ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ CISCO SAFE»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бородань В.В.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ВСТУП

Актуальність дослідження. Сьогодні такі атаки, як фішинг, програми-вимагачі та вдосконалення постійних мережевих загроз, стали звичним явищем для функціонування локальних та корпоративних мереж. Жодна компанія на сучасному ринку, а також жоден продукт, який виходить на ринок, не може бути 100% застрахованим від цих ризиків та вразливостей.

Потрібен архітектурний підхід, який буде спроможним охопити весь спектр складових компонентів — від кінцевих користувачів до мережевих пристроїв та програм. Будь-які дані в організації передаються з офісів, віддалених вузлів до центру обробки даних у хмару. При цьому суттєвим залишається твердження, що є два типи компаній: ті, які були зламані, і ті, які цього не усвідомлюють.

Коли зловмисники порушують мережу, наявність захисту від інформаційних загроз, яка допоможе адекватно реагувати, мінімізувати вплив атаки, або зовсім знешкодити, є головною для організацій та установ.

Складність у реалізації — одна з головних проблем, з якою стикаються професіонали з безпеки. Технології, які використовують організації, частіше за все представлені десятками продуктів, які не сумісні між собою, та призводять до все більшого кола проблем. В свою чергу, це збільшує площу атаки та, як результат, ускладнює захист. Зловмисники використовують цю вразливість для розробки та впровадження все нових, складних загроз. Тому галузь інформаційної безпеки потребує ресурсів та реалізацій, які були б здатні спростити цю актуальну проблему. Рішення має бути комплексним, надійним і стосуватися не лише IT продуктів, які використовуватиме компанія, а й зосередитися на загрозах для актуальних вимог бізнесу. Рішення Cisco SAFE відповідає цій потребі.

Об'єкт дослідження – процес забезпечення безпеки корпоративних мереж із використанням Cisco SAFE.

Предмет дослідження – технології та засоби забезпечення безпеки корпоративних мереж на базі рішення Cisco SAFE.

Мета роботи – розробка покрокових алгоритмів щодо побудови захищеної корпоративної мережі на базі рішення Cisco SAFE.

Наукові завдання:

- проаналізувати особливості розгортання Cisco SAFE;
- привести деталізацію складових компонентів;
- привести перелік засобів та технологій Cisco SAFE, які здатні нейтралізувати сучасні загрози та вразливості;
- розробити покрокові алгоритми щодо налаштування складових компонентів Cisco SAFE для здійснення безпечного функціонування корпоративної мережі.

Методи дослідження – теорія інформації, стандарти у сфері кібербезпеки, алгоритми оцінки загроз інформаційної безпеки підприємства, практичне тестування програмного забезпечення.

Практичне значення одержаних результатів полягає в розробці покрокових алгоритмів щодо побудови захищеної корпоративної мережі на базі рішення Cisco SAFE.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на конференції:

1) Всеукраїнська науково-технічна конференція «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., 129-130 стр.

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ФУНКЦІОНУВАННЯ МОДЕЛІ БЕЗПЕКИ CISCO SAFE

1.1 Еталонна модель безпеки Cisco SAFE

При сучасних викликах в сфері інформаційної безпеки, використання моделі безпеки Cisco SAFE може бути зведено до представлення різноманітних бізнес та IT-функцій до формату блоків. Модель включає: сучасні методи безпеки, архітектурні рішення та лабораторно перевірені проекти, які стосуються критичних питань безпеки. Вони були розгорнуті, протестовані, і задокументовані.

Cisco SAFE містить:

- деталізовані випадки, що ілюструють мережу, яку можуть атакувати зловмисники;
- можливості безпеки, зіставлені з поширеними загрозами;
- еталонні архітектурні рішення, які логічно можуть бути впровадженні в безпеку організації чи установи;
- проекти з використанням еталонних архітектурних рішень для загальних сценаріїв розгортання та рішень Cisco SAFE.

Модель безпеки Cisco SAFE здатна бути переналаштованою під вимоги компанії, які є найбільш актуальними. Використовуючи увесь наявний інструментарій Cisco SAFE, компанії можуть аналізувати загрози та ризики, та обирати саме те рішення, яке здатне захистити бізнес в режимі реального часу.

Модель Cisco SAFE являється довідником для загальних загроз, ризиків та коректного функціонування політик безпеки. Це не означає, що всі компанії однакові, та функціонують із використанням однотипних рішень та засобів. Очевидно, що проблеми, наприклад, роздрібних торговців не збігаються з потребами організацій охорони здоров’я. Однак, коли розглядаються виклики безпеки в їх повноті, починають виявлятися певні закономірності. Незалежно від галузі, методи та засоби, ймовірно, будуть використовуватися схожі.

Основні можливості та функціональні елементи керування необхідні для захисту від мережевих атак. Наприклад, доступ до мережі, використання бізнес-додатків, листування за допомогою електронної пошти або комунікація з використанням сервісів для миттєвого обміну повідомленнями, притаманно більшості сучасних компаній та організацій. Підключення до мережі Інтернет для перегляду веб-сторінок, доступу до послуг, що підключаються або ж взаємодіють із хмарою, спонукають до появи додаткових проблем в сфері інформаційної безпеки.

Модель Cisco SAFE надає вказівки щодо загальних бізнес-функцій, які вимагають можливостей безпеки, завершуючись посиланням на наскрізну безпеку. Метод Cisco SAFE налаштовує найкращі практики для окремих компаній, та гарантує, що бізнес-цілі вимірювано забезпечені відповідно до політики безпеки кожної компанії та схильності до ризику [1]. При цьому, використовуються наступні кроки:

- Визначення бізнес-цілей;
- Розбиття мережі на керовані частини (сегменти);
- Встановлення критеріїв успіху бізнесу;
- Класифікація ризиків, загроз та політик безпеки;
- Створення узагальненого рішення безпеки.

1.2 Огляд набору інструментів та засобів забезпечення безпеки Cisco SAFE

Cisco SAFE усуває розрив між діловими та технічними спірними питаннями: орієнтовані на безпеку, на вирішення бізнес-проблем та на технічні рішення. Використовуючи інноваційний підхід щодо візуалізації за допомогою блоків та піктограм, кожна лінія демонструє технічне рішення, спрямоване на розв’язання питань щодо інформаційної безпеки організації в цілому, та окремого сегменту корпоративної мережі, якщо більш узагальнено описувати.

Інструменти Cisco SAFE включають:

- Піктограми (або блоки) можливостей для представлення потоків трафіку і відповідних елементів керування інформаційною безпекою;
- Піктограми (або блоки) щодо архітектури взаємодії відповідних рівнів безпеки та обґрунтування їх функціонування;
- Піктограми (або блоки) щодо проектування. Запропоновані рішення з покроковими інструкціями щодо налаштування інфраструктури на основі Cisco SAFE, перевірені лабораторними дослідженнями (рис.1.1).

Рис.1.1. Ієрархія Cisco SAFE

Структура корпоративної мережі. Структура корпоративної мережі – це будь-що та будь-хто, на що можна націлитися при підключенні (рис.1.2).

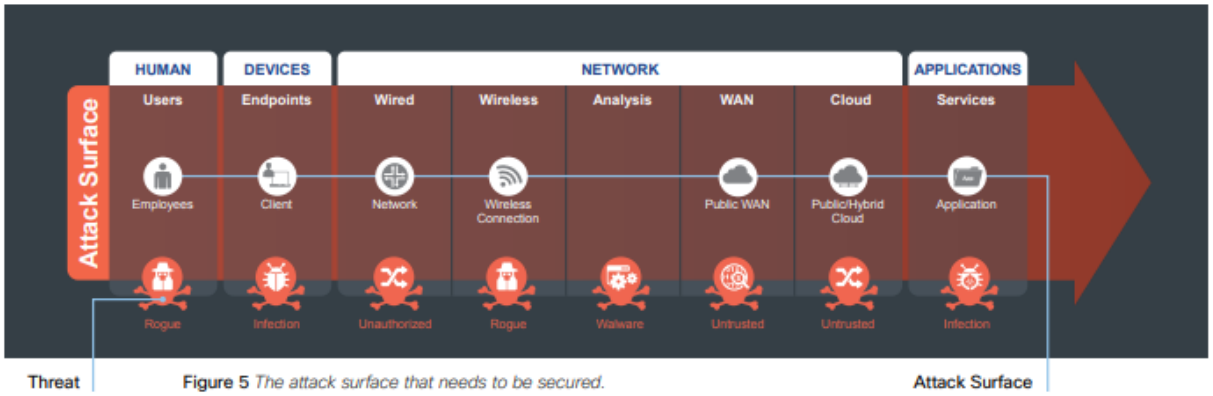

Рис.1.2. Структура корпоративної мережі

Будь-яка людина, яка використовує будь-який пристрій (принесений із собою або ж отриманий в організації), у будь-якій мережі (локальна, персональна, глобальна), має доступ до будь-якої програми (чи сервісу/додатку), та може бути атакована.

Захист структури корпоративної мережі. Структура корпоративної мережі має бути захищена відповідними засобами. Кожна ціль може бути частиною більшої загальної атаки. Визначивши інформаційні потоки компанії, які представляють структуру корпоративної мережі, можна застосувати відповідні засоби безпеки.

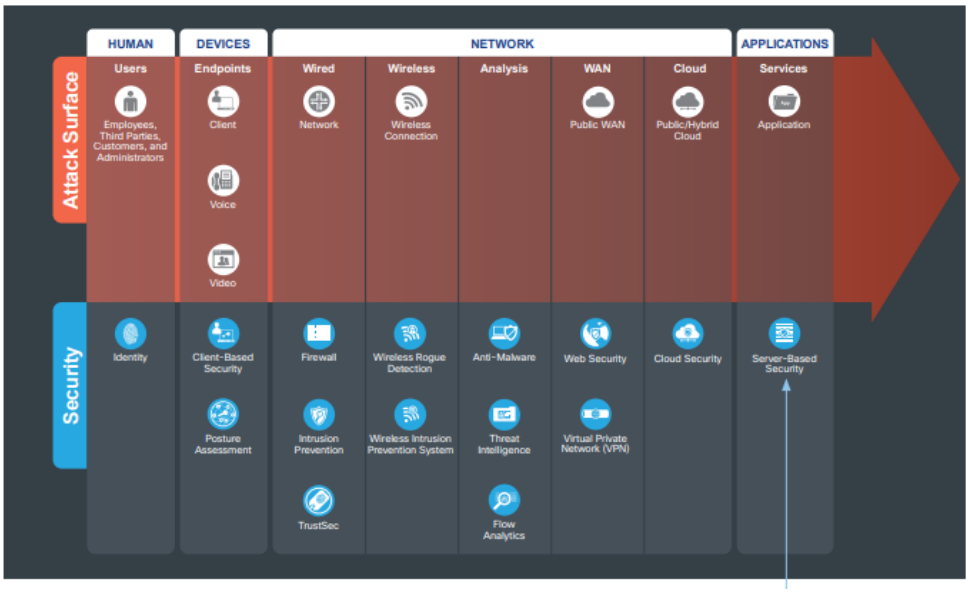

Рис.1.3. Можливості безпеки застосовуються логічно для пом’якшення загроз в структурі корпоративної мережі

Інформаційні потоки компанії (бізнес-потоки). У корпоративній мережі важливу роль віддано трьом категоріям користувачів:

— Внутрішній сегмент – це діяльність працівників організації чи підприємства, які обмінюються інформацією та даними в середині корпоративної мережі та поза нею.

— Зовнішній сегмент — це активність гостей, клієнтів, постачальників послуг або партнерів, які отримують доступ до мережі компанії.

— Клієнтський сегмент – може бути представлений різноманіттю послуг, (портали, веб-сайти) та інформацією про клієнтів.

Політика, ризики та загрози впливають на кожен з них, вимагаючи технічних рішень щодо захисту (рис.1.4).

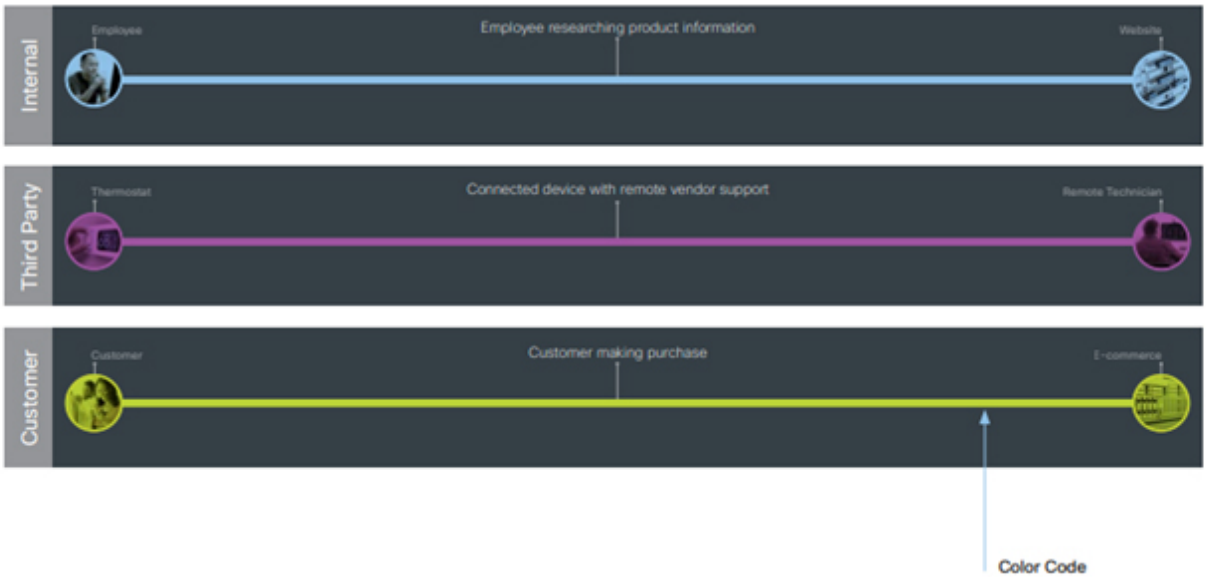

Рис.1.4. Представлення трьох категорій користувачів в Cisco SAFE

На рис.1.4 представлено три категорії користувачів в Cisco SAFE, та проілюстровано необхідність забезпечення безпеки для кожної із категорій. Ці потоки представлено у форматі структури корпоративної мережі, забезпечуючи легке врахування елементів керування [2].

Наприклад, коли співробітник підключається до мережі Інтернет, щоб провести дослідження, або клієнт робить покупку на сайті із використанням

складових електронної комерції, ці дії дають зловмисникам можливість атакувати мережу.

Завдяки документуванню та плануванню рішень безпеки всіх бізнес-потоків у корпоративній мережі компанії забезпечення необхідного рівня безпеки спрощується.

Функціональні засоби контролю. Функціональні засоби контролю – це загальні міркування щодо безпеки, які випливають із технічних аспектів бізнес-потоків (табл.1.1).

Таблиця 1.1

Характеристики загальних функціональних засобів контролю

Засіб контролю	Опис
Безпечні програми	Програми потребують достатнього контролю безпеки для захисту.
Захищені дані трафіку Схід/Захід	Дані, які безпечно переміщуються між внутрішніми та зовнішніми ресурсами.
Безпечний доступ	Співробітники, сторонні особи, клієнти та пристрої, які мають безпечний доступ до мережі.
Безпечний віддалений доступ	Безпечний віддалений доступ для співробітників і партнерів, які не належать до мережі компанії.
Безпечний зв’язок	Електронна пошта, голосовий і відеозв’язок пов’язані з потенційними загрозами поза контролем компанії та повинні бути захищені.
Захищений доступ до мережі Інтернет	Елементи керування доступом до мережі Інтернет забезпечують дотримання політик безпеки щодо використання та запобігають зараженню мережі.

На рис.1.5. представлено функціональні засоби контролю, які необхідно захистити, для трьох категорій користувачів в Cisco SAFE.

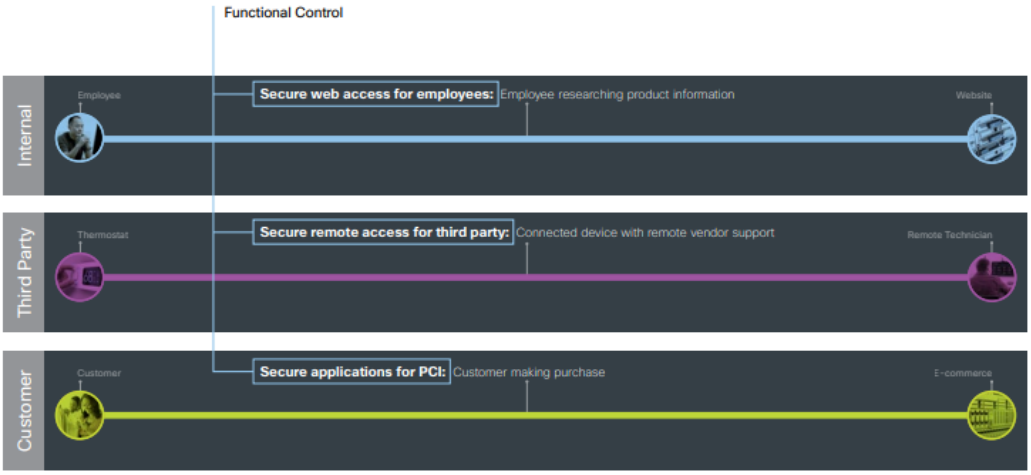

Рис.1.5. Представлення функціональних засобів контролю для трьох категорій користувачів в Cisco SAFE

1.3 Дослідження можливостей Cisco SAFE

Можливості Cisco SAFE спрощують обговорення безпеки, зосереджуючи увагу на функціях, необхідних для виконання конкретних завдань. Наприклад, Cisco реалізовує продукти Adaptive Security Appliances, Firepower appliances, маршрутизатори Meraki з міжмережевими екранами, Cisco ISR з брандмауерами. Для простоти будь-який із них ідентифікується за своїми можливостями.

Рис.1.6. Бізнес-потік із необхідними можливостями безпеки

Залежно від того, де вони застосовуються, можливості безпеки можна згрупувати в три типи: основні (базові), можливості доступні та бізнес можливості.

Основні можливості. Основні можливості працюють разом для захисту програм і трафіку. Вони використовують сегментацію, видимість і аналіз у комплексному архітектурному підході. Усі бізнес-потоки вимагають фундаментальних можливостей безпеки [3].

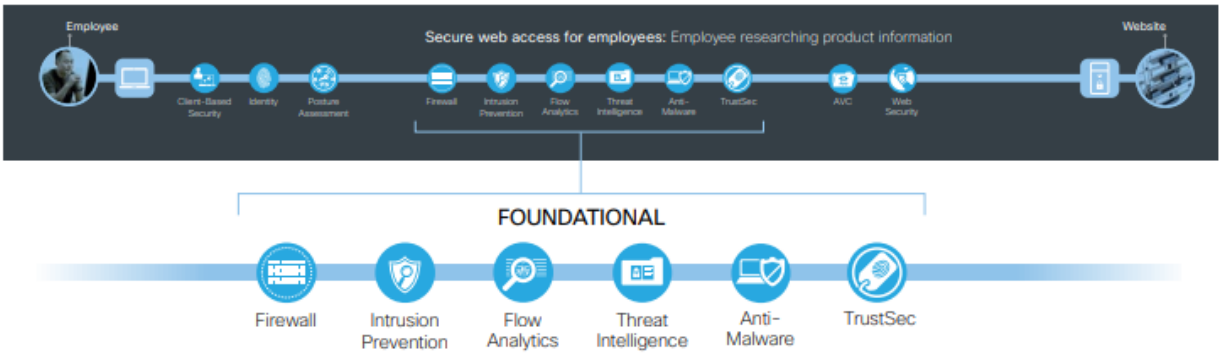

Рис.1.7. Основна група можливостей

Таблиця 1.2.

Характеристика щодо основних можливостей

Можливість безпеки	Загроза
Брандмауер: фільтрація стану та перевірка протоколів між рівнями та зовнішніми підключеннями до мережі Інтернет та постачальника послуг	Несанкціонований доступ і неправильно сформовані пакети між відділеннями та всередині них
Запобігання вторгненням: блокування атак за допомогою сигнатур і аналізу аномалій	Атаки за допомогою хробаків, вірусів або інших методів
Flow Analytics: метадані мережевого трафіку, що ідентифікують інциденти безпеки	Вилучення трафіку, телеметрії та даних від успішних атак
Розвідка загроз: контекстне знання існуючих і нових небезпек	Зловмисне програмне забезпечення нульового дня та атаки
Захист від зловмисних програм: ідентифікація, блокування та аналіз шкідливих файлів	Поширення зловмисного програмного забезпечення в мережах або між серверами та пристроями
TrustSec: сегментація на основі політик безпеки	Несанкціонований доступ і зловмисний трафік між рівнями

Можливості доступу. Можливості доступу захищають користувачів, пристрої та сервери під час доступу або надання мережевих послуг (рис.1.8).

Рис.1.8. Група можливостей доступу: безпечний доступ

Таблиця 1.3.

Характеристика щодо можливостей доступу

Можливість безпеки	Загроза
Безпека на основі клієнт/сервера	Системи захисту від шкідливих програм
Антивірус	Системи, що компрометують віруси
Cloud Security	Перенаправлення користувача на шкідливий веб-сайт
Персональний брандмауер	Неавторизований доступ і неправильні пакети, що підключаються до клієнта
Доступ на основі ідентифікації	Зловмисники отримують доступ до інформаційних ресурсів з обмеженим доступом
Перевірка відповідності кінцевої точки клієнта та авторизація	Зламані пристрої, що підключаються до інфраструктури

Бізнес-можливості. Використовуються для захисту від ризиків, пов’язаних із бізнес-практикою, якою не керують базові групи та групи доступу.

Електронна пошта, веб-доступ і віддалений доступ безпосередньо підключаються до потенційно зловмисних об’єктів (наприклад, мережі Інтернет,

фішингу та скомпрометованих вузлів), які знаходяться поза контролем компанії та потребують додаткових можливостей безпеки.

Рис.1.9. Група бізнес-можливостей: безпечний зв'язок, безпечний веб-доступ, безпечний віддалений доступ

Таблиця 1.4.

Характеристика щодо можливостей доступу

Можливість безпеки	Загроза
Веб-безпека: веб-захист, DNS та безпека IP-рівня та контроль для філій	Атаки зловмисного програмного забезпечення, вірусів і перенаправлення на шкідливі URL-адреси
Безпека електронної пошти: цілісність і захист повідомлень	Проникнення та ексфільтрація через електронну пошту
Видимість і контроль програм (AVC): глибока перевірка пакетів (DPI) потоків програм	Інструменти атаки ховаються в дозволених програмах
Брандмауер веб-додатків: розширена перевірка та моніторинг додатків	Атаки на погано розроблені програми
Захист від DDoS: захист від масштабованих форм атак	Масштабні атаки, які переповнюють служби
Віртуальна приватна мережа (VPN): зашифровані комунікаційні тунелі	Викриті служби та крадіжка даних віддалених працівників і третіх осіб

Діаграма можливостей бізнес-потоків. Поєднання можливостей із бізнес-потоками створює карту можливостей безпеки для бізнесу.

