для портів доступу

Вкладка Посилання (URLs) (рис.3.23) є можливість застосувати правило

безпеки окремого на посилання, надаючи чи забороняючи доступ до окремих сторінок на сайті.

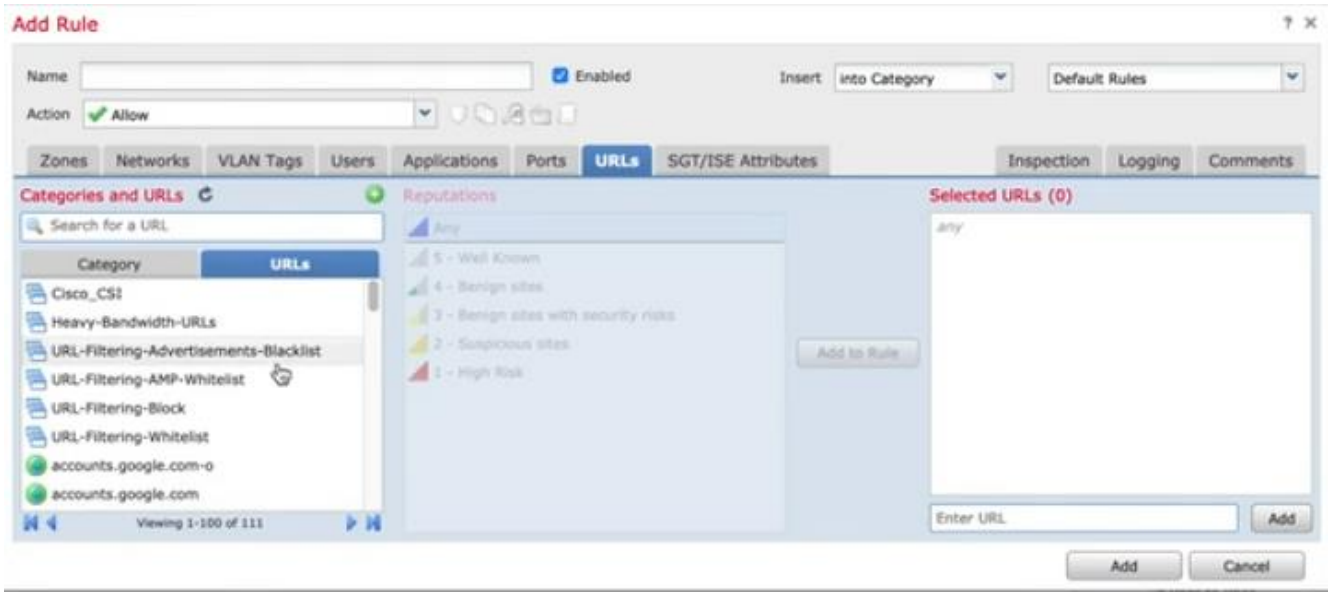

Рис.3.23. Правило безпеки, яке застосовується для посилань

Усі ці налаштування дають можливість розширення можливостей виявлення загроз і зловмисного програмного забезпечення відповідно до політик безпеки організації. Всі ці правила будуть застосовувати для захисту вашої мережі.

Наступна не менш важлива вкладка Cisco Secure Firewall Management Center – Devices. Пристрої (рис.3.24) – де ми добавляємо нові пристрої (Фаєрволи, маршрутизатори) так і сенсори для моніторингу трафіку (IDS/IPS).

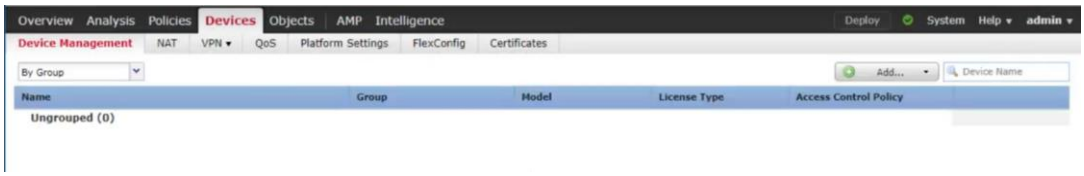

Рис.3.24. Вкладка – Пристрої

Для додавання нового пристрою до Cisco Secure Center потрібно натиснути на кнопку ADD – додати у верхній правій частині екрану. У відкритому вікні (рис. 3.25) необхідно заповнити усі необхідні поля (IP-адреса хоста – 192.168.99.142, назву – PF-PASSIVE, ключ для підключення до хоста – C1sc0123, групу до якої

