ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВІДДАЛЕНИМ КОРИСТУВАЧАМ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ»

на здобуття освітнього ступеня магістра

зі спеціальності _____125_____

Кібербезпека_____
(код, найменування спеціальності)

освітньо-професійної програми_Інформаційна та кібернетична безпека____
(назва)

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

_____ ЄВТУШЕНКО Борис

Виконав: здобувач вищої освіти групи БСДМ-63

ЄВТУШЕНКО Борис
(ПРІЗВИЩЕ, ім'я)

Керівник
к.т.н, доцент СОБЧУК Андрій
(ПРІЗВИЩЕ, ім'я)

Рецензент
к.т.н, доцент _____
(ПРІЗВИЩЕ, ім'я)

КИЇВ – 2024

ВСТУП

Актуальність дослідження. Кожна сучасна організація, що використовує ІТ-технології, потребує якісної та ретельно захищеної мережі. ІТ-безпека є ключовим фактором нормального функціонування всієї організації та всіх окремих підрозділів. Існують різні методи та концепції, що здатні забезпечувати суттєвий, високий рівень інформаційної безпеки. Деякі є досить важливими і повинні бути реалізовані в кожній сучасній корпоративній мережі, адже і її межах та поза ними надається велика кількість послуг.

Тенденції останніх років вимагають надавати можливість не лише фізичної присутності працівників організації на робочих місцях, але й можливість якісної та безпечної дистанційної роботи. Зростають і вимоги до дистанційного доступу до таких служб, як: веб-служби, поштові та файлові служби, банкінг, доступ до БЗ та спеціалізованого ПЗ тощо. З іншого боку, кількість можливих проблем безпеки також зростає.

Методи безпеки до кожної із послуг, що надаються, також різні і потребують професійної підтримки та захисту. Лише зміцнення антивірусного ПЗ, покращення ОС та мережевих додатків не гарантує якість підключення віддалених користувачів. Методи налаштування проксі-сервера чи брандмауерів у поєднанні з простими, налаштованими пристроями безпеки можуть бути значно ефективнішими. Тому, вибір правильних технологій та методів при проєктуванні захищеної мережі є важливим та доцільним сьогодні.

Вищенаведені аргументи актуалізують тему даної кваліфікаційної роботи, зміст якої становлять дослідження щодо технології забезпечення кібербезпеки віддаленим користувачам корпоративної мережі організації.

Об’єкт дослідження – процес безпечного функціонування корпоративної мережі.

Предмет дослідження – технології та рішення безпечного з'єднання віддалених користувачів з корпоративною мережею.

Мета роботи – розробка комплексного рішення для забезпечення безпеки підключення віддалених користувачів до ресурсів корпоративної мережі.

Наукові завдання:

- проаналізувати особливості розгортання сучасних корпоративних мереж;
- проаналізувати підходи до забезпечення безпеки корпоративної мережі;
- дослідити мережеве обладнання для проєктування корпоративної мережі;
- дослідити налаштування рішень для безпечної роботи віддалених працівників в корпоративній мережі;
- розробити комплексне рішення для забезпечення безпеки підключення віддалених користувачів до ресурсів корпоративної мережі.

Методи дослідження – стандарти кібербезпеки, методи шифрування та аутентифікації, аналіз систем моніторингу та виявлення інцидентів безпеки, оцінка ризиків віддаленого доступу, теорія інформації.

Практичне значення одержаних результатів полягає в розробці комплексного рішення для забезпечення безпеки підключення віддалених користувачів до ресурсів корпоративної мережі.

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

1 ОСОБЛИВОСТІ РОЗГОРТАННЯ СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖ

1.1. Основні частини корпоративної мережі

Корпоративна мережа, як правило, складається з двох основних частин: периферійної (або граничної) мережі та внутрішньої мережі. Периферійна мережа визначається як та частина мережі, що забезпечує з'єднання з іншими мережами через WAN (Wide Area Network, або широкосмугова мережа). Внутрішня мережа забезпечує зв'язок всередині корпорації і підключається до периферії через одне або декілька мережевих з'єднань (рис.1.1).

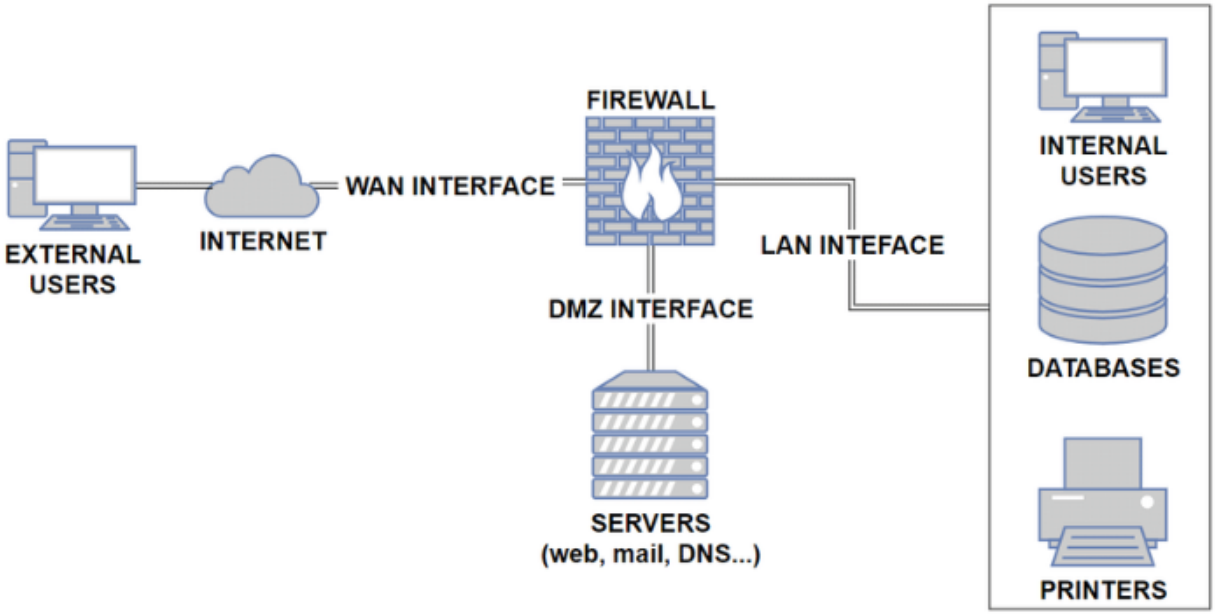

Рис.1.1. Приклад реалізації архітектури корпоративної мережі

Основні компоненти більшості внутрішніх мереж включають клієнтські хости, сервери відділів, центральні сервери, пристрої керування та інфраструктуру комутованих та маршрутизованих мереж.

Гранична мережа. Деякі з корпоративних мереж можуть мати більше однієї периферійної мережі. Кількість периферійних мереж залежать від вимог та послуг, що надаються всередині та за межами всієї організації.

Основні компоненти граничній мережі це:

• Приватні канали глобальної мережі – для надання та отримання послуг;

• Підключення до Інтернет - для отримання спеціалізованих послуг і доступу до мережі Інтернет;

• Загальнодоступні сервери - сервери для надання послуг, які доступні з зовнішніх мереж і з внутрішньої мережі;

• Site-to-site VPN – приватні «тунелі» для підключення окремих «гілок» або офісів корпоративної мережі;

• VPN-тунелі віддаленого користувача - для підключення подорожуючих і віддалених користувачів до корпоративних ресурсів, таких як системи ERP та інші служби;

• Комутована телефонна мережа загального користування (ТмЗК/PSTN) – додатковий спосіб для підключення подорожуючих і віддалених користувачів. Філії та офіси також можна дистанційно підключити черезТмЗК;

• Екстранет-підключення - для резервного копіювання та підключення деяких корпоративних партнерів;

• Мережі електронної комерції – ці мережі призначені лише для корпорацій, що надають послуги електронної комерції. Однак вони можуть підключити до граничної мережі різні типи посилань, але їх слід відокремити від іншої частини мережі з використанням додаткового маршрутизатора або брандмауера [1].

Внутрішня мережа. Частина мережі підключена до периферійної мережі через одну або кілька мереж. У цій частині розміщені всі корпоративні сервери для внутрішніх служб і всі робочі станції системи, за винятком тих, які підключаються до мережі через VPN.

Усі основні частини внутрішніх корпоративних мереж включають:

• Клієнтські хости – комп’ютери кінцевих користувачів, робочі станції тощо;

• Сервери відділів - сервери та програми, які обмежені для деяких з користувачів у внутрішній мережі;

• Центральні сервери – сервери та програми, доступні всім користувачам (сервер електронної пошти, сервер служби доменних імен (DNS), веб-сервер, файловий сервер тощо);

• Пристрої керування – усі пристрої, які мають функції моніторингу різних типів послуг і протоколів, які використовуються. Більшість пристроїв використовують простий протокол керування мережею (SNMP) або інший для спеціального моніторингу подій безпеки;

• Комутована/маршрутизована мережева інфраструктура - усі маршрутизатори, усі комутатори Ethernet, IDS, брандмауери та інші інфраструктурні пристрої, які забезпечують зв’язок між внутрішньою мережею, периферійною мережею та зовнішніми мережами[2].

1.2. Актуальність питання корпоративної безпеки

ІТ-безпека – це захист систем, ресурсів та інформації від ненавмисного і несанкціонованого доступу або неправомірного використання. Огляд найбільш розголошених атак за останні роки вказує на те, що безпека мережі відіграє важливу роль у досягненні попередньо виокремлених цілей.

Крім того, ІТ-додатки, а останнім часом і Інтернет-додатки, стають дедалі більш критично важливими для організацій. Складність цих програм, поряд з операційними системами та обчислювальними платформами, на яких вони працюють, роблять їх вразливими до атак, загроз та нападів. Оскільки додаток часто контролює доступ до інформації, безпека програми набуває більшої важливості.

Мережа забезпечує канал для взаємодії користувачів із програмою та з даними. З цього випливає, що безпека мережі є обов’язковою, як перший рядок захисту в ІТ-безпеці організації чи корпорації. Без захищеної мережі програми та

інформація можуть зазнавати постійних негативних впливів з боку безлічі хакерів та зловмисників.

Окрім чинного списку актуальних загроз та атак, сучасні інженери із мережевої безпеки стурбовані вразливістю новітніх мережевих технологій. В останні кілька років, VPN (та IPSec) рекламувалася як більш економічно ефективна і гнучка технологія для безпечного підключення користувачів та клієнтів (рис.1.2).

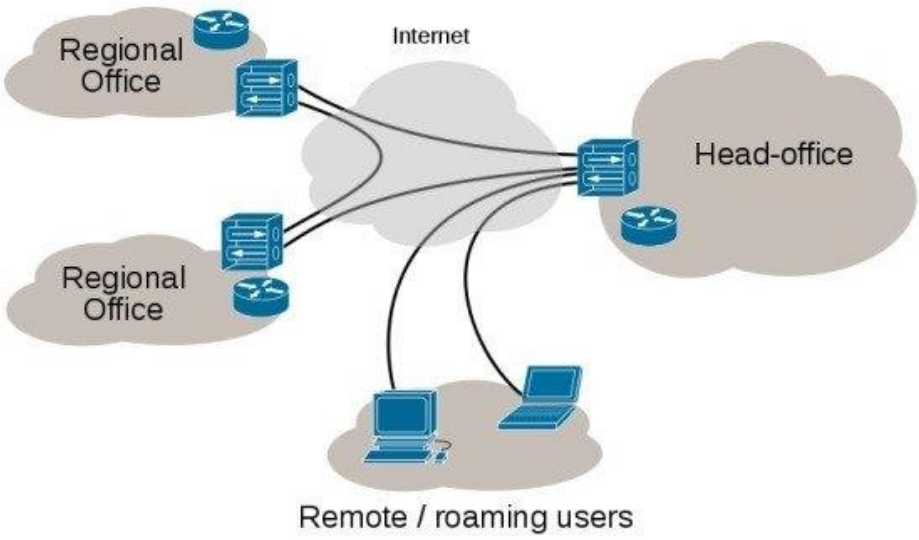

Рис.1.2. Схематичне представлення використання VPN

Звичайно, механізми шифрування та автентифікації, зазначені в IPSec забезпечує надійну техніку для захисту конфіденційності переданих даних інформації, але збільшення кількості підключень до мережі Інтернет розширює вразливі сегменти мережі[3].

Подібним чином, в безпроводових локальних мережах виокремлено цілий набір нових вразливостей, наприклад можливості неавторизованого доступу до корпоративної мережі через відкриті мережі Wi-Fi. Зловмисникам потрібно лише бути всередині компанії, щоб отримати доступ до середовища передачі інформації.

Тому, щоб підтримувати безпеку корпоративної мережі, інженер-проектувальник повинен одночасно інтегрувати постійно оновлювальні технології безпеки, найкращі практики та хорошу надійність стратегії, оскільки кожна нова технологія впроваджується в мережу.

1.3. Ключові послуги в корпоративних мережах

Служби електронної пошти. Коли в організації намагаються надати захищені послуги електронної пошти, необхідно врахувати два основні аспекти - відокремлення серверів вхідної та вихідної пошти та надання якісного антивірусу (або іншого, аналогічного ПЗ) для сканування. Розміщення центрального антивірусного сервера в центрі обробки даних є кращим рішенням встановлення поштового антивірусного програмного забезпечення на кожному з комп'ютерів користувачів, через управління оновленнями

Базовий дворівневий дизайн електронної пошти. На рис.1.3 показано схему з внутрішнім і зовнішнім поштовими серверами. Цей дизайн хороший вибір для середніх і малих організацій, які хочуть мати власні поштові сервери.

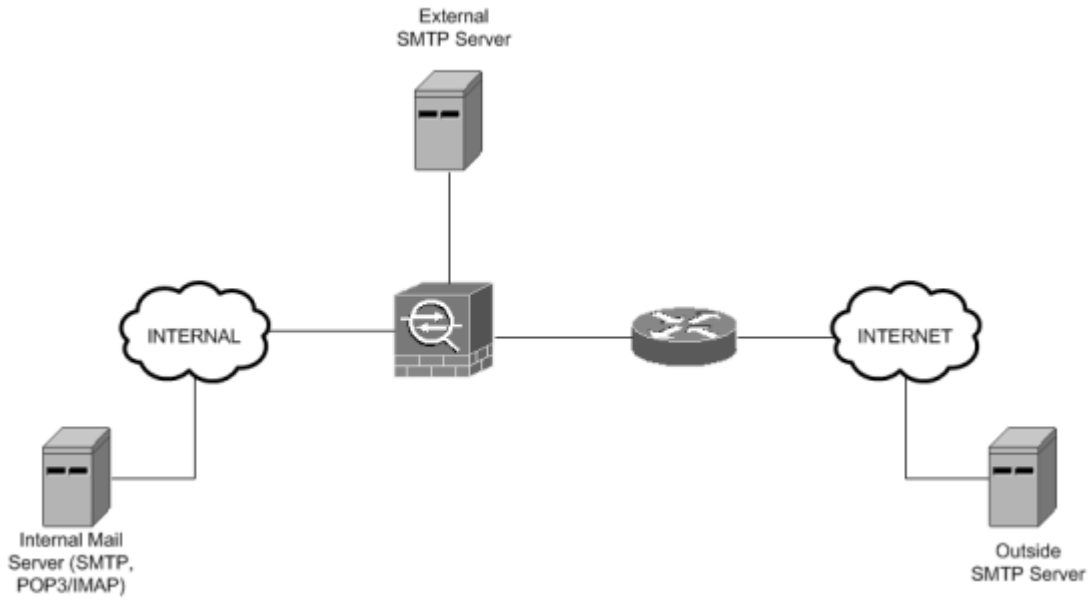

Рис.1.3. Базовий дворівневий дизайн електронної пошти

Зовнішній сервер може надсилати пошту лише на зовнішній SMTP і може доставляти повідомлення на внутрішній поштовий сервер. Зовнішній використовує сервер і коли необхідно надіслати листи з внутрішньої мережі на Інтернет, можна заблокувати весь інший трафік SMTP. Це своєрідна гарантія, що листи будуть відправлятися тільки з реальних корпоративних серверів[4].

Внутрішній поштовий сервер має дві основні функції - маршрутизувати повідомлення всередині внутрішньої мережі та надсилати повідомлень на зовнішній сервер SMTP, а також для використання внутрішніми користувачами щоб отримати свою пошту через протоколи POP3 або IMAP. Можна додати антивірусний сервер до цієї топології або встановити антивірусне програмне забезпечення на розташованих серверах.

Дворівневий дизайн розподіленої електронної пошти. На рис.1.4 показано дизайн розподіленої електронної пошти. Така реалізація складніша, і притаманна для імплементації у великих організаціях.

До основних відмінностей з базовим дворівневим дизайном електронної пошти можна віднести:

- Відділення внутрішніх вхідних серверів (POP3 та IMAP) від вихідних сервер (SMTP), який забезпечує більшу масштабованість усієї поштової системи;
- Розміщення виділеного сервера для антивірусної перевірки.

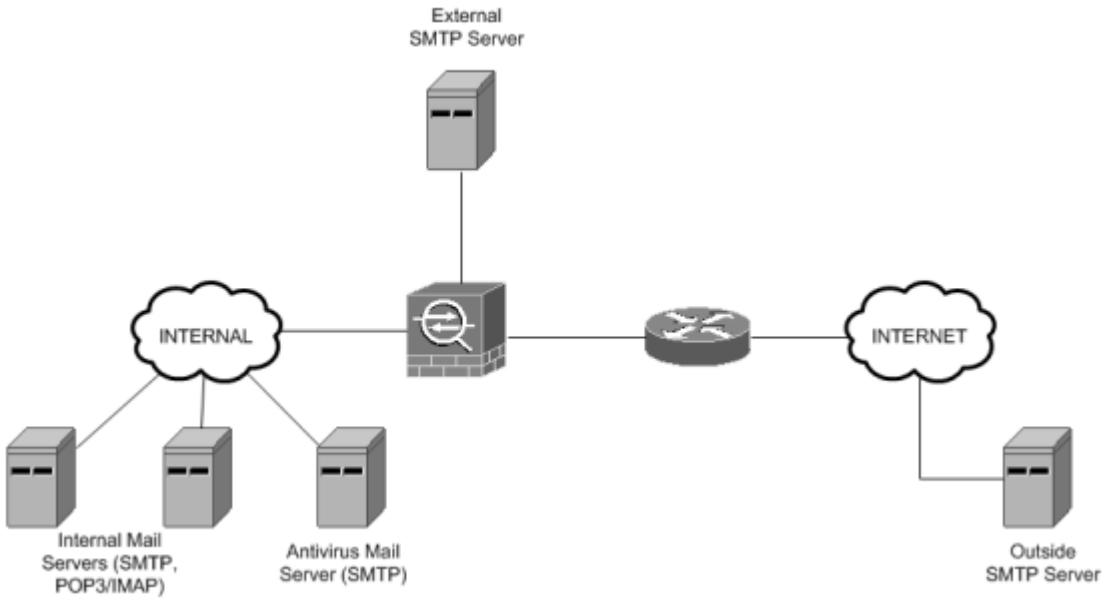

Рис.1.4. Розподілена дворівнева структура електронної пошти

Наявність антивірусного сервера є найважливішою перевагою цього варіанту реалізації, адже він сканує повідомлення від і до внутрішньої мережі. Функція внутрішнього поштового сервера дозволяє внутрішнім користувачам отримувати пошту через протоколи POP3 або IMAP.

- Зовнішній сервер SMTP. Сервер SMTP зберігає ті самі функції, що й у попередньому дизайні.

Служби DNS. Принцип розміщення DNS-серверів схожий на поштові сервери – наявність окремого DNS-сервер для внутрішньої мережі та зовнішнього DNS-сервера.