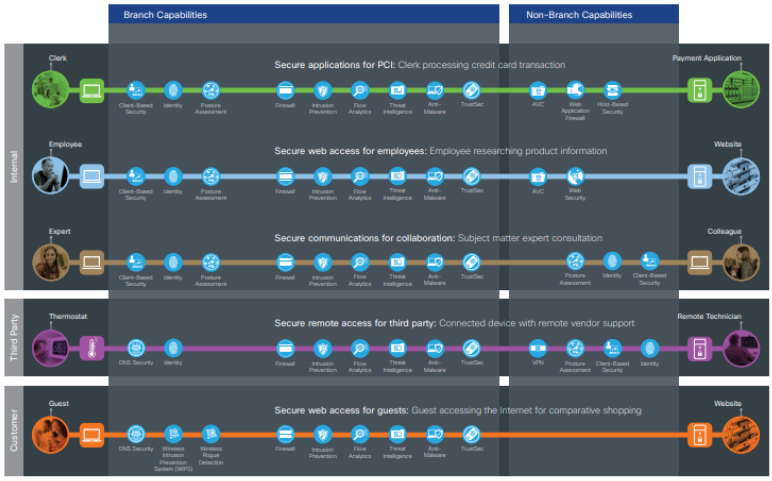

Рис.1.10. Діаграма можливостей бізнес-потоків для філії корпоративної мережі організації

Рис.1.10 використовується як основа для наступного етапу розгортання Cisco SAFE – побудови архітектури безпеки для корпоративної мережі [4].

Висновки до 1 розділу

Проаналізовано особливості розгортання Cisco SAFE, приведено деталізацію складових компонентів, та зазначено що дана модель здатна бути переналаштованою під вимоги корпоративної мережі компанії, які є найбільш актуальними.

Підкреслено, що модель Cisco SAFE являється довідником для загальних загроз, ризиків та коректного функціонування політик безпеки.

Проаналізовано три типові категорії користувачів, які взаємодіють із корпоративною мережею, та зазначено, що політики, ризики та загрози впливають на кожну з категорій, вимагаючи технічних рішень щодо захисту.

Виокремлено характеристику загальних функціональних засобів контролю в корпоративній мережі, а також приведено діаграму можливостей бізнес-потоків для організації, яка використовується як основа для наступного етапу розгортання Cisco SAFE – побудови архітектури безпеки для корпоративної мережі.

2 ДОСЛІДЖЕННЯ СКЛАДОВИХ ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ РІШЕННЯ CISCO SAFE

2.1 Дослідження розподілу корпоративної мережі на логічні області із використанням Cisco SAFE

Найбільшою проблемою у захисті компаній сьогодні є складність. Забагато атак, але також забагато захисту. І вони продовжують рости. Cisco SAFE використовує модель для організації мережі в логічні області, які називаються місцями в мережі (PIN). Кожен PIN-код має загальні бізнес-випадки використання, які вимагають загальних можливостей безпеки.

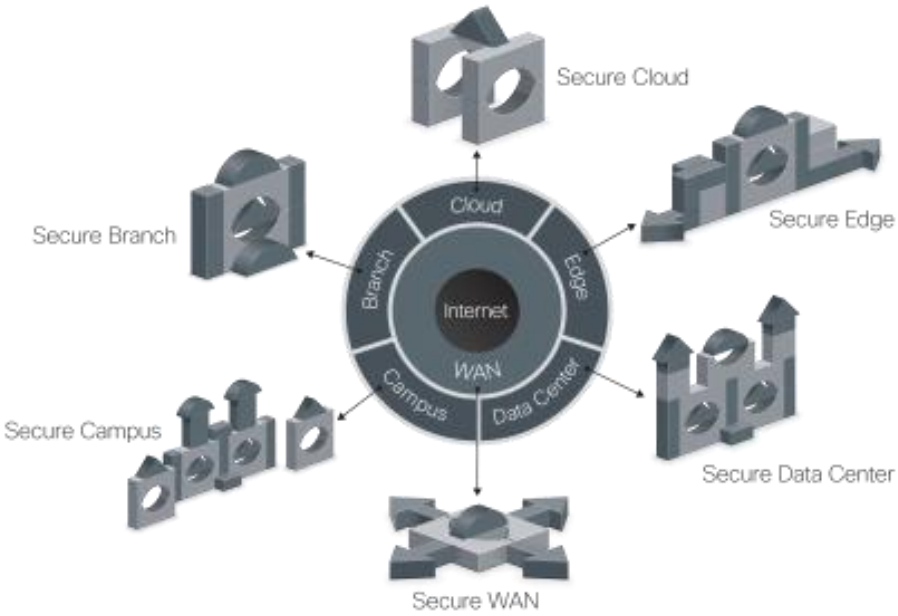

Рис.2.1. Поділ на логічні області мережі із використанням Cisco SAFE

Місця в мережі поділяються:

— Відділення;

— Кампус;

— WAN;

— Центр обробки даних;

— Edge;

— Cloud.

PIN-коди – це місця, які зазвичай зустрічаються в мережах і концептуально представляють інфраструктуру, розгорнуту в цих місцях. Це узагальнення стосується сучасної організації: автентифікація, маршрутизація, комутація, безпроводовий зв'язок, брандмауер, виявлення вторгнень тощо.

Відділення. Відділення, як правило, менш безпечні, ніж кампуси і центри обробки даних. Економіка часто диктує, що при масштабуванні до сотень відділень копіювати всі засоби контролю безпеки, які зазвичай є в місцях, є непомірним завданням. Однак це робить філії головними цілями та більш вразливими до дій зловмисників. У відповідь на це важливо включити життєво важливі можливості безпеки, одночасно забезпечуючи економічно ефективні проекти у відділенні.

На рис.2.2 показано розвиток можливостей безпеки, які використовуються для захисту від атак, поширених у філії.

Рис.2.2. Структура відділення і можливості безпеки

Найпопулярніші загрози, які притаманні саме відділенням:

— Зловмисне програмне забезпечення для кінцевих точок (зловмисне

програмне забезпечення POS);

— Експлуатація безпроводової інфраструктури (несанкціонована точка доступу, людина посередині);

— Неавторизована/зловмисна діяльність клієнта;

— Експлуатація довіри.

Кампус. Кампуси містять велику кількість користувачів із різноманітними типами пристроїв і традиційно мало внутрішніх засобів контролю безпеки. Через велику кількість зон безпеки (підмереж і VLAN) безпечна сегментація є складною. Через відсутність контролю безпеки, видимості та доступу гостей/партнерів кампуси є основними цілями для атак.

Рис.2.3. Структура кампусу і можливості безпеки

На рис.2.3. показано приклад використання можливостей безпеки для захисту від атак, поширених у кампусі.

Найпопулярніші загрози, які пом’якшуються в кампусі є:

— фішинг;

— веб-експлойти;

— неавторизований доступ до мережі;

— розповсюдження зловмисного програмного забезпечення;

— BYOD;

— зараження ботнетами.

Центри обробки даних. Центри обробки даних містять більшість інформаційних активів та інтелектуальної власності компанії. Тому і не дивно, що являють собою основну ціль для всіх цілеспрямованих атак. Як висновок, захист ЦОДів вимагає суттєвих зусиль.

Центри обробки даних містять від сотень до тисяч фізичних і віртуальних серверів, сегментованих за типом програм, класифікацією даних та іншими методами. Створення та керування належними правилами безпеки для контролю доступу до (північ/південь) і між (схід/захід) ресурсами може бути надзвичайно складним.

На рис.2.4 показано розвиток можливостей безпеки, які використовуються для захисту від атак, поширених у центрі обробки даних. Найпопулярніші загрози, які пом’якшуються в центрі обробки даних

— вилучення даних (втрата даних);

— розповсюдження зловмисного програмного забезпечення;

— неавторизований доступ до мережі (компрометація програми);

— зараження ботнетом (скрампінг), втрата даних, підвищення привілеїв, розвідка.

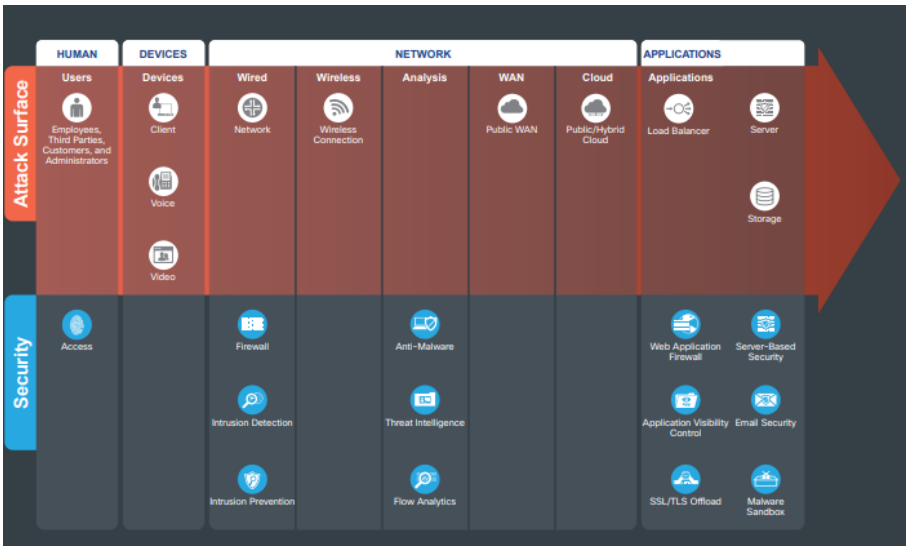

Рис.2.4. Структура ЦОД і можливості безпеки

Edge. Edge PIN-код є найбільш ризикованим, оскільки він є основною точкою входу для публічного трафіку з мережі Інтернет та основною точкою виходу для корпоративного трафіку до мережі Інтернет. Водночас це найважливіший бізнес-ресурс у сучасній економіці, що базується на глобальній мережі.

На рис.2.5 показано розвиток можливостей безпеки, які використовуються для захисту від атак, поширених в Edge.

Найпопулярніші загрози, які пом’якшуються в Edge:

— уразливості веб-сервера;

— розподілена відмова в обслуговуванні (DDoS);

— втрата даних;

— Man-in-the-Middle (MitM)[5].

Рис.2.5. Структура Edge і можливості безпеки

Cloud. Більшість ризиків безпеки в Cloud виникає через втрату контролю, брак довіри, спільний доступ і тіньові IT. Угоди про рівень обслуговування (SLA) є основним інструментом для компаній, який дозволяє керувати можливостями безпеки, вибраними в хмарних службах. Незалежні аудити сертифікації та оцінки ризиків повинні використовуватися для підвищення довіри.

На рис.2.6. показано розвиток можливостей безпеки, які використовуються для захисту від атак, поширених у Cloud.

Основні загрози, які пом’якшуються в Cloud:

— вразливості веб-сервера;

— втрата доступу;

— віруси та зловмисне програмне забезпечення;

— Man-in-the-Middle (MitM)

Рис.2.6. Структура Cloud і можливості безпеки

WAN. Глобальна мережа з’єднує всі підрозділи компанії, щоб забезпечити єдину точку контролю та доступу до всіх ресурсів. Управління політиками безпеки та якості обслуговування (QoS) для контролю зв’язку може бути надзвичайно важким і складним[6].

На рис.2.7 показано розвиток можливостей безпеки, які використовуються для захисту від атак, поширених у WAN.

Найпопулярніші загрози, які пом’якшуються в глобальній мережі:

— розповсюдження зловмисного програмного забезпечення;

— неавторизований доступ до мережі;

— перехоплення глобальної мережі та атаки MitM.

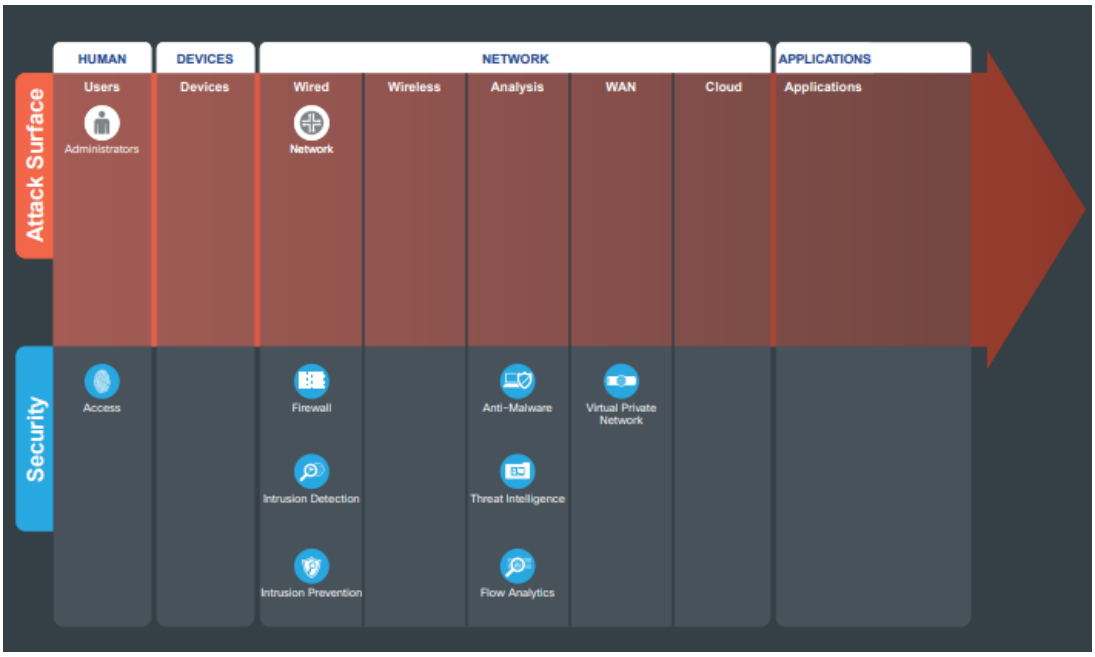

Рис.2.7. Структура WAN і можливості безпеки

2.2 Дослідження особливостей організації захищенних доменів

Захищені домени. Захищені домени представляють робочу сторону ключа. Операційна безпека поділяється за функціями та людьми в організації, які відповідають за них [7]. Кожен домен має певний клас можливостей безпеки та операційних аспектів, які необхідно враховувати. (рис.2.8.)

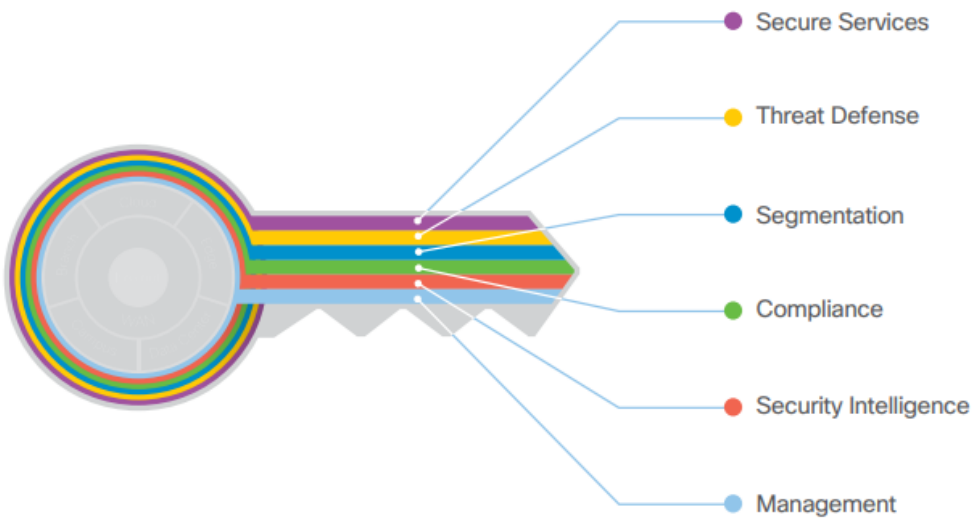

Рис.2.8. Захищені домени моделі Cisco SAFE

Управління. Управління пристроями та системами за допомогою централізованих служб має вирішальне значення для послідовного розгортання політики, керування змінами робочого процесу та здатності підтримувати системи в установленому порядку. Керівництво координує політики, об’єкти та оповіщення.

Рис.2.9. показує розвиток можливостей безпеки, які використовуються для операцій управління.

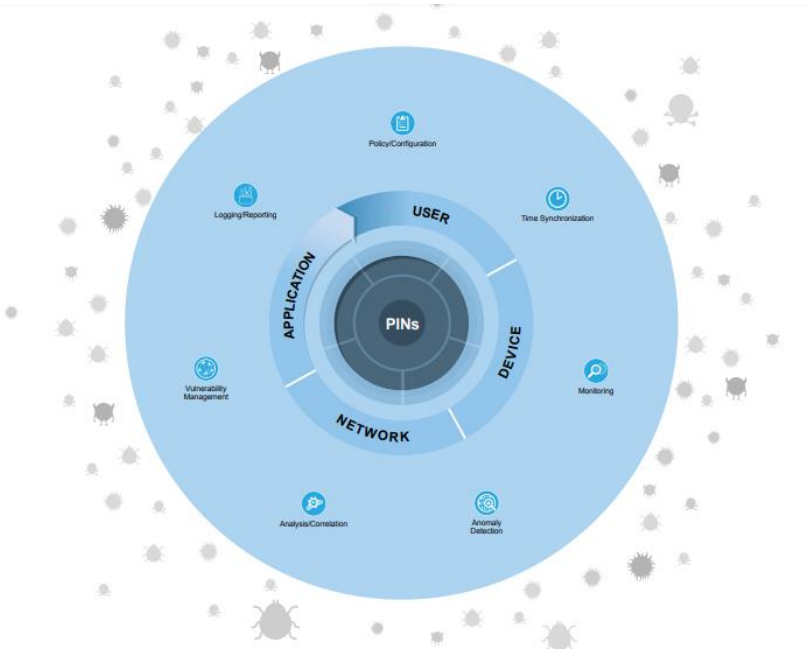

Рис.2.9. Можливості домену керування

Розвідка безпеки. Security Intelligence забезпечує глобальне виявлення та агрегування нових зловмисних програм і загроз. Це дає змогу інфраструктурі динамічно впроваджувати політику, оскільки репутація доповнюється контекстом нових загроз, забезпечуючи точний і своєчасний захист безпеки.

На рис.2.10 показано розвиток можливостей безпеки, які використовуються для операцій служби безпеки.

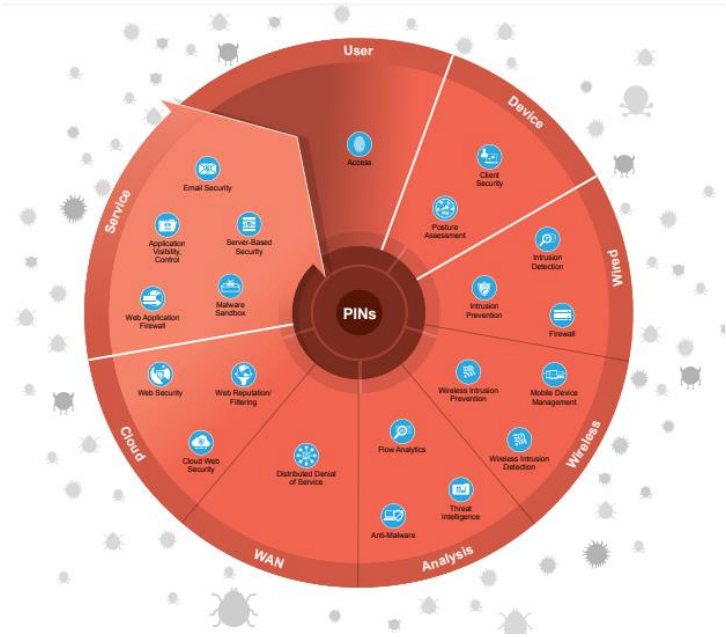

Рис.2.10. Можливості аналізу безпеки

Відповідність. Відповідність стосується внутрішньої та зовнішньої політики. Показує, як багато елементів керування можна задовольнити одним рішенням. Приклади зовнішньої відповідності включають PCI, HIPAA та Sarbanes-Oxley (SOX). На рис.2.11. показано розвиток можливостей безпеки, які використовуються для відповідності.

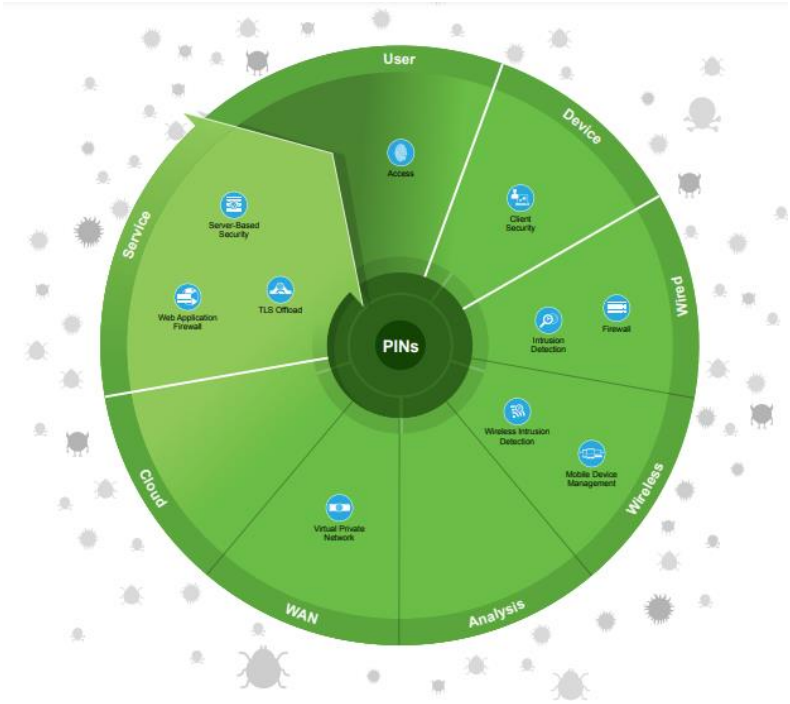

Рис.2.11. Можливості відповідності

Сегментація. Сегментація встановлює межі для даних і користувачів. Традиційна сегментація вручну використовує комбінацію мережевої адресації, мереж VLAN і брандмауерів для застосування політики. Розширена сегментація використовує інфраструктуру з підтримкою ідентифікаційних даних для застосування автоматизованих і масштабованих політик.