відноситься даний пристрій – LAB, а також галочками відмітити які ліцензії застосовувати для обробки трафіку). Натиснувши кнопку Register – реєструємо новий пристрій у системі.

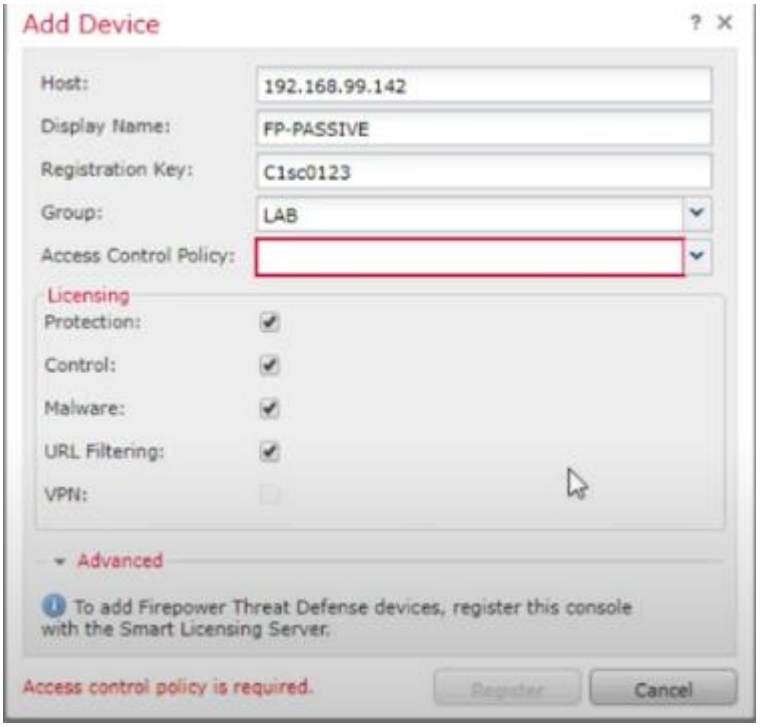

Рис.3.25. Додавання нового пристрою

Зайшовши на відповідний пристрій у консолі вводимо команду «configure manager add 192.168.99.157 C1sc0123» (рис. 3. 26) для з'єднання даного пристрою з системою, де ми вказуємо IP-адресу Cisco Secure Firewall Management Center 192.168.99.157 та ключ для підключення (C1sc0123).

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.1.0 (build 37)
Cisco NGIPSv for VMware v6.1.0.5 (build 45)

> configure manager add 192.168.99.157 C1sc0123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

Рис.3.26. З'єднання пристрою з системою

Після проведення усіх дій у вікні Пристрої з’явиться необхідний запис з усіма налаштуваннями (рис.3.27).

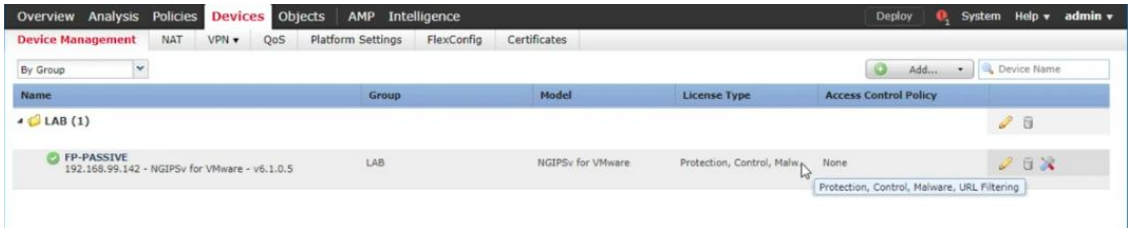

Рис.3.27. Доданий пристрій у системі

Однією з важливий задач при налаштуванні Cisco Secure Firewall Management Center – є налаштування автоматичного оновлення для усіх пристроїв якими ми керуємо (рис.3.28). У правому верхньому куті екрану натискаємо на вкладку System – Updates, натиснувши кнопку Download update система автоматично перевірить наявність оновлень для усіх пристроїв та закачає їх собі на жорсткий диск, після чого запропонує оновити наші пристрої.