Кілька перевірених практик щодо проєктування мережевої інфраструктури DNS:

• Усі DNS-сервери мають бути більш відокремленими – потрібно щонайменше два DNS-сервери. Важливо розмістити їх у різних місцях, тому що таким чином вони отримають кращий захист від атак відмови в обслуговуванні (DoS);

• Більш авторитетний DNS-сервер – за допомогою цієї практики забезпечується ще один захист для атак DoS, оскільки зловмисник може спробувати атакувати сервер DNS і таким чином може вплинути/зупинити його роботу;

• Зовнішні DNS-сервери мають функціонувати тільки як сервери, що не виконують рекурсивні запити. Існує два основних типи запитів у DNS: рекурсивні та нерекурсивні. Рекурсивний запит означає, що якщо DNS-сервер не знає відповіді, він запитує інші сервери, щоб знайти потрібну інформацію. Натомість нерекурсивний запит обмежується інформацією, яка вже є в наявності на сервері, і такий сервер не буде звертатися до інших серверів для пошуку відповідей на запити, які він не знає;

• Захист внутрішніх серверів DNS. Для забезпечення безпеки внутрішніх DNS-серверів важливо мати окрему систему для обробки запитів від співробітників і користувачів. Коли зовнішні DNS-сервери налаштовані тільки на нерекурсивну обробку запитів, потрібен внутрішній сервер, який буде виконувати рекурсивні запити. Це можна зробити, використовуючи внутрішній DNS-сервер для обробки запитів, що стосуються внутрішньої мережі, та окремі проксі-сервери (експедитори) для запитів, які виходять за межі корпоративної мережі;

• Для забезпечення безпеки в мережі важливо контролювати передачу зон даних між авторизованими DNS-серверами. Передача зон використовується підлеглими серверами імен, щоб отримувати дані від основних серверів імен. Однак цей процес передачі даних повинен бути обмежений і дозволений лише в необхідних випадках, щоб зменшити ризики безпеки та забезпечити контроль над передачею інформації в мережі.

На рис.1.5. показано найпростіший дизайн DNS. Зовнішній DNS-сервер не є частиною мережі, зазвичай це DNS-сервер провайдера. Головним недоліком такої конструкції є дуже низький рівень безпеки. Якщо знадобиться додатковий захист, можна використовувати деякі функції безпеки програмного забезпечення DNS[5].

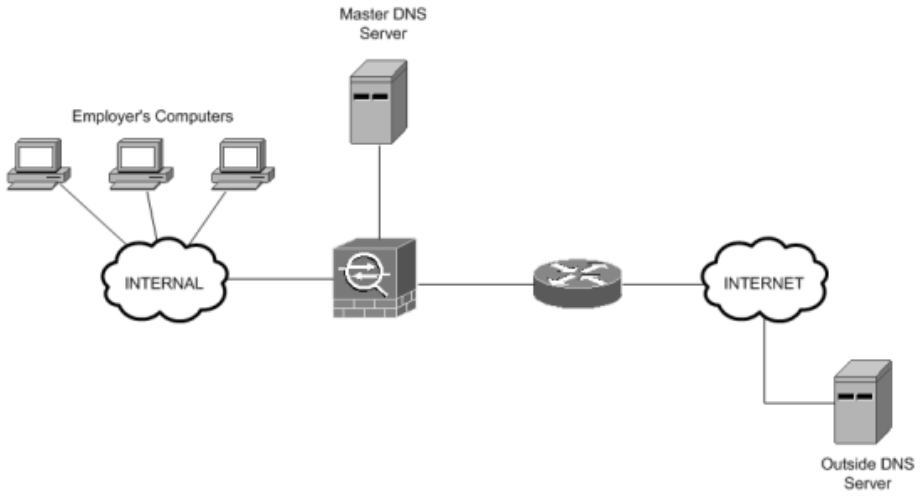

Рис.1.5. Приклад дизайну одного сервера

У цій системі фаєрвол (брандмауер) може захистити DNS-сервер, блокуючи всі порти, крім порту DNS (UDP 53). Такий підхід підходить переважно для невеликих мереж.

На рис.1.6 представлено приклад розподіленої системи DNS. Ця конструкція підходить для компаній середнього та великого розміру. Кількість використовуваних серверів залежить від потреб компанії. Високий рівень безпеки в такій системі досягається за рахунок розділення DNS-серверів.

Безпеку DNS можна покращити, використовуючи різні рівні DNS-архітектури. Якщо внутрішній комп'ютер звертається до свого DNS-сервера, цей

сервер перенаправляє запити, які він сам не може обробити, до спеціалізованої групи серверів. Ці сервери мають дозвіл на виконання запитів за межами внутрішньої мережі.

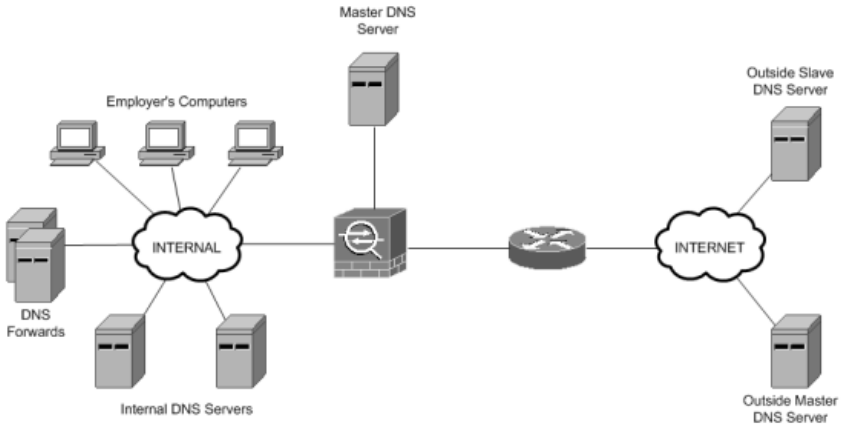

Рис.1.6. Дизайн розподіленого DNS-сервера

Служби HTTP/HTTPS. Безпека веб-сервісів, які працюють через HTTP та HTTPS, залежить від використовуваного програмного забезпечення. Кожен веб-додаток має свої способи для забезпечення безпеки. Конструкція мережі та розташування веб-серверів є ключовими для підвищення безпеки, включаючи налаштування параметрів балансування навантаження.

На рис.1.7 представлено базовий дизайн мережі з веб-сервером. Цей сервер підключений до третього порту фаєрволу, який розділяє внутрішню мережу та Інтернет. Фаєрвол налаштовано так, щоб блокувати усі порти на веб-сервері, дозволяючи лише використання необхідних портів, як-от TCP 80 для HTTP.

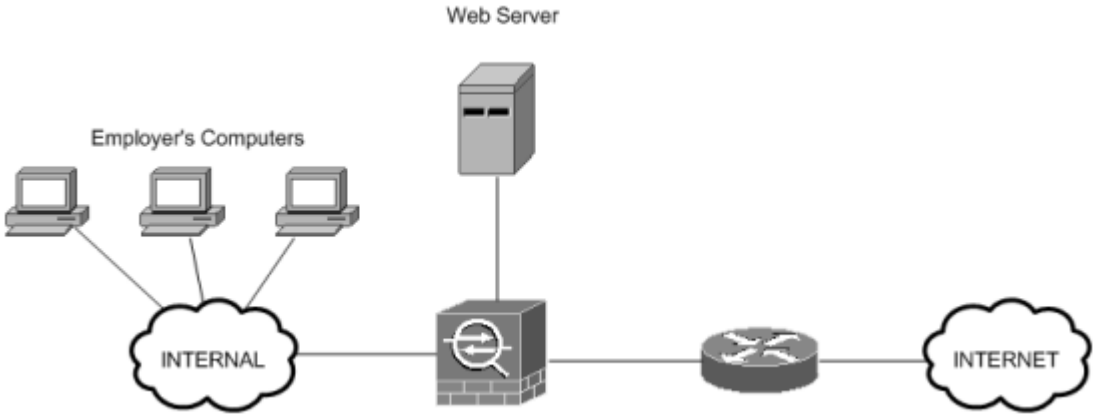

Рис.1.7. Проста конструкція мережі

Для надання послуг з динамічним контентом часто потрібні додаткові компоненти, такі як додатки та, у більшості випадків, сервер бази даних. На рис.1.8 показано структуру, де основний веб-сервер відділений від серверів додатків та баз даних. Таке розділення ускладнює завдання для зловмисників, які бажають вкрасти інформацію або завдати шкоди, оскільки тільки веб-сервер має доступ до серверів додатків і бази даних.

Розміщення всіх серверів в одному сегменті мережі небезпечно, адже якщо зловмисник атакує один сервер, він може легко атакувати інший. Використання приватної віртуальної локальної мережі (VLAN) також не є оптимальним рішенням, оскільки серверам потрібно взаємодіяти між собою[6].

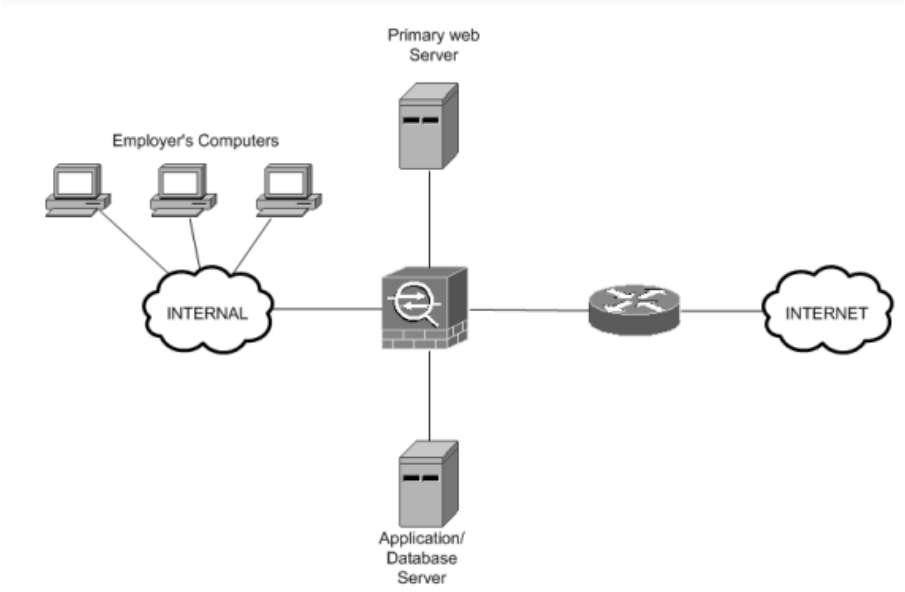

Рис.1.8. Дизайн архітектури Two-Tire

Фаєрвол повинен бути налаштований так, щоб він дозволяв доступ до веб-сервера тільки через специфічні порти (наприклад, TCP 80) і блокував будь-який доступ до серверів додатків та бази даних, якщо трафік не походить від веб-сервера.

Існує два основних способи реалізації трирівневої мережевої структури. Перший варіант використовує два фаєрволи, як показано на малюнку 1.9. Другий підхід передбачає використання трьох фаєрволів, і це демонструється на малюнку 1.10. У цих конструкціях сервери додатків та бази даних відділяються та розміщуються на різних фізичних машинах і в окремих сегментах мережі.

Конфігурація фаєрволів у цих двох варіантах схожа на вищезазначений дизайн, але вона виконується на різних фаєрволах в залежності від того, чи використовуються два чи три фаєрволи у відповідній конструкції.

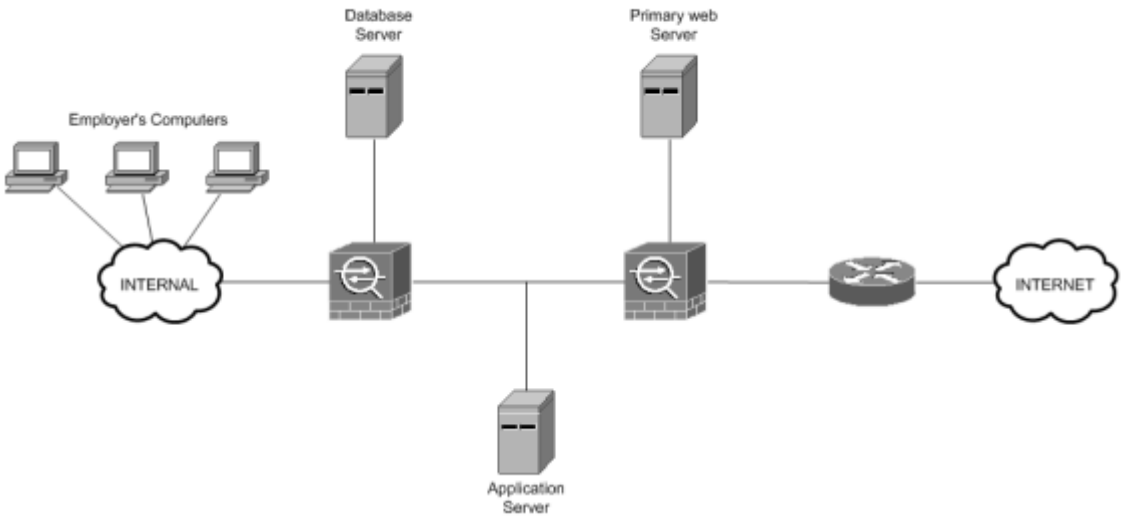

Рис.1.9. Трирівневий дизайн із двома брандмауерами

Конструкція з двома брандмауерами має майже такий же рівень безпеки, як і конструкція з три, але це дешевше.

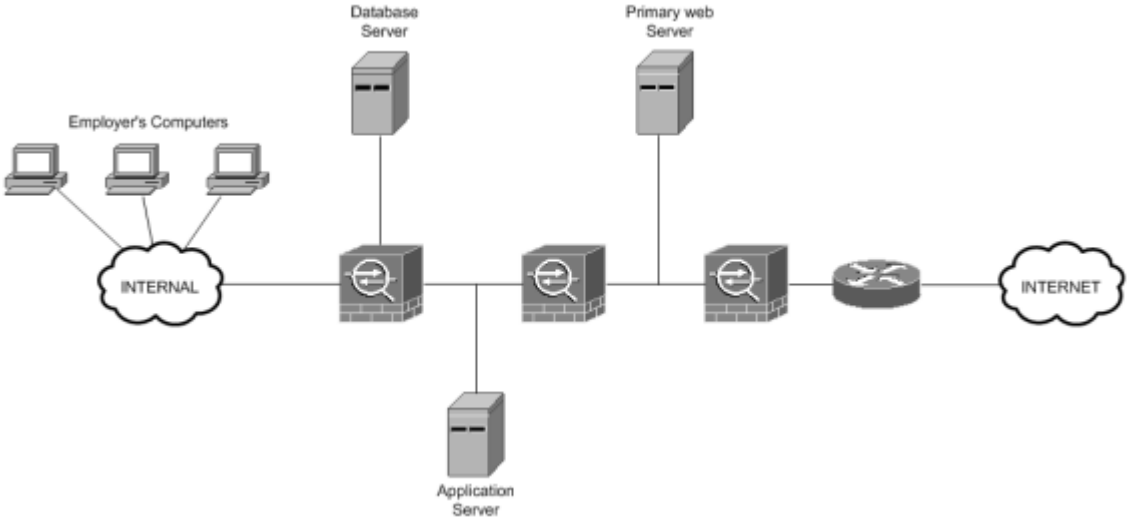

Рис.1.10. Трирівневий дизайн із трьома брандмауерами

Сервіси FTP. FTP-служби використовуються для простої передачі файлів. Безпечнішою альтернативою є SFTP, який базується на SSH. Цю функцію можна інтегрувати в наш веб-сервер для зручного завантаження чи оновлення файлів,

наприклад, для оновлення статичного вмісту веб-сторінок. Існують два режими FTP: пасивний та активний.

Активний режим FTP є стандартним, але може виникнути складнощі при проходженні через фаєрвол. У цьому режимі сервер ініціює з'єднання з клієнтом, що може бути проблематично з точки зору безпеки, особливо якщо фаєрвол не підтримує FTP. У разі наявності сумісного фаєрвола, він буде відслідковувати команди PORT від клієнта та відкривати з'єднання динамічно.

Пасивний режим FTP є безпечнішим, оскільки всі з'єднання ініціюються клієнтом, і сервер не встановлює додаткових з'єднань. Цей режим зазвичай використовують інтернет-браузери для передачі файлів через FTP. Рекомендується використовувати пасивний режим, коли це можливо.

На рис.1.11 представлено приклад мережі з FTP-сервером. Безпека такого сервісу залежить більше від програмного забезпечення сервера, ніж від мережевої інфраструктури. Захист мережі можна посилити, дозволяючи трафік FTP тільки через певні порти фаєрволу, до якого підключено сервер.

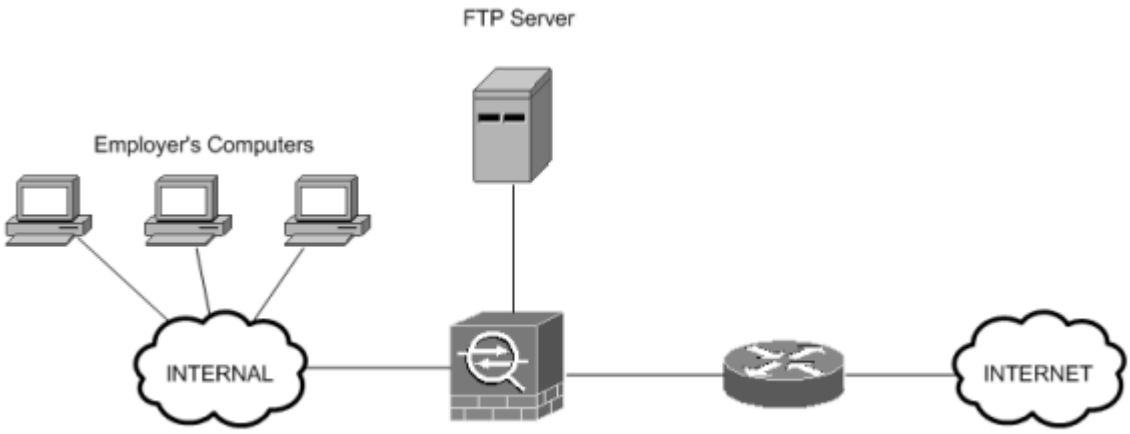

Рис.1.11. Дизайн FTP-сервера

Служби обміну миттєвими повідомленнями. Служби обміну миттєвими повідомленнями можуть становити проблему з точки зору безпеки, але не тільки через можливість крадіжки конфіденційної інформації, оскільки цей ризик існує для більшості протоколів передачі файлів, таких як FTP та SSH (Secured Shell). Ці послуги можуть бути необхідними для певних типів корпорацій. Основна проблема

полягає в тому, що спілкування між користувачами часто відбувається не безпосередньо між користувачами, а через сервер (користувач-сервер, сервер-користувач), що створює ризик прослуховування інформації. Перешкодити такому спілкуванню важко та дорого.

Більшість програм обміну миттєвими повідомленнями можуть тунелювати свій трафік через порт 80, який зазвичай не блокується фаєрволами, оскільки він необхідний для веб-перегляду. Один із способів зупинити цей вид трафіку в корпоративній мережі - використання спеціального програмного забезпечення для блокування трафіку миттєвих повідомлень.

Два додаткові методи підвищення корпоративної безпеки при використанні миттєвих повідомлень включають:

- *Навчання співробітників.* Навчити співробітників користуватися безпечними службами обміну миттєвими повідомленнями та інформувати їх про потенційні ризики безпеки, пов'язані з використанням таких служб.
- *Приватний сервер миттєвих повідомлень*. Використання приватних серверів миттєвих повідомлень, розташованих у внутрішній корпоративній мережі та обмежених для використання в межах корпорації, що дозволяє контролювати трафік та забезпечувати безпеку обміну повідомленнями.