На рис.2.12. показано розвиток можливостей безпеки, які використовуються для сегментації.

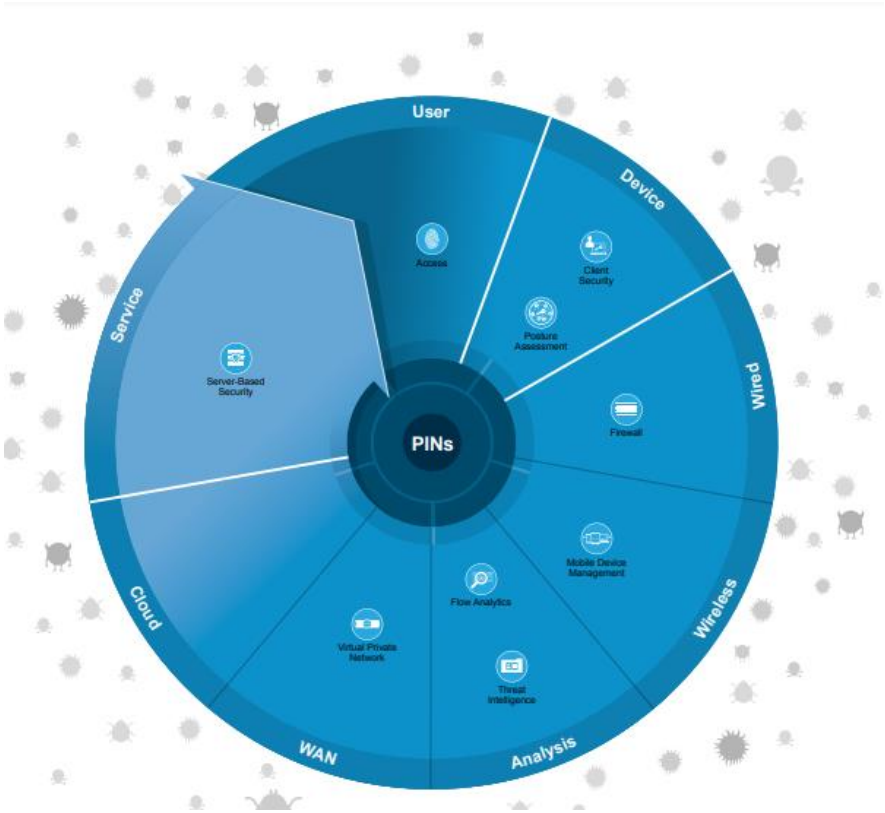

Рис.2.12. Можливості сегментації

Захист від загроз. Захист від загроз забезпечує видимість найбільш обхідних і небезпечних кіберзагроз. Використовуючи телеметрію мережевого трафіку, репутацію та контекстну інформацію, він дає змогу оцінити характер і потенційний ризик підозрілої діяльності, щоб ви могли вжити заходів для виправлення.

На рис.2.13. показано розвиток можливостей безпеки, які використовуються для операцій захисту від загроз

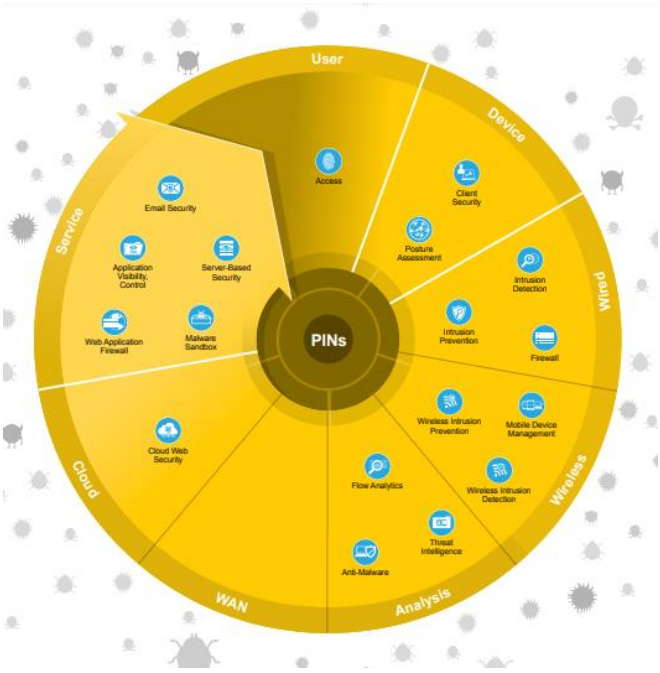

Рис.2.13. Можливості захисту від загроз

Безпечні служби. Безпечні служби надають такі технології, як контроль доступу, віртуальні приватні мережі та шифрування [8]. Цей домен включає захист для незахищених служб, таких як програми, співпраця та бездротовий зв'язок. На рис.2.14. показано розвиток можливостей безпеки, які використовуються для безпечних служб.

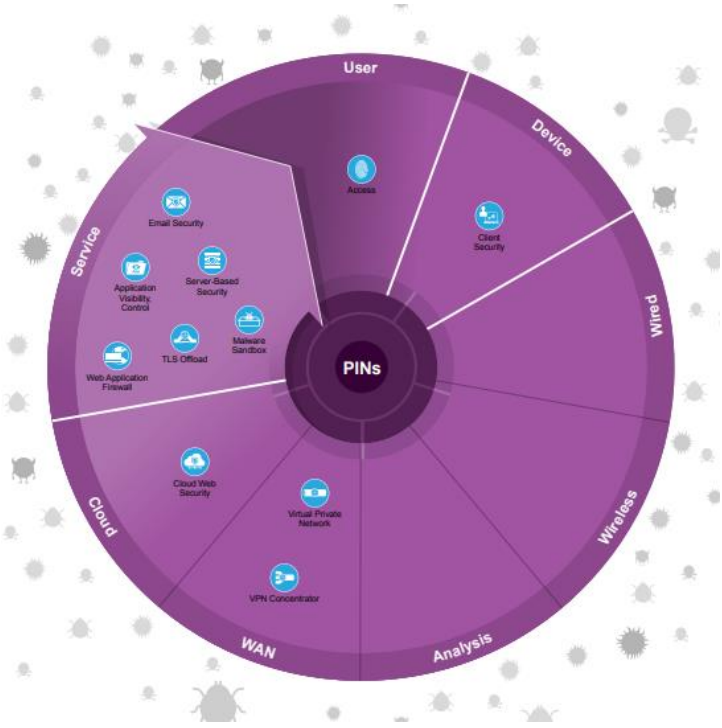

Рис.2.14. Можливості безпечних служб

2.3 Виокремлення головних загроз та можливостей Cisco SAFE

Таблиця 2.1.

Виокремлення головних загроз та можливостей безпеки Cisco

Атака	Поверхневі можливості	Загрози	Місця в мережі	Рекомендовані продукти
Працівники	Ідентифікація/авторизація: обмеження доступу користувача до послуг і ресурсів	Несанкціонований доступ до мережі: зловмисники отримують доступ до інформації з обмеженим доступом	Відділення, кампус Cloud, ЦОД, Edge, WAN	Identity Services Engine
Клієнти	Безпека на основі клієнта: програмне забезпечення безпеки для захисту клієнтів.	Зловмисне програмне забезпечення: віруси або системи, що компрометують зловмисне програмне забезпечення.	Відділення, кампус зовнішні зони	Cisco Advanced malware Protection for Endpoint, Антивірус, AnyConnect, Cisco Umbrella
	Антивірус.	Системи, що компрометують віруси.		
	Cloud Security	Перенаправлення користувача на шкідливий веб-сайт.		
	Персональний брандмауер.	Неавторизований доступ і неправильні пакети.		
	Оцінка стану: перевірка відповідності кінцевої точки та авторизація	Вірус і зловмисне ПЗ: скомпрометовані пристрої, які підключаються до інфраструктури	Відділення, кампус зовнішні зони	AnyConnect Agent Centralized Identity Services Engine

Можливості описують основні функції служби безпеки. У табл.2.1 наведено визначення можливостей, які використовуються в Cisco SAFE.

Таблиця 2.2.

Можливості безпеки Cisco та загрози

Атаки	Можливості	Загрози	Місця в мережі	Рекомендовані продукти
Голос: Телефон	охоплено доменом безпечних служб	Зловмисники отримують доступ до приватної інформації.	Відділення, кампус	Cisco Unified Communications
Відео: Дисплеї				Cisco TelePresence

Таблиця 2.3.

Виокремлення головних загроз та можливостей для сегменту інфраструктури проводової мережі

Атаки	Можливості	Загрози	Місця в мережі	Рекомендовані продукти
Інфраструктура фізичної мережі	Сегментація брандмауера: фільтрація стану та перевірка протоколу	Несанкціонований доступ і неправильно сформовані пакети	Відділення кампус Cloud, зовнішні зони, Edge, WAN	Adaptive Security Appliance Integrated Services Router Meraki MX
			ЦОД, Edge	Adaptive Security Appliance Integrated Services Router
	Виявлення та запобігання вторгненням: ідентифікація атак за допомогою сигнатур та аналізу аномалій	Атаки за допомогою хробаків, вірусів або інших методів	Кампус, ЦОД, Edge, зовнішні зони, WAN	Cisco Firepower Services on Adaptive Security Appliance FirePOWER Appliance Firepower Virtual Appliance
			Відділення	Cisco FirePOWER Services on ASA and UCS-E Meraki MX
			Cloud	Firepower Virtual Appliance
	Access Control + TrustSec: контекстна сегментація	Несанкціонований доступ до мережі: поширення інфікування	Відділення Кампус	Wireless Controller/ Catalyst Switch Centralized Identity Services Engine
			ЦОД, Edge	Adaptive Security Appliance, Aggregation Services Router Nexus/Catalyst Switch

Рекомендовані продукти зіставляються з кожною можливістю, де й коли вона використовується, а основні загрози пом’якшуються[9].

Таблиця 2.4.

Виокремлення головних загроз та можливостей для сегменту інфраструктури безпроводової мережі

Атаки	Можливості	Загрози	Місця в мережі	Рекомендовані продукти
Безпроводова мережа	Керування мобільними пристроями (MDM): контроль доступу кінцевої точки на основі політик	Зламані пристрої, що підключаються до інфраструктури	Edge	Identity Services Engine, Meraki Mobile Device Management
	Виявлення безпроводових зловмисників: виявлення та стримування шкідливих безпроводових пристроїв, які не контролюються компанією	Несанкціонований доступ і порушення роботи бездротової мережі	Відділення, кампус	Wireless LAN Controller Mobility Services Engine Centralized Mobility Services Engine Centralized Wireless LAN Controller Cisco Meraki
	Wireless Intrusion Prevention (WIPS): Блокування бездротових атак за допомогою сигнатур і аналізу аномалій.	Атаки на інфраструктуру через бездротові технології.		

Таблиця 2.5.

Виокремлення головних загроз та можливостей для сегменту інфраструктури глобальної мережі (WAN)

Атаки	Можливості	Загрози	Місця в мережі	Рекомендовані продукти
WAN: загальнодоступні та ненадійні глобальні мережі	Концентратор VPN: зашифрований віддалений доступ	Викриті послуги та крадіжка даних	Edge	Adaptive Security Appliance Aggregation Services Router
	Віртуальна приватна мережа (VPN): зашифровані комунікаційні тунелі	Легко збирати інформацію та ідентифікацію	Відділення, кампус	Adaptive Security Appliance Integrated Services Router Meraki MX
			ЦОД	Adaptive Security Appliance Aggregation Services Router Firepower Appliance
			Cloud, WAN	Adaptive Security Appliance Aggregation Services Router AnyConnect Meraki MX
	DDoS Protection: захист від масштабованих форм атак	Масштабні атаки, які переповнюють службы.	Edge	Партнер із технології розподіленої відмови в обслуговуванні

Таблиця 2.6.

Виокремлення головних загроз та можливостей для сегменту інфраструктури Cloud

Атаки	Можливості	Загрози	Місця в мережі	Рекомендовані продукти
Cloud	Хмарна безпека: безпека та контроль для розподіленого підприємства	Атаки зловмисного програмного забезпечення, вірусів і шкідливих URL-адрес	Відділення кампус, Cloud, Edge, ЦОД, зовнішні зони, WAN	Web Security Meraki MX Firepower URL Web Security Appliance AnyConnect Agent Cisco Umbrella Захищений Інтернет-шлюз (SIG) Cloudlock
	DNS Security	Перенаправлення користувача на шкідливий веб-сайт		
	Хмарний брандмауер	Неавторизований доступ і неправильні пакети, що підключаються до служб		
	Програмно-визначений периметр (SDP/SD-WAN)	Простий збір інформації та ідентифікаційних даних		
	Веб-безпека: цілісність доступу до мережі Інтернет	Проникнення та ексфільтрація через HTTP		
	Веб-репутація/фільтрування: відстеження загроз на основі URL-адрес	Атаки, спрямовані на шкідливу URL-адресу		
	Cloud Access Security Broker (CASB)	Неавторизований доступ і втрата даних		

2.4 Дослідження рівнів архітектури Cisco SAFE

Еталонна архітектура безпеки CISCO SAFE логічно відображає бізнес-потоки на можливості безпеки від джерела до місця призначення за допомогою місць у мережі (PIN). Кожен PIN-код має архітектурні рівні, які визначають чому використовуються елементи керування безпекою [10].

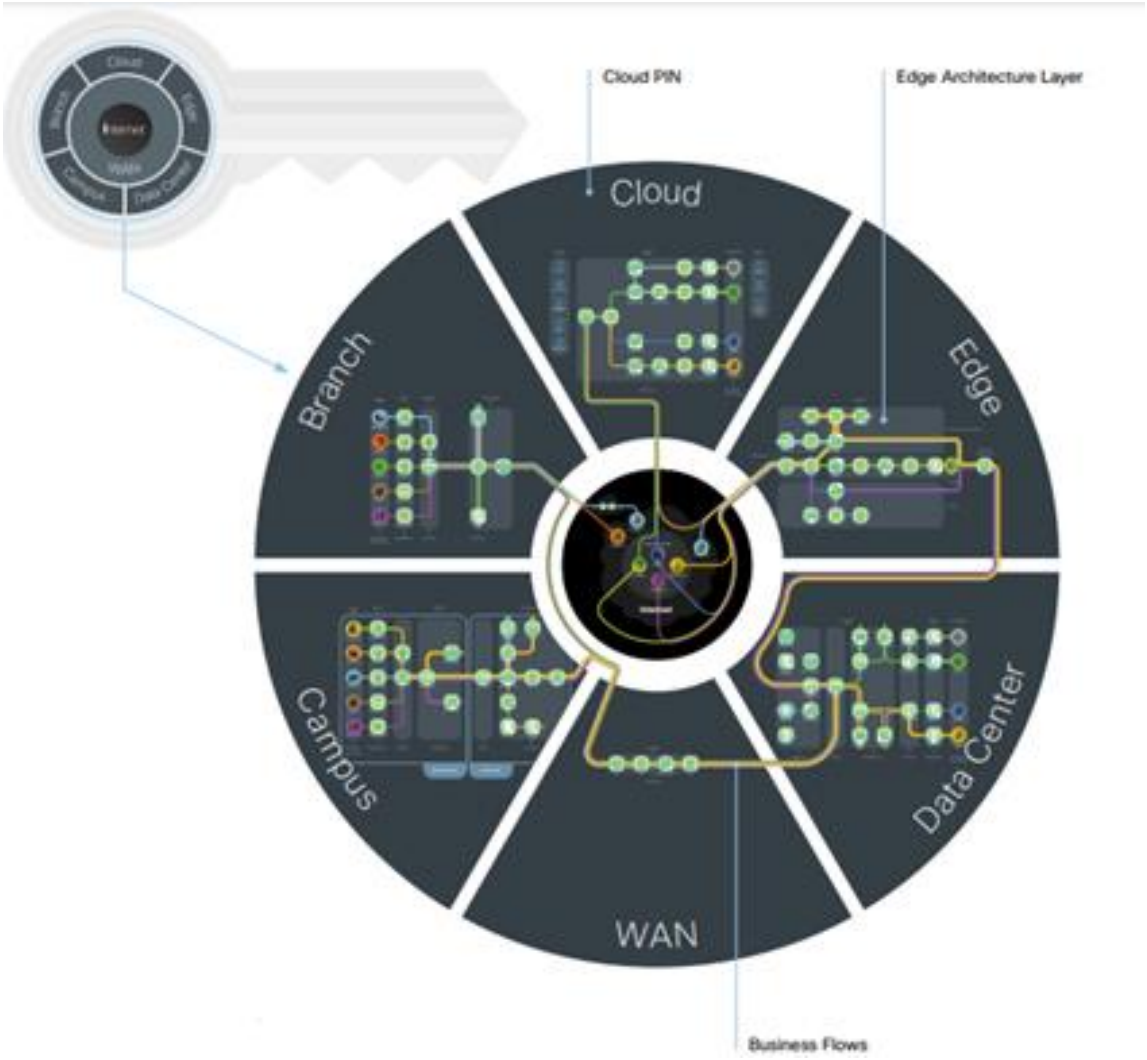

Рис.2.15. Модель Cisco SAFE

Архітектура Cisco SAFE використовує рівні, які узгоджуються з структурою атаки. Кожен рівень має стандартизовані елементи керування, що стосуються його функції. Деякі рівні забезпечують доступ і видимість, тоді як інші виконують примусове виконання.

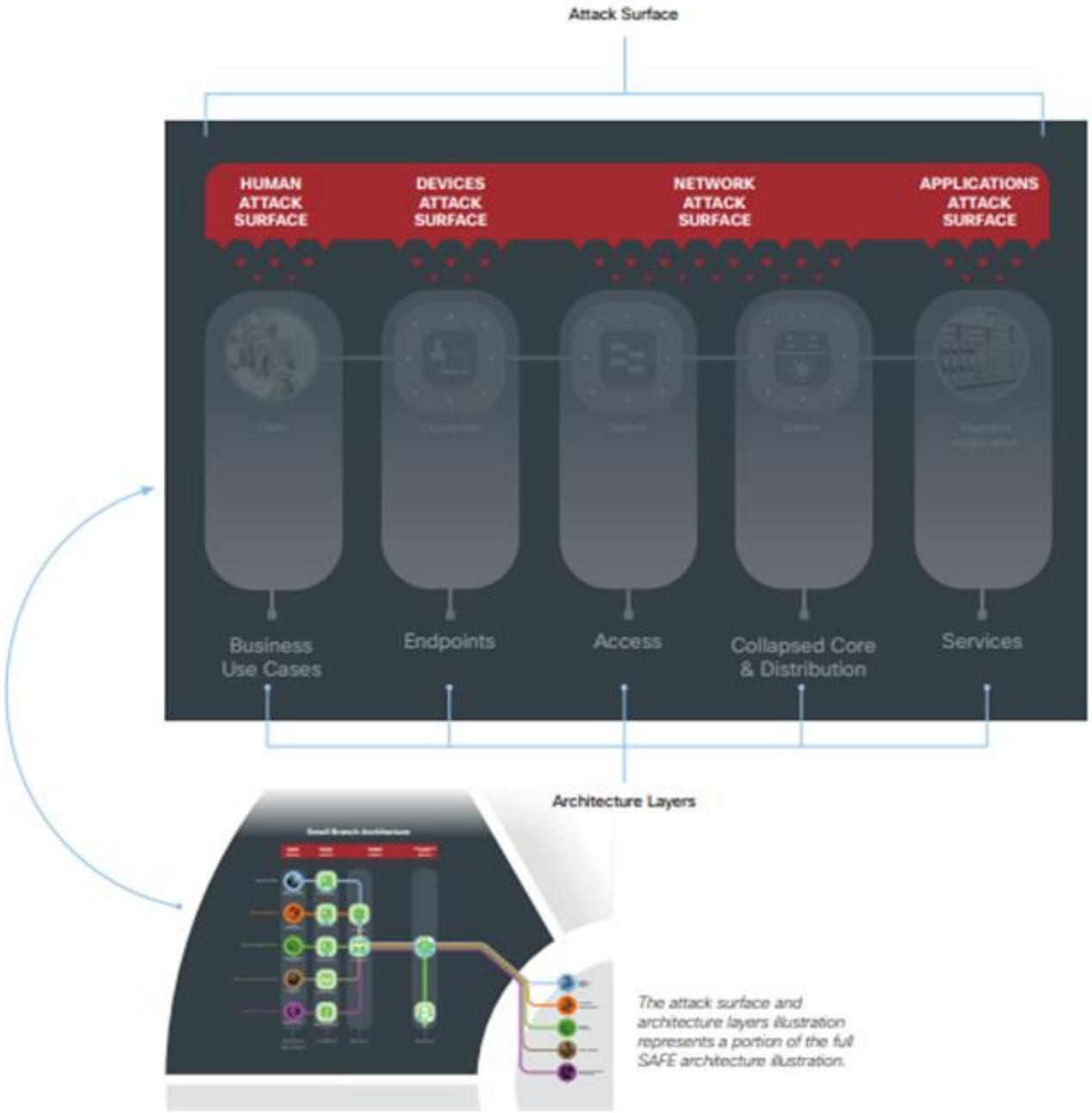

Рис.2.16. Деталізація структури атаки щодо рівнів архітектури

Рівень бізнес-функцій. Користувачі використовують мережеві служби для виконання різного набору необхідних службових функцій. З урахування того, які функції більш частіше виконуються, туди й спрямовуватиметься потік даних. Деякі користувачі виконуватимуть кілька ролей одночасно, що вимагатиме відповідної безпеки.

При цьому, саме користувачі можуть бути найслабшою ланкою в корпоративній мережі. Якщо їхній пристрій чи дані скомпрометовано, технічні

засоби контролю можна обійти. Видимість і сегментація обмежують вплив скомпрометованих співробітників, зловмисних партнерів або клієнтів [11].

Рівень «Пристрої» включає різні пристрої: від традиційних комп'ютерів і ноутбуків до смартфонів, планшетів і дедалі частіше таких пристроїв, як засоби керування будівлями, камери та робототехніка. Для пристроїв потрібна відповідна безпека на основі клієнта, визначена політикою.

Рівень кінцевих точок. Атаки Zero Day та інші просунуті атаки можуть обійти існуючий захист. Захищена компанія використовує мережу та пристрої, що підключаються до неї, як основу поведінки. Під час атаки нова поведінка порівняно з базовими лініями викликає тривогу. Використовуючи мережу як датчик, забезпечується ефективне стримування за допомогою інтелектуального архітектурного дизайну.

Модель Cisco SAFE відповідає традиційній моделі мережі доступу, розподілу та ядра. Кожен рівень ієрархії виграє, розділяючи плоску мережу на масштабовані блоки. Трафік залишається локальним, якщо він не призначений для інших мереж, і він піднімається на вищий рівень. Мережа діє як датчик, який використовує аналітику потоку для виявлення аномалій і забезпечення видимості атак [12].