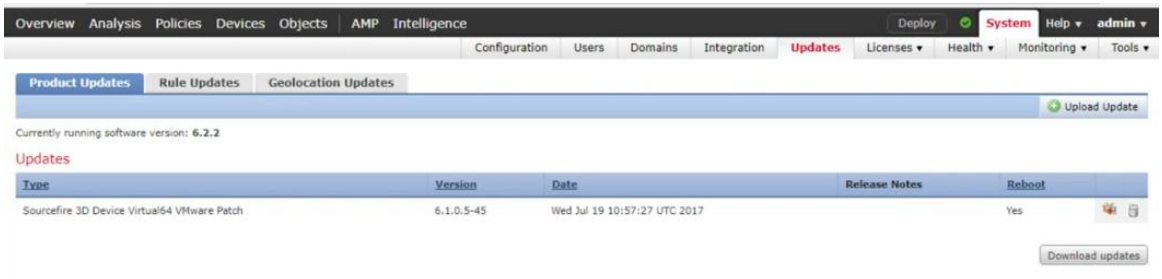

Рис.3.28. Оновлення програмного забезпечення

Другою задачею захисту мережі в організації є захист на рівні мережевого обладнання (маршрутизаторах). За допомогою налаштувань портів і правил, які до них застосовуються, можливо відкинути частину трафіку на межі маршрутизатора, завдяки таким налаштуванням зменшується навантаження на ядро мережі. Ці всі налаштування застосовуються за допомогою списків контролю доступу – ACL, для фільтрації трафіку та пом’якшення мережевих атак (рис.3.29), таким чином небажаний трафік забороняється поблизу вихідної мережі без перетину мережевої інфраструктури.

```
R1(config)# access-list ?
  <1-99>        IP standard access list
  <100-199>     IP extended access list
  <1100-1199>   Extended 48-bit MAC address access list
  <1300-1999>   IP standard access list (expanded range)
  <200-299>     Protocol type-code access list
  <2000-2699>   IP extended access list (expanded range)
  <700-799>     48-bit MAC address access list
  rate-limit    Simple rate-limit specific access list
  template      Enable IP template acls
R1(config)# access-list
```

Рис.3.29. Списки контролю доступу – ACL

ACL — це серія команд IOS, які використовуються для фільтрації пакетів на основі інформації, знайденої в заголовку пакета. За замовчуванням маршрутизатор не має налаштованих ACL. Однак, коли ACL застосовується до інтерфейсу, маршрутизатор виконує додаткове завдання оцінки всіх мережевих пакетів, коли вони проходять через інтерфейс, щоб визначити, чи можна переслати пакет.

ACL використовує послідовний список операторів дозволу або заборони, відомих як записи керування доступом (ACE).

Коли мережевий трафік проходить через інтерфейс, налаштований за допомогою ACL, маршрутизатор порівнює інформацію в пакеті з кожним ACE у послідовному порядку, щоб визначити, чи відповідає пакет одному з ACE. Цей процес називається фільтрацією пакетів.

ACL визначають набір правил, які надають додатковий контроль для пакетів, які надходять у вхідні інтерфейси, пакетів, які ретранслюються через маршрутизатор, і пакетів, які виходять із вихідних інтерфейсів маршрутизатора.

ACL можна налаштувати для застосування до вхідного та вихідного трафіку, як показано на рисунку 3.30.