Служби DHCP. Протокол динамічної конфігурації вузла (DHCP) часто стає об'єктом атак, оскільки використовується для налаштування мережевої конфігурації комп'ютерів користувачів. Простота роботи DHCP робить його вразливим, адже він не передбачає механізмів авторизації чи автентифікації. Його безпека залежить від безпеки фізичної мережі, проте створення фальшивих серверів або клієнтів DHCP не є складним завданням і може призвести до різних мережевих проблем.

Використання фільтрації за MAC-адресами, коли тільки відомі комп'ютери з певними MAC-адресами можуть отримувати мережеві параметри, є поширеною практикою, особливо у великих корпораціях. Однак, існує ризик підробки MAC-адрес. Якщо зловмисник набуває контролю над DHCP-серверами або встановлює свій власний сервер у мережі, він може налаштувати свої DNS-сервери,

перенаправляючи веб-сторінки на шкідливі сайти, які можуть встановлювати шкідливе програмне забезпечення на пристрої користувачів. Також зловмисник може змінити шлюз за замовчуванням усіх комп'ютерів, перенаправляючи та перехоплюючи весь корпоративний трафік.

Для покращення безпеки важливих служб DHCP, можна вжити кілька кроків:

- Використання авторизації серверів DHCP у Active Directory. Сервери DHCP повинні бути перевірені через Active Directory, щоб підтвердити їх автентичність перед наданням дозволу на видачу мережевих адрес. Однак, цей метод має обмеження, оскільки він не сумісний з серверами, що використовують інші операційні системи, окрім Microsoft Windows Server 2000 або новіших версій.
- Резервування IP-адрес і заповнення вільних IP-адрес недійсними MAC-адресами. Це дозволяє захистити мережу від несанкціонованих клієнтів. Проте, цей метод має обмежену ефективність, якщо використовуються підроблені MAC-адреси.
- Аудит і моніторинг DHCP-серверів. Застосування аудиту та інструментів моніторингу може виявити спроби атак або виявити нові DHCP-сервери в мережі, що допоможе забезпечити безпечне та належне функціонування DHCP-серверів.

Служба віддаленої автентифікації користувача. Служба віддаленої автентифікації користувача (RADIUS) є мережевим протоколом, який забезпечує централізоване управління автентифікацією, авторизацією та обліком (AAA) для забезпечення доступу комп'ютерів до мережевих служб.

RADIUS функціонує як клієнт-серверний протокол на прикладному рівні, використовуючи UDP для транспортування пакетів. До компонентів, що використовують RADIUS, належать сервери віддаленого доступу, сервери віртуальних приватних мереж, мережеві комутатори з автентифікацією на основі порту та мережеві сервери доступу, які контролюють доступ до мережі. Всі ці компоненти включають клієнтську частину RADIUS, яка забезпечує зв'язок із сервером RADIUS. Сервери RADIUS, як правило, працюють як фонові процеси на системах UNIX або Windows.

Три основні функції RADIUS включають:

- Автентифікацію користувачів або пристроїв перед наданням доступу до мережі,
- Авторизацію користувачів або пристроїв для певних мережевих послуг,
- Облік використання цих послуг.

Сервери RADIUS використовують двоетапний процес, відомий як «транзакція AAA», для управління доступом до мережі. Автентифікація та авторизація в RADIUS описані в RFC 2865, а облік — у RFC 2866. Приклади розміщення та використання RADIUS-серверів у мережевій інфраструктурі і модель зв'язку між клієнтом і сервером можна знайти на рис.1.12 та 1.13 відповідно.

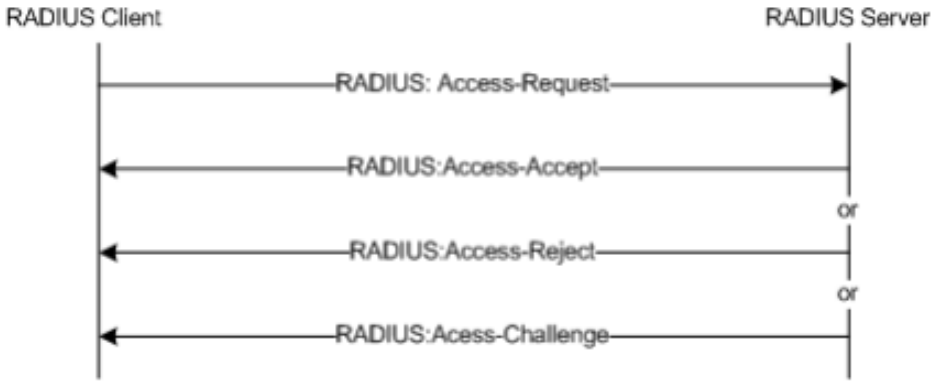

Рис.1.12. Модель зв'язку клієнт-сервер RADIUS

Сервер RADIUS здійснює перевірку вхідних даних, використовуючи методи автентифікації, такі як PAP, CHAP або EAP. Цей процес включає підтвердження ідентифікації користувача, а також, за потреби, інші відомості, пов'язані з запитом, включаючи мережеву адресу користувача, номер телефону, статус облікового запису та специфічні привілеї доступу до мережевих послуг.

Історично RADIUS-сервери порівнювали інформацію користувача з даними, збереженими у локальних базах даних або плоских файлах. Сучасні RADIUS-сервери продовжують використовувати цей підхід або можуть звертатися до зовнішніх джерел, таких як SQL-сервери, Kerberos, LDAP або Active Directory, для перевірки користувацьких облікових даних.

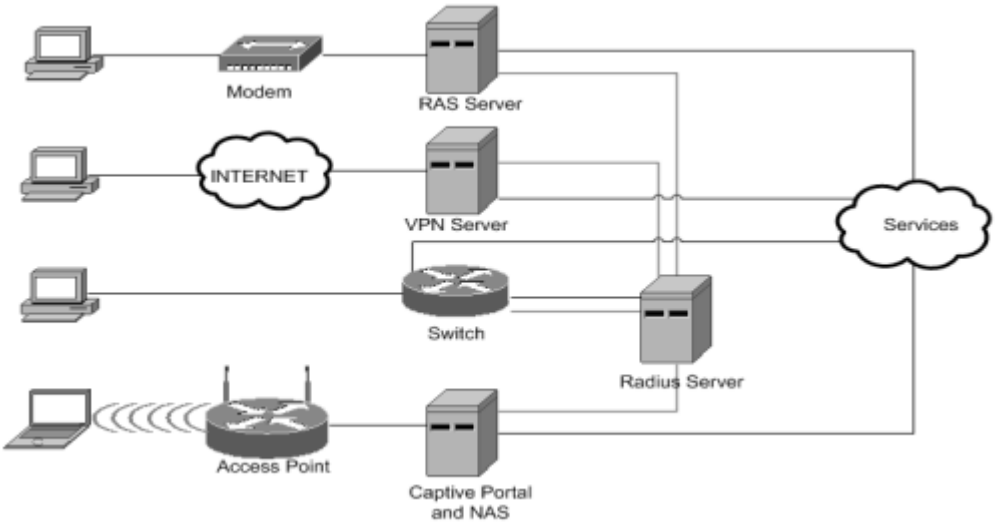

Рис.1.13. Розташування сервера Radius

1.4. Різновиди підходів до забезпечення безпеки корпоративної мережі

1.4.1. Ідентифікація

Технології ідентифікації використовуються для визначення особи користувача в мережі. Ці технології є частиною системи AAA (автентифікація, авторизація та облік).

Основні технології включають:

- *Багаторазові паролі.* Ця технологія часто зустрічається у вигляді імен користувачів та паролів у системах Windows і UNIX. Вона легка в реалізації, не впливає на продуктивність та важка для обходу зловмисниками. Також ця технологія захищає комп'ютери та інше мережеве обладнання від прямого доступу.
- *RADIUS і TACACS+*. Ці технології забезпечують централізовані послуги аутентифікації. RADIUS (Remote Authentication Dial-In User Service) і TACACS+ (Terminal Access Controller Access-Control System Plus) складніші в реалізації та працюють трохи повільніше, ніж парольні системи, але забезпечують більшу безпеку від зловмисних обходів та також запобігають прямому доступу. При виборі між RADIUS і TACACS+ варто враховувати, що RADIUS є відкритим стандартом і широко підтримується, тоді як TACACS+ є протоколом Cisco і

підтримується лише обладнанням Cisco. TACACS+ часто використовується для управління автентифікацією, а RADIUS - для автентифікації користувача. RADIUS має дві основні переваги:

- Використання UDP-пакетів, які менші за TCP-пакети TACACS+;
- Шифрування лише пароля, а не всього зв'язку, що збільшує продуктивність;
- Сервери AAA можуть бути інтегровані з технологією одноразових паролів (OTP) для посилення безпеки.

- *OTP*. Використання одноразових паролів (OTP) разом із RADIUS є ефективним засобом для забезпечення безпеки. Реалізація OTP є складною, а їх обхід зловмисниками важким. OTP усуває ризик використання слабких паролів, оскільки користувачам потрібно запам'ятати лише PIN-код, і будь-який пароль, який може бути перехоплений у мережі, буде недійсний для подальшого використання. Однак, використання OTP має певні недоліки:
  - Користувачам потрібно мати фізичний токен для автентифікації;
  - OTP вимагає додаткового сервера для обробки запитів, які поступають від сервера автентифікації;
  - Введення паролю займає більше часу;
  - OTP може бути занадто дорогим для використання в масштабних мережах.

- *PKI*. Інфраструктура відкритих ключів (PKI) є складнішою у керуванні та реалізації, але також важкою для обходу зловмисниками. PKI призначена для розповсюдження цифрових сертифікатів, які ідентифікують користувачів. Існують два типи систем PKI: відкриті та закриті. Відкриті системи PKI, як наприклад, використовуються у веб-браузерах для перевірки SSL-сертифікатів, підтримують ідентифікацію широкого кола організацій, тоді як закриті системи PKI ідентифікують одну організацію або обмежену групу. Ключі у системі PKI підписуються центром сертифікації (CA).

- *Технологія смарт-карт.* Технологія смарт-карт є простою для впровадження та управління, а також складною для обходу зловмисниками. Смарт-

карти мають здатність зберігати інформацію про користувачів у своїй внутрішній пам'яті, яка зчитується спеціальними картрідерами. Ці картрідери можуть бути підключені до персональних комп'ютерів для ідентифікації користувачів при використанні VPN чи інших мережевих систем.

- *Біометрія*. Біометрія використовує унікальні фізичні характеристики для ідентифікації особи. Вона може бути комбінована з іншими ідентифікаційними технологіями. Біометрична ідентифікація охоплює методи, які включають розпізнавання відбитків пальців, голосу, обличчя та сканування райдужної оболонки ока. Може бути використано один або декілька з цих методів ідентифікації. При виборі біометричної технології ідентифікації важливо забезпечити безпеку передачі інформації між біометричним сканером та сервером автентифікації, оскільки ця інформація може бути перехоплена та використана для несанкціонованого доступу[7].

1.4.2. Безпека хосту та програми

Технології безпеки хостів та програм можна використовувати для підвищення безпеки кінцевих систем. Важливо, що кінцеві системи повинні бути захищені, тому що багато проблем безпеки походять від них.

Цілісність файлової системи. Засоби перевірки цілісності файлової системи повідомляють, чи встановлено віруси або руткіти на комп'ютері. Це особливо важливо для критично важливих серверів. Ця технологія функціонує, зберігаючи хеш-значення критичних файлів, і показує будь-які зміни у файлах за допомогою порівняння хеш-значень при наступній перевірці. Ця система не відновлює автоматично, вимагаючи додаткових заходів. Вона проста в реалізації і не впливає на продуктивність системи[8].

Встановлення брандмауерів на основі хоста. Встановлення брандмауерів на основі хоста додає додатковий рівень безпеки на персональних комп'ютерах всередині та поза корпорацією. Важливо встановити персональні брандмауери на всіх комп'ютерах, які використовуються співробітниками поза корпоративною

мережею. Головною проблемою є управління цими брандмауерами, особливо якщо вони не мають централізованого керування і складно налаштувати вручну велику кількість комп'ютерів.

Система виявлення вторгнень на хост. Система виявлення вторгнень на хост надає інформацію про події на вибраному комп'ютері, забезпечуючи інструменти для аналізу та аудиту системи. Ці системи потребують оптимізації, щоб надавати лише релевантну інформацію.

Антивірусні програми для хостів. Антивірусні програми для хостів є поширеними технологіями для підвищення безпеки хоста. Їх встановлення рекомендується на всіх серверах та робочих станціях, особливо тих, що працюють під управлінням Microsoft Windows. Антивірусні програми працюють з вірусними базами даних, порівнюючи їх з інформацією в системах.

1.4.3. Мережеві брандмауери

Мережеві брандмауери використовуються для захисту периметра мережі. Існують різні типи брандмауери:

Маршрутизатори зі списками ACL рівня 3/4 без збереження стану. ACL використовується для фільтрації мережевого трафіку, обмежуючи доступ до певних протоколів, таких як TCP (Transmission Control Protocol) та UDP (User Datagram Protocol), а також IP-адрес. Обходження таких обмежень є складним завданням, оскільки вони визначають строгі правила для трафіку.

Брандмауери з контролем стану. Ці брандмауери включають характеристики брандмауерів без збереження стану, але мають додаткову здатність відстежувати стан активних мережевих з'єднань. Вони моніторять такі параметри, як порт джерела, порт призначення, вихідний IP, IP призначення, і важливо - порядкові номери з'єднань. Особливість полягає в тому, що без знання правильного порядкового номера з'єднання зловмисник не зможе приєднатися до вже встановленого з'єднання. Додатково, ці брандмауери забезпечують захист від атак типу TCP-SYN, що є важливим аспектом для забезпечення цілісності мережі.

Обидва типи брандмауерів відіграють важливу роль у забезпеченні безпеки мережі, кожен з них має свої особливості та застосування в залежності від потреб та інфраструктури мережі[9].

1.4.4. Фільтрування вмісту

Фільтрування вмісту використовується разом із брандмауерами для підвищення рівня безпеки мережі, зокрема через проксі-сервери, веб- та поштову фільтрацію.

Фільтрація проксі. Проксі-сервери, хоч і схожі на брандмауери, працюють повільніше через необхідність перевстановлення сесій для кожного клієнтського з'єднання. Однак, використання проксі-серверів для кешування може прискорити обробку даних. Проксі-сервери можуть мати проблеми з підтримкою деяких програм, тому для коректної роботи потрібно налаштувати проксі-сервер з достатньою інформацією про протоколи, які використовують ці програми.

Веб-фільтрація. Існує два основних типи веб-фільтрації - фільтрація за URL та фільтрація мобільного коду. Фільтрація за URL використовується для блокування доступу до певних веб-сайтів. Фільтрація мобільного коду допомагає перевіряти HTTP-трафік та блокувати шкідливий код, який може бути в ньому прихований.

Фільтрування електронної пошти. Цей тип фільтрації виконує подібні функції до веб-фільтрації. Сервери фільтрації електронної пошти сканують вхідну та вихідну електронну пошту на наявність шкідливого вмісту, зокрема вірусів. Пониження продуктивності сервера фільтрації пошти не є значною проблемою, оскільки електронна пошта не вимагає спілкування в реальному часі, і невелике затримання не має великого впливу на більшість корпоративних операцій.

Ці технології фільтрації вмісту відіграють важливу роль у захисті мережі від різних загроз і дозволяють забезпечити більш високий рівень безпеки для корпоративних даних.

1.4.5 Системи виявлення мережевих вторгнень

Системи виявлення мережевих вторгнень (NIDS) служать для додавання додаткового рівня безпеки до мереж. Існують два основних типи NIDS: на основі підпису та на основі аномалій, кожен з яких має свої характеристики.

NIDS на основі підписів. Ці системи працюють схоже до мережевих сніферів. Вони моніторять мережевий трафік і порівнюють його з базою відомих підписів атак. У випадку виявлення збігу з підписом, система сповіщає про можливу загрозу. Підписи можуть включати відомі вірусні сигнатури, відбитки вразливостей або шаблони поведінки, характерні для зловмисного програмного забезпечення.

NIDS на основі аномалій. Ці системи визначають «нормальну» поведінку мережі на основі встановленого профілю або початкової конфігурації. Вони постійно аналізують мережевий трафік, виявляючи будь-які відхилення від звичайної поведінки, які можуть вказувати на вторгнення або атаку. Цей тип NIDS особливо корисний для виявлення нових, раніше невідомих атак.

Обидва типи NIDS відіграють ключову роль у забезпеченні безпеки мереж, доповнюючи інші механізми захисту, такі як брандмауери та антивірусні програми. Важливо регулярно оновлювати бази даних підписів для NIDS на основі підписів, а також точно налаштовувати параметри нормальної мережевої поведінки для NIDS на основі аномалій.

1.4.6 Криптографія

Криптографія використовується для захисту комунікації між двома сторонами, пропонуючи такі переваги: повідомлення, які неможливо прочитати сторонніми особами; здатність учасників взаємно ідентифікувати один одного у групі; гарантія, що повідомлення не змінюються під час передачі без відома відправника або отримувача.

Криптографія 2-го рівня. Ця криптографія використовується на 2-му рівні моделі OSI. Прикладом є Wired Equivalent Privacy (WEP) в стандарті IEEE 802.11b. Вона застосовується для захисту WAN-з'єднань між фінансовими установами.

Мережева криптографія. Internet Protocol Security (IPSec) є стандартом мережевої криптографії, визначеним в RFC 2401 від Internet Engineering Task Force (IETF). IPSec, як гнучкий метод криптографії 3-го рівня, дозволяє шифрувати мережевий трафік різних протоколів за допомогою єдиної угоди про безпеку.

Криптографія від 5-го до 7-го рівня. Цей тип криптографії є альтернативою IPSec для певних додатків. Secure Sockets Layer (SSL) використовується для шифрування веб-трафіку, де IPSec не підходить. Secure Shell (SSH) та SSL застосовуються для управлінських комунікацій та специфічних потреб додатків.

Криптографія файлової системи. Хоча цей вид криптографії безпосередньо не пов'язаний з безпекою мережі, він може надавати опосередкований захист, шифруючи всю файлову систему комп'ютера. Це допомагає захистити конфіденційність даних, навіть якщо фізична безпека комп'ютера була скомпрометована.

1.5. Методи та рішення для безпеки корпоративної мережі

Необхідно розглянути деякі базові та поширені рішення для підвищення безпеки мережі. Через велику кількість доступних рішень та методів, фокус зосереджується на важливих аспектах, таких як використання демілітаризованих зон (DMZ), стратегії посилення основних пристроїв у корпоративній мережі та виявлення несанкціонованих пристроїв.

Демілітаризовані зони (DMZ). DMZ – це мережева зона, розташована між внутрішньою та зовнішньою мережею. Вміст DMZ залежить від корпоративних потреб і може варіюватися від одного сервера до великої серверної ферми. Використання DMZ дозволяє захистити корпоративні сервери від прямого доступу з зовнішньої мережі, захищаючи важливі корпоративні дані.

Дизайн DMZ. Конфігурація DMZ може бути простою або складною залежно від вимог безпеки. Вона забезпечує кілька рівнів захисту для серверів і машин всередині зони. Різні сценарії використання DMZ визначають, який тип дизайну є найбільш відповідним.

Базова мережа з єдиним брандмауером. Простий дизайн DMZ з одним брандмауером і однією зоною, як показано на рис.1.14, може використовуватися для створення окремої, захищеної частини великої корпоративної мережі.