Рівень доступу. Метою рівня доступу є безпечне підключення користувачів та пристроїв до мережі. Він підключається до рівня розповсюдження та є першою лінією контролю для решти корпоративної мережі. Його метою є ідентифікація та сегментація користувачів, а також оцінка відповідності пристроїв, які шукають доступ. Цей рівень дозволяє примусово застосовувати порушення ідентичності або аномальну поведінку.

Рівень розподілу. Цей рівень є точкою агрегації для всіх комутаторів доступу. Він контролює межу між рівнем доступу та основним рівнем і служить точкою інтеграції для можливостей безпеки, таких як IPS та застосування мережевої політики.

Основний рівень. Основний рівень забезпечує пересилання масивів даних між високошвидкісними службами з високим ступенем резервування, з'єднуючи рівень

розподілу з рівнем послуг. У невеликих мережах, які не вимагають масштабування, рівні розподілу або доступу підключаються безпосередньо до ядра.

Метою рівня послуг є надання та захист послуг, які використовуються співробітниками корпоратвиної мережі та користувачами.

Рівень служб. Рівень служб зазвичай підключається до основного рівня та надає базові можливості. Можливості безпеки сегментують трафік і забезпечують видимість окремих бізнес-потоків. Завдяки аналітиці кожне місце в мережі захищено від відомих зловмисних програм та інших шкідливих вторгнень. У разі атак нульового дня, де загрозу не було класифіковано, аналіз потоку визначає аномальну поведінку, скорочуючи час на виявлення [13].

Політика контролюється проти порушень. Безпека, заснована на бізнесі, захищає від загроз, створених за межами компанії, таких як листування електронною поштою, веб-серфінг і віддалений доступ.

Багатьом підприємствам необхідно відповідати вимогам дотримання нормативних вимог, використовуючи фальшиве виявлення безпроводового зв’язку незалежно від того, чи сама компанія використовує безпроводовий зв’язок. Якщо компанія використовує безпроводовий зв’язок для бізнес-функцій, WIPS потрібен на додаток до базової IPS [14].

Висновки до 2 розділу

Досліджено особливості поділу корпоративної мережі на логічні області із використанням Cisco SAFE. Виокремлено наступні області: відділення (філія); кампус; WAN; Центр обробки даних; Edge; Cloud.

Зазначено, що це узагальнення стосується безпечного функціонування наступних послуг: автентифікація, маршрутизація, комутація, безпроводовий зв’язок, брандмауер, виявлення вторгнень тощо.

Приведено перелік найпопулярнішіх загроз та вразливостей, які притаманні виокремленими логічним областям, та перераховано перелік засобів та технологій

Cisco SAFE, які здатні нейтралізувати загрозу, помякшити або сповістити про вразливість чи аномалію.

Досліджено архітектуру Cisco SAFE, при якій використовуються рівні, кожен з яких узгоджується із структурою атаки. Зазначено, що кожен рівень має стандартизовані елементи керування, що стосуються його функції. При цьому, деякі рівні забезпечують доступ і видимість, тоді як інші виконують лише примусові фукнції.

3 ТЕХНОЛОГІЯ ПОБУДОВИ ЗАХИЩЕНОЇ МОДЕЛІ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ВИКОРИСТАННЯМ CISCO SAFE

Співробітники, вендори та партнери часто потребують доступу до мережі під час подорожі або дистанційної роботи, коли знаходяться в інших місцях, за межами корпоративної мережі. Через це значна кількість організацій потребує небхідності надавати користувачам доступ до ресурсів даних, у віддалених місцях з доступною для них мережею підключення.

Рішення для безпечного підключення клієнтів повино підтримувати:

- Широкий вибір кінцевих пристроїв;
- Безперебійний доступ до мережевих ресурсів;
- Контроль автентифікації та політик, що інтегруються із ресурсами автентифікації;
- Криптографічний захист для запобігання витоку конфіденційних даних при умові впливу неавторизованих сторін які випадково чи навмисно перехоплюють дані[15].

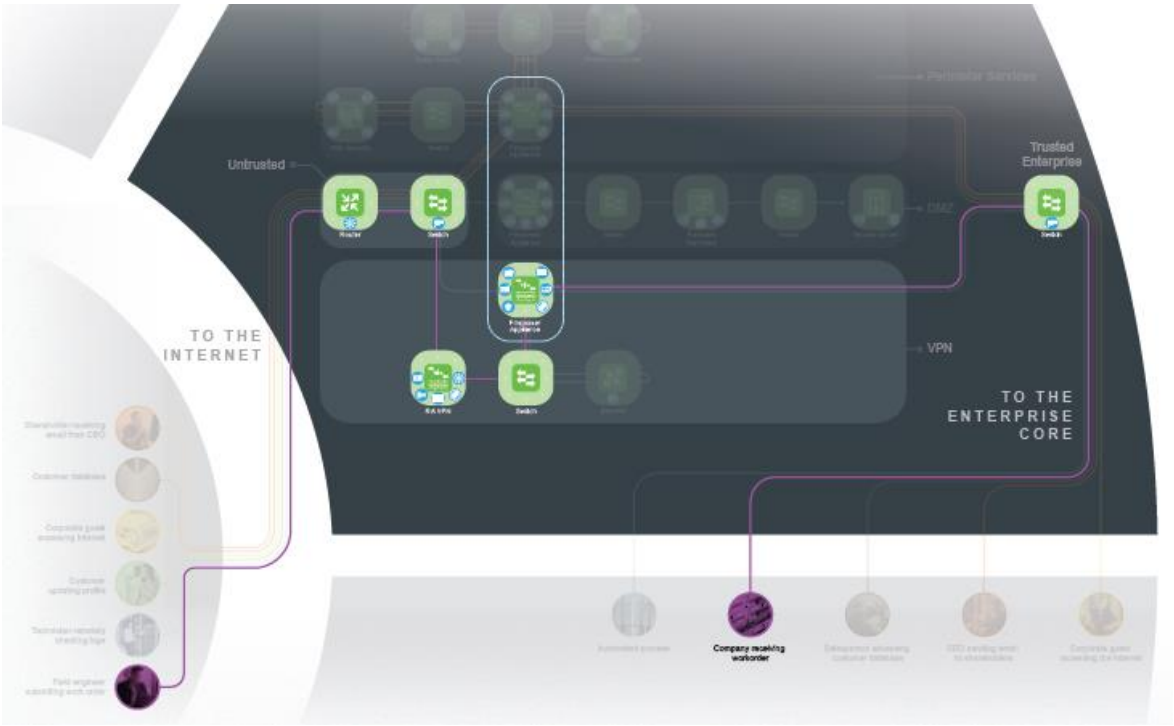

Рис.3.1. Еталонна архітектура Internet Edge – RA VPN Highlight

Дизайни для Edge розгортає сімейство Cisco ASA/Firepower і Cisco AnyConnect Secure Mobility Client. Віртуальна приватна мережа віддаленого доступу (RA VPN Highlight) реалізує виділені ресурси для підключення віддалених користувачів і сайтів (рис.3.1).

Необхідно описати особливості функціонування дистанційного керування при використанні доступу в межах PIN-коду Internet Edge, який є одним із шести описаних сценаріїв, описаних у першом розділі (архітектура Cisco SAFE). При цьому включаючи такі елементи, як безпека клієнта, балансування навантаження або безпека сервера.

3.1 Аналіз рішення Internet Edge RA VPN

Цей дизайн для Edge реалізує VPN, розгорнуте на парі налаштованих пристроїв Cisco Firepower 9300, що використовують образ ASA для високої доступності та віддалений доступ VPN Radware DefensePro (протидія DDoS). Додаток (vDP на FP9300) також встановлюється для забезпечення додаткового захисту точок підключення VPN.

В архітектуру також включено декілька Cisco ASA (для захисту від загроз FTD), образ програмного забезпечення та налаштований Next-Generation Intrusion Prevention (NGIPS) в додаток до брандмауера наступного покоління (NGFW) для перевірки сеансів віддалених користувачів після закінчення тунелю. Ця архітектура має кращу видимість, масштабованість та рівень безпеки[16].

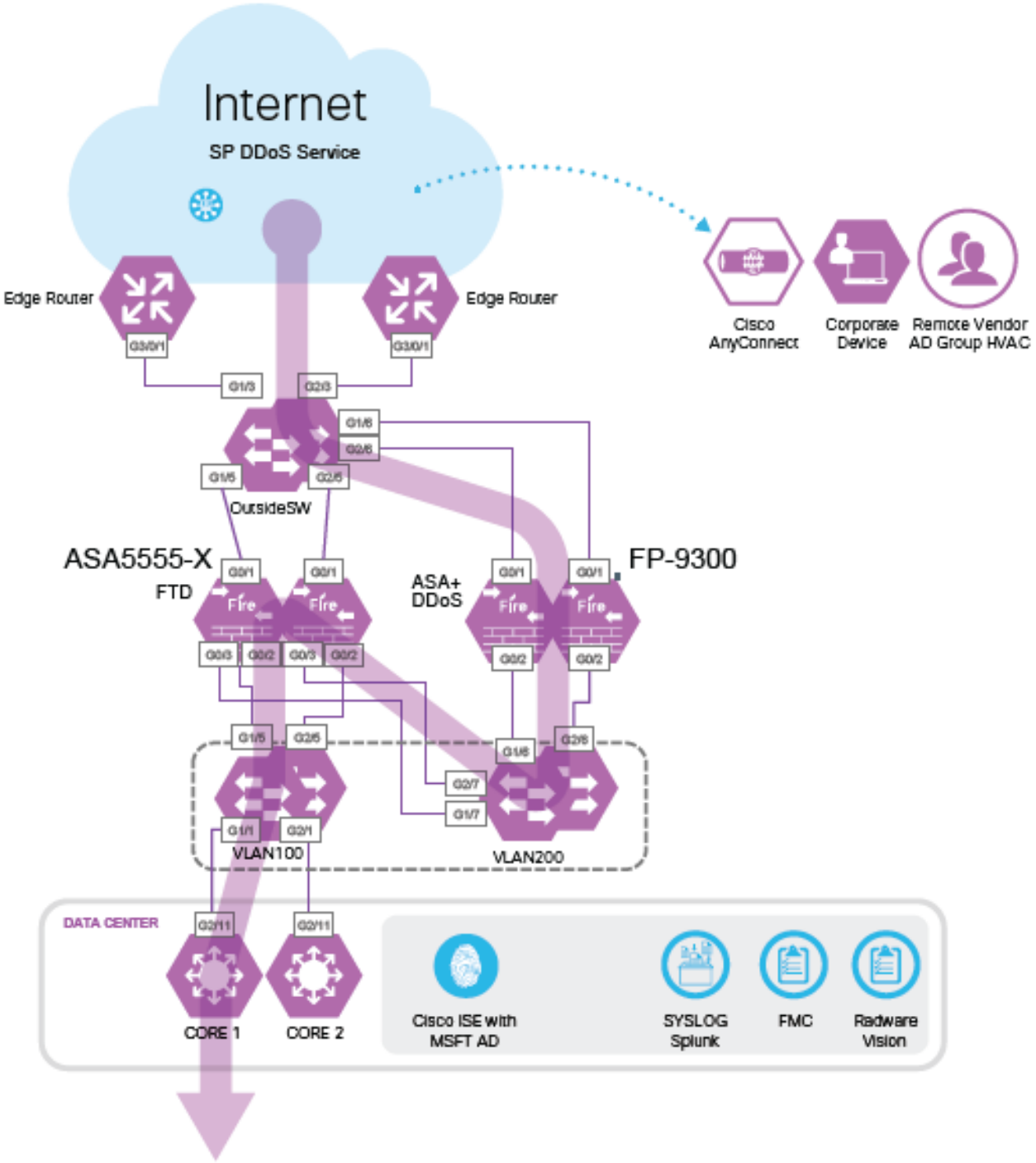

Рис.3.2. Потік проектування VPN високого рівня Internet Edge RA

На рис.3.2. представлено огляд запропонованої архітектури та сценарію функціонування, де фіолетова лінія вказує на комунікаційний потік RA VPN.

Таблиця 3.1.

Характеристика складових компонентів

Випуск	Апаратне забезпечення	Ролі	Компонента
Cisco Firepower Next- Generation Firewall (NGFW) Appliance	Брандмауер головної станції віддаленого доступу	Firepower 9300 з FPR9K-SM-36 running ASA image	Firepower Chassis Manager Ver.1.1(4.85g) Cisco ASA Software Release 9.6(0)124
Radware Virtual Defense Pro	Керує захистом від DDoS	Virtual module within FP 9300	Radware VDP ver 1.01.02
Cisco AnyConnect VPN Client	VPN-клієнт віддаленого доступу	встановлено у віддаленому клієнті, ПК	Version 4.2.02075
Cisco Adaptive Security Appliance (ASA)	Edge NGFW Security	ASA5555-X Firepower Threat Defense	FTD6.0.1
Firepower Management Console	Edge intrusion policy management	FMC-3500	6.0.1 (build 1213)
Cisco Identity Services Engine (ISE)	Керування політикою / сервер автентифікації на основі ролей	Віртуальна машина (VMware)	Version 2.0.0.306
Radware Vision Console	Керування та налаштування профілів DDoS	APSolute Vision VA	Version 3.330
Edge маршрутизатори	Інтернет-шлюз	ASR1002-X	15.3(1)S
Edge комутатори	Комутатор доступу	C9372PX	nxos.7.0.3.I2.2b.bin
Cisco Nexus 7000	Агрегація та комутатор доступу FlexPod	Cisco Nexus 7004 Cisco Nexus 7010	NX-OS version 6.1(2)
Radware-Raptor Attack Tool	DDoS attacks	VM	Version 2.6.37

3.1.1 Характеристики впровадження Edge маршрутизаторів

Зовнішній Edge маршрутизатор забезпечує підключення користувача або працівника від постачальника послуг, яким він користується до підприємства, в якій працює.

Найкращі методи роботи полягають у застосуванні базової фільтрації на зовнішніх і внутрішніх інтерфейсах для блокування підробленого та небажаного трафіку, ретельно відповідаючи середовищу організації (наприклад, блокування запитів (RFC 1918), що надходять із зовнішньої мережі).

Пристрої налаштовані на автентифікацію на основі ролей AAA для корпоративного Identity Services Engine за допомогою TACACS+. Журнали відправляються на централізований сервер збору, при чому пристрої синхронізуються з відомими та надійними джерелами.

Edge маршрутизатори розгортаються в парі високої доступності за допомогою HSRP у внутрішніх інтерфейсів.

Великі організації зазвичай впроваджують протоколи маршрутизації чрез зовнішній шлюз, ретранслюючи власний IP. Для простоти цієї перевірки використовуються статичні маршрути[17].

Приклад налаштування грубої фільтрації:

interface GigabitEthernet0/0/1
ip access-group INTERNAL-FILTER-IN in
interface GigabitEthernet0/0/3
ip access-group COARSE-FILTER-INTERNET-IN in
ip access-group COARSE-FILTER-INTERNET-OUT out
ip access-list extended COARSE-FILTER-INTERNET-IN
remark ---Block Private Networks---
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 172.16.0.0 0.15.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any

remark -
remark ---Block Autoconfiguration Networks---
deny ip 169.254.0.0 0.0.255.255 any log
remark -
remark ---Block Loopback Networks---
deny ip 127.0.0.0 0.0.255.255 any log
remark -
remark ---Block Multicast Networks---
deny ip 224.0.0.0 15.255.255.255 any log
remark -
remark ---Block Traffic targeted at DMZ Network Edge Devices---
deny ip any 10.11.206.0 0.0.0.255 log
deny ip any 1.1.1.0 0.0.0.255 log
remark -
remark ---Block Spoofing of your networks---
remark enter your IP block here
remark ---Permit all other traffic---
permit ip any any

Приклад налаштування автентифікації на основі ролей

aaa new-model
aaa group server tacacs+ PRIMARY1
server name PRIMARY
ip tacacs source-interface GigabitEthernet0/0/1
!
aaa authentication login COMPLIANCE group PRIMARY1 local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo

aaa accounting exec default

action-type start-stop

group tacacs+

!

aaa accounting commands 15 default

action-type start-stop

group tacacs+

!

aaa accounting system default

action-type start-stop

group tacacs+

aaa session-id common

tacacs server PRIMARY

address ipv4 10.11.230.111

key 7 <removed>

Приклад налаштування централізованого логінга (або журналювання)

logging buffered 50000 informational

no logging rate-limit

login block-for 1800 attempts 6 within 1800

login quiet-mode access-class 23

login on-failure log

login on-success log

archive

log config

logging enable

notify syslog contenttype plaintext

hidekeys

logging trap informational

logging source-interface GigabitEthernet0/0/1
logging host 10.11.230.161

Приклад налаштування синхронізації часу

clock timezone PST -8 0
clock summer-time PST recurring
ntp authentication-key 555 md5 mysecretkey
ntp trusted-key 555
ntp authenticate ntp source GigabitEthernet0/0/3
ntp server 171.68.10.80 prefer
ntp server 171.68.10.150

Приклад налаштування протоколів безпечного керування

ip ssh version 2
ip scp server enable
no service pad
no ip http server
no ip http secure-server
line vty 0 15
session-timeout 15 output
access-class 23 in
exec-timeout 15 0
ipv6 access-class BLOCKALL-IPv6 in
logging synchronous
login authentication COMPLIANCE
transport input ssh

3.1.2 Характеристики впровадження Edge комутаторів

Edge комутатори забезпечують підключення між різними системами DMZ. Два комутатори серії Nexus 9000 були обрані, оскільки вони зазвичай мають найбільш доступні порти 10G для необхідного набору послуг. Інтерфейс керування використовується через зовнішній канал мережі для доступу, налаштування та моніторингу.

Пристрої налаштовані на роль AAA, ідентифікація із використанням TACACS+. Netflow і логи надсилаються на централізовані сервери реєстрації/збору даних. Час пристрою синхронізується з відомим і надійним часом джерела. Щоб відповідати різним вимогам політик безпеки, банери для входу та інтерфейс реалізовано на основі списків доступу для обмеження адміністративного доступу до системи. Увімкнено та використовуються лише захищені протоколи.

Комутатори розгорнуті в режимі високої доступності - одна пара зовнішня і одна пара як DMZ сегмент. Усі невикористовувані інтерфейси вимикаються[21].

Приклад налаштування автентифікації на основі ролей

feature tacacs+
tacacs-server key 7 “<removed>”
tacacs-server host 10.11.230.111
aaa group server tacacs+ CiscoISE
server 10.11.230.111
use-vrf management
source-interface mgmt0
aaa group server tacacs+ tacacs
feature password encryption aes
aaa authentication login default group CiscoISE
aaa authentication login console group CiscoISE
aaa authorization ssh-certificate default group CiscoISE

aaa accounting default group CiscoISE

aaa authentication login error-enable

Приклад налаштування централізованого логінга (або журналювання) та NetFlow

logging server 10.11.230.161 5 use-vrf management

logging source-interface mgmt0

feature sflow

sflow sampling-rate 50000

sflow max-sampled-size 200

sflow counter-poll-interval 100

sflow max-datagram-size 2000

sflow collector-ip 10.11.230.154 vrf management

sflow collector-port 7000

sflow agent-ip 10.11.230.154

sflow data-source interface ethernet 1/1-7

hardware access-list tcam region sflow 256

Приклад налаштування синхронізації часу

clock timezone PST -8 0

clock summer-time PDT 2 Sun Mar 02:00 1 Sun Nov 02:00 60

ntp server 10.11.255.1 prefer use-vrf management

ntp server 10.11.255.2 use-vrf management

ntp server 172.26.129.252 use-vrf management

ntp server 172.28.189.1 use-vrf management

ntp source-interface mgmt0

Приклад налаштування протоколів безпечного керування

!NexOS only uses SSHv2, and does not have HTTP/s, other protocols disabled by default

ssh key rsa 2048

line vty

exec-timeout 15

logout-warning 20

access-class SwitchMgmt in

3.2 Огляд фізичної топології RA VPN Security Appliances

Топологія VPN для архітектури межі включає принаймні два засоби безпеки Firepower 9300 або 4100, що працюють з програмним забезпеченням ASA з Radware DDoS Virtual Defense Pro (образ розгорнуто як активний компонент із високою доступністю при налаштуванні).

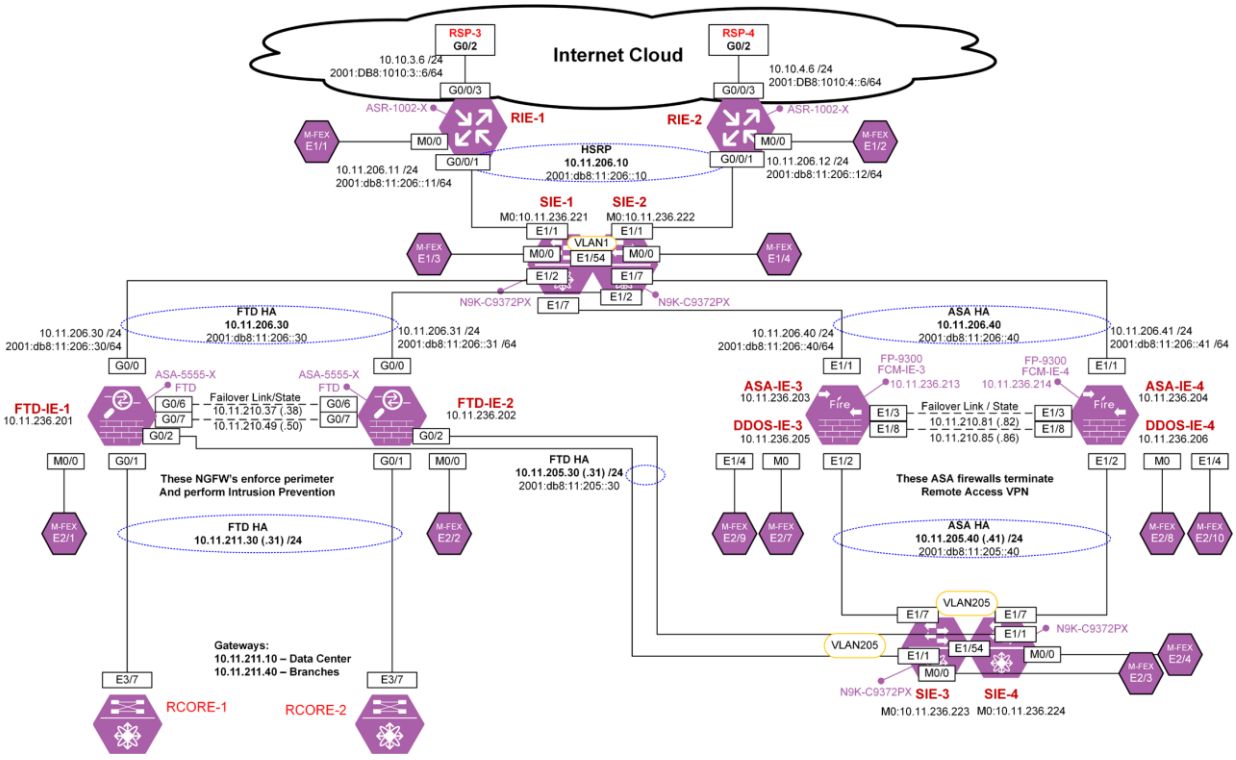

Рис.3.3. Фізична топологія для еталонної архітектури Edge

З'єднання між комутаторами відбувається через порти високої доступності – 10 Гбіт/с. Конфігурація ASA виконується через CLI, Cisco Adaptive Security Device Manager (ASDM) або Cisco Security Manager (CSM).