Рис.3.30. Вхідний та вихідний трафіку – ACL

Також на рівні маршрутизатора можливо налаштовувати VLAN мережі. За допомогою VLAN мереж можливо розділити співробітників по підмережам з подальшим наданням доступу до мережевих ресурсів організації. Таким чином унеможливить іншим користувачам отримати доступ до заборонених мережевих ресурсів.

Наступним етапом захист мережі є захист на рівні комутатора. Пристрої рівня 2 вважаються найслабшою ланкою в інфраструктурі безпеки компанії. Атаки рівня 2 є одними з найпростіших для хакерів, але ці загрози також можна пом’якшити за допомогою деяких поширених рішень.

Усі порти (інтерфейси) комутатора мають бути захищені перед розгортанням комутатора для виробничого використання. Спосіб захисту порту залежить від його функції. Простий метод, який використовується, щоб захистити мережу від несанкціонованого доступу, полягає в тому, щоб вимкнути всі невикористовувані порти на комутаторі (рис.3.31).

```
S1(config)# interface f0/1
S1(config-if)# shutdown
S1(config-if)# end
S1#
```

Рис. 3.31. Команда вимкнення порту на комутаторі

Перейдіть до кожного невикористаного порту та виконайте команду shutdown в Cisco IOS . Якщо порт необхідно повторно активувати пізніше, його можна ввімкнути за допомогою команди no shutdown.

Щоб налаштувати діапазон портів, можна скористатися командою діапазону інтерфейсу – interface range (рис.3.32).

```
Switch(config)# interface range type module/first-number - last-number
```

Рис. 3.32. Команда вимкнення діапазону портів на комутаторі

Наприклад, щоб вимкнути порти від Fa0/8 до Fa0/24 на S1, потрібно ввести

таку команду (рис..3.33).

```
S1(config)# interface range fa0/8 - 24
S1(config-if-range)# shutdown
S1(config-if-range)#
```

Рис. 3.33. Команда вимкнення діапазону з 8 по 24 порт

Для захисту від несанкціонованого доступу до мережі за допомогою іншого пристрою застосовується захист по MAC-адресі, вручну налаштовується статична MAC-адреса за допомогою команди для кожної безпечної MAC-адреси на порту (рис.3.34):

```
Switch(config-if)# switchport port-security mac-address  mac-address
```

Рис. 3.34. Команда захисту по MAC-адресі

Безпека кінцевої точки. Історично кінцевими точками співробітників були комп'ютери, видані компанією, які знаходилися в межах чітко визначеного периметра локальної мережі. Ці хости були захищені міжмережевими екранами та пристроями IPS, які добре працювали з хостами, підключеними до локальної мережі, брандмауером та антивірусним програмним забезпеченням на пристроях користувачів.

В розглянутій мною мережі захист кінцевих пристроїм забезпечує Trellix Endpoint Security (раніше відомий як Webroot) — це рішення для захисту кінцевих пристроїв, яке забезпечує антивірусний захист, виявлення загроз і управління безпекою.

Основними характеристиками та функціями Trellix Endpoint Security є:

Основні характеристики:

Антивірусний захист: Використовує технології машинного навчання для виявлення та блокування шкідливих програм, вірусів, шкідливого програмного забезпечення та інших загроз.

Виявлення та реагування на загрози (EDR): Забезпечує можливості для

виявлення, аналізу та реагування на загрози в реальному часі, включаючи функції для розслідування інцидентів.

Повна видимість та контроль: Дозволяє адміністраторам бачити активність на всіх кінцевих пристроях, що допомагає виявляти аномалії і потенційні загрози.

Автоматизовані оновлення: Постійно оновлює бази даних загроз, щоб забезпечити актуальний захист від нових шкідливих програм.

Запобігання втраті даних (DLP): Інструменти для контролю за витоками чутливої інформації, що дозволяють організаціям захистити конфіденційні дані.

Інтеграція з іншими рішеннями безпеки: Trellix може бути інтегровано з іншими системами управління безпекою для комплексного підходу до захисту.

Хмарна архітектура: Використання хмарних технологій для поліпшення швидкості реагування та зменшення навантаження на локальні ресурси.