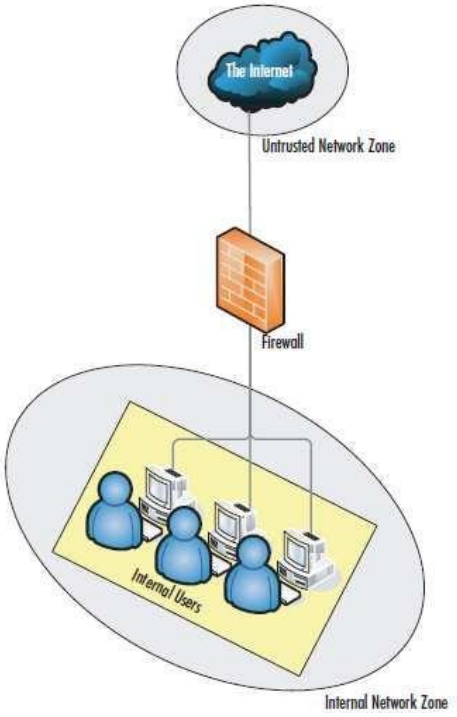

Рис.1.14. Базова мережа з одним брандмауером

Цей варіант ідеально підходить для ізоляції окремих відділів від решти корпоративної мережі та захисту даних від зовнішніх загроз або інших відділів компанії. Переваги такого дизайну включають відносну дешевизну, простоту налаштування та низькі витрати на обслуговування. Однак, головні недоліки полягають у низькому рівні безпеки та обмежених можливостях розширення.

На рис.1.15 показаний транспортний потік першої розрахункової моделі. Вихідний трафік необмежений, але базова конфігурація не дозволить вхідні підключення, які не запускаються з внутрішньої мережі.

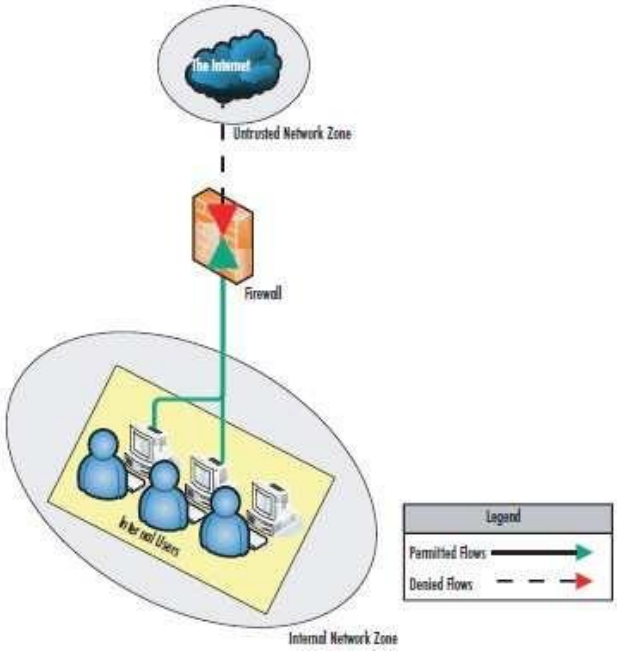

Рис.1.15. Потік трафіку базової мережі з одним брандмауером

Базова мережа з єдиним брандмауером та хостом Bastion. На рис.1.16 представлена конструкція частини або всієї мережі, що дозволяє надавати послуги, доступні як внутрішній, так і зовнішній мережі. Важливо забезпечити високий рівень безпеки на хості Bastion, активувавши на ньому лише ключові послуги.

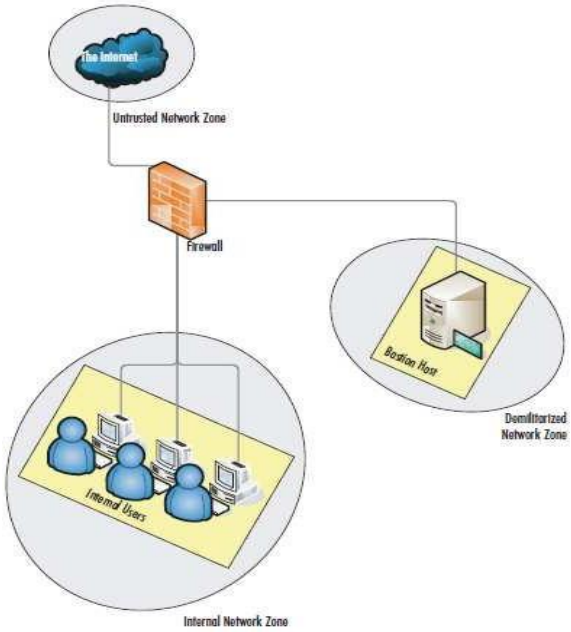

Рис. 1.16. Базова мережа з єдиним брандмауером і хостом Bastion

Цей дизайн не підходить для сценаріїв, де потрібно надавати віртуальні приватні мережі (VPN), служби передачі файлів (FTP) або інші послуги, які вимагають частого оновлення вмісту. Переваги цього дизайну полягають у простоті та низьких витратах. Однак, важливо врахувати, що хост Bastion є вразливим і не дозволяє масштабування. Хост Bastion - це спеціалізований сервер, який розташовується у DMZ і володіє підсиленою безпекою на рівні хоста, працюючи лише з мінімальним набором активних послуг для зниження ризиків безпеки.

На рис. 1.17 демонструється потік трафіку в конструкції мережі з єдиним брандмауером і хостом Bastion. В цьому сценарії, хоча брандмауер не забезпечує безпосередньо захист для хосту Bastion, всі правила трафіку налаштовані на брандмауері, що дозволяє контролювати доступ до хоста.

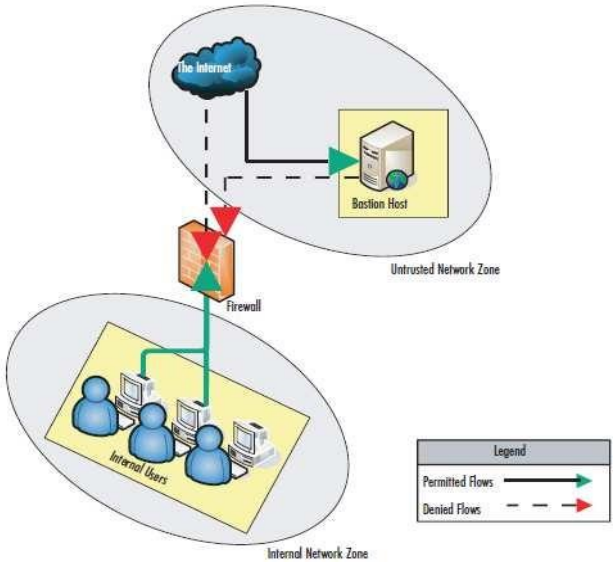

Рис. 1.17. Потік трафіку в базовій мережі з єдиним брандмауером та хостом Bastion

Вхідний трафік з зовнішньої мережі блокується брандмауером для захисту внутрішньої мережі, тоді як вихідний трафік з внутрішньої мережі дозволений. Ручне налаштування правил на брандмауері вимагає ретельного управління та періодичного оновлення для забезпечення безперервного захисту. Цей підхід до мережевої безпеки використовується для створення буферної зони між зовнішнім інтернет-підключенням та внутрішньою корпоративною мережею. Хоча хост

Bastion є відносно захищеним, він вимагає ретельного моніторингу та управління безпекою, оскільки становить критичну точку в мережевій інфраструктурі[10].

Потік трафіку в базовій мережі з єдиним брандмауером та хостом Bastion. На рис. 1.18 представлено схему, в якій брандмауер блокує весь трафік із зовнішньої мережі до хосту Bastion, окрім трафіку, що надходить до певних портів, таких як порт 80 для веб-сервісів. Це дозволяє оновлювати вміст веб-сайтів з внутрішньої мережі за умови, що брандмауер правильно налаштований.

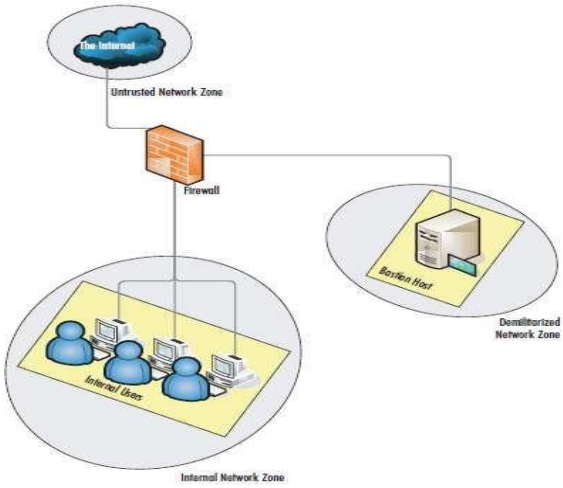

Рис. 1.18. Базова мережа з брандмауером і DMZ

На рис. 1.19 демонструється транспортний потік третього прикладу дизайну. Вхідний трафік дозволяється до хосту Bastion, якщо брандмауер налаштований на це.

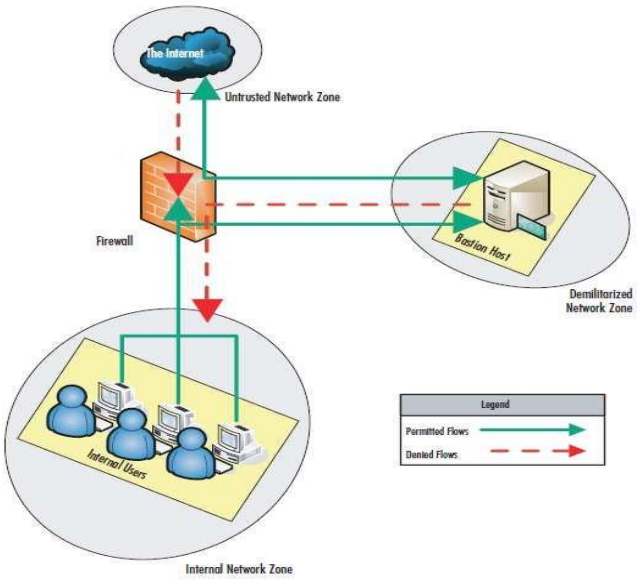

Рис. 1.19. Потік трафіку в базовій мережі з брандмауером і DMZ

Вихідний трафік з внутрішньої мережі дозволений, включаючи трафік до DMZ. Трафік із DMZ до внутрішньої мережі блокується брандмауером. Переваги цієї конструкції полягають у тому, що брандмауер забезпечує захист внутрішньої мережі та хосту Bastion, мінімізуючи ризик компрометації та надаючи певний рівень гнучкості. Недоліки включають високу складність конфігурації та необхідність використання розділеного DNS для управління мережевим трафіком.

Ці конструкції важливі для розуміння різних способів, якими можна захистити мережеву інфраструктуру, кожна з яких має свої переваги та обмеження в залежності від специфічних вимог безпеки.

Багаторівневий брандмауер із DMZ. Рис. 1.20 демонструє базову багаторівневу конструкцію DMZ, де брандмауер може використовувати віртуальні мережі (VLAN) із підтримкою стандарту IEEE 802.1q.

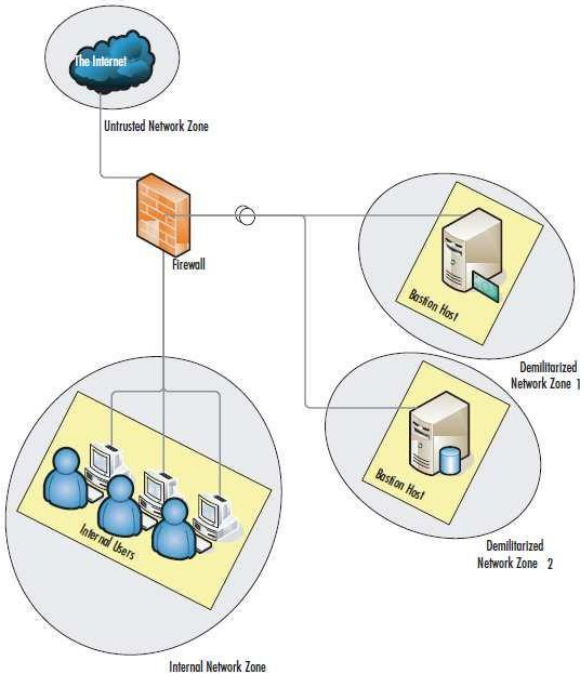

Рис. 1.20. Багаторівневий брандмауер із DMZ

Цей підхід відмінний від традиційного використання декількох фізичних брандмауерів чи інтерфейсів, оскільки він дозволяє застосовувати різні політики безпеки до віртуальних портів, використовуючи теги VLAN. Однак, у випадку використання VLAN, важливо враховувати ризики, пов'язані зі стрибками VLAN, і в разі потреби використовувати окремі фізичні інтерфейси для кожної зони DMZ.

Брандмауер в цій конфігурації може надавати доступ до кожного хосту Bastion зовні, зсередини або навіть з іншого хосту Bastion, розташованого у другій DMZ.

Рис. 1.21 представляє більш складний потік трафіку, де реалізована захищена DMZ – DMZ2. Брандмауер регулює трафік між внутрішньою мережею та DMZ2. Користувачі внутрішньої мережі мають доступ до зовнішньої мережі та DMZ, але хости в DMZ не можуть отримати доступ до користувачів внутрішньої мережі. Переваги цього дизайну включають захист хосту Bastion, можливість збільшення кількості послуг та обмеження потенційно скомпрометованих хостів.

Недоліки цього підходу включають потребу в додатковому апаратному та програмному забезпеченні, підвищену складність, а також необхідність більш інтенсивної роботи з налаштування та моніторингу.

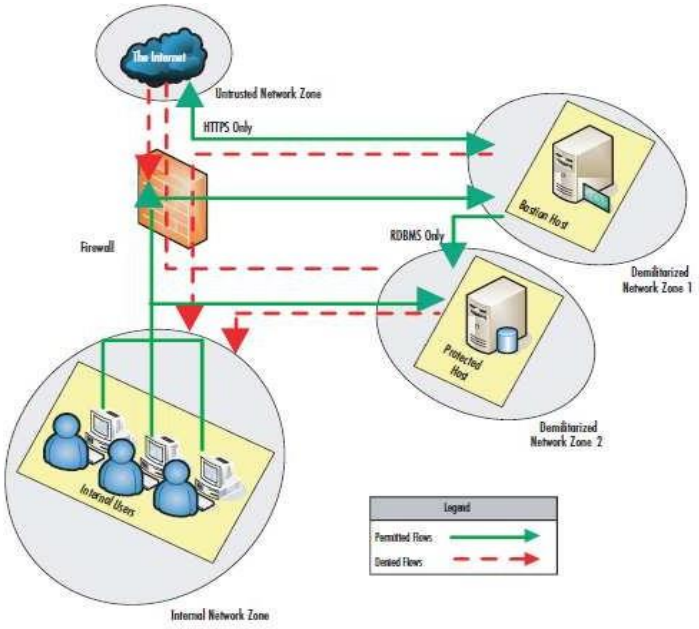

Рис. 1.21. Потік трафіку в багаторівневому брандмауері з DMZ

Ці схеми важливі для розуміння складних мережевих конструкцій, які дозволяють забезпечити високий рівень безпеки в корпоративних мережевих середовищах.

Дизайн DMZ. Проектування демілітаризованої зони (DMZ) є ключовим елементом у загальній архітектурі безпеки корпоративної мережі. Правильно спроектована DMZ може ефективно ізолювати різні типи мережевого трафіку та

з'єднань. Вона також забезпечує захист корпоративних даних від внутрішніх та зовнішніх загроз. Багаторівневий підхід у проектуванні DMZ може забезпечити комплексний захист корпоративних ресурсів, мінімізуючи ризики та втрати безпеки з різних причин.

Протоколи в DMZ. Вибір протоколів у DMZ залежить від специфічних корпоративних потреб, але деякі протоколи можуть створювати вразливості у безпеці DMZ. Ось деякі з найбільш вразливих протоколів та потенційні проблеми безпеки, пов'язані з ними:

- Протокол передачі файлів (FTP). Цей протокол не підтримує шифрування, інформація для авторизації передається у відкритому вигляді, що становить ризик для безпеки;
- Telnet. Авторизаційні дані передаються у відкритому тексті, створюючи ризик контролю над системами, що використовують цей протокол;
- Протокол передачі гіпертексту (HTTP). Має численні проблеми безпеки на різних платформах веб-серверів. Погано налаштований веб-сервер може легко бути скомпрометований;
- Легкий протокол доступу до каталогу (LDAP). Схильний до різних атак на переповнення буфера та атак типу відмови в обслуговуванні (DoS);
- Простий протокол керування мережею (SNMP). Високий ризик переповнення буфера та DoS-атак, особливо при використанні стандартних налаштувань;
- Secure Shell (SSH). Часто стає об'єктом DoS-атак. У випадку отримання зловмисником прав root, можливе виконання довільного коду;
- Служба доменних імен (DNS). Багато проблем безпеки на різних платформах DNS-серверів. Доступ зловмисника до DNS-сервера може призвести до перенаправлення веб-трафіку.

Ці вразливості протоколів вимагають ретельного розгляду при проектуванні DMZ для забезпечення ефективного захисту мережі. Важливо розуміти потенційні ризики та розробляти стратегії їх усунення або мінімізації.

Методи захисту мережевих ресурсів DMZ

- Використання брандмауерів. Брандмауери є ключовою складовою більшості реалізацій і дизайнів DMZ. Кількість та тип брандмауерів, що використовуються, залежать від корпоративних вимог. Різні підходи до використання брандмауерів були продемонстровані раніше у цьому документі. Тестування різних типів брандмауерів, як програмних, так і апаратних, є важливою частиною проектування DMZ.
- Використання екранованих підмереж. Для складніших вимог до DMZ можуть бути застосовані екрановані підмережі. Цей підхід може вимагати додаткового обладнання та може бути дорожчим порівняно з іншими методами. Одним з варіантів є використання брандмауера з кількома інтерфейсами, що дозволяє фільтрувати трафік на кожному порту. Цей метод дозволяє ефективно контролювати доступ до захищених послуг, таких як веб-сервіси, електронна пошта, VPN та FTP.
- Захист публічного доступу до екранованої підмережі. Цей метод передбачає використання маршрутизатора для базового рівня безпеки та брандмауера для забезпечення глибшої безпеки.

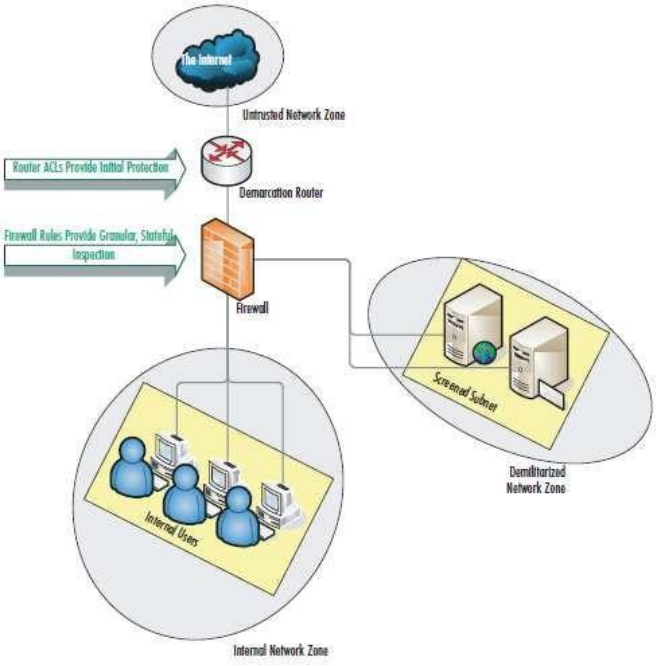

Рис. 1.22. Базова екранована підмережа

Як показано на рис. 1.22, захист починається з маршрутизатора, на якому можна налаштувати списки доступу (ACL) для блокування небажаних IP-адрес. Далі, брандмауер забезпечує другий рівень безпеки, дозволяючи фільтрувати або блокувати різні типи трафіку. Цей дворівневий підхід до безпеки дозволяє ефективно захистити ресурси DMZ від зовнішніх загроз.