Управління політиками для брандмауерів через ADSM або CSM. Об'єкти пристрою користувача/сервера управляються в Cisco Identity Services Engine (ISE) разом із створенням політики TrustSec для решти платформ. Облікові записи користувачів і автентифікації пов’язані з Active Directory виконуються через механізм служб ідентифікації (ISE).

Віддалений доступ до брандмауера Cisco ASA AnyConnect. AnyConnect Secure Mobility Client збільшує видимість і контроль через розширену корпоративну мережу, запобігаючи зараженим кінцевим точкам отримувати доступ до критично важливих ресурсів. Це призводить до:

- Вибору найбільш ефективного протоколу тунелювання;
- Вибору розширеного доступу рівня 2 для полегшення одночасної аутентифікації пристрою та користувача;
- Надання доступу для віддаленої (дистанційної) роботи зі смартфонів чи планшетів для відділення чи філії організації;
- Надання високозахищеного доступу для кінцевих точок при використанні проводового, безпроводового зв’язку та VPN;
- Забезпечення додаткової мережевої безпеки та розширеного захисту від шкідливих програм;
- Відстеження використання програм кінцевих точок для виявлення підозрілої поведінки.

AnyConnect забезпечує виконання політик безпеки за допомогою служб ідентифікації Cisco (ISE). Також можете використовувати його, щоб розгорнути Cisco Advanced Malware Protection (AMP) для кінцевих точок. Його активатор AMP розширює захист кінцевих точок від загроз з підтримкою VPN або будь-де, де Cisco AnyConnect використовується.

Новим у Cisco AnyConnect 4.2 є vодуль видимості мережі в Windows і платформи Mac OS. Тепер адміністратори можуть відстежувати використання

програм для кінцевих точок, щоб виявити потенційні аномалії поведінки та зробити більш обґрунтовані рішення щодо проектування мережі.

Даними про використання можна поділитися зі зростаючими номерами експорту інформації про Інтернет-протокол (IPFIX). Хоча AnyConnect підтримує різноманітність функцій безпеки, варто зосередитися лише на розгортанні функціональності AnyConnect VPN та Firepower 9300 під керуванням образу ASA як фінальної складової VPN [16].

3.3 Алгоритм налаштування Firepower 9300

Крок 1. Налаштування IP-адреси керування. Отримавши блок FP9300, необідно використати консольний порт для ініціалізації налаштування, щоб указати FXOS IP-адресу керування. Це залежить від IP-адреси керування, яку потрібно вказати для інтерфейсу керування ASA. Використовуючи IP-адресу керування FXOS, можна отримати доступ до її графічного інтерфейсу для налаштування більшості налаштувань апаратного забезпечення та відображення інтерфейсу.

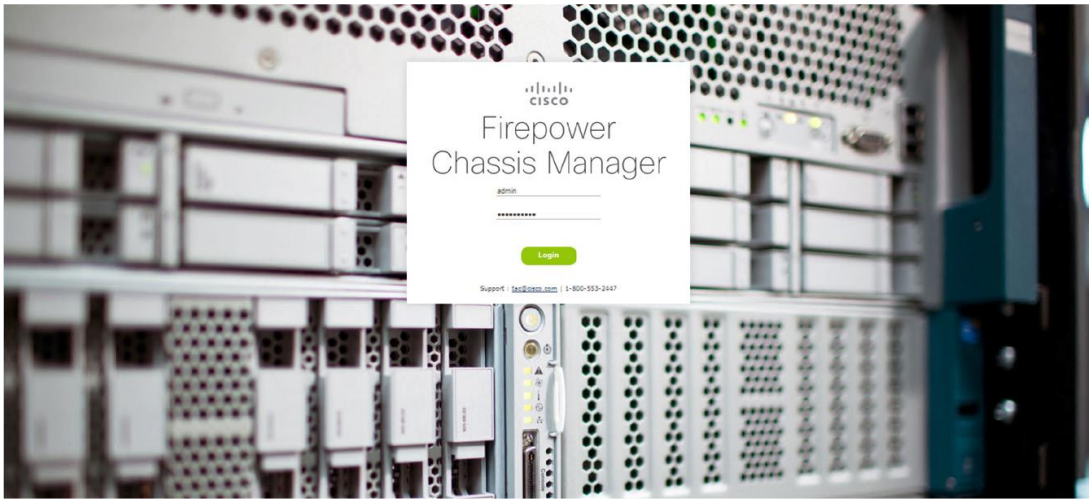

Рис.3.4. Сторінка для початкового налаштування Firepower 9300

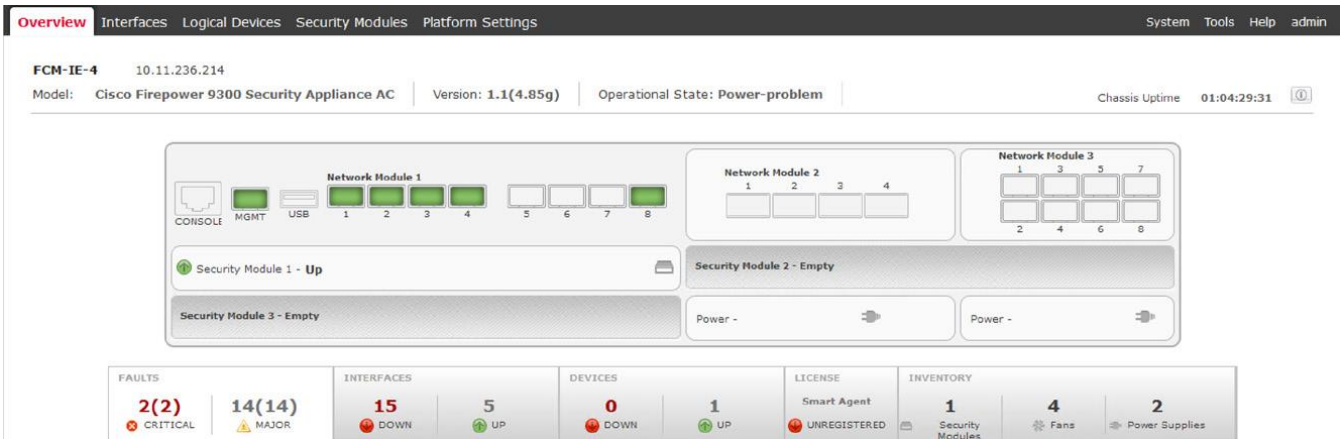

Рис.3.5. Продовження налаштування Firepower 9300

Крок 2. Конфігурація інтерфейсу та його розподіл.

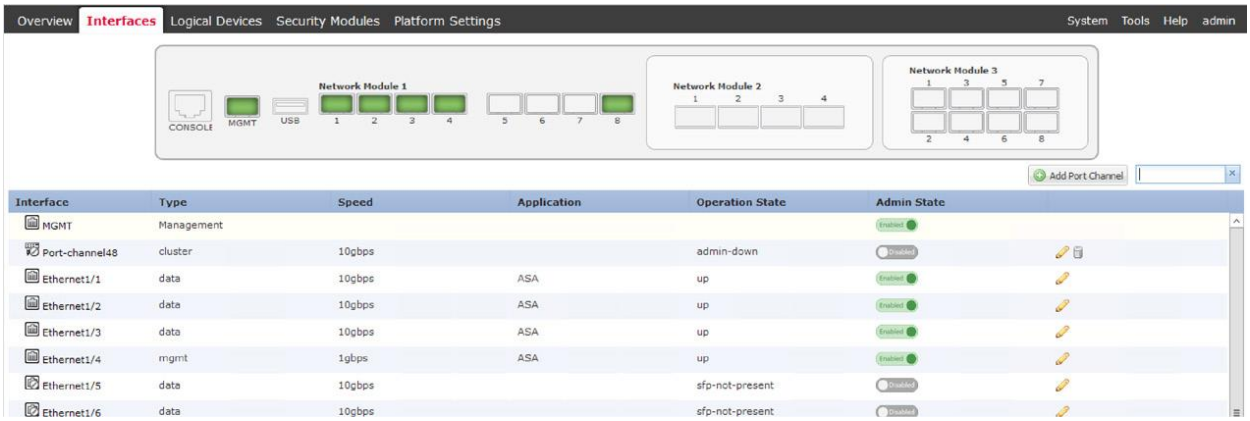

Рис.3.6. Конфігурація інтерфейсу

Обравши вкладку «Інтерфейс», будуть увімкнені пов’язані інтерфейси. Можна налаштувати його як інтерфейс даних або керування.

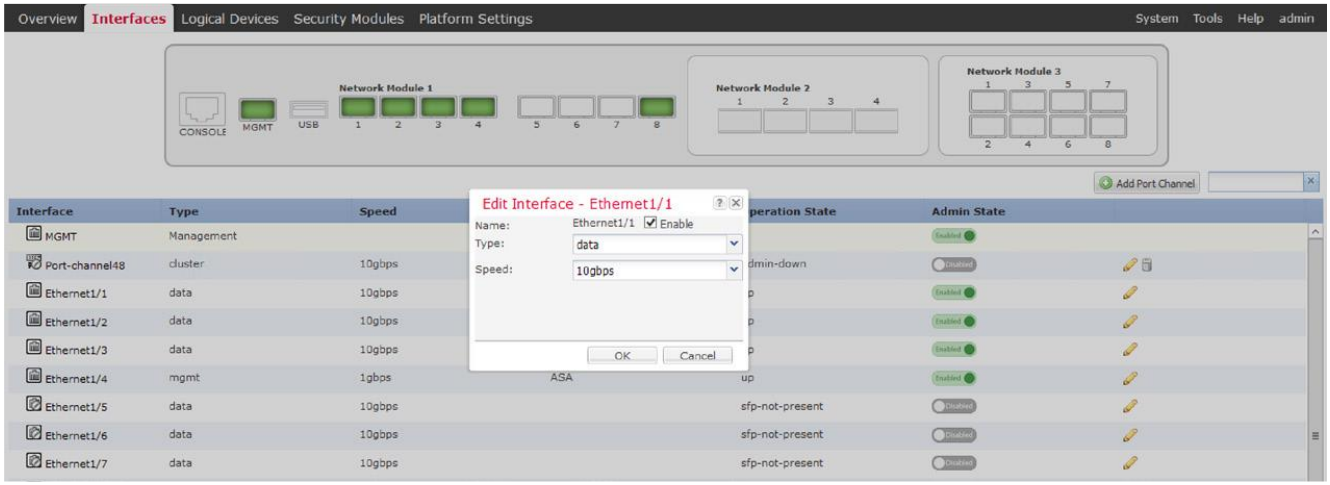

Рис.3.7. Увімкнення пов’язаних інтерфейсів

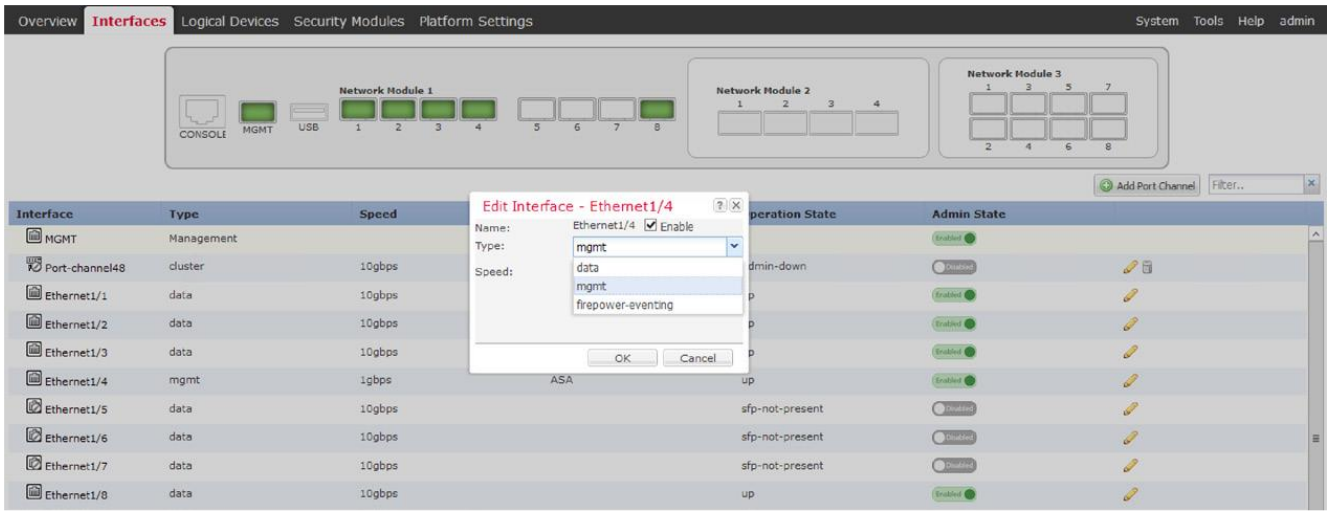

Рис.3.8. Налаштування інтерфейсу як інтерфейсу даних або керування

Крок 3. Призначення інтерфейсів для логічних пристроїв. Обираючи вкладку «Логічний пристрій», а можна обрати інтерфейси, які потрібно призначити логічному пристрою.

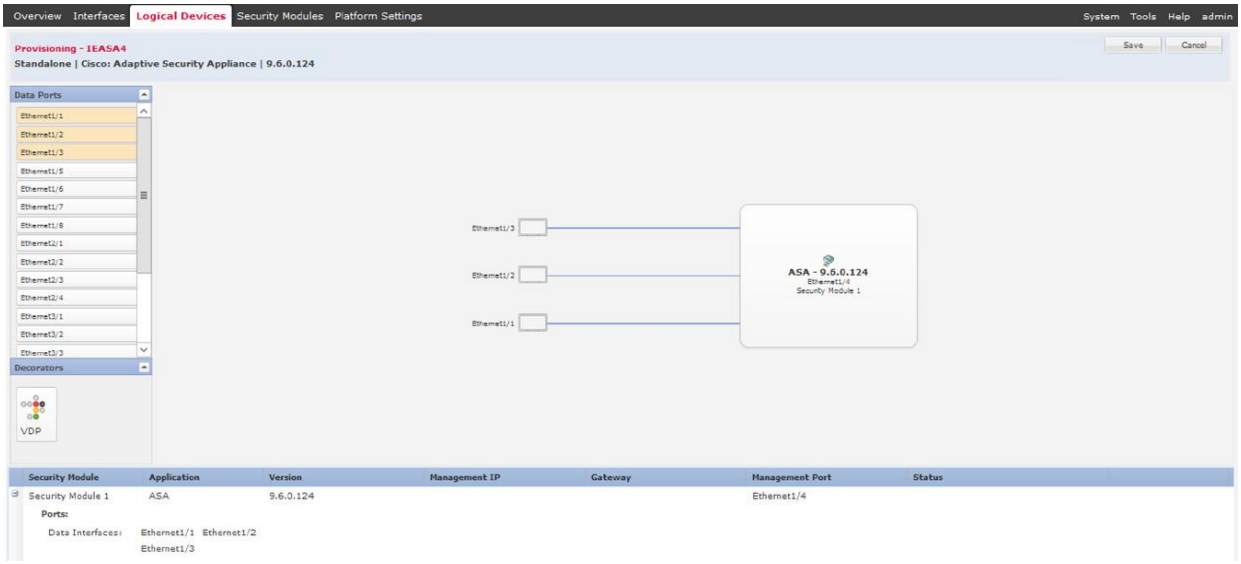

Рис.3.9. Призначення інтерфейсів для логічних пристроїв

Якщо логічний пристрій не відобразився, необхідно перейти до вкладки «Security Module», перевірити чи модуль увімкнуто та активовано.

Рис.3.10. Активація «Security Module»

Крок 4. Увімкнення ліцензії (рис.3.11). Вкладка «Система», далі - «Ліцензування», щоб отримати доступ до сторінки ліцензування, де можна ввести дані ліцензії для ввімкнення функцій. Щоб отримати доступ до ASDM, потрібна ліцензія 3DES (розпізнається на Smart License Server).

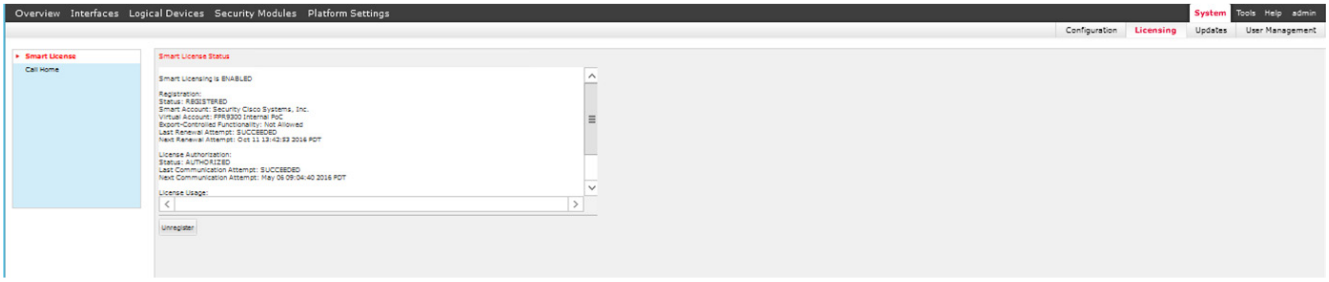

Рис.3.11. Увімкнення ліцензії

Крок 5. Запуск ASDM, щоб налаштувати VPN і брандмауер за допомогою майстра VPN для VPN AnyConnect [17].

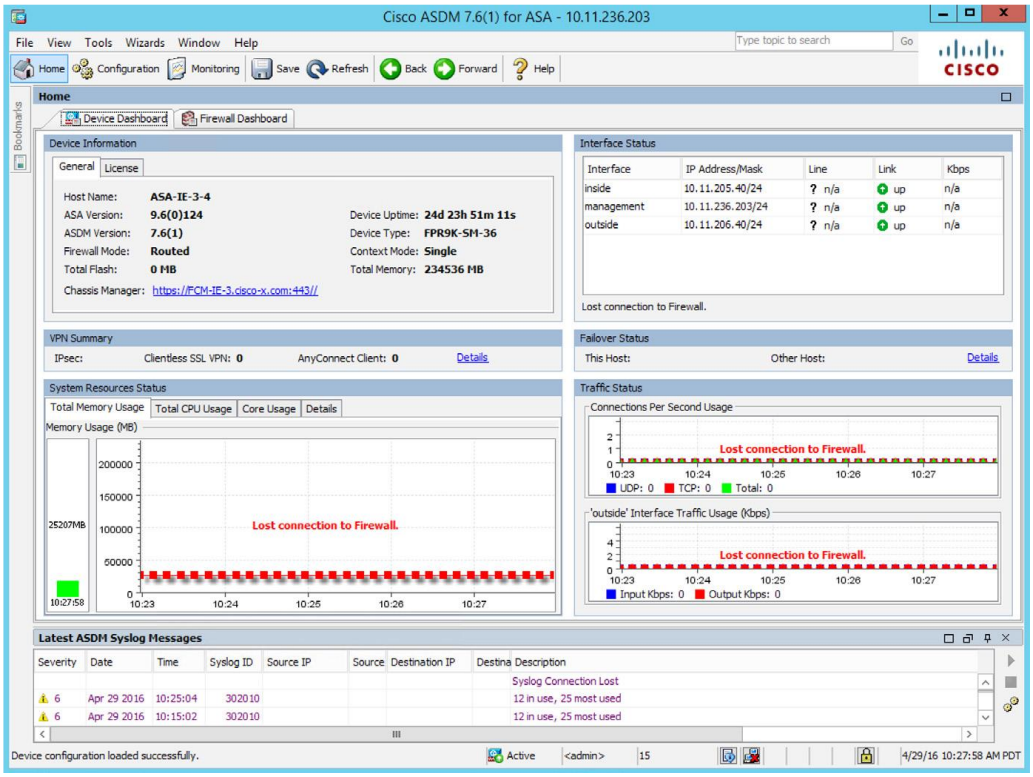

Рис.3.12. Запуск ASDM для налаштувати VPN

Крок 6. Встановлення Radware vDP. Для цього потрібно завантажити Radware vDP на пристрій. Редагувати логічний пристрій ASA. У лівому стовпці обрати піктограму vDP, щоб налаштувати vDP. Вибрати один із портів даних, який

буде пов’язанам з vDP. Інтерфейси керування може бути тим самим інтерфейсом, що й інтерфейс керування ASA, але потрібна інша IP-адреса.

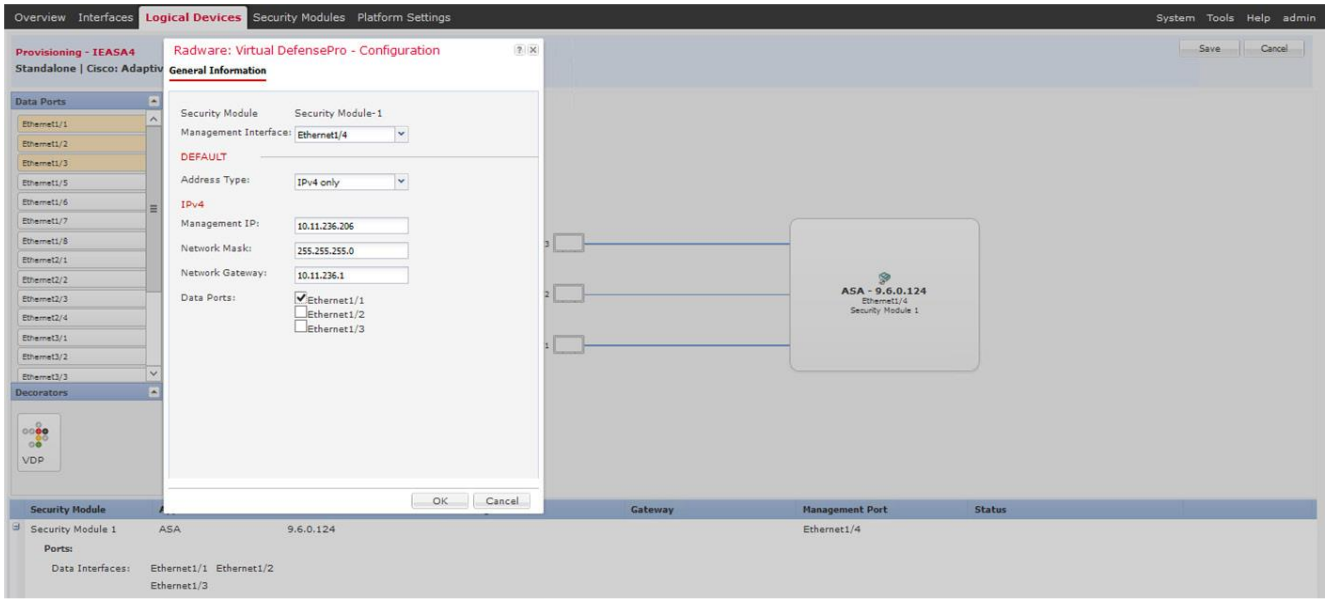

Рис.3.13. Встановлення Radware vDP

Початок процесу встановлення vDP.