Користувацький інтерфейс: Простий та інтуїтивно зрозумілий інтерфейс для адміністраторів, що дозволяє легко налаштовувати політики безпеки та моніторити активність.

Переваги використання Trellix Endpoint Security: Проактивний захист: Завдяки сучасним технологіям, система здатна передбачати та запобігати атакам до їх виникнення.

Ефективність: Низький вплив на продуктивність системи при скануванні та виявленні загроз.

Гнучкість: Можливість адаптувати політики безпеки під конкретні потреби організації.

Trellix Endpoint Security є надійним рішенням для захисту кінцевих пристроїв у різних середовищах, включаючи корпоративні, гібридні та віддалені налаштування.

3.3. Рекомендації щодо застосування технології забезпечення мережевої безпеки на базі Cisco

Забезпечення мережевої безпеки на базі технологій Cisco включає

використання ряду продуктів і рішень для захисту мереж від різноманітних загроз і атак. Cisco пропонує широкий спектр інструментів для забезпечення безпеки на різних рівнях мережевої архітектури — від міжмережевих екранів і систем виявлення вторгнень до рішень для управління доступом і захисту даних. Ось кілька ключових рекомендацій щодо застосування технологій Cisco для забезпечення мережевої безпеки:

1. Міжмережеві екрани (Firewalls)

Використовуйте Cisco ASA (Adaptive Security Appliance) або новіші рішення на базі Cisco Firepower для створення перешкод між зовнішньою мережею (Інтернет) та внутрішніми ресурсами.

Конфігуруйте контроль доступу до мережі через політики для контролю над трафіком і блокування несанкціонованих з'єднань.

Використовуйте Cisco Firepower для інтегрованого підходу до захисту від загроз, включаючи вбудовані функції виявлення атак (IDS/IPS) і аналіз трафіку в реальному часі.

2. Виявлення і запобігання вторгненням (IDS/IPS)

Впровадьте рішення Cisco Firepower IPS або Cisco Secure IPS для виявлення та попередження атак за допомогою аналітики поведінки та підписів.

Встановіть системи виявлення вторгнень, які працюють на рівні застосунків та з'єднань, щоб своєчасно виявляти аномалії і зловмисний трафік.

3. VPN та шифрування

Використовуйте Cisco AnyConnect Secure Mobility Client для забезпечення безпечного віддаленого доступу до корпоративних ресурсів через VPN.

Конфігуруйте IPsec VPN або SSL VPN для захисту з'єднань між віддаленими користувачами та внутрішньою мережею.

4. Керування доступом (AAA - Authentication, Authorization, Accounting)

Налаштуйте рішення Cisco Identity Services Engine (ISE) для централізованого керування доступом до мережі, включаючи автентифікацію користувачів та пристроїв.

Використовуйте 802.1X для контролю доступу на основі політик для користувачів і пристроїв, що підключаються до мережі.

Інтегруйте Cisco ISE з іншими системами безпеки для створення єдиного захищеного середовища для користувачів і пристроїв.

5. Захист від атак на прикладному рівні

Використовуйте Cisco Web Security Appliance (WSA) для захисту від веб-загроз, таких як фішинг, зловмисні програми, та блокування небажаних веб-сайтів.

Впровадьте Cisco Email Security для захисту від спаму, фішингу та шкідливих вкладень в електронних листах.

6. Оцінка та моніторинг загроз

Використовуйте Cisco SecureX для інтеграції всіх рішень безпеки в єдину платформу для моніторингу та аналітики безпеки в реальному часі.

Використовуйте Cisco Stealthwatch для глибокого аналізу мережевого трафіку і виявлення аномалій за допомогою машинного навчання та аналізу поведінки.

Регулярно здійснюйте моніторинг подій безпеки (SIEM) за допомогою інтеграції з іншими платформами для кореляції подій.

7. Захист від атак типу DDoS

Використовуйте рішення Cisco Cloud Web Security для захисту від атак DDoS (розподілених відмов у наданні послуг) через автоматичне виявлення та блокування шкідливих трафіків.