Типи серверів у DMZ

- Сервери додатків. Сервери додатків у DMZ вимагають ретельного налаштування. Важливо встановити всі патчі безпеки для вибраної операційної системи та вимкнути або видалити невикористані служби. Послуги, що надаються через ці сервери, мають бути налаштовані для роботи тільки з дозволеними даними корпорації. Важливо не зберігати критичну або конфіденційну інформацію у DMZ. У випадку необхідності розміщення SQL-сервера у DMZ, потрібно забезпечити, щоб він не містив чутливих даних. Не рекомендується розміщувати сервери, які зберігають інформацію про внутрішню мережеву інфраструктуру або дані користувачів, наприклад DNS- або поштові сервери. Для таких послуг краще використовувати проксі-сервери всередині DMZ для пересилання запитів. Трафік з внутрішньої мережі до служб у DMZ має проходити через брандмауер.
- Контролер домену. Сервери контролера домену або сервери авторизації Active Directory не повинні розміщуватися у DMZ. Це пов'язано з ризиком, що зловмисник, отримавши доступ до таких серверів, може контролювати всю внутрішню мережу. Використання серверів контролерів домену в DMZ допустимо лише у випадках необхідності з'єднання кількох серверів, але при цьому потрібно ретельно контролювати їх конфігурацію, щоб мінімізувати ризики безпеки.
- Сервери автентифікації на основі RADIUS. Сервери RADIUS (Remote Authentication Dial-In User Service) повинні мати високий рівень захисту та бути оновленими. Оскільки ці сервери надають послуги автентифікації для систем каталогів, контроль над ними може дозволити зловмисникам отримати різні рівні доступу. Ідеальний сценарій використання сервера RADIUS, розміщеного в внутрішній мережі, - це обробка проксі-запитів від серверів RRAS (Routing and

Remote Access Service), з дозволом доступу через брандмауер тільки від певних серверів RRAS. Рекомендується використовувати IPsec для захисту трафіку між цими компонентами.

- VPN-сервери. Застосування VPN (Virtual Private Network) стало широко поширеним у багатьох корпораціях для з'єднання головного офісу з філіями. Всі вхідні підключення від філій мають оброблятися через один або декілька VPN-серверів. Розміщення VPN-серверів у DMZ вимагає створення окремої зони, ізольованої від інших мережевих ресурсів та DMZ. Ця нова зона DMZ служитиме воротами до внутрішньої корпоративної мережі і повинна бути ретельно спроектована та захищена. Використання IPsec з його можливостями автентифікації та шифрування, а також інтеграція IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) є рекомендованими для забезпечення оптимальної безпеки.
- Веб- та FTP-сервери в DMZ. Розміщення веб- та FTP-серверів у корпоративній мережі впливає на дизайн DMZ. Часто клієнтам або партнерам компанії потрібен доступ до цих ресурсів. Під час проектування безпеки важливо забезпечити, що привілеї доступу клієнтів та партнерів не створюють вразливостей безпеки. Оптимальним рішенням є відокремлення веб-серверів та FTP-серверів для зовнішнього використання від тих, що призначені для внутрішньої корпоративної мережі.
- Сервери електронної комерції в DMZ. Сервери електронної комерції можна розмістити у DMZ, але потрібно використовувати додаткові заходи безпеки для захисту інформації клієнтів, такої як номери кредитних карток та особисті дані. Заходи безпеки можуть включати застосування SSL (Secure Sockets Layer) для шифрування та обмеження брандмауера, щоб дозволити доступ лише з відомих IP-адрес клієнтів. Багаторівнева структура DMZ дозволяє обмежити комунікацію між різними компонентами системи електронної комерції, такими як основні веб-сервери, сервери баз даних та сервери автентифікації.
- Поштові сервери в DMZ. Поштові сервери є одними з найчастіше використовуваних ресурсів у корпораціях. SMTP-шлюзи повинні бути розташовані

у окремих підмережах DMZ, із брандмауерами, налаштованими на обробку запитів на портах TCP 25 і UDP/TCP 53. Важливо спланувати дві ключові конфігурації: по-перше, зовнішній брандмауер має блокувати вихідний SMTP-трафік, який не походить від SMTP-шлюзу. По-друге, сервер повинен бути налаштований так, щоб він міг надсилати електронні листи лише хостам у внутрішній мережі або іншим довіреним IP-адресам[11].

Висновки до розділу 1

Досліджено корпоративні мережі та основні питання безпеки, що наразі висуваються до них.

Зазначено особливості організації різновидів підходів до забезпечення безпеки корпоративної мережі.

Деталізовано та досліджено методи та рішення безпеки, що активно використовуються при проєктуванні та використанні компонентів корпоративної мережі.

2 ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

На рис. 2.1 представлена схема корпоративної мережі, розроблена згідно з рекомендаціями фахівців у сфері інформаційної безпеки. Рекомендовано розділити мережу на дві основні частини: Edge та внутрішню мережу. Edge мережа забезпечує підключення до Інтернету та внутрішньої мережі. Використання кількох підключень до Інтернету є важливим не тільки для безпеки, але й для забезпечення високої доступності та стабільності корпоративних серверів. Додатково це може забезпечити захист від атак типу flood за допомогою балансування навантаження[12].

Рис.2.1. Пропонована принципова конструкція

2.1. Вимоги до дизайну мережі Edge

При проєктуванні мережі Edge серед низки основних вимог слід враховувати наступні:

- Підключення до мережі Інтернет та інших зовнішніх мереж. Це критично важливий аспект дизайну;
- Сервери. Необхідно визначити, які сервери потрібні для підтримки корпоративних операцій. Серед них можуть бути DNS-сервери, поштові сервери, веб-сервери тощо. Також важливо розглянути розміщення VPN-сервера;
- VPN-тунелі. Ця опція включена для забезпечення доступу віддалених та мобільних співробітників до корпоративної мережі;
- Висока доступність підключення до Інтернету. Необхідно забезпечити максимальну безвідмовність серверів та послуг, що надаються зовні. Хоча це не пряма вимога безпеки, вона включена для забезпечення стабільної роботи мережі;

- Моніторинг мережі. Слід інтегрувати інструменти та методи для моніторингу мережі, спроб вторгнень та атак;
- Безпека. Забезпечення високого рівня безпеки мережі та серверів є фундаментальним принципом.

На рис.2.2 показана запропонована модель дизайну мережі Edge корпоративної мережі.

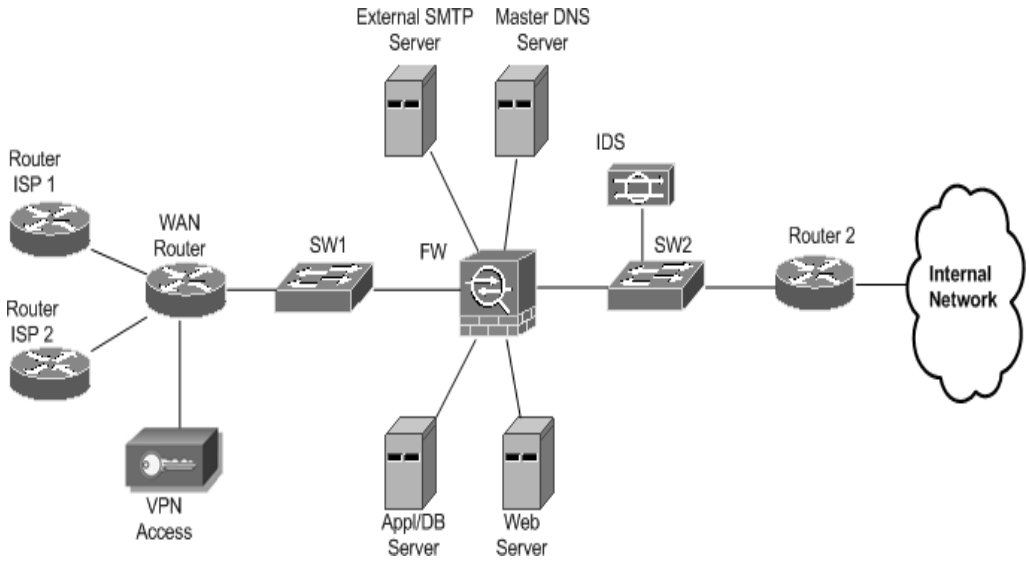

Рис.2.2. Пропонований дизайн мережі Edge

Поштові сервери. Пропонується використання розподіленої, дворівневої структури електронної пошти. Зовнішній SMTP-сервер виконує подвійну роль: передає повідомлення ззовні на антивірусний поштовий сервер у внутрішній мережі та надсилає скановані повідомлення назовні. Такий дизайн забезпечує масштабованість і вимагає ретельного серверного посилення (hardening).

Веб-сервери. Використовується модифікований дворівневий веб-дизайн. Зовнішній веб-сервер надає послуги за межами мережі. Важливою характеристикою є використання серверів додатків і баз даних на одному фізичному сервері. Використовується єдиний брандмауер із різними налаштуваннями безпеки на окремих портах. Основна функція брандмауера полягає в моніторингу трафіку та блокуванні всього, що не призначено для цих серверів. Також необхідно забезпечити посилення (hardening) сервера та операційної системи, а також перевірку цілісності файлової системи.

DNS-сервери. Доцільно передбачити використання розподіленої системи DNS. Основний DNS-сервер розміщується в периферійній частині мережі. Для підвищення безпеки DNS-служби використовується стратегія розділення архітектурних рівнів. Внутрішній DNS-сервер пересилає невирішені запити до спеціалізованих серверів, які мають доступ для роботи з запитами поза мережею. Застосування заходів безпеки для DNS-серверів аналогічне тим, що використовуються для інших серверних систем.

VPN-сервери. VPN-сервери займають важливе місце в мережевій архітектурі, підключаючись безпосередньо до початкових маршрутизаторів мережі. Хоча можливості створення VPN з'єднань типу Site-to-Site для забезпечення безпечних зв'язків із філіями чи партнерами не розглядаються детально в цьому проекті, важливо відзначити ключові вимоги для таких з'єднань. Рекомендується обмежити доступ до серверів VPN Access лише для IPSec трафіку. Це вимагає додаткових налаштувань на маршрутизаторі WAN у дизайні Edge, щоб гарантувати, що тільки відповідний трафік досягає VPN-серверів.

Вимоги для забезпечення безпеки пристроїв у захищеній корпоративній мережі можуть включати наступні:

1) VPN-сервери:

- Застосування методів посилення (hardening) пристроїв;
- Обмеження підключень тільки IPSec VPN;
- Активація та налаштування списків контролю доступу (ACL) маршрутизатора для допуску лише IPSec-трафіку до VPN-пристроїв доступу;
- Використання цифрової сертифікації для автентифікації, з впровадженням моделі PKI для Site-to-Site VPN та моделі одноразових паролів (OTP) для одиночних VPN-з'єднань;

2) WAN маршрутизатори:

- Застосування методів посилення пристроїв;
- Використання фільтрації L3 з ACL при потребі;
- Впровадження одноадресного Reverse Path Forwarding (RPF) для фільтрації згідно RFC 2827 у вхідних та вихідних напрямках;

- Фільтрація згідно RFC 1918 у вхідних та вихідних напрямках;
- Фільтрація пакетів ICMP, використовуючи кращі практики;
- Застосування передових методів захисту від DDoS-атак, включно з CAR (Committed Access Rate).

3) Брандмауери з контролем стану:

- Проведення посилення брандмауерів;
- Використання фільтрації згідно з RFC 1918 і RFC 2827 у вхідних та вихідних напрямках;
- Реалізація спеціальної фільтрації для пристроїв, які безпосередньо підключені до інтерфейсів брандмауерів;
- Фільтрація пакетів ICMP за кращими практиками;
- Застосування передової практики захисту від TCP SYN флуд-атак для забезпечення безпеки мережі

Для забезпечення безпеки корпоративної мережі, особливу увагу потрібно приділити ще таким аспектам:

4) Системи виявлення вторгнень у мережу (NIDS):

- Посилення систем виявлення вторгнень;
- Налаштування NIDS для моніторингу трафіку між периферійною (EDGE) та внутрішньою мережами;
- Обмеження спостереження NIDS до трафіку, що проходить через зазначені мережеві сегменти;

5) Ethernet комутатори (SW1 і SW2):

- Виконання процедур посилення для комутаторів;
- Застосування кращих практик для управління протоколом L2;
- Активація та налаштування захисту портів на всіх комутаторах мережі;
- Реалізація кращих практик VLAN на комутаторах, де використовуються VLAN.

Таблиця 2.1

Стійкість до атак запропонованого дизайну мережі Edge

Тип атаки	Спосіб виявлення	Спосіб запобігання
Атака переповнення буфера	Перевірка файлової системи, Host IDS, Network IDS	Зміцнення ОС, зміцнення додатків
Вірус/хробак/троянський кінь	Перевірка файлової системи, IDS мережі, NIDS аномалії, найкраща практика DDoS	Антивірус хоста та фільтрація електронної пошти
Прямий доступ	Host IDS	Багаторазові паролі, PKI, маршрутизатор із ACL, шифрування сеансів, приватні VLAN, автентифікація протоколу маршрутизації
Зонд/сканування	Ідентифікатори хоста та мережі, посилення додатків/ОС, брандмауер із збереженням стану	Захист мережевих пристроїв, передовий досвід ICMP
Атаки flooding (затоплення) програм	Ідентифікатори хоста та мережі, ідентифікатори аномалії мережі	Зміцнення програм і ОС
Rootkit	Перевірка файлової системи	Зміцнення програм і ОС
Програмне забезпечення для дистанційного керування	IDS хоста, IDS мережі	Хост-антивірус, захист додатків і ОС
Підробка ідентифікаційної інформації	Багаторазові паролі	PKI та шифрування сеансу програми
Веб-додаток	Перевірка файлової системи, Host IDS, Network IDS	Зміцнення програм і ОС
TCP SYN flood	IDS хоста, IDS мережі	Stateful Firewall, Найкращі практики TCP SYN

Брандмауери з контролем стану можуть захистити лише від певних типів атак, таких як TCP SYN flood і атаки з прямим доступом. Потрібно врахувати інші загрози, що не входять до цього списку, які також потребують захисту за допомогою брандмауера.

У таблиці 2.1 показано, як запропонований дизайн корпоративної мережі здатен протистояти найпопулярнішим атакам. Адже, процес посилення пристроїв є одним із найважливіших способів підвищення безпеки. IDS – це пристрої, які можуть допомогти нам уникнути та зупинити більшість атак у таблиці.

Брандмауери з підтримкою стану можуть захистити нас лише від двох типів атак у таблиці: TCP SYN flood і Атаки з прямим доступом, але є багато інших атак і загроз, яких немає в таблиці, і їх можна зупинити лише за допомогою цього типу брандмауера[13].

2.2. Вимоги до дизайну внутрішньої мережі

Для внутрішньої мережі можна запропонувати використовувати один головний брандмауер, який контролюватиме та відстежуватиме трафік у мережі.До вимоги можна ще додати наступні:

- Забезпечити підключення кількох типів серверів, розташованих у корпоративному ЦОД;
- Можливість надати різним підмережам клієнтів дозволений доступ до цих серверів;
- Сервери, які можуть бути використанні це: DNS-сервер, поштовий сервер, веб-сервер, LDAP-сервер та інші корпоративні сервери.

На рис.2.3 показано проєктування внутрішньої корпоративної мережі. Цей дизайн може задовольнити вимоги щодо безпеки, і також можна надати додатково кілька центрів обробки даних. Організація мережі виконана за допомогою одного центрального брандмауера (Main FW). Коли обирається конкретна модель для цього брандмауера, необхідно зафіксувати, що він знаходиться в середині мережі і буде під великим навантаженням. Цей головний брандмауер безпосередньо підключений до всіх основних частин внутрішньої мережі.

FW1, FW2 і FW3 — це брандмауери, які повинні захищати різні сегменти серверів (поштові сервери, DNS-сервери та веб-сервери). Вони також безпосередньо підключені до головного брандмауера через комутатор SW3. Це потрібно, щоб зменшити використання портів брандмауера та розділити параметри безпеки та вимоги між усіма брандмауерами.

Функції IDS1 і IDS2 полягають у перевірці, аналізі та моніторингу трафіку, що надходить і надходить до LDAP і корпоративних сегментів серверів. Роль

комутатора під назвою Access SW полягає в підключенні всіх інших комутаторів на рівні доступу мережі. Додатково можна налаштувати окремі функції на комутаторі, такі як ACL та QoS, якщо потрібно зменшити основне навантаження на брандмауер.

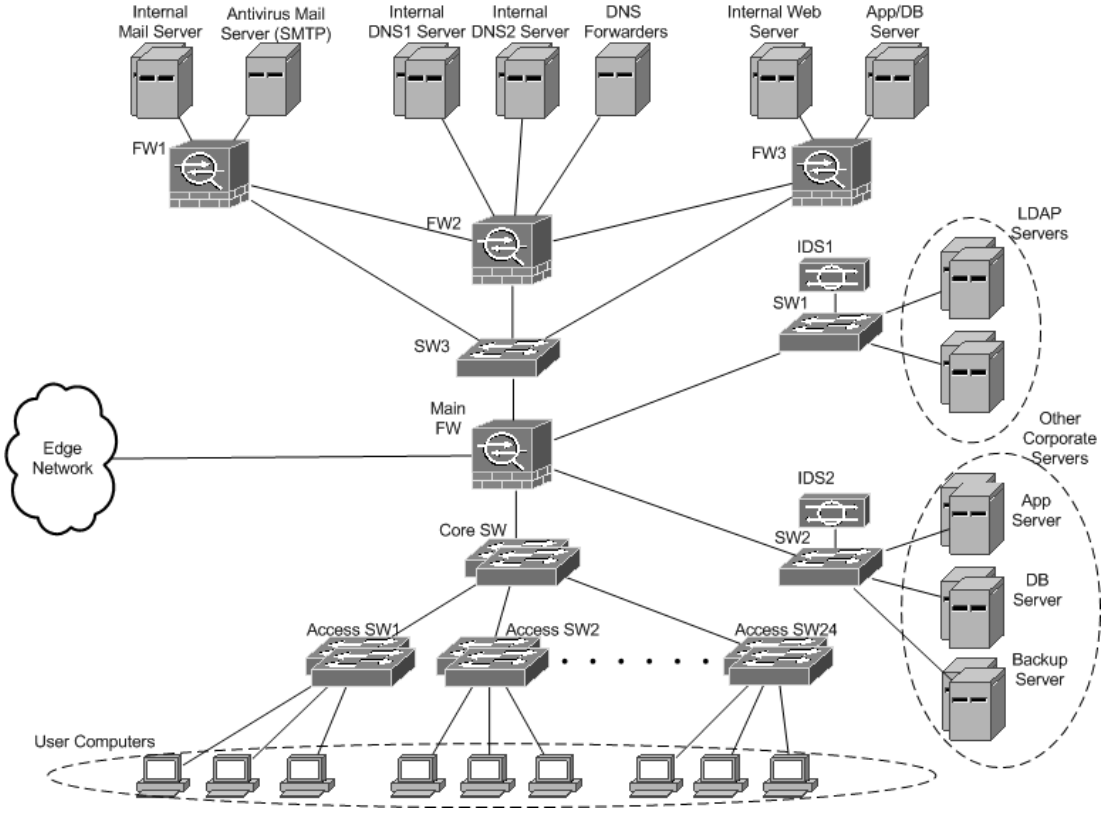

Рис.2.3. Дизайн внутрішньої мережі

1) Комутатори Ethernet (SW1, SW2 і SW3). В архітектурі мережі, кожен пристрій відіграє ключову роль у забезпеченні високого рівня безпеки. Для досягнення цієї мети, наступні техніки та вимоги є необхідними:

- Застосування методів загартування пристрою;
- Реалізація кращих практик для протоколів L2 і L3;
- Включення та налаштування захисту портів на усіх комутаторах мережі;
- Використання кращих практик VLAN на комутаторах, що підтримують VLAN;
- Обмеження кількості MAC-адрес на порту комутатора через параметр безпеки порту;

- Впровадження перевірки ARP на цих комутаторах для підвищення рівня безпеки;
- Використання ACL VLAN для захисту мережі від несанкціонованих серверів DHCP.