Рис.3.14. Процесу встановлення vDP

Крок 7. Встановлення Vision. Vision — це сервер керування для vDP, його можна імплементувати на гіпервізорі VMWare.

Після встановлення відкривається доступ до Vision із браузера. Після входу потрібно ввести дані щодо ліцензії, отримані в Radware. Ім'я користувача та пароль за замовчуванням - radware/radware[22].

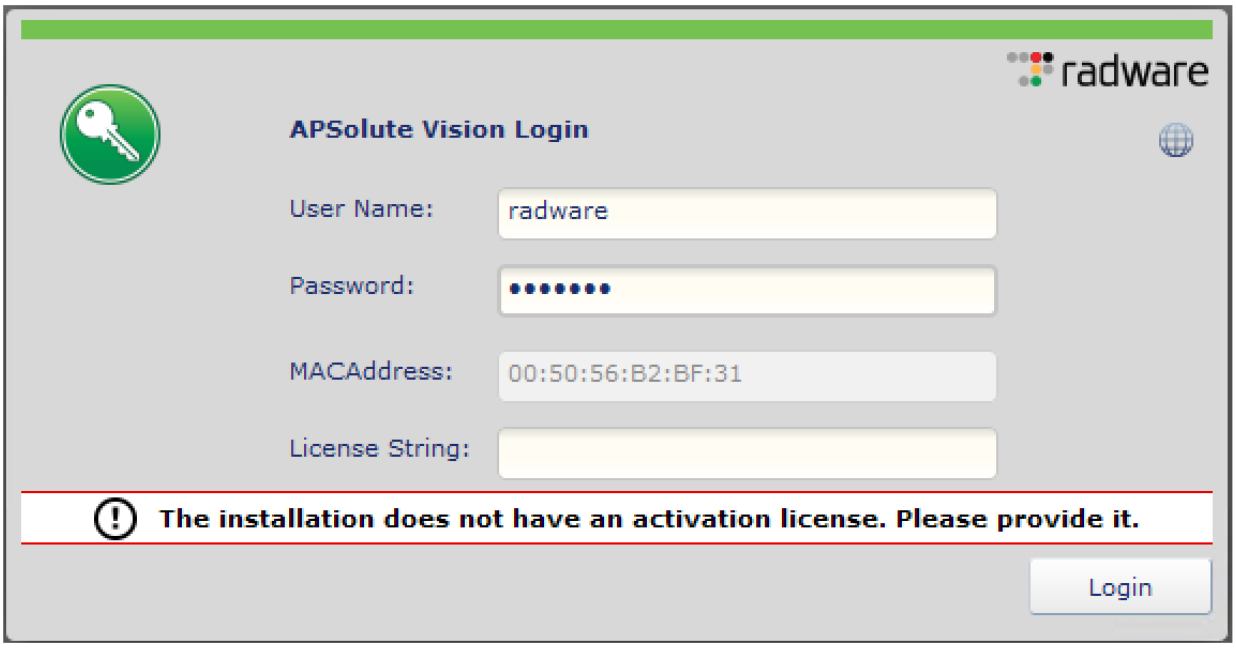

Рис.3.15. Ім'я користувача та пароль за замовчуванням

Крок 8. Додавання vDP у Vision та налаштування. На екрані Vision у розділі «Сайти та кластери» необхідно обрати «+», щоб додати пристрій. Обрати DefensePro зі спадного списку та встановити назву, IP-адресу керування, SNMP версія та іншу необхідну інформацію.

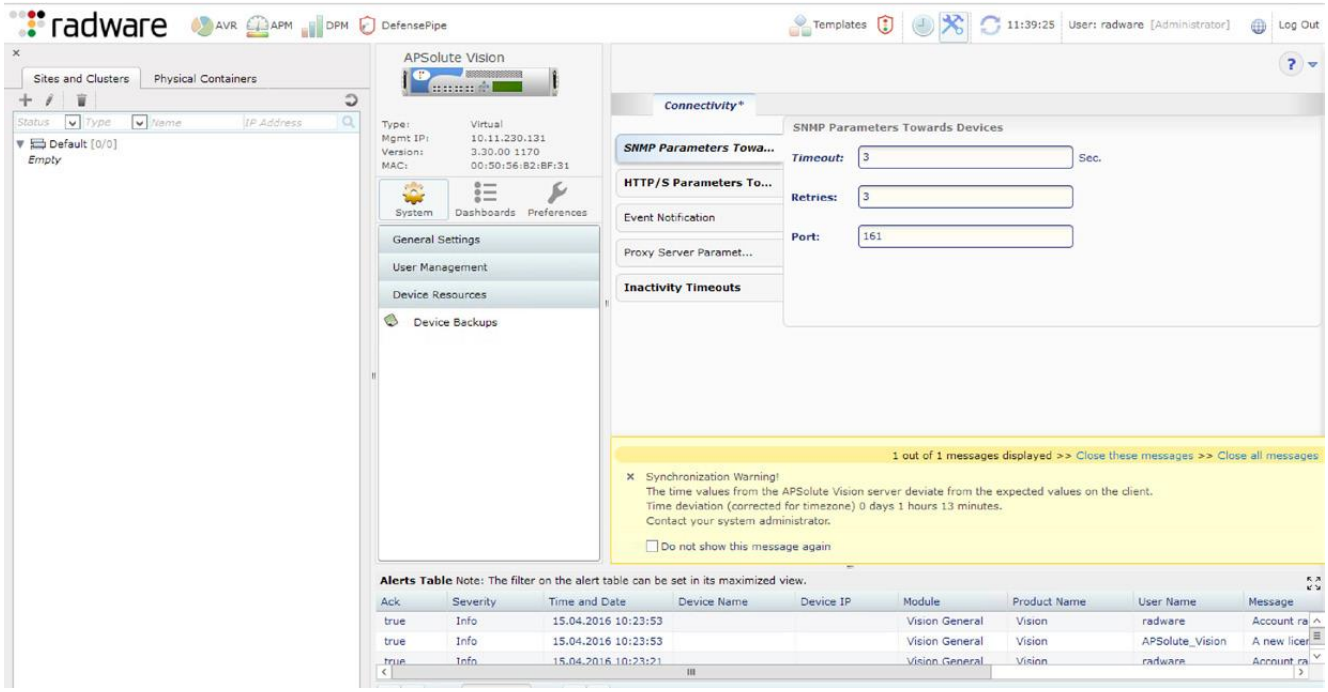

Рис.3.16. Додавання vDP у Vision

Крок 9. Налаштування конфігурації кількох пристроїв. Незважаючи на те, що два пристрої ASA перебувають у стані високої активності, vDP працює самостійно. Vision має функцію зв'язування кількох пристроїв як одного, заощаджуючи час для адміністратора на налаштування кількох пристроїв.

На вкладці «Сайти та кластери» необхідно вибрати кілька vDP (наприклад, DDoS-IE-3 та DDoS-IE4) і натиснути кнопку зі стрілкою, щоб оновити екран. Якщо вибрати кнопку «Конфігурація», з'явиться вікно конфігурації кількох пристроїв для вибору головного пристрою та інших пристроїв, які потрібно оновити. Необхідно обрати «Перейти», щоб увімкнути режим кількох пристроїв.

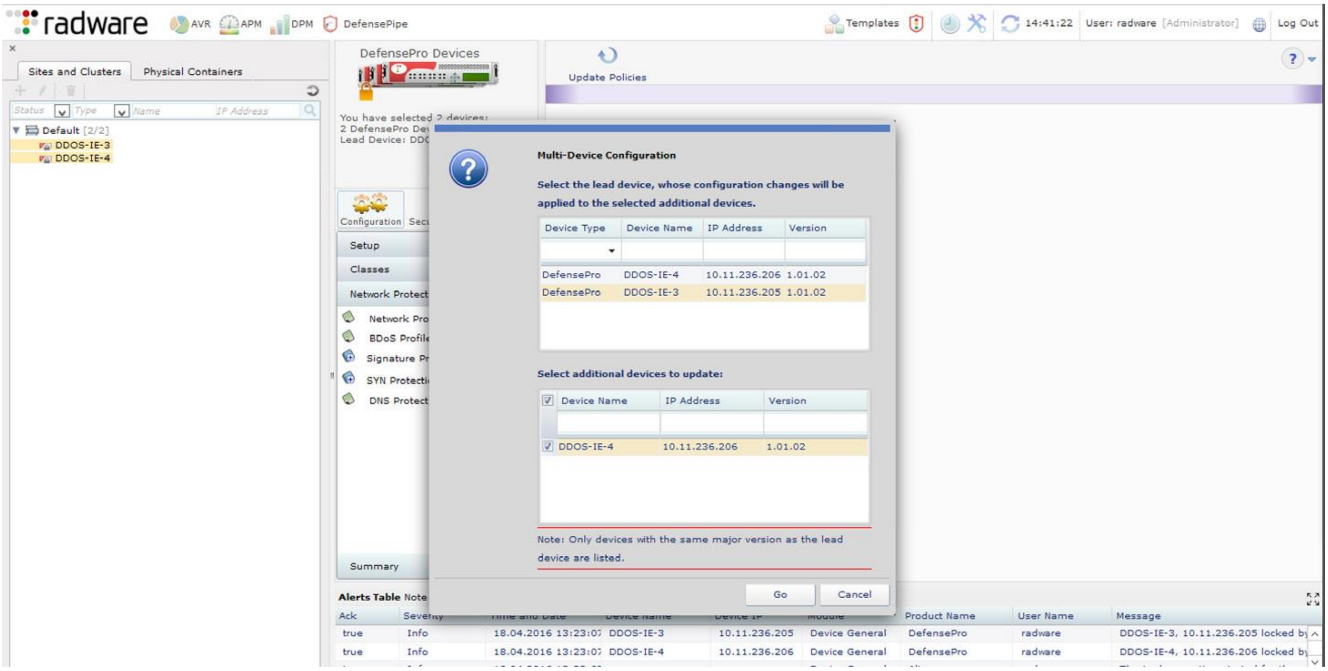

Рис.3.17. Налаштування конфігурації кількох пристроїв

3.4 Алгоритм додавання та налаштування нових пристроїв

Після того, як системи були оновлені та додані до центру управління (FMC), необхідно налаштувати нові пристрої [18].

3.4.1 Алгоритм налаштування високої доступності

Далі приведено етапи налаштування високої доступності.

Крок 1. Під'єднання інтерфейсів зв'язку відмов та стану між двома пристроями за допомогою двох перехресних кабелів. Для цієї перевірки були використані інтерфейси G0/6 і G0/7.

Крок 2. У FMC вибрати «Пристрої» > «Керування пристроями».

Крок 3. У спадному меню «Додати» у верхньому правому куті обрати «Додати високу доступність».

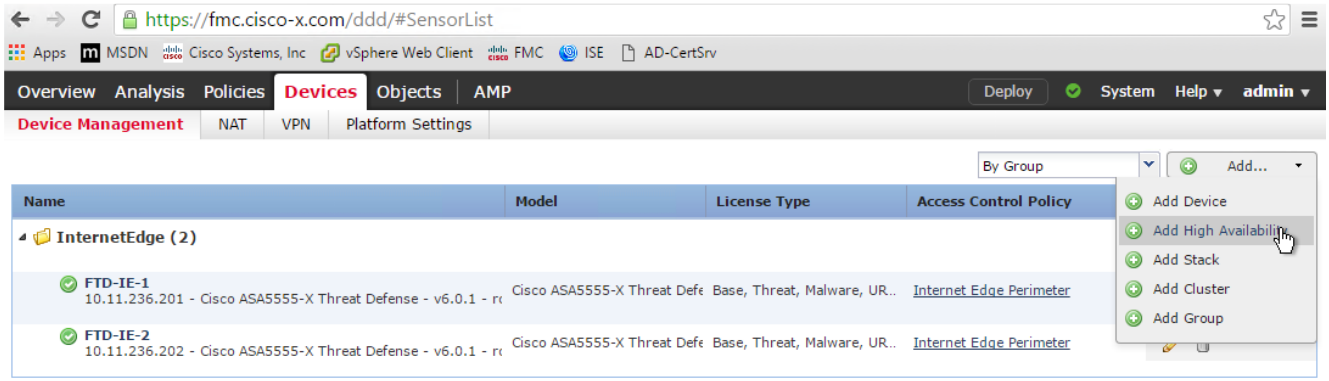

Рис.3.18. Додавання високої доступності

Крок 4. Необхідно ввести відображуване ім'я для пари високої доступності (наприклад, FTD-IE-HA)

Крок 5. Для типу пристрою обирається Firepower Threat Defense.

Крок 6. Далі, обирається основний одноранговий пристрій для пари високої доступності, і вторинний одноранговий пристрій для пари високої доступності.

Крок 7. Натиснувши «Продовжити», у розділі LAN Failover Link обирається Interface G0/6 для обміну даними. Після чого, вводиться *folink* для ідентифікаційного логічного імені.

Крок 8. IP-адреса 10.11.210.37 призначається як основну для посилання відновлення після відмови на активному пристрої.

Крок 9. IP-адреса 10.11.210.38 призначається як вторинна для посилання відновлення після відмови на резервний блок.

Крок 10. Необхідно ввести 255.255.255.252 для маски підмережі первинної та вторинної IP-адреси.

Крок 11. У розділі Stateful Failover Link обирається інтерфейс G0/7 для зв'язку стану, та вводиться *statelink* для ідентифікаційного логічного імені.

Крок 12. IP-адреса 10.11.210.49 призначається як основна для посилання стану на активному пристрої.

Крок 13. IP-адреса 10.11.210.50 призначається як вторинна для зв'язку стану на резервному пристрої.

Крок 14. Необхідно ввести 255.255.255.252 для маски підмережі первинної та вторинної IP-адреси.

Рис.3.19. Приклад введення налаштувань

Крок 15. Увімкнення шифрування за посиланнями, при виборі Enabled і Auto для ключа. Метод генерації для шифрування IPsec між резервними посиланнями представлено на рис.3.20.

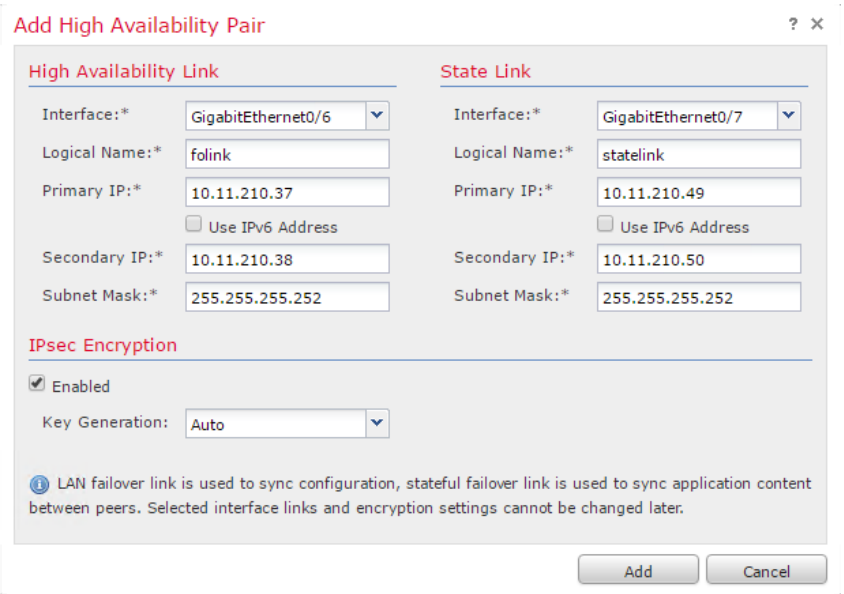

Рис.3.20. Метод генерації для шифрування IPsec між резервними посиланнями

Крок 16. Натиснувши «Додати», необхідно почекати поки система синхронізує дані. Керування пристроєм тепер показуватиме дві системи у високій доступності.

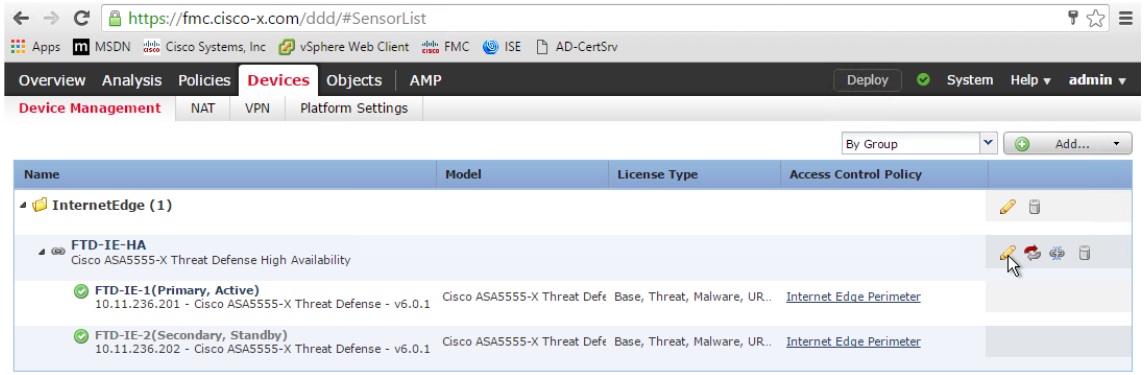

Рис.3.21. Синхронізація даних

Крок 17. Для редагування, необхідно перейти до «Інтерфейси», щоб налаштувати внутрішні, зовнішні та RA VPN мережі. Натиснувши «редагування», внести зміни на GigabitEthernet0/0. Після чого потрібно ввести дані щодо імені, увімкнівши відповідний прапорець.

Крок 18. Обираючи «Інтернет», можна ввести дані щодо будь-якої назви.

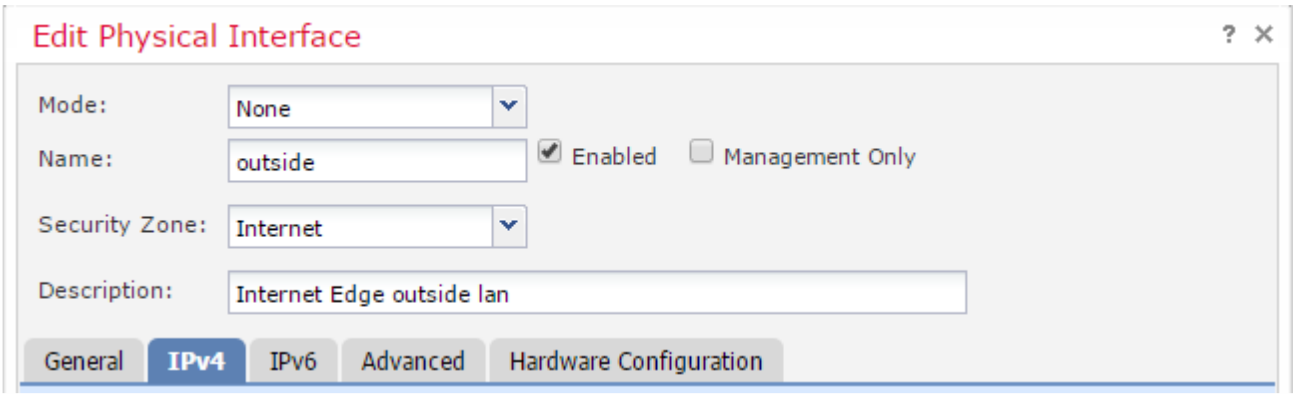

Рис.3.22. Додавання описової назви

Крок 19. На вкладці IPv4 необхідно зазначити 10.11.206.30/24 для IP-адреси

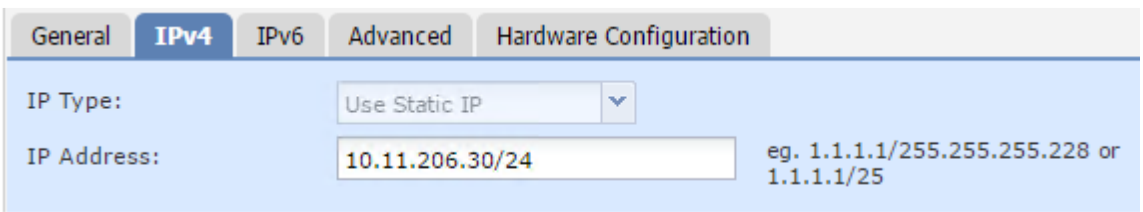

Рис.3.23. Внесенн змін щодо IP адреси.

Крок 20. У вкладці «Додатково» краще вказати активну MAC-адресу 0011.0206.30aa та резервну: 0011.0206.30bb [22].

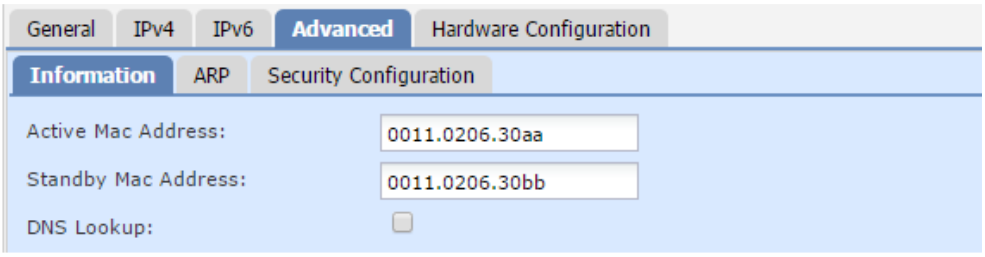

Рис.3.24. Внесення інформації щодо активної та резервної MAC-адреси

Крок 21. Після натискання «OK» необхідно повторити ці ж кроки і щодо внутрішнього інтерфейсу VPN і RA VPN.