Впровадьте Cisco Guard для захисту від мережевих атак в реальному часі, зокрема для захисту веб-сайтів та серверів від перегрузок.

8. Політики безпеки та тренування користувачів

Регулярно перевіряйте та оновлюйте політики безпеки, зокрема правила доступу, паролі та шлях до даних.

Проводьте тренування персоналу для підвищення обізнаності щодо загроз соціальної інженерії, фішингу та інших атак.

9. Захист на рівні інфраструктури

Використовуйте Cisco TrustSec для сегментації мережі та забезпечення

контролю доступу на основі політик.

Впровадьте Cisco ACI для забезпечення безпеки даних і додатків у хмарних та гібридних середовищах.

10. Аудит і відповіді на інциденти

Використовуйте Cisco SecureX для автоматизації відповідей на інциденти і впровадження політик швидкого реагування.

Налаштуйте платформи для аудитів і моніторингу в реальному часі, щоб забезпечити своєчасне виявлення та аналіз загроз.

Висновки до розділу 3

Застосування технологій Cisco для забезпечення мережевої безпеки потребує інтегрованого підходу, що включає в себе застосування різних рішень на різних рівнях мережі: від засобів контролю доступу до рішень для моніторингу та виявлення загроз. Крім того, важливо не тільки налаштувати відповідні технології, а й регулярно проводити аудит, тестування та оновлення безпекових політик і систем, щоб забезпечити надійний захист вашої мережі.

ВИСНОВКИ

Дослідження технологій забезпечення мережевої безпеки на базі Cisco є надзвичайно актуальним у сучасних умовах, коли кіберзагрози постійно еволюціонують, а вимоги до безпеки стають все більш жорсткими. Cisco надає потужні, масштабовані і інтегровані рішення, які дозволяють ефективно захищати корпоративні мережі від загроз і відповідати сучасним вимогам безпеки. Ця тема є важливою для тих, хто працює в сфері інформаційної безпеки, оскільки технології Cisco допомагають зберігати стабільність і захищеність цифрової інфраструктури в умовах зростаючих викликів.

Технології Cisco, які спрямовані на забезпечення мережевої безпеки, представляють собою потужні і комплексні рішення для захисту від різноманітних кіберзагроз, таких як атаки типу DDoS, фішинг, шкідливе програмне забезпечення, несанкціонований доступ та багато інших. Враховуючи постійне зростання складності і кількості кіберзагроз, а також інтеграцію нових технологій у сучасні інформаційні інфраструктури, Cisco пропонує потужний арсенал інструментів для ефективного захисту організаційних мереж.

Забезпечення мережевої безпеки на базі технологій Cisco є надзвичайно важливим і актуальним для організацій, які прагнуть ефективно захистити свої мережі та дані від сучасних кіберзагроз. Рішення Cisco забезпечують багаторівневий захист, інтеграцію з іншими системами та гнучкість для організацій будь-якого масштабу. Завдяки автоматизації, передовим методам виявлення загроз і зручності управління, Cisco допомагає організаціям не лише захищати свої мережі, але й залишатися конкурентоспроможними в умовах сучасного цифрового середовища. Технології Cisco є надійним інструментом для ефективного управління безпекою в корпоративних мережах, що робить їх незамінними в умовах сучасних кіберзагроз.

В роботі проведено дослідження проблеми забезпечення мережевої безпеки для працівників організації, визначено його мету та завдання.

Проведено аналіз існуючих технологій забезпечення мережевої безпеки на

базі Cisco Secure Firewall Management Center для керування кібербезпекою організації. Cisco Secure Firewall Management Center (раніше відоме як Cisco Firepower Management Center) є потужним рішенням для централізованого управління безпекою мереж, яке дозволяє адмініструвати, налаштовувати та моніторити політики безпеки на основі технологій фаєрволів Cisco. Це рішення забезпечує високий рівень захисту корпоративних мереж від загроз, надаючи гнучкі та масштабовані можливості для управління мережевою безпекою.