2) Ethernet комутатори (програмне забезпечення доступу). Для забезпечення необхідного рівня безпеки на цих пристроях, важливо врахувати наступні техніки та вимоги:

- Використання одноадресного RPF для фільтрації згідно RFC 2827 у вхідних та вихідних напрямках;
- Блокування потоків трафіку на L3/L4 за необхідності та відповідно до політики безпеки;
- Використання підмереж на основі ролей для сегментації користувачів.

Застосування VLAN забезпечує легкість у впровадженні та управлінні, уникаючи використання численних комутаторів L2 при фізичному розділенні мереж. Також можливе використання маршрутизації InterVLAN з комутаторами та маршрутизаторами для майбутнього розширення мережі.

3) Системи виявлення вторгнень у мережу (IDS). Основними системами виявлення вторгнень (IDS) є IDS1 та IDS2, які підключені до комутаторів головних серверних сегментів. Це дозволяє моніторити весь трафік, що йде до і від серверів у визначеному центрі обробки даних. Ефективне налаштування та фільтрація записів з цих IDS є критично важливими через великий обсяг переданих даних. Наступні техніки та вимоги рекомендовані для досягнення високого рівня безпеки:

- Застосування методів загартування пристрою;
- Налаштування пристроїв для виявлення атак, типових для даного виду серверів та інфраструктури.

4) Брандмауери з відстеженням стану (основне програмне забезпечення). Проєкт включає використання основного брандмауеру, який має забезпечити захист всієї внутрішньої мережі. Для досягнення оптимального рівня безпеки на цих пристроях, наступні техніки та вимоги є рекомендованими:

- Застосування методів загартування пристрою;

- Впровадження контролю доступу з урахуванням стану;
- Використання одноадресного RPF для фільтрації згідно з RFC 2827 у вхідних і вихідних напрямках;
- Застосування передових практик TCP SYN для захисту мережі від атак TCP SYN.

5) Брандмауери з відстеженням стану (FW1, FW2 і FW3). У центрі обробки даних використовуються три брандмауери (FW1, FW2, і FW3) для забезпечення додаткового захисту серверів. Для досягнення необхідного рівня безпеки на цих пристроях, рекомендуються наступні техніки та вимоги:

- Застосування методів загартування пристрою;
- Впровадження контролю доступу, що враховує стан. Брандмауери мають бути підключені між собою, забезпечуючи обмін інформацією про стан. У випадку виходу одного з брандмауерів з ладу, інші повинні мати змогу перевіряти стан підключених сесій;
- Використання одноадресного RPF для фільтрації згідно з RFC 2827 у вхідних і вихідних напрямках;
- Застосування передових практик TCP SYN для захисту мережі від атак типу TCP SYN, що особливо важливо для цих двох брандмауерів.

6) Комп'ютери користувача. У контексті захисту внутрішніх серверів, важливо враховувати, що зловмисники часто отримують доступ до комп’ютерів користувачів через хробаки, віруси та інші шкідливі програми. Для забезпечення необхідного рівня безпеки на цих пристроях, слід використовувати наступні техніки та вимоги:

- Користувачі повинні використовувати систему аутентифікації з використанням імен користувачів та паролів для доступу до своїх систем;
- Забезпечення захисту операційних систем та програмних додатків, зокрема через використання структур Active Directory для керування операційними системами та профілями користувачів;
- Встановлення антивірусної програми на кожному комп’ютері у

внутрішній мережі;

- Налаштування хост-брандмауера на кожному комп’ютері для забезпечення додаткового рівня захисту;
- Використання шифрування файлових систем, особливо на комп’ютерах, що використовуються віддаленими працівниками, для захисту даних.

В таблиці 2.2 представлено найпопулярніші атаки на внутрішні мережі та методи виявлення та запобігання.

Таблиця 2.2

Стійкість до атак запропонованого дизайну внутрішньої мережі

Тип атаки	Метод виявлення	Спосіб запобігання
Підробка ідентифікаційної інформації	Багаторазові паролі, RADIUS/TACACS+	Криптографічний захист, шифрування файлової системи, PKI
Вірус, хробак, троянський кінь	Перевірка файлової системи, IDS	Антивірус хоста та фільтрація електронної пошти
Sniffer		Криптографічний захист, безпека портів, передові методи ARP, передові методи DHCP, приватні VLAN
Атака Man-in-the-middle		Криптографічний захист, методи виявлення фальшивих пристроїв, ARP BP, найкращі практики DHCP
Direct access	IDS хоста та мережі	Багаторазові паролі, RADIUS/TACACS+, PKI, брандмауери хостів, шифрування, захист мережі, додатків і ОС, маршрутизатор із ACL, брандмауер із збереженням стану
Перенаправлення та підробка ARP	Мережева IDS	ARP BP, приватні VLAN
Віддалений контроль доступу	IDS хоста та мережі	Хост-антивірус, хост-брандмауери, захист додатків/ОС, шифрування, фільтрація електронної пошти
Переповнення буфера	Перевірка файлової системи, IDS хоста та мережі	Зміцнення програм і ОС

2.3. Вибір мережевого обладанання для проєктування корпоративної мережі

Мережеве обладнання. При проєктуванні вибір конкретного мережевого обладнання відбувається на основі вимог, визначених замовником. Розглядаючи різноманітність продуктів, які пропонують виробники для побудови корпоративних мереж, особлива увага звертається на ті компанії, які використовують власні протоколи, наприклад, протокол маршрутизації EIGRP від Cisco[14].

У контексті інструментів моделювання GNS3 виокремлюється як найбільш підходящий. Цей симулятор підтримує реальні файли зображень майже всього мережевого обладнання Cisco та дозволяє інтегрувати сервери, змодельовані з іншими інструментами моделювання операційних систем, створюючи повну віртуальну модель корпоративної мережі. Використання GNS3 забезпечить зручність та гнучкість у виборі моделей мережевого обладнання, що відповідають сучасним вимогам. У реальних умовах, вибране обладнання може бути замінено на альтернативне з аналогічними характеристиками та функціоналом.

Брандмауери. З урахуванням різних вимог до кожної моделі, вибір має бути ретельним і відповідним до конкретних потреб. Лінійка брандмауерів Cisco, відома як Cisco ASA, включає сім різних моделей з унікальними характеристиками.

Edge мережа. Для частини корпоративної мережі, відомої як гранична мережа, розглядається використання лише одного мережевого брандмауера. Вимоги до вибору моделі включають:

- Призначення для розташування в мережі Internet Edge або Campus;
- Наявність мінімум 6 конфігурованих портів з різними правилами трафіку та обмеженнями;
- Брандмауер з можливістю збереження стану;
- Параметри для захищених VPN-з’єднань;
- Підтримка 100 VPN-з'єднань одночасно, що складає 10% користувачів усієї корпоративної мережі.

Всі моделі Cisco, починаючи з ASA5510, задовольняють встановлені вимоги, однак ASA5510 не підтримує параметри високої доступності. З огляду на те, що до обраного брандмауера будуть підключені всі загальнодоступні сервери, рекомендується вибрати модель із середніх або вищих класів, таких як ASA5520 або ASA5540, які пропонують більшу кількість з'єднань та з'єднань за секунду. Крім того, модель ASA5540 має вдвічі більше пам'яті, що забезпечує можливість розширення мережі у майбутньому. Таким чином, для граничної мережі вибрано брандмауер Cisco ASA5540.

Маршрутизатори. З огляду на різноманітність вимог до кожної моделі, вибір має бути ретельно обдуманим. Два маршрутизатори передбачені для використання в корпоративній мережі, розміщені у крайовій частині мережі. Перший маршрутизатор встановлено на початку крайової мережі, другий – у кінці. Існує значна різниця у трафіку через перший маршрутизатор через розташування багатьох серверів, чиї послуги доступні через Інтернет, а також через весь трафік із внутрішньої мережі до Інтернету.

Для мереж середнього розміру компанія пропонує новіші моделі Cisco 2900 і Cisco 3900. Потужніші моделі також підходять для розглядуваного дизайну, але вони не використовуються до повної потужності та є дорогими. Моделі Cisco 2800 і Cisco 3800 також відповідають вимогам, але як попередні версії 2900 і 3900, вони можуть незабаром втратити підтримку, тому вибір падає на новішу серію.

Серія Cisco 3900 має чотири інтегровані порти, а Cisco 2900 — три. Обидві серії пропонують слоти розширення, але рекомендується залишити їх вільними для майбутніх розширень мережі та додаткових функцій. Моделі Cisco 3900, що задовольняють вимогу щодо чотирьох маршрутизованих портів, - це 3945E та 3925E. Основні відмінності між ними включають кількість слотів для сервісних модулів та модульні порти комутатора локальної мережі, а також деякі функції VoIP. Вибрано маршрутизатор WAN Cisco 3925E без додаткових портів і модулів, залишаючи можливість для майбутнього розширення мережевих послуг. Функція другого маршрутизатора включає маршрутизацію внутрішньої мережі та розділення периферійної мережі від внутрішньої. Необхідність у двох

маршрутизованих портах задовольняє лише модель 2901, яка також має чотири додаткових інтерфейсних слоти для майбутнього розширення мережі. Цей маршрутизатор також має потенціал для виконання функцій IPS, що підключається до SW2, але потребує додаткової ліцензії. Вибір для Router2 у запропонованій мережі - Cisco 2901.

Комутатори. Комутатори Cisco поділяються на п'ять основних категорій: Campus LAN – основні комутатори, Campus LAN – комутатори доступу, комутатори центру обробки даних, постачальник послуг – комутатори агрегації та постачальники послуг – комутатори доступу Ethernet.

Перший комутатор, SW1 призначений для з'єднання WAN-маршрутизатора та основного брандмауера у периферійній мережі. Комутатори з класу постачальника послуг – агрегаційні комутатори є ідеальними для цієї частини мережі. Однак, вибір буде здійснено серед комутаторів нижчого класу, оскільки не потрібно використовувати усі функції більш потужних моделей. Серед можливих варіантів, Cisco 3800X є придатним для дизайну мережі.

Для внутрішньої мережі передбачено кілька комутаторів, які виконують різні функції. SW1 і SW2 відіграють схожі ролі, але підключені до різних портів брандмауера. Існують IDS-системи, підключені до цих комутаторів, що вимагає настроюваних портів для контролю всього трафіку через них. Оскільки Cisco не пропонує відокремлену лінійку продуктів з системами виявлення вторгнень, рішення полягає у заміні цих комутаторів на маршрутизатори з вбудованими модулями IDS та комутаційними модулями. Таке рішення додає додатковий рівень безпеки для всіх серверів, розміщених за цими маршрутизаторами. Найкращим вибором для заміни SW1 і SW2 є Cisco 2911, який має слот для сервісного модуля для встановлення модуля IDS та модульний комутатор LAN з 24 портами. Моделі Cisco 3900 виявилися занадто потужними, тому вибір зроблено на користь меншої серії – 2900. Cisco 2901 не підходить, оскільки не має слотів для сервісних модулів, а Cisco 2921 має занадто багато портів LAN, які не використовуватимуться.

SW3 виконує функцію з'єднання трьох брандмауерів з основним мережевим брандмауером. Важливим є вибір моделі з можливостями VLAN для майбутнього

розширення мережі. Серія Cisco Catalyst 2960 є оптимальним вибором для SW3, оскільки вона підтримує VLAN та не має зайвих функцій.

Головний комутатор – Core SW – повинен відповідати специфікаціям базової мережі локальної мережі кампусу. Моделі Cisco Catalyst 6500, надто функціональні для цієї ролі. Краще підходить Cisco Catalyst 4900, який має 48 портів 10/100/1000-Gbps та 24 порти 10 Gigabit Ethernet, що дозволить підключити цей основний комутатор до інших комутаторів доступу.

Комутатори доступу будуть 48-портовими, підключеними до основного комутатора через оптоволоконний порт 10 Гбіт/с. Загальна кількість портів, доступних для клієнтських комп'ютерів, становить 1152, що покриває потребу до 1000 користувачів. Модель Cisco Catalyst 2975 відповідає цим вимогам, маючи версію з 48 портами та до чотирьох модульних слотів для оптоволоконного порту 10 Гбіт/с, що дозволить підключення до основного комутатора. Додаткові функції безпеки, такі як ACL і NAC, також підтримуються цією моделлю[15].

Системи виявлення вторгнень (IDS). Після аналізу різних типів систем виявлення вторгнень (IDS) на веб-сайті виробника мережевого обладнання було виявлено відсутність окремого продукту IDS. Як альтернатива, існує можливість використання додаткового модуля, який може бути інтегрований з існуючими сервісними маршрутизаторами. Цей підхід дозволяє ефективно відмовитися від використання комутатора SW2 у крайовій частині мережі, замінюючи його на модуль IDS, встановлений у маршрутизаторі Router2. Модуль, який надає можливості IDS для маршрутизаторів, ідентифікований як NME-IPS. Враховуючи вищезазначену стратегію, комутатори SW1 і SW2 можна замінити на маршрутизатори з встановленими модулями комутаторів. Додатково, до цих маршрутизаторів можна інтегрувати модуль NME-IPS для впровадження функцій IDS у мережеву структуру. Це дозволить забезпечити ефективне виявлення та моніторинг вторгнень у мережевому середовищі.

Сервери. У периферійній частині мережі розміщені чотири сервери, тоді як у внутрішній мережі їх щонайменше дванадцять. Кількість серверів варіюється залежно від конкретних корпоративних потреб та навантаження на сервери. У

випадку значного навантаження, можливе включення другого сервера для кожного з них у режимі кластера з балансуванням навантаження. Сервери, здатні до такої конфігурації, позначені на схемах як подвійні сервери. З точки зору безпеки, необхідно використовувати потужні сервери для захисту від DoS- і DDoS-атак.

В реальній ситуації, коли організація вибирає програмне забезпечення для реалізації послуг, вона повинна обрати сервери з відповідними апаратними параметрами.

DNS-сервери. У тестовому віртуальному середовищі буде використовуватися DNS-сервер BIND, який є одним із найпопулярніших для UNIX-систем. Вимоги до апаратного забезпечення DNS-сервера BIND доступні на веб-сайті BIND[16].

Поштові сервери. Для тестування та впровадження служб електронної пошти в віртуальному середовищі планується використання Sendmail, який є частиною більшості дистрибутивів Linux і може бути легко встановлений[17].

Веб-сервери. Веб-сервер Apache буде використовуватися для надання http та https послуг в мережевій реалізації у віртуальному середовищі. Apache, як і Sendmail, є частиною більшості дистрибутивів Linux і легко налаштовується[18].

Сервери LDAP. Для надання послуг LDAP у мережі планується використання сервера OpenLDAP, який є популярною платформою з відкритим вихідним кодом[19].

Сервери SQL. У тестовому середовищі використовуватиметься сервер SQL MySQL для зберігання даних, необхідних для динамічних веб-сторінок, систем ERP та серверів LDAP. MySQL, як і OpenLDAP, є відкритим вихідним кодом і включений у більшість дистрибутивів Linux[20].

Сервери ERP. Цей тип серверів не аналізується детально в рамках цього проекту. Залежно від того, чи базується ERP-система на мережі чи програмі, вимоги до апаратного забезпечення можуть варіюватися. Специфічні вимоги до апаратного забезпечення ERP-серверів залежать від обраної корпорацією системи.

2.4. Приклад організації кінцевих точок працівників у різних корпоративних підрозділах

Організація кінцевих точок працівників у корпоративній мережі є ключовою складовою планування безпеки мережі. У запропонованій мережевій структурі, усі настільні системи підключені до одного порту брандмауера. Це означає, що у випадку фізичного розділення кінцевих точок працівників у різних підрозділах корпорації, необхідно застосовувати однакові правила та обмеження для всіх цих систем. Таке розділення може бути ефективним у деяких ситуаціях, проте воно не є гнучким, оскільки будь-яка заміна або роз'єднання секцій вимагатиме нової кабельної інфраструктури.

На рис.2.4 показано приклад схеми мережі, де розміщені всі настільні системи.

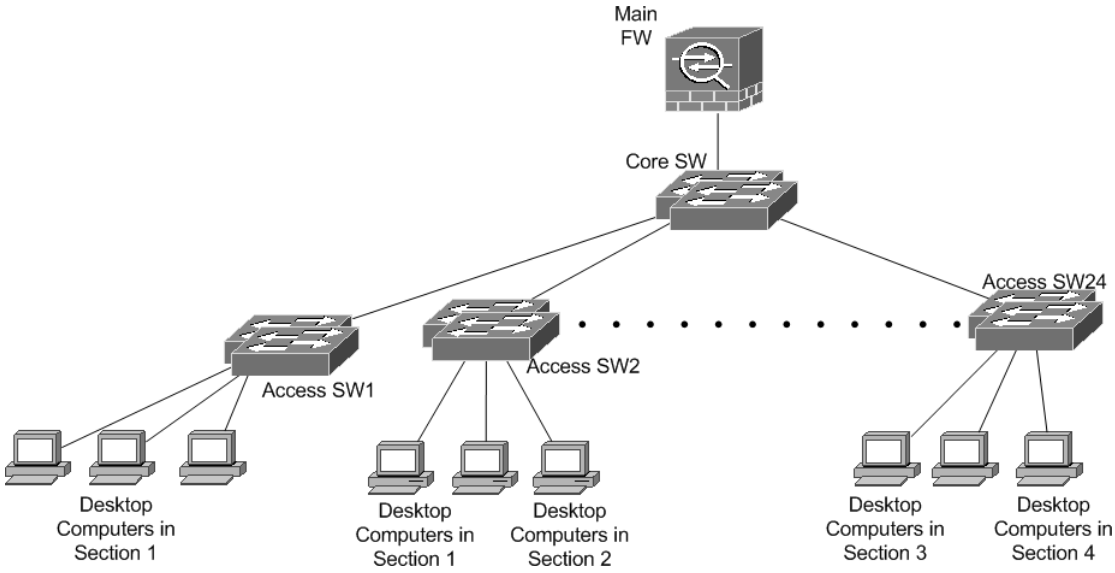

Рис.2.4. Організація кінцевих точок працівників з логічним розділенням

Більш гнучким рішенням є використання логічного розділення мережі за допомогою створення декількох мереж з меншими мережевими масками або застосування VLAN, за умови, що мережеве обладнання підтримує таку функціональність. В роботі мережеве обладнання було вибране з урахуванням підтримки VLAN, що дозволяє реалізувати такий тип поділу для мереж настільних комп'ютерів.

В разі потреби, обраний брандмауер також підтримує VLAN, що дає можливість створювати окремі правила брандмауера для кожної VLAN, надаючи різні права та дозволи для різних корпоративних підрозділів.

Логічне розділення цієї частини мережі надає гнучкість у з'єднанні двох або більше груп настільних комп'ютерів на одному мережевому комутаторі, з можливістю їх подальшого розділення у різні мережі з відповідними мережевими дозволами через додаткове налаштування комутатора.

Ще одна мета розділення кінцевих точок працівників за допомогою VLAN полягає в тому, що нам не потрібні додаткові кабелі в будівлі, якщо необхідно буде внести зміни в топологію мережі. Планується використання лише сумісних VLAN комутаторів, щоб можна було виконувати будь-які види реорганізаційних робіт без будь-яких змін у фізичній мережевій інфраструктурі. На рис.2.5 та рис.2.6 показаний можливий, остаточний дизайн мережі[21].

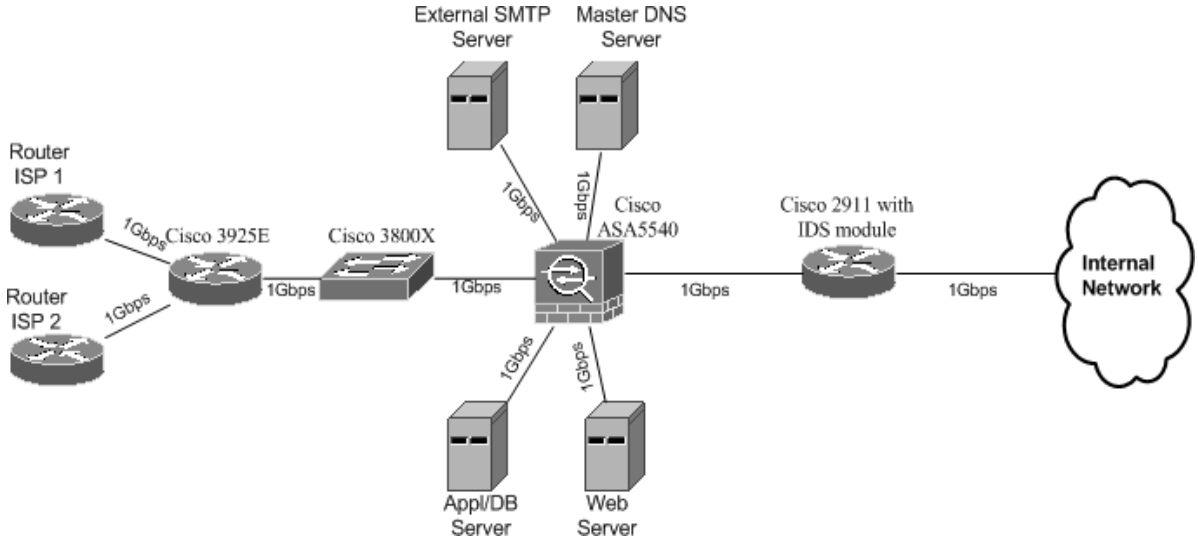

Рис.2.5. Пропонований дизайн Edge мережі

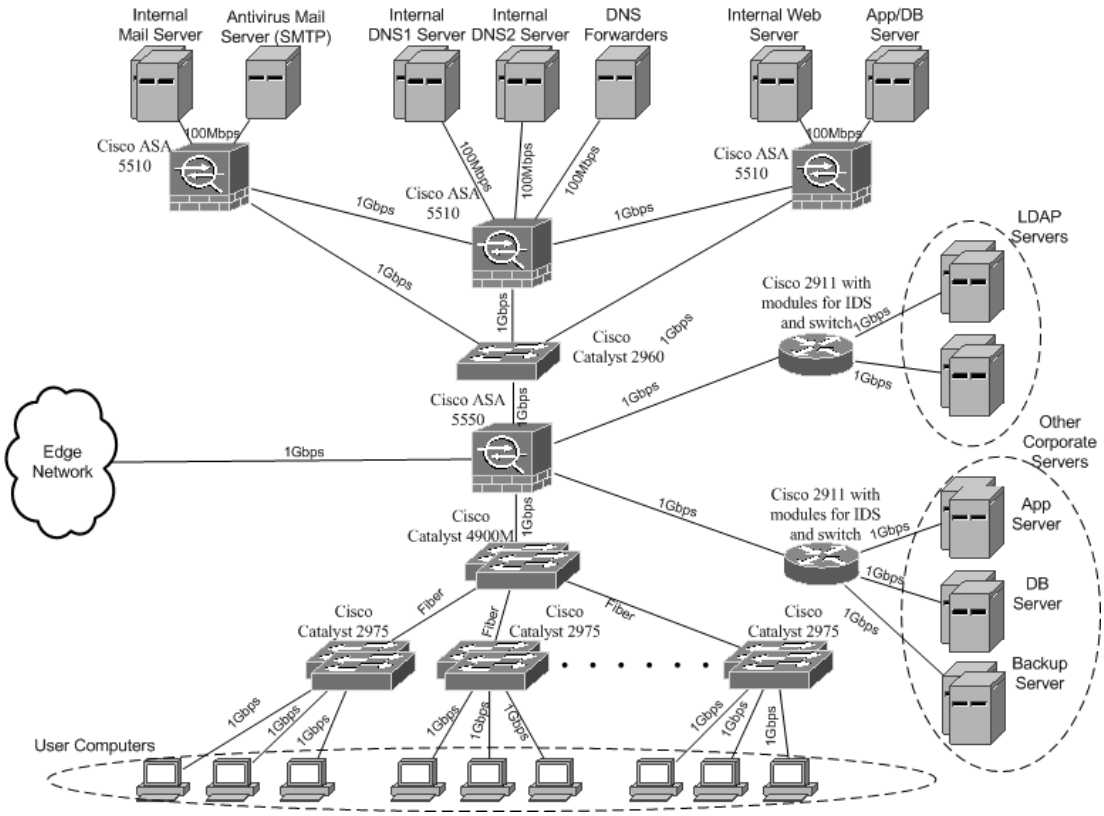

Рис.2.6. Пропонований дизайн внутрішньої мережі

2.5. Тестування мережевого обладнання та вимог безпеки у віртуальному середовищі

Віртуальне середовище тестування. Тестова модель створена у віртуальному середовищі, яке базується на двох різних технологіях віртуалізації. Одним із обраних інструментів є VMware Workstation 7.0, який був вибраний через його сумісність з усіма технологіями віртуалізації, що надаються виробниками центральних процесорних одиниць (ЦП).

VMware Workstation вирізняється своєю простотою у використанні та функціональністю, що дозволяє додавати кілька віртуальних мережевих адаптерів, встановлювати різноманітні операційні системи, налаштовувати необхідні апаратні ресурси та об'єднувати декілька віртуальних машин у одну групу. Таке об'єднання віртуальних машин у групу спрощує їх управління, порівняно з окремою роботою кожної машини.

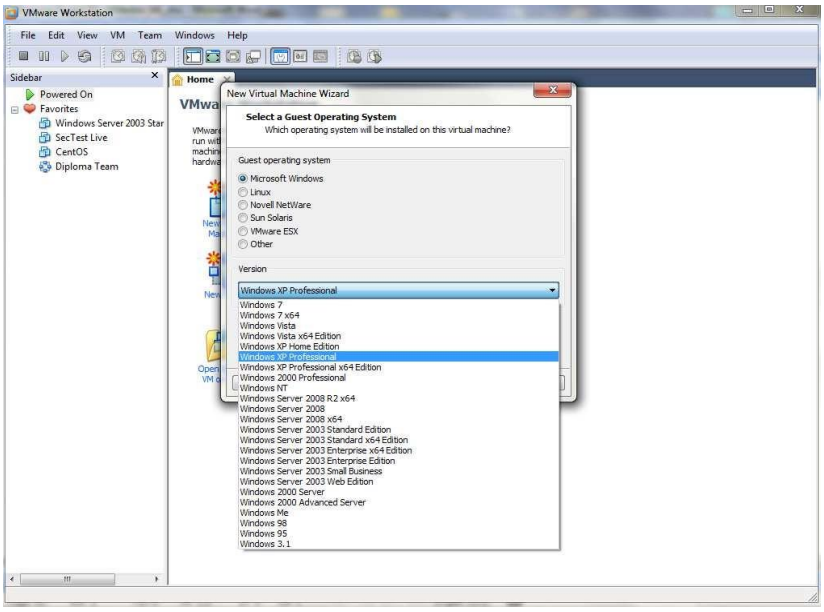

Рис.2.7. Вибір ОС в параметрах створення віртуальної машини

Також існує можливість організації мережі в різних топологіях, використовуючи різні сегменти локальної мережі, що дозволяє більш гнучко налаштовувати тестове середовище під конкретні потреби та цілі (рис.2.8-рис.2.10) [22].

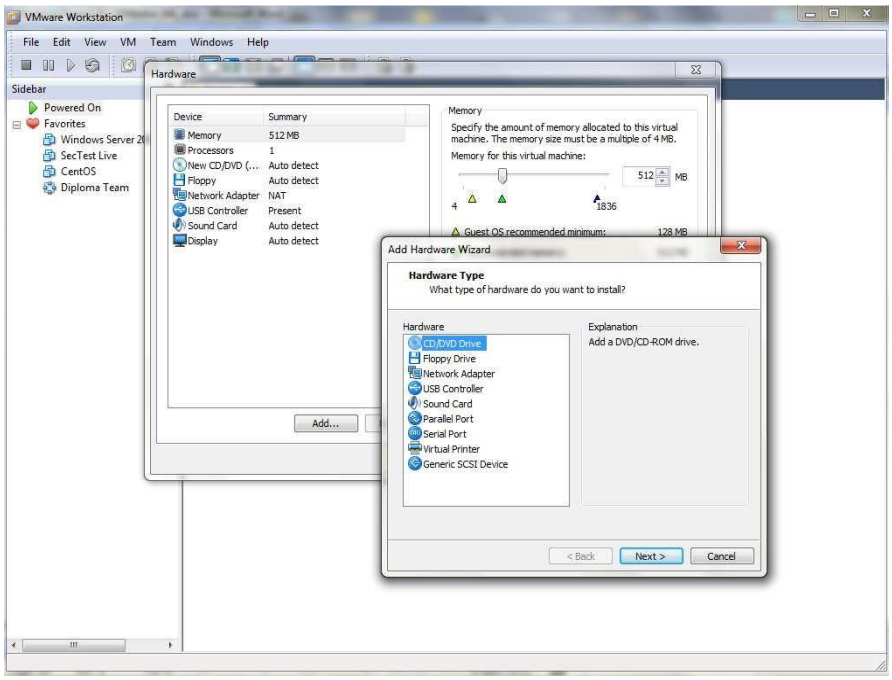

Рис.2.8. Налаштування обладнання

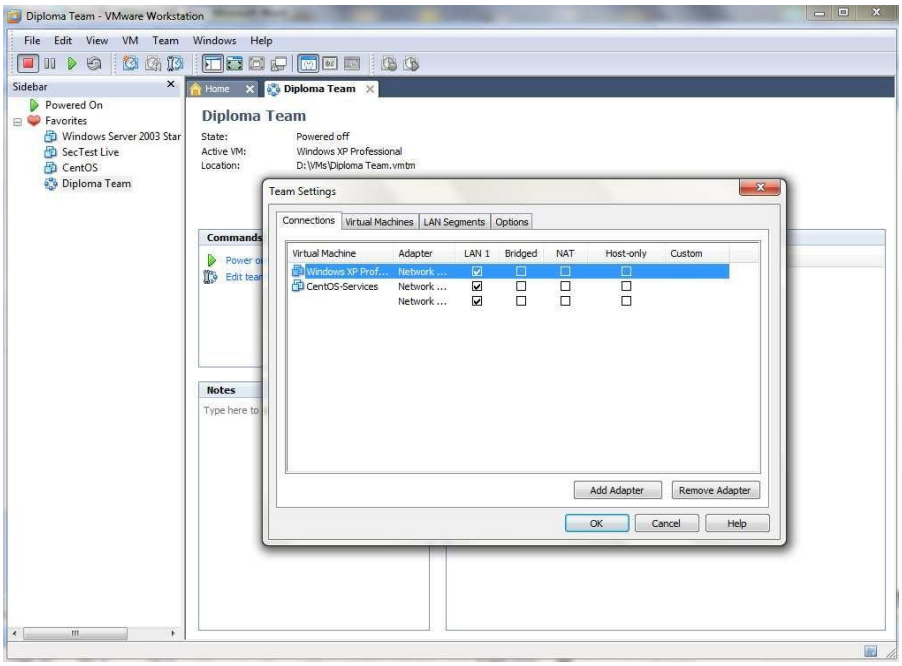

Рис.2.9. Конфігурація мережевого підключення

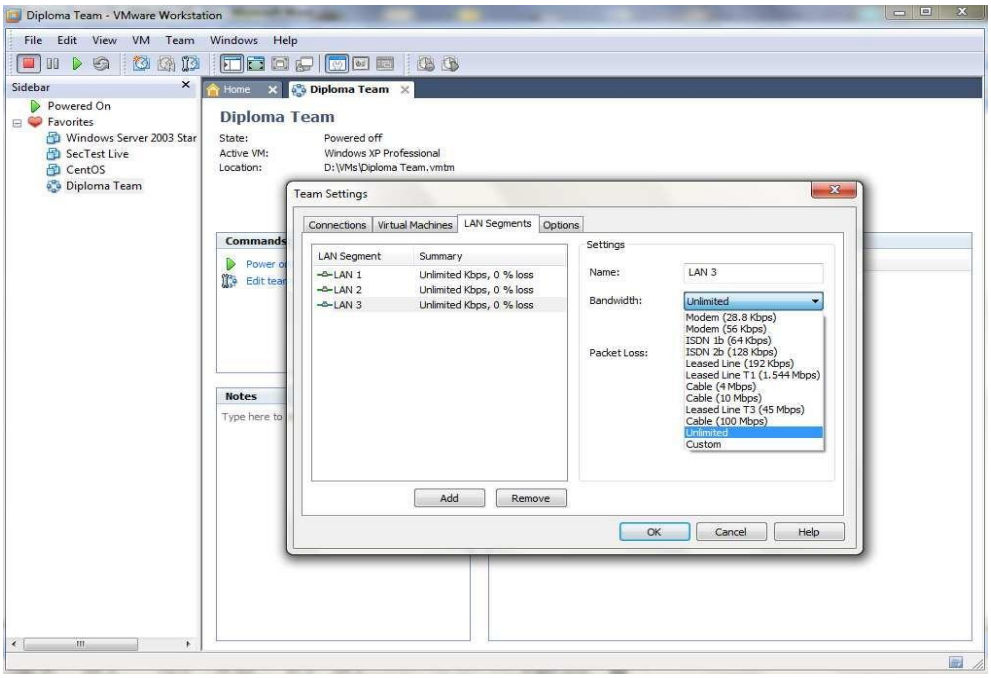

Рис.2.10. Конфігурація сегментів локальної мережі

Другий інструмент віртуалізації, обраний для моделювання мережевих пристроїв у мережі, – це GNS3. Цей інструмент вибрано через його здатність працювати з реальними маршрутизаторами, комутаторами та образами міжмережевих екранів, що управляються реальними операційними системами, аналогічними тим, що встановлені на фізичних пристроях.

GNS3 ефективно симулює мережеве обладнання CISCO та може імітувати майже всі типи мережевих пристроїв.

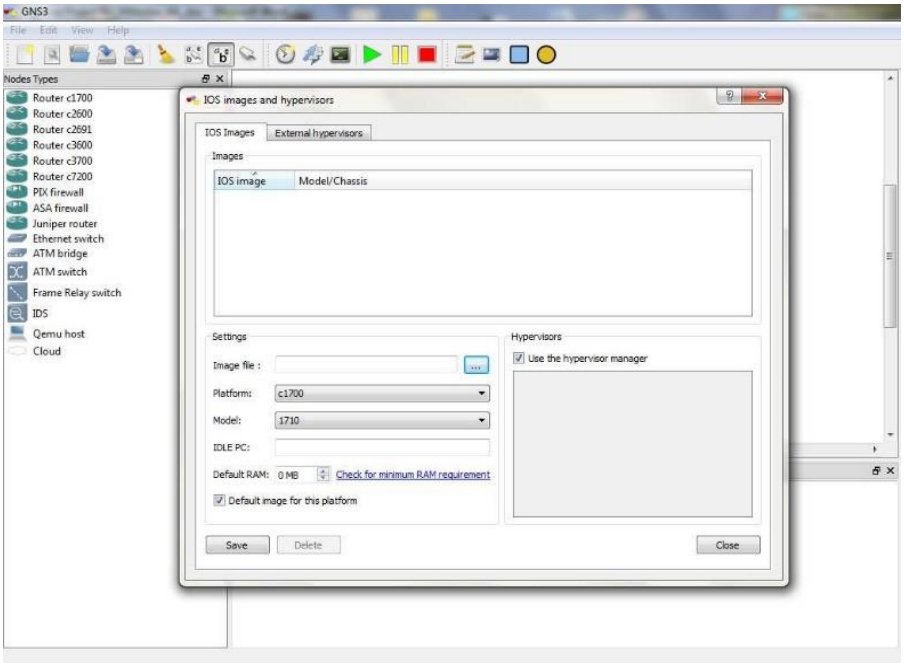

Рис.2.11. Додавання IOS в GNS3

Одна з ключових переваг GNS3 полягає у можливості додавання або видалення додаткових карт розширення, що є важливим, оскільки у запропонованому дизайні та обраному мережевому обладнанні використовувалися різні такі карти (рис.2.11).

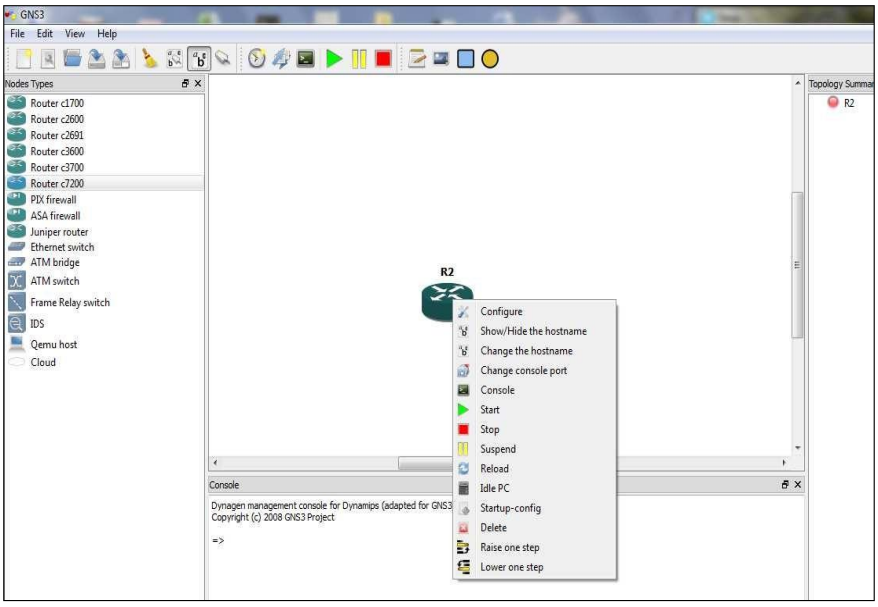

Рис.2.12. Додавання параметрів пристрою в GNS3

Крім того, у GNS3 можна додати ATM-комутатор, комутатор Frame Relay, імітувати всю мережеву хмару та інтегрувати в неї додаткові пристрої (рис.2.12).

Вибір GNS3 обумовлений його здатністю ефективно інтегрувати всі віртуальні машини, які виконують роль серверів, і все мережеве обладнання в одному місці, що дозволяє здійснювати необхідні конфігурації та тести (рис.2.13) [23].

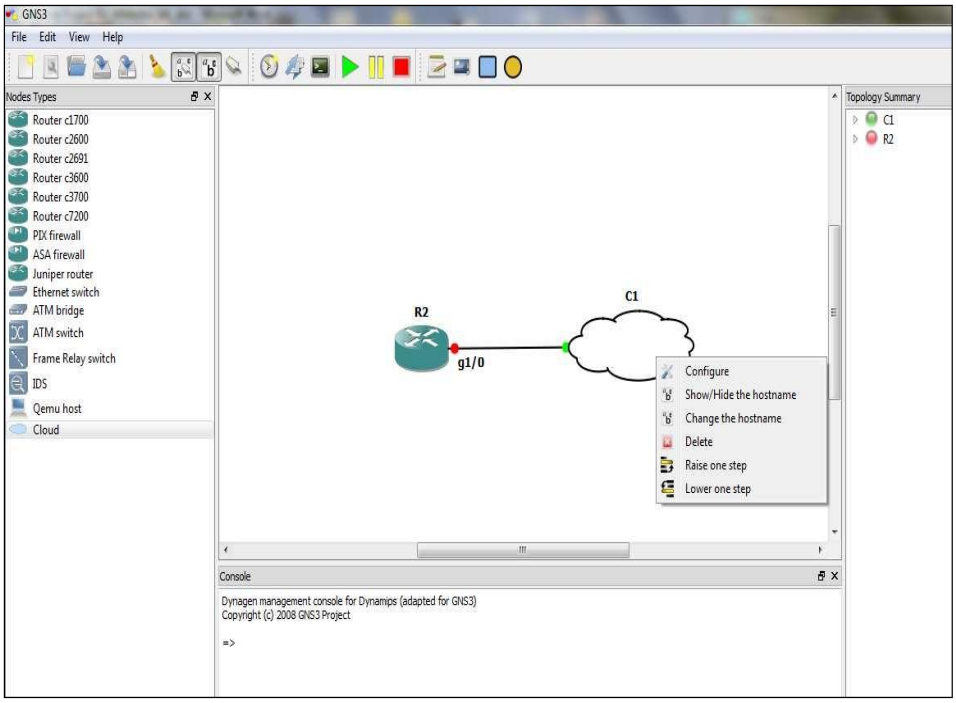

Рис.2.13. Підключення Router-Cloud в GNS3

Віртуальне середовище тестування. Віртуальне середовище реалізоване за допомогою двох продуктів віртуалізації: одного для віртуалізації серверів та іншого для віртуалізації мережевих пристроїв. Ця комбінація використовується для імплементації та перевірки запропонованого дизайну на обраних пристроях.

Додатково, в рамках тестування, використовується віртуальна машина з операційною системою Windows XP, на якій інстальовано Tenable Nessus 3 (TN3). TN3 є професійним інструментом для аудиту IT-безпеки, який здатен перевіряти безпеку обраного хоста, сервера або мережевого пристрою. Цей інструмент включає тисячі алгоритмів для сканування та дозволяє додавати різноманітні плагіни для специфічного типу сканування (рис.2.14).

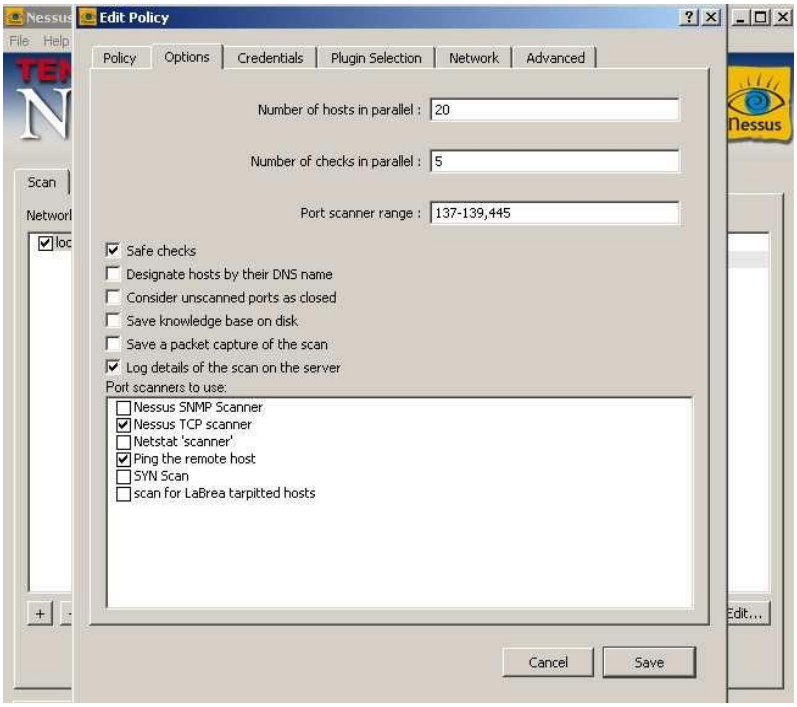

Рис.2.14. Основні функції і параметри Nessus3

Результати тестування та аналіз. Для зручності керування та конфігурації віртуального сервера на базі Linux використовувалася панель адміністрування Webmin. В усіх тестових сценаріях TCP-порт 10000 був відкритим, оскільки він використовується для зв'язку з операційною системою. Тести проводилися на двох різних об'єктах: віртуальному сервері та віртуальному мережевому пристрої.

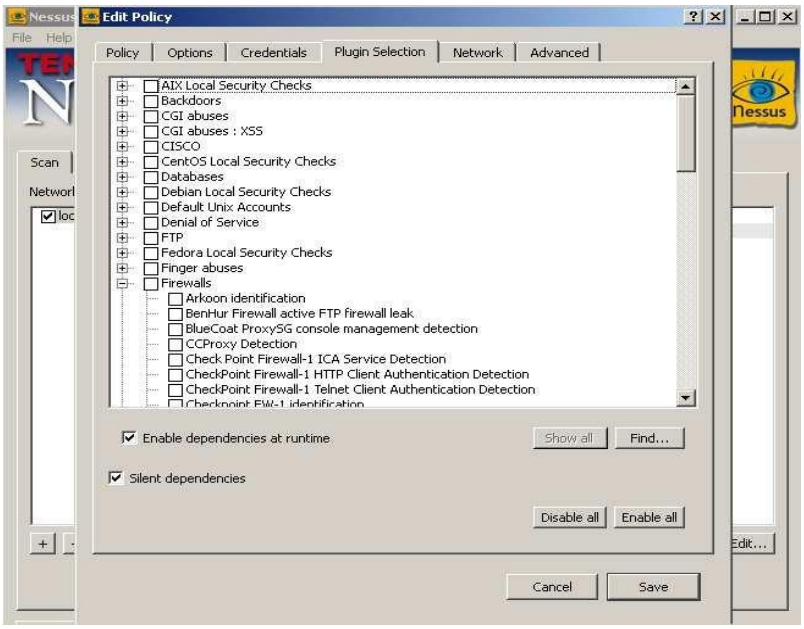

Рис.2.15. Вибір плагіна Nessus3

Тестування сервера. Основний веб-сервер, розташований у внутрішній частині мережі, було протестовано на предмет безпеки. Цей сервер реалізовано на Apache та сконфігуровано з урахуванням усіх заходів безпеки, що були описані в роботі. Це включає застосування методів загартування операційної системи та програм, використання криптографічних методів для https-служб та розміщення сервера в захищеній зоні мережі. Інформація, отримана в результаті тесту:

- Невідомих відкритих портів немає;
- Брандмауер захищає навіть порт, який використовується панеллю адміністрування, і не відображається як відкритий;
- TCP-порт 80 і 443 було відкрито (TCP-порт 22 також був відкритий, але це було виправлено після сканування).

Тестування брандмауера. Головний брандмауер, який розміщений у крайовій частині мережі, також було протестовано. Для цього використовувався віртуальний образ моделі брандмауера Cisco ASA5540. Результати тестування включають:

- Відсутність невідомих відкритих портів. Це свідчить про те, що брандмауер ефективно захищає мережу від несанкціонованого доступу;
- TCP-порт 22 виявлений відкритим і використовується для віддаленого доступу. Однак, списки контролю доступу (ACL) налаштовані так, що дозволяють доступ лише обмеженій кількості користувачів. Це забезпечує контрольований і безпечний доступ до мережевих ресурсів;
- Перевірка брандмауера на збереження стану також проведена. Брандмауер з збереженням стану важливий для відстеження та контролю мережевих сесій, що забезпечує додатковий рівень безпеки.

Ці результати тестування дозволяють зробити висновок про високий рівень безпеки, який забезпечує брандмауер у запропонованій мережевій структурі[24].

Висновки до розділу 2

Досліджено загальний дизайн корпоративної мережі, включаючи дві основні компоненти: дизайн крайової (Edge) мережі та дизайн внутрішньої мережі. Підкреслено важливість гнучкості дизайну, яка дозволяє ефективно адаптуватися до змінних корпоративних потреб і вимог.

Проаналізовано з'єднання між крайовою мережею та внутрішньою мережею, включаючи ключові аспекти дизайну, такі як визначення вимог, огляд можливих рішень та розгляд альтернативних підходів.

Особливу увагу приділено питанням безпеки та стабільності ключових послуг, таких як Mail, Web, DNS, які розміщені у периферійній мережі та доступні через Інтернет. Важливість правильного розміщення та налаштування серверів VPN, серверів AAA, серверів резервного копіювання та інших критичних корпоративних серверів також відзначена як ключовий елемент дизайну.

Оцінено важливість інтеграції та координації між різними компонентами мережі для забезпечення цілісності та високого рівня безпеки у всій корпоративній мережевій інфраструктурі.

Проаналізовано виклики, пов'язані з тестуванням сегментів мережі, зокрема проблеми з програмним забезпеченням впровадження мережевих пристроїв (GNS3) на операційній системі MS Windows. Встановлено, що проблеми з відкриттям попередньо збережених проектів можуть бути вирішені зміною основної операційної системи.

Зазначено, що незважаючи на виниклі проблеми, тести мережі були успішно виконані, демонструючи відсутність невідомих відкритих портів та інших серйозних проблем із безпекою, як підтверджено скануванням програмного забезпечення.

3 КОМПЛЕКСНЕ РІШЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДКЛЮЧЕННЯ ВІДДАЛЕНИХ КОРИСТУВАЧІВ ДО РЕСУРСІВ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1. Виклики при інтеграції віддалених користувачів в корпоративну мережу організації

Зростання сучасної розподіленої робочої сили ставить перед підприємствами будь-якого розміру нові виклики. У сучасному світі безпечний віддалений доступ працівників до хмарних сервісів, приватних центрів обробки даних та загальнодоступних інтернет-ресурсів набуває особливої важливості. Переваги таких ресурсів значні, однак ризики, пов'язані з їх використанням, також є великими.

IT-команди повинні забезпечити можливість безпечного доступу своїх користувачів до необхідних ресурсів з мінімальними взаємодіями, забезпечуючи при цьому максимальну безпеку. Це вимагає захисту кінцевих точок, на яких працюють користувачі, безпеки з'єднань з цих пристроїв, верифікації їхньої особи та захисту даних від потенційних загроз.

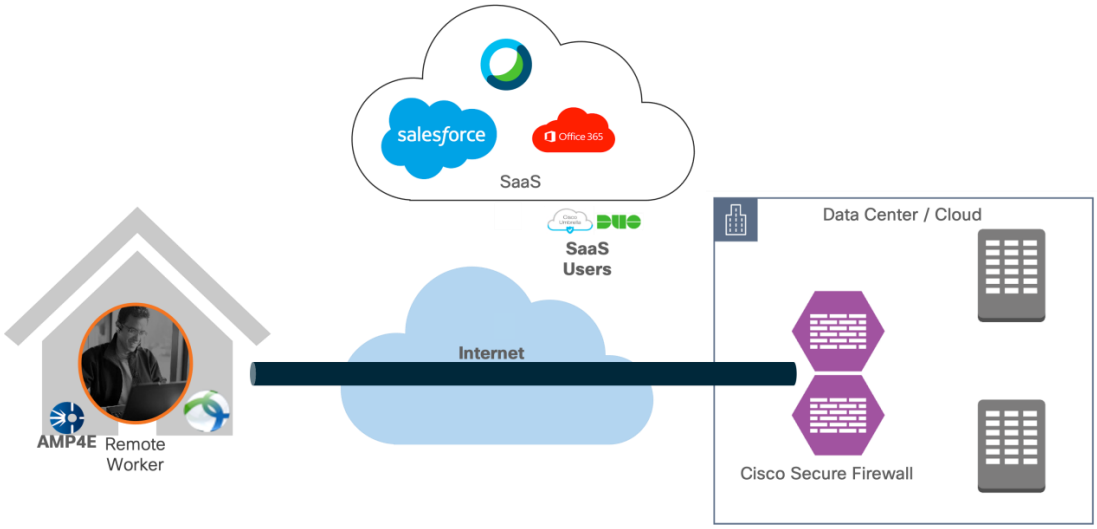

Рис.3.1. Cisco Remote Access VPN у приміщенні з безпечним брандмауером Cisco

Ефективне рішення передбачає застосування комплексного підходу, що включає використання надійних VPN-з'єднань для шифрування трафіку, розгортання систем ідентифікації та аутентифікації для перевірки осіб користувачів, а також впровадження політик кібербезпеки та методів керування кінцевими точками для забезпечення цілісності та конфіденційності даних. Захищені рішення для впровадження віддалених працівників в архітектуру корпоративної мережі використовують: Cisco Secure VPN, Cisco Secure Firewall, Cisco Secure Access by Duo, Cisco Umbrella та Cisco Secure Endpoint.

Статичний розділений тунель проти динамічного розділеного тунелю. Поведінка VPN-клієнта за замовчуванням полягає в тунелюванні всього трафіку. Працівник надсилає все через тунель, якщо не визначено розділений тунель. Роздільні тунелі бувають двох типів: статичні та динамічні.

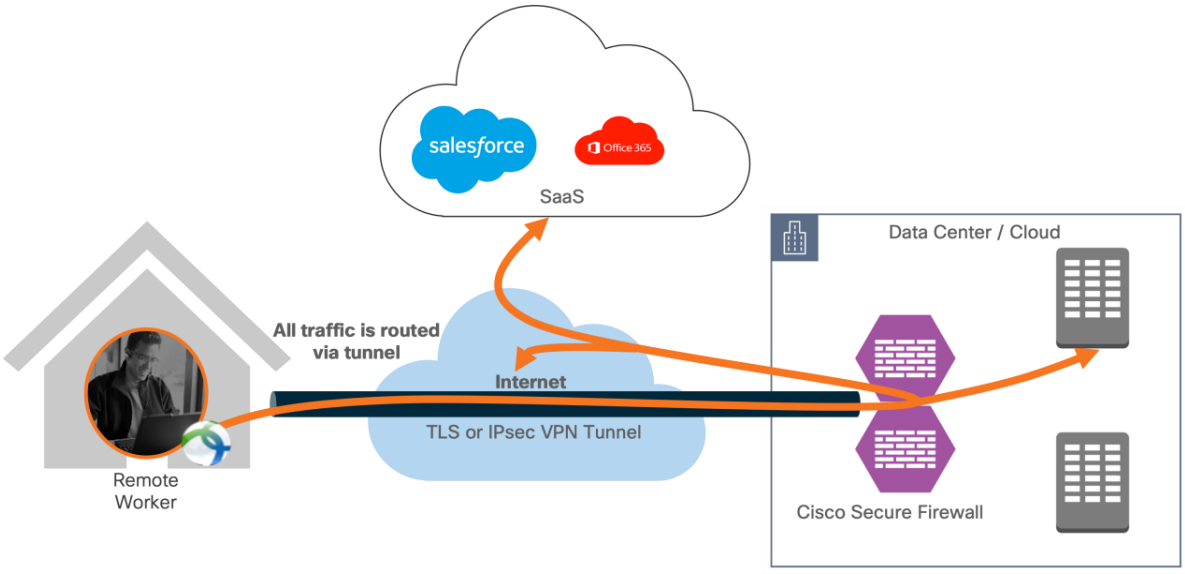

Рис.3.2. Приклад отримання доступу до корпоративних ресурсів віддаленим співробітником

Статичний розділений тунель. Статичне розділене тунелювання використовується для визначення IP-адрес хостів і мереж, які потрібно включати або виключати з VPN-тунелю віддаленого доступу. Основна обмеженість статичного розділеного тунелювання полягає в тому, що воно ґрунтується на статичних IP-адресах, зазначених у списку контролю доступу (ACL) розділеного

тунелю. Такий підхід може бути обмежуючим, оскільки не дозволяє адаптуватися до змін у мережевій інфраструктурі.

Динамічний розділений тунель. У відповідь на обмеження статичного тунелювання, динамічне розділене тунелювання дозволяє точніше налаштувати розділене тунелювання за допомогою доменних імен DNS. Завдяки використанню доменних імен DNS, які можуть асоціюватися з різними IP-адресами, що змінюються час від часу або різняться в залежності від географічного регіону, динамічне розділене тунелювання дозволяє більш гнучко визначати, який трафік має бути включений чи виключений з VPN-тунелю (рис.3.3.).

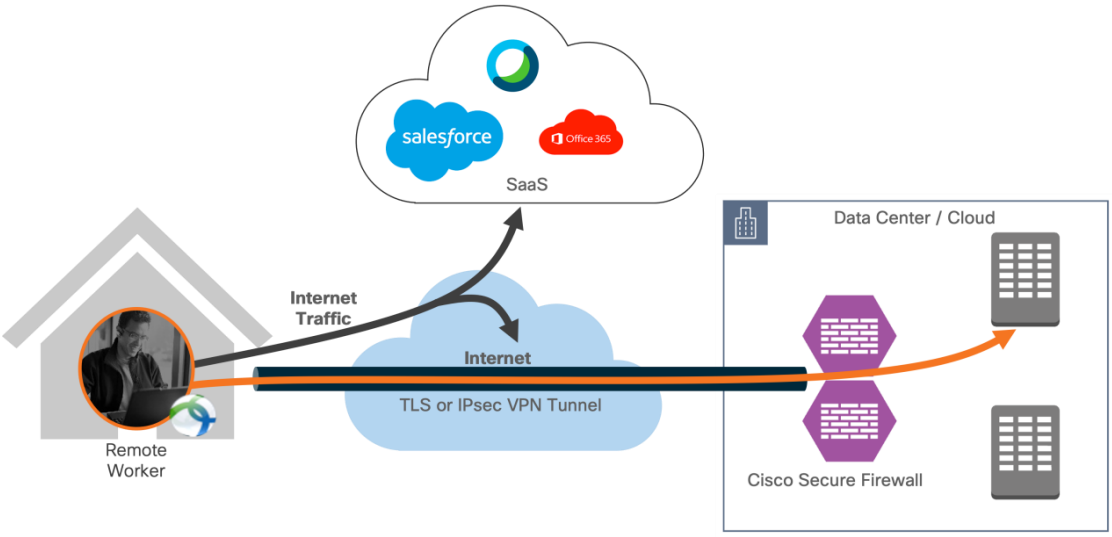

Рис.3.3. Надсилання трафіку через тунель VPN

Це забезпечує динамічне визначення маршрутизації трафіку, що підвищує ефективність віддаленого доступу через VPN. Важливо відмітити, що якщо будь-які IP-адреси, асоційовані з виключеними доменними іменами, знаходяться в межах пулу адрес, які включені до VPN, ці IP-адреси будуть автоматично виключені з тунелю, забезпечуючи точніше управління трафіком.

Модулі Cisco Secure VPN забезпечують захист, коли користувачі працюють у мережі VPN із увімкненим розділеним тунелем.

- Cisco Umbrella Roaming Module продовжує забезпечувати безпеку через Cisco Umbrella для трафіку, не призначеного для тунелю VPN;

● Cisco Secure Endpoint Enabler продовжує забезпечувати захист від вірусів і шкідливих програм;

● Cisco Secure Access від Duo продовжує надавати MFA для програм[25].

3.2. Дослідження рішень для розширення безпеки віддалених працівників

Для доповнення дизайну та архітектури корпоративної мережі, можна запропонувати розглянути наступні рішення Cisco, що використовуються для розширення безпеки віддалених працівників.

Таблиця 3.1

Пристрої та модулі для розширення безпеки для віддалених працівників в корпоративній мережі

Пристрої / Модулі	**Функціональність**
Cisco Secure VPN Mobility Client	VPN Client for endpoints
Cisco Secure Firewall (FTD)	VPN шлюз/VPN концентратор
Cisco Secure Access від Duo	Багатофакторна аутентифікація
Cisco Umbrella Roaming Security Module	Хмарна безпека
Cisco Secure Endpoint Enabler	Захист кінцевих точок від вірусів і шкідливих програм

Cisco Secure Access від