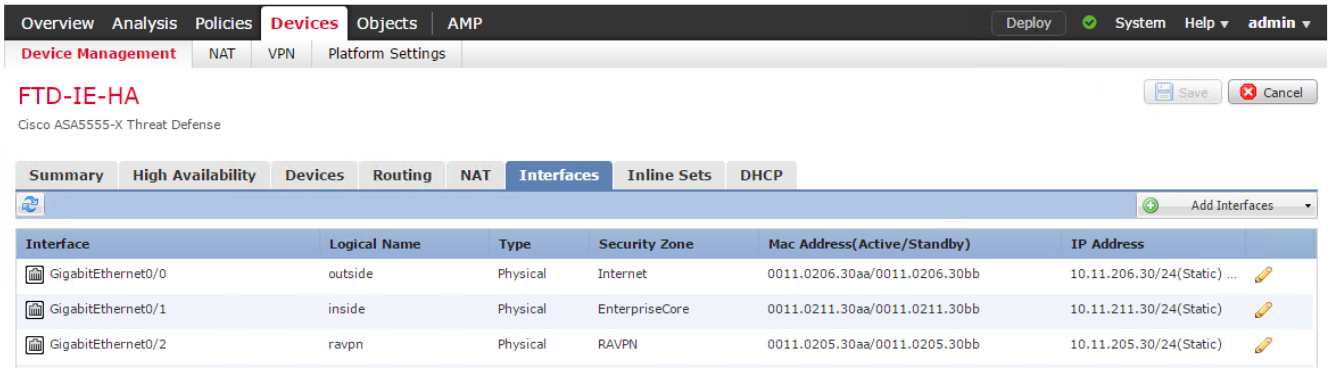

Рис.3.25. Фінальні налаштування

Крок 22. На вкладці «High Availability» необхідно відредагувати «Monitored Interfaces» і додати Standby IP-адресу

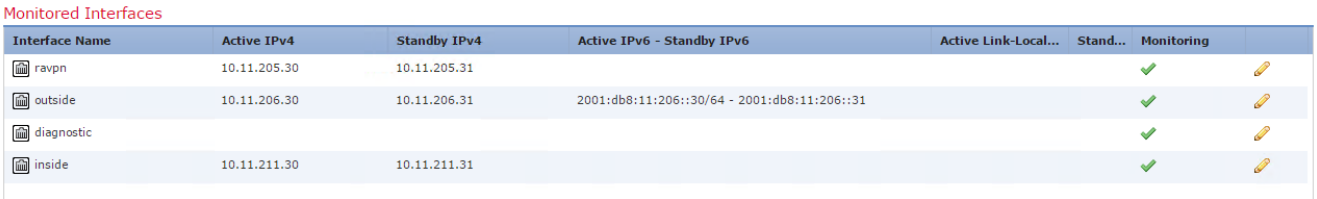

Рис.3.26. Додавання Standby IP-адреси

Крок 23. На вкладці «Маршрутизація» необхідно обрати «Статичний маршрут» і натиснути «Додати маршрут». Після чого, обрати зовнішній інтерфейс, і додати будь-який IPv4, при цьому обравши шлюз маршрутизаторів Edge, і натиснувши «OK»

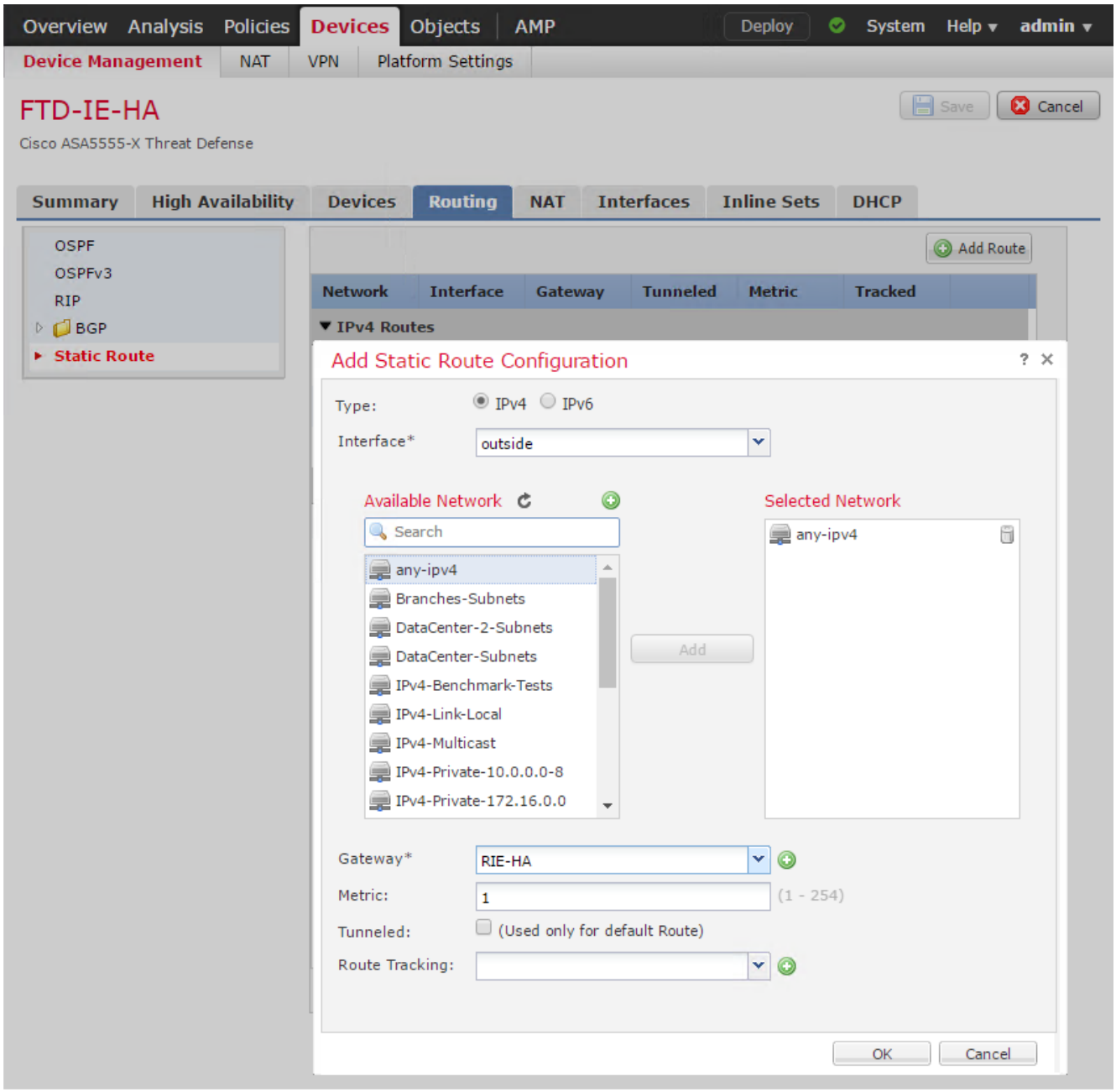

Рис.3.27. Додавання даних щодо маршруту

Крок 24. Натиснувши «Зберегти» у верхньому правому куті, налаштування ASA за допомогою операційної системи Firepower Threat Defense вважаються завершеними.

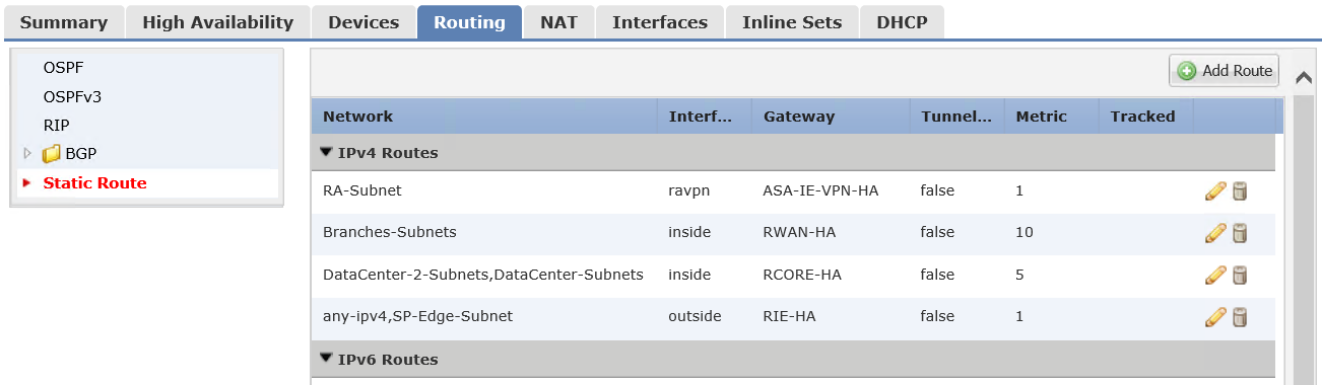

Рис.3.28. Завершення налаштування ASA за допомогою операційної системи Firepower Threat Defense

3.4.2 Налаштування політик контролю доступу Firepower

Взаємодія відбувається із областю центру керування Firepower

Крок 1. Необхідно обрати пункт «Система», далі – «Інтеграція»

Крок 2. У вкладці «Realms» необхідно клацнути «New Realm» у верхньому правому куті, та ввести описову назву: «LAB-AD» (рис.3.29)

Крок 3. Наступним кроком потрібно ввести основний домен: cisco-x.com, та додати ім’я користувача, пароль для доступу до каталогу домену (бажано не адміністратора)

Крок 4. Введення DN бази та групи: dc=cisco-x,dc=com, та натиснути «ОК».

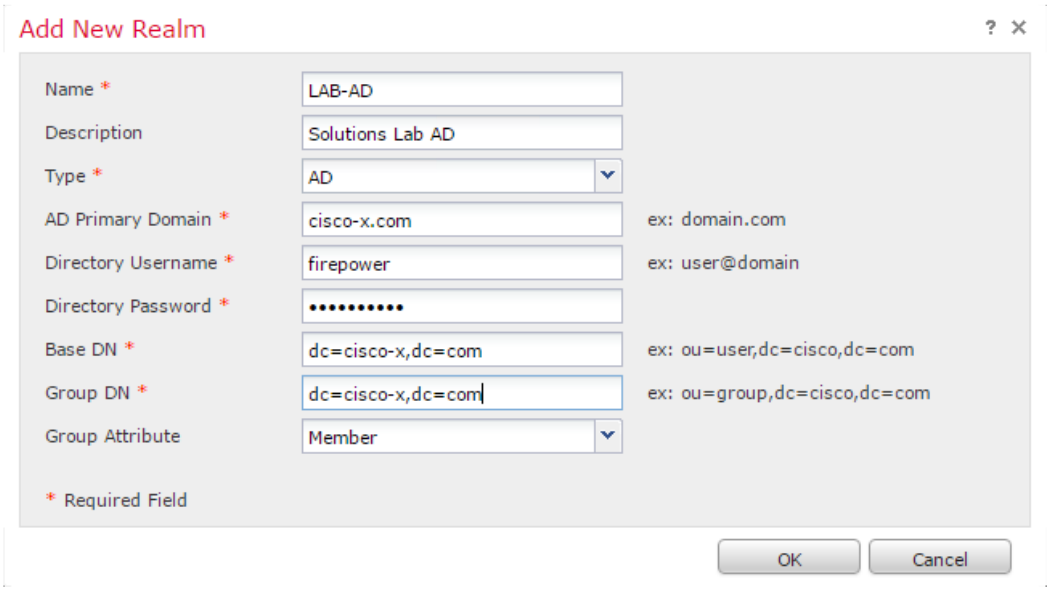

Рис.3.29. Налаштування області центру керування Firepower

Крок 5. В щойно створеній області можна «Додати каталог», та внести дані щодо імені хосту для сервера AD: activedirectory.cisco-x.com

Крок 6. Далі, необхідно обрати LDAP для безпечного з'єднання, завантажити та обрати відповідний сертифікат [23].

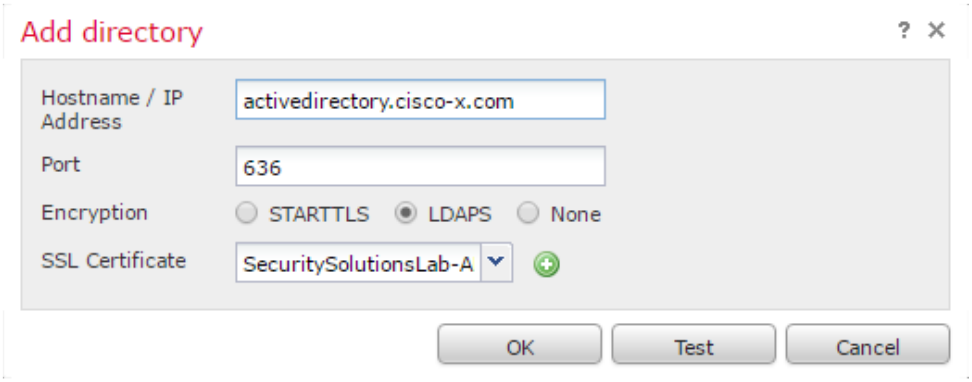

Рис.3.30. Додавання каталогу до AD

Крок 7. При виборі опції «Перевірити», можна перевірити підключення.

Крок 8. У вкладці «Завантаження користувача» можна обрати групи, які потрібно включити/виключити.

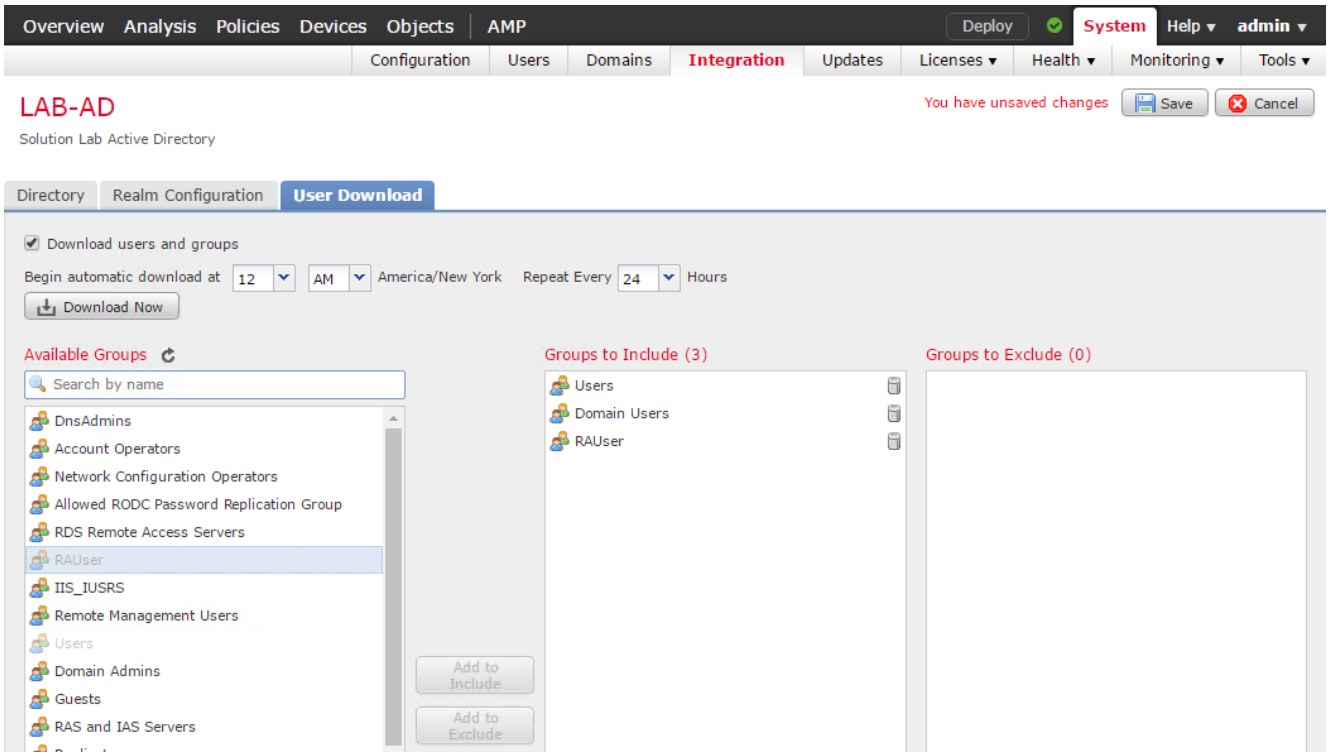

Рис.3.31. Перевірка підключення

Крок 9. Натиснувши «Зберегти» у верхньому правому куті, можна перейти до наступного кроку, а саме - «Налаштування інтеграції ISE».

3.4.3 Налаштування інтеграції ISE

Крок 1. Налаштування починаються з вибором вкладки «Система», а далі – «Інтеграція»

Крок 2. При відкриванні вкладки «Джерела ідентифікаційних даних», необхідно обрати «Identity Services Engine» для типу служби, щоб увімкнути підключення ISE.

Крок 3. Введення даних щодо імені та IP-адреси основного хосту ISE.

Крок 4. Необхідно обрати відповідні центри сертифікації з pxGrid Server CA та MNT Server (розкривні списки CA) та відповідний сертифікат із розкривного списку FMC Server Certificate (рис.3.32).

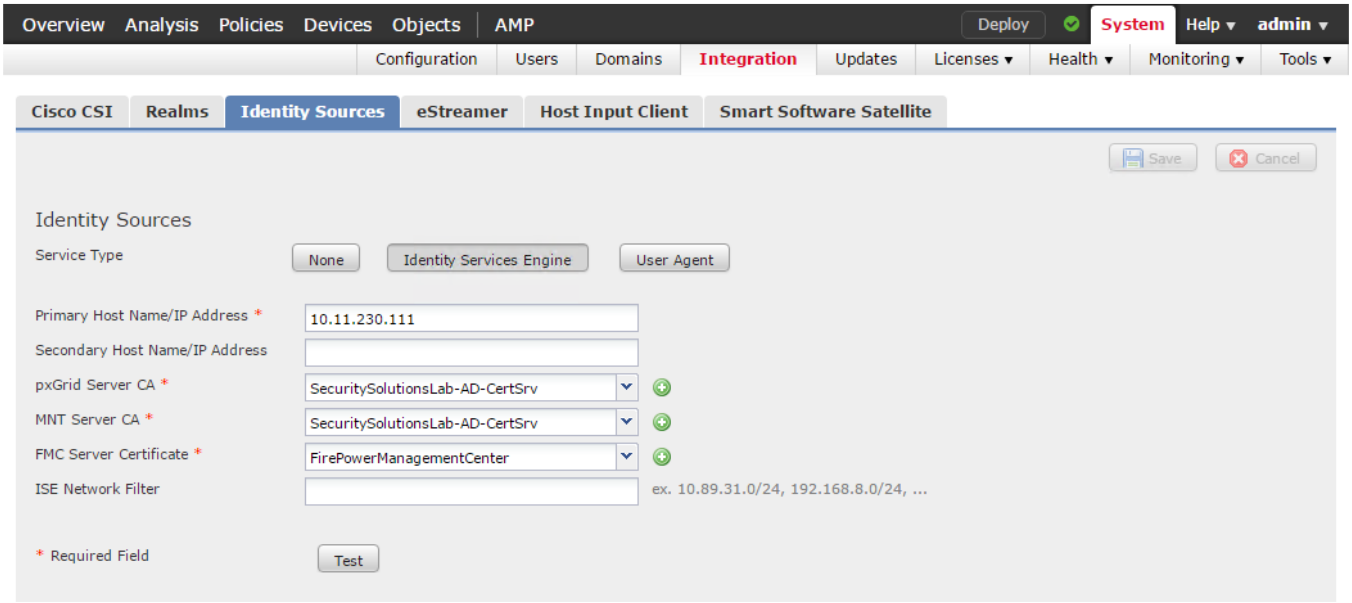

Рис.3.32. Вибір центрів сертифікації

Крок 5. При натисканні «Перевірити», можна перевірити підключення, а потім зберегти інформацію у верхньому правому куті натиснувши «Зберегти» [19].

3.4.4 Налаштування політик ідентифікації

Крок 1. У FMC необхідно перейти до вкладинки «Політика», далі - «Контроль доступу» - «Ідентифікація».

Крок 2. Натиснувши «Додати політику» у верхньому правому куті, потрібно ввести описову назву: «Lab-ISE-Policy», та зберегти внесені дані.

Крок 3. Натиснувши «Додати правило», обирається «Дія», та «Пасивна автентифікація».

Крок 4. Обрати «Realm»: Lab-AD, та зберегти внесені зміни.

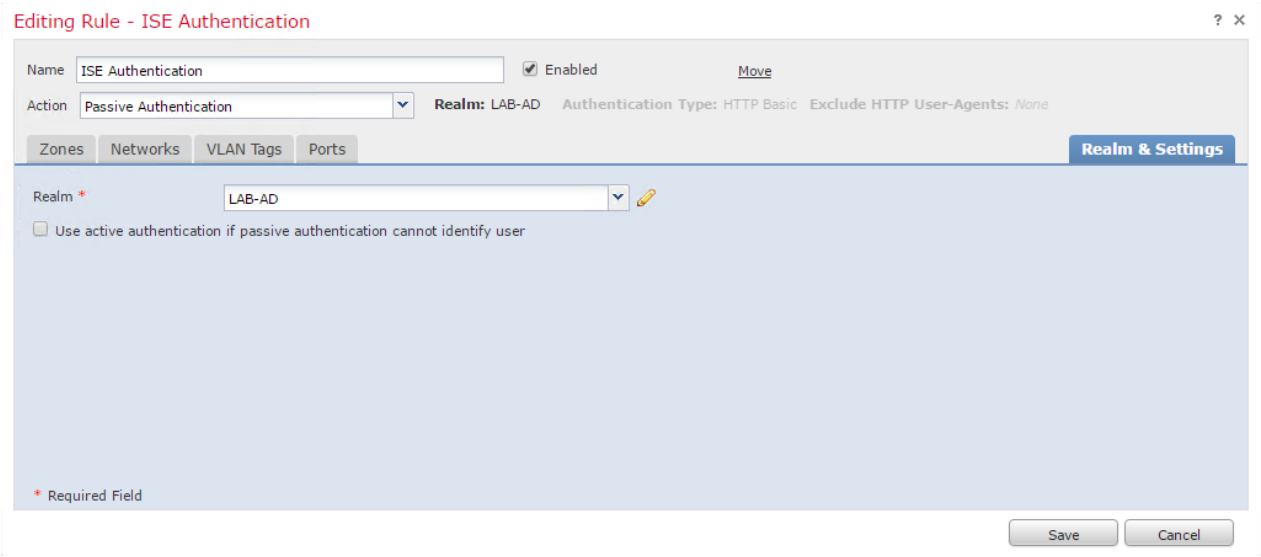

Рис.3.33. Внесення змін щодо пасивної автентифікації

3.4.5 Політика контролю доступу

Наступні кроки описують основну політику контролю доступу, реалізовану для тестування.

Реалізація виробництва вимагатиме повнішого набору правил, щоб відповідати додатковим випадкам використання і прийнятні профілі ризику [20].

Крок 1. У FMC обрати «Політики», далі - «Контроль доступу».

Крок 2. Натиснути «Нова політика» у верхньому правому куті, та ввести ім’я для політики: «Internet Edge Perimeter»

Крок 3. Обрати цільовий пристрій FTD-IE-HA та натиснути «Додати до політики».

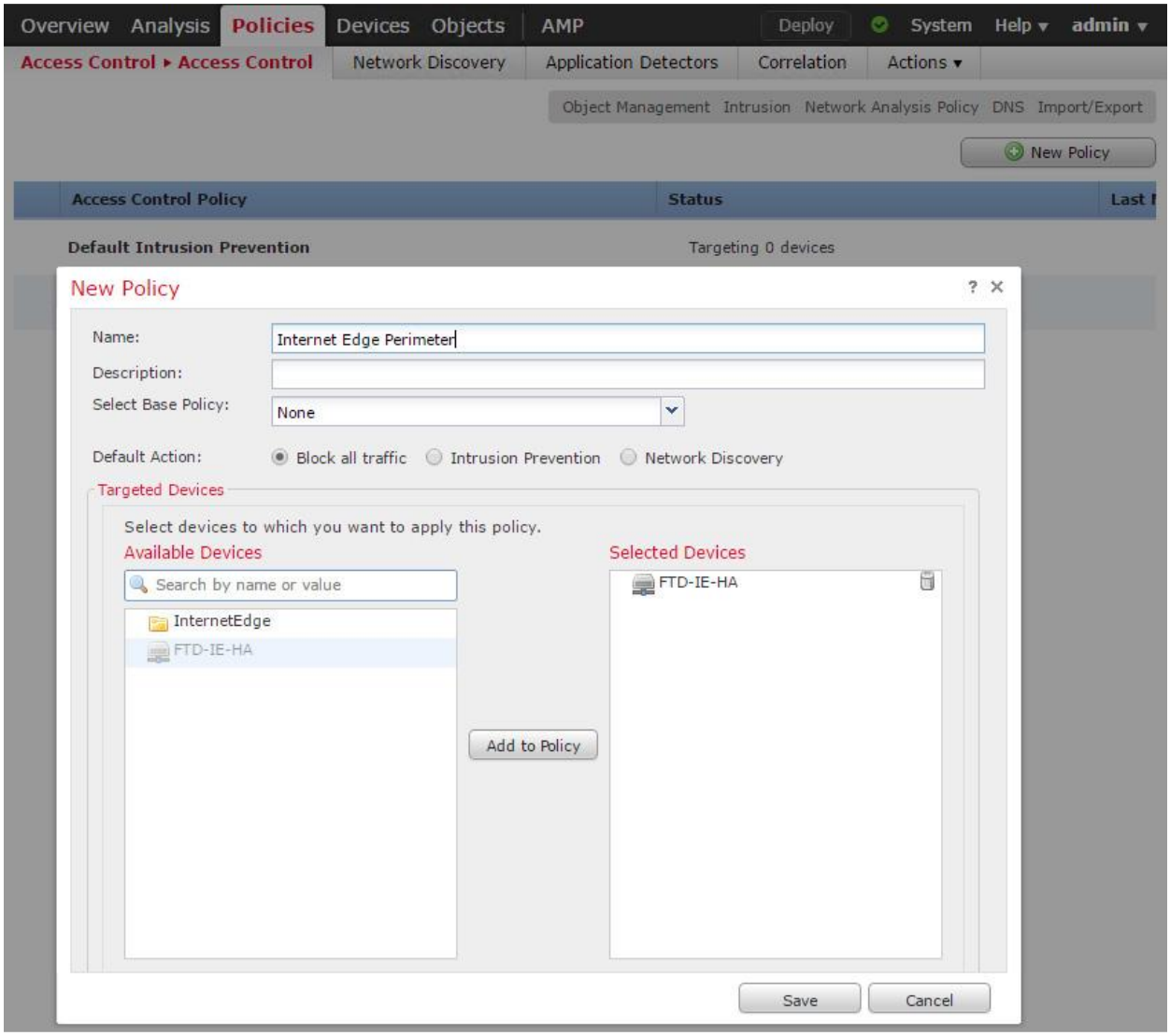

Рис.3.34. Внесення даних щодо політики контролю доступу

Крок 5. Зберегти внесені зміни. Після створення нової політики необхідно відредагувати її, щоб додати правила та зв’язати щодо інших політик (рис.3.35).

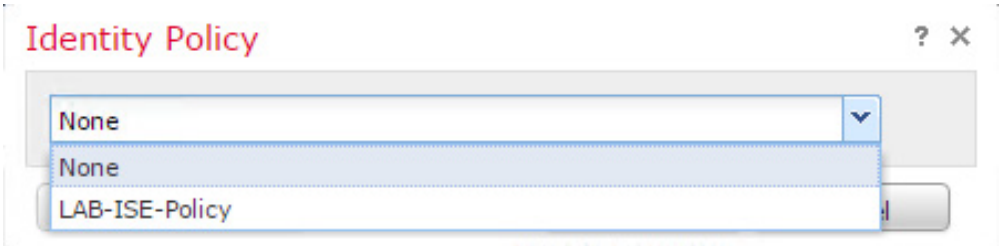

Рис.3.35. Редагування політики контролю доступу

Крок 6. Обравши вкладинку «Політика ідентифікації: немає», потрібно відмітити відповідну політику ідентифікації, та зберегти зміни (рис.3.36).

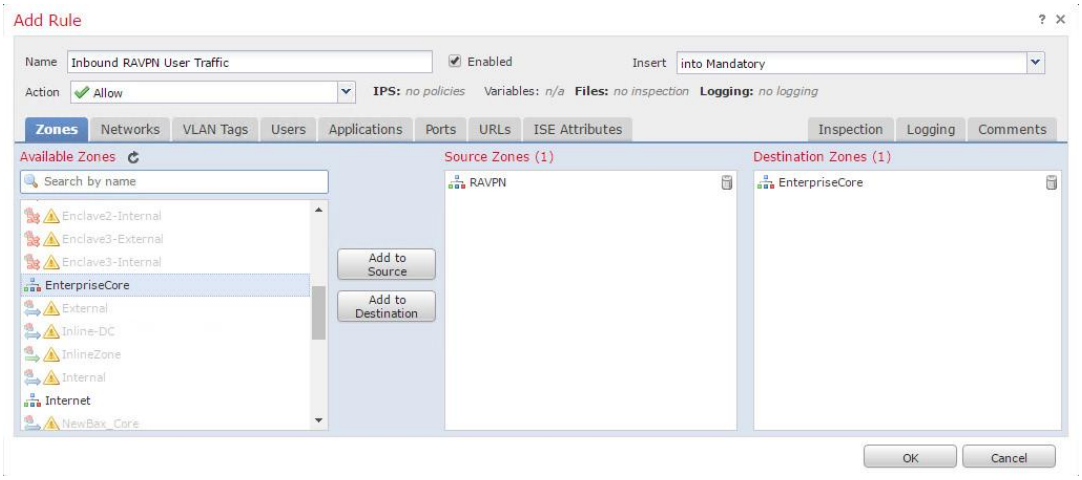

Рис.3.36. Призначення інформації щодо відповідності користувачів

Крок 7. Наступним кроком неохідно додати правило щодо функціонування політики. Ввести відображуване ім’я: вхідний трафік користувача RA VPN, та призначити відповідні зони джерела та призначення (рис.3.37)

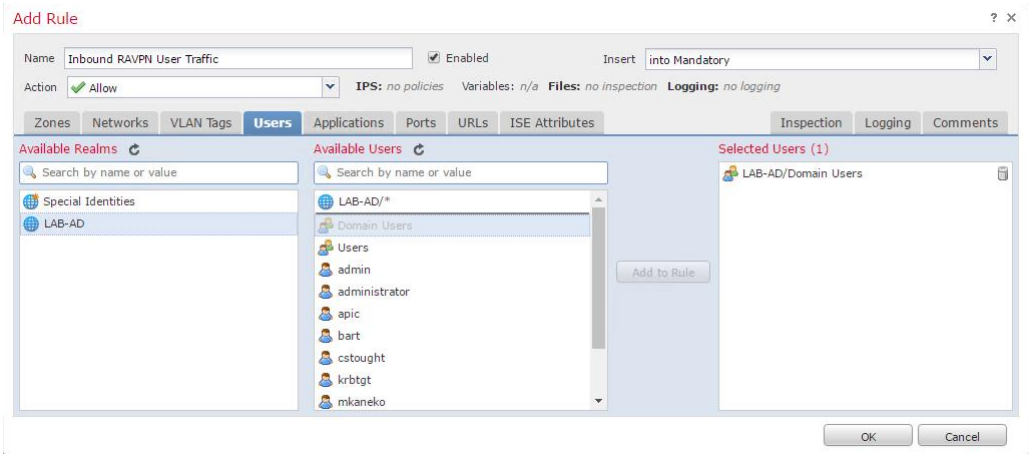

Рис.3.37. Блокування небажаних URL-адрес

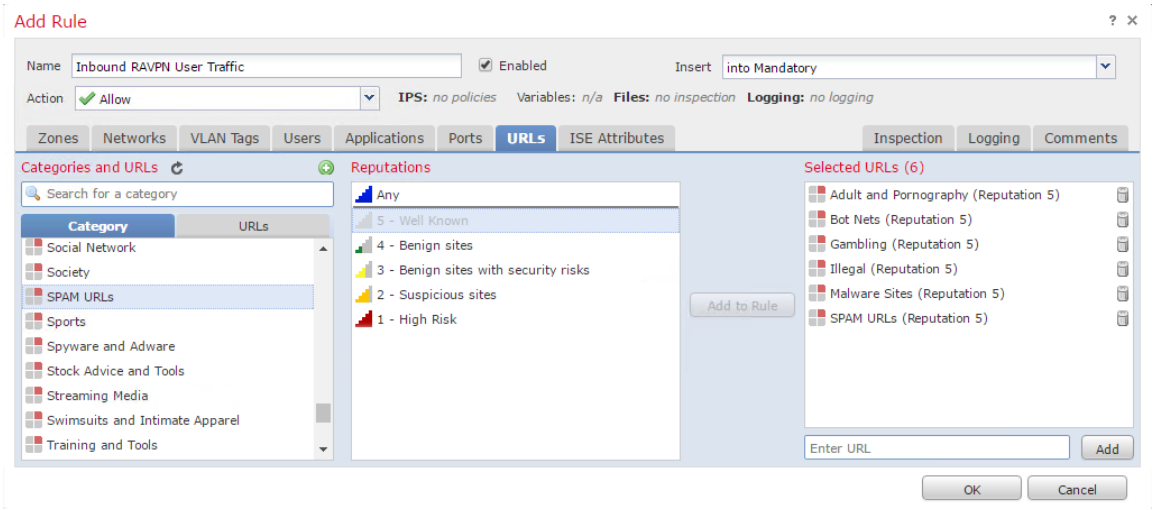

Рис.3.38. Призначення відповідної політики вторгнення

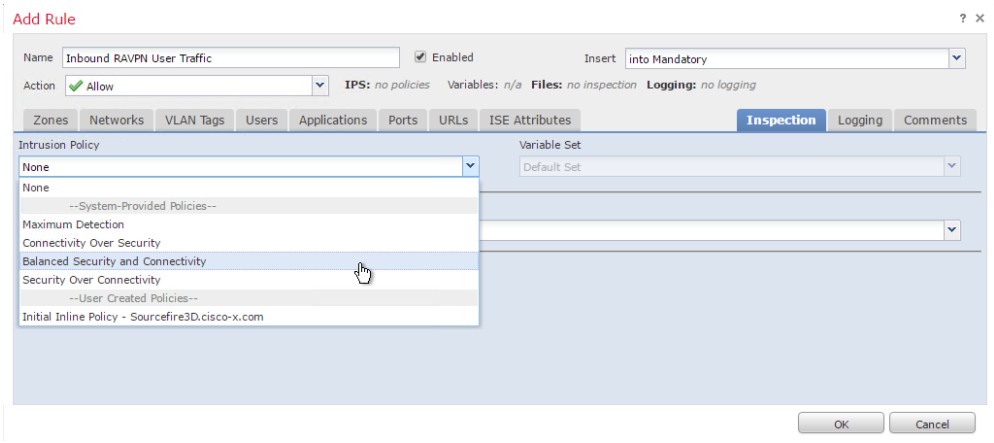

Рис.3.39. Внесення інформації щодо журналу підключень

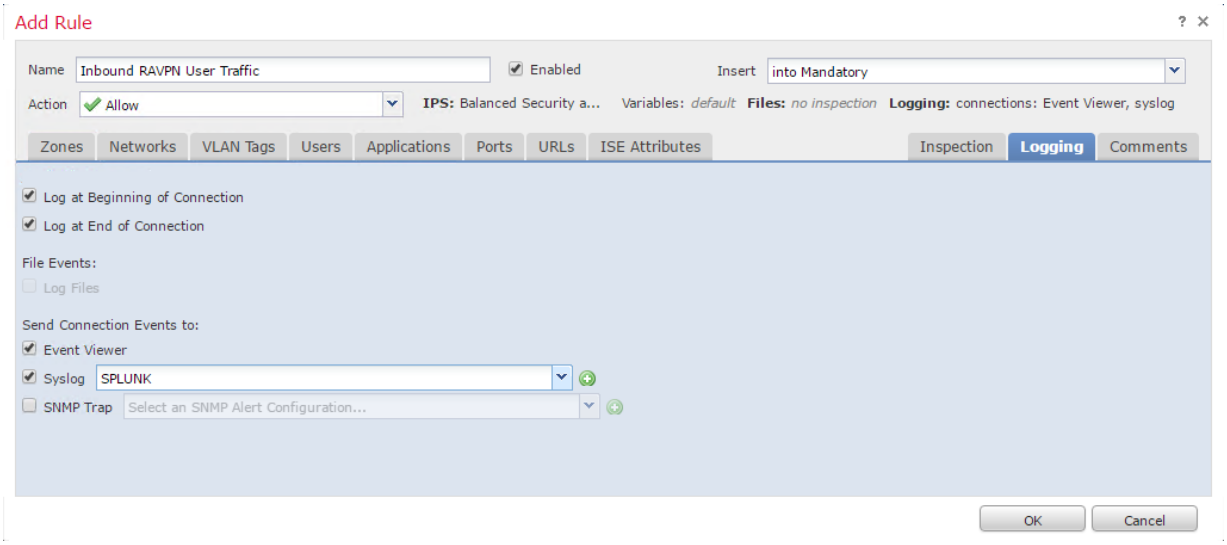

Рис.3.40. Внесення інформації щодо логінгу (ведення журналу) для підключень

Крок 8. Після внесення інформації (рис.3.38, 3.39 та 3.40), потрібно натиснути «ОК», щоб завершити додавання правила. Зберегти зміну інформації.

3.5 Перевірка тестування

Перевірка включає різноманітні тести для перевірки функціональності розгорнутих можливостей. DDoS, AnyConnect VPN і відновлення після відмови були протестовані та працювали задовільно.

Таблиця 3.2

Сценарії тестування

Тестування	Методика
Зв’язок між клієнтами AnyConnect і Firepower 9300 із запущеним кодом ASA	З зовнішнього боку AnyConnect (ПК, iOS та інша платформа) створюється сеанс VPN до FP9300 із запущеним кодом ASA
Безклієнтська перевірка SSL VPN	Налаштування Clientless VPN за допомогою різних браузерів для доступу до внутрішніх серверів
Збій і відновлення Physical Firepower 9300	У цьому сценарії збою Firepower 9300 вручну вимикається і відновлюється живлення головного пристрою ASA, щоб ініціювати збій
Помилка зв’язку для відновлення після відмови FP9300	Помилка та відновлення наступних посилань: • помилка зв'язку даних з Master; • помилка обох каналів передачі даних до Master; • помилка зв’язку даних із Slave; • помилка обох каналів передачі даних до Slave.
Управління транспортними потоками	Забезпечення централізованого доступу до керування через приватну VLAN і правила контролю доступу брандмауера
Інтеграція Cisco Identity Services Engine (ISE).	Підтвердження інтеграції ISE з компонентами: служби автентифікації та авторизації ISE в усій інфраструктурі; перемикання Nexus; домен UCS; платформи FP9300/ASA; інтеграція служби каталогів; служби Microsoft Active Directory
RadWare vDP (Virtual Defense Pro) з ASA, що працює в FP9300	Переконатися, що vDP забезпечить захист від шлюзу VPN FP9300 від DDoS-атаки

Підсумок проведених тестів. Тести призначені для перевірки інтеграції та загальної функціональності VPN для віддаленого доступу. Загальна структура архітектури базується на дизайні Cisco SAFE Internet Edge[24].

Таблиця 3.3

Підсумок результатів

Опис тесту	Компоненти	Результат
Підключення AnyConnect до Firepower 9300 з автентифікацією ISE	• AnyConnect • FP9300 • ISE	Успішно встановлено з'єднання SSL VPN за допомогою ISE як сервера автентифікації з Active Directory Переривання трафіку та повідомлення системного журналу не записано
Збій зв'язку FP9300 на каналі передачі даних	• FP9300	Відсутність переривання трафіку та вихід системного журналу сповіщень із прийнятною втратою пакетів
Radware DDoS тест	• FP9300 • AnyConnect •RadWare vDP	На IP-адресу шлюзу було ініційовано кілька типів DDoS-атак. vDP успішно ідентифікував атаки та скинув пакет для захисту шлюзу VPN
Інтеграція IPS	• FP9300 • ASA5555	ASA5555 під керуванням Firepower Threat Defense успішно захищає мережу за допомогою функцій IPS після того, як трафік VPN розшифровується FP9300 під керуванням образу ASA

Висновки до 3 розділу

Зазначено, що топологія VPN при використанні Cisco SAFE включає принаймні два засоби безпеки Firepower 9300 або 4100, що працюють з програмним забезпечення ASA з Radware DDoS Virtual Defense Pro.Підкреслено, що образ розгорнуто як активний компонент із високою доступністю при налаштуванні.

Приведено покроковий алгоритм налаштування Firepower 9300 та головних складових, в тому числі і політик безпеки.

Проведено тестування з перевіркою результатів із функціональності розгорнутих можливостей. DDoS, AnyConnect VPN і відновлення після відмови були протестовані та працювали задовільно.

Виокремлено, що:

— при тестуванні зв’язку між клієнтами AnyConnect і Firepower 9300 із запущеним кодом ASA із зовнішнього боку AnyConnect (ПК, iOS та інша платформа) створюється сеанс VPN до FP9300 із запущеним кодом ASA;

— при сценарії збою і відновлення Physical Firepower 9300 - Firepower 9300 вручну вимикається і відновлюється живлення головного пристрою ASA, щоб ініціювати збій;

— при інтеграція Cisco Identity Services Engine (ISE) – підтверджується інтеграція ISE з компонентами: служби автентифікації та авторизації ISE в усій інфраструктурі; платформи FP9300/ASA; інтеграція служби каталогів; служби Microsoft Active Directory;

— при управлінні транспортними потоками - забезпечується централізований доступ до керування через приватну VLAN і правила контролю доступу брандмауера.

Як висновок зазначено, що загальна структура архітектури тестування базується на дизайні Cisco SAFE Internet Edge. Перевірка інтеграції та загальної функціональності VPN для віддаленого доступу виконується без збоїв та аномалій. ASA5555 під керуванням Firepower Threat Defense успішно захищає мережу за допомогою функцій IPS після того, як трафік VPN розшифровується FP9300 під керуванням образу ASA

ВИСНОВКИ

В магістерській роботі отримано наступні наукові та науково-практичні результати:

1. Проаналізовано особливості розгортання Cisco SAFE, приведено деталізацію складових компонентів, та зазначено що дана модель здатна бути переналаштованою під вимоги корпоративної мережі компанії, які є найбільш актуальними.

2. Виокремлено характеристику загальних функціональних засобів контролю в корпоративній мережі, а також приведено діаграму можливостей бізнес-потоків для організації, яка використовується як основа для наступного етапу розгортання Cisco SAFE – побудови архітектури безпеки для корпоративної мережі.

3. Досліджено особливості поділу корпоративної мережі на логічні області із використанням Cisco SAFE. Виокремлено наступні області: відділення (філія); кампус; WAN; Центр обробки даних; Edge; Cloud.

4. Приведено перелік найпопулярніших загроз та вразливостей, які притаманні виокремленими логічним областям, та перераховано перелік засобів та технологій Cisco SAFE, які здатні нейтралізувати загрозу, пом’якшити або сповістити про вразливість чи аномалію.

5. Зазначено, що топологія VPN при використанні Cisco SAFE включає принаймні два засоби безпеки Firepower 9300 або 4100, що працюють з програмним забезпечення ASA з Radware DDoS Virtual Defense Pro.Підкреслено, що образ розгорнуто як активний компонент із високою доступністю при налаштуванні.

6. Приведено покроковий алгоритм налаштування Firepower 9300 та головних складових, в тому числі і політик безпеки.

7. Проведено тестування з перевіркою результатів із функціональності розгорнутих можливостей. DDoS, AnyConnect VPN і відновлення після відмови були протестовані та працювали задовільно.

8. Виокремлено, що:

- при тестуванні зв’язку між клієнтами AnyConnect і Firepower 9300 із запущеним кодом ASA із зовнішнього боку AnyConnect (ПК, iOS та інша платформа) створюється сеанс VPN до FP9300 із запущеним кодом ASA;
- при сценарії збою і відновлення Physical Firepower 9300 - Firepower 9300 вручну вимикається і відновлюється живлення головного пристрою ASA, щоб ініціювати збій;
- при інтеграція Cisco Identity Services Engine (ISE) – підтверджується інтеграція ISE з компонентами: служби автентифікації та авторизації ISE в усій інфраструктурі; платформи FP9300/ASA; інтеграція служби каталогів; служби Microsoft Active Directory;
- при управлінні транспортними потоками - забезпечується централізований доступ до керування через приватну VLAN і правила контролю доступу брандмауера

9. Як висновок зазначено, що загальна структура архітектури тестування базується на дизайні Cisco SAFE Internet Edge. Перевірка інтеграції та загальної функціональності VPN для віддаленого доступу виконується без збоїв та аномалій. ASA5555 під керуванням Firepower Threat Defense успішно захищає мережу за допомогою функцій IPS після того, як трафік VPN розшифровується FP9300 під керуванням образу ASA.