Cisco Secure Firewall Management Center забезпечує централізоване управління політиками безпеки для всіх фаєрволів Cisco, дозволяючи адміністраторам легко налаштовувати та впроваджувати заходи безпеки через єдину точку управління. Це дозволяє знизити складність адміністрування і спростити процеси конфігурації фаєрволів, особливо в великих і складних інфраструктурах.

Cisco Secure Firewall Management Center інтегрується з іншими рішеннями Cisco. Надає потужні можливості для виявлення загроз за допомогою інтегрованої аналітики.

Cisco Secure Firewall Management Center пропонує високу масштабованість, що дозволяє ефективно управляти великою кількістю фаєрволів у розподілених середовищах. Це важливо для великих організацій з численними філіями або віддаленими офісами. Крім того, система дозволяє адаптуватися до змін в інфраструктурі, масштабуючи можливості безпеки в залежності від потреб бізнесу.

Cisco Secure Firewall Management Center включає в себе вбудовані інструменти для розслідування та аналізу інцидентів безпеки. Адміністратори мають змогу не лише моніторити інциденти в реальному часі, але й отримувати детальну інформацію для подальшого аналізу і планування дій, що дозволяє швидше та точніше вирішувати проблеми безпеки.

Cisco Secure Firewall Management Center є потужним і гнучким рішенням для централізованого управління безпекою, яке дає змогу організаціям значно покращити захист мережі та мінімізувати ризики від сучасних загроз. Вдосконалені інструменти для управління політиками безпеки, автоматизація процесів,

інтеграція з іншими рішеннями Cisco та можливості для глибокого аналізу трафіку роблять це рішення важливим для великих організацій і підприємств, які мають складні або розподілені інфраструктури.

Проте для ефективного використання цієї технології потрібні висококваліфіковані фахівці з безпеки, оскільки налаштування та оптимізація політик безпеки вимагають глибоких знань і досвіду. Незважаючи на можливі виклики, це рішення є відмінним інструментом для забезпечення високого рівня безпеки корпоративних мереж і відповідає сучасним вимогам безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. М. В. Грайворонський, О. М. Новіков. Безпека інформаційно-комунікаційних систем— 2009.— 608 с. (дата звернення: 26.10.2024).

2. ДСТСЗІ СБ України. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»— 2003.— 16 с. (дата звернення: 26.10.2024).

3. Cisco IDS/IPS Fundamentals. 2024р. URL: https://learningnetwork.cisco.com/s/question/0D53i00000KsuxDCAR/cisco-idsips-fundamentals (дата звернення: 11.11.2024).

4. Cisco Secure Firewall Management Center: https://www.cisco.com/site/us/en/products/security/firewalls/firewall-management-center/index.html 2024 р. (дата звернення: 26.10.2024).

5. В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / – Київ., 2015р. (дата звернення: 20.10.2024).

6. В. М. Богуш, О. К. Юдін. Основи інформаційної безпеки держави – Київ., 2005р. (дата звернення: 17.11.2024).

7. Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI. Київ. 2010р. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 19.11.2024).

8. В. Бурячок, В. Богуш, Ю. Борсуковський, П. Складанний, та В. Борсуковська, "Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України", Інформаційні технології та засоби навчання, т. 67, № 5, с. 277-291, Київ., 2018. URL: http://nbuv.gov.ua/UJRN/ITZN_2018_67_5_24 (дата звернення: 20.11.2024).

9. Jackson Kathleen. A Phased Approach to Network Intrusion Detection— 1991 р. (дата звернення: 26.11.2024).

10. Syngress. Snort IDS and IPS Toolkit— 2007. (дата звернення: 12.11.2024)

11. В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. Технології забезпечення безпеки мережевої інфраструктури. Київ. 2019р. (дата звернення: 10.10.2024).

12. Сайчук В. Д. Технологія забезпечення мережевої безпеки на базі Cisco. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 25 жовтня 2024. Тези доповідей. С. 146-148. URL: https://duikt.edu.ua/uploads/p_2661_48963150.pdf (дата звернення: 14.11.2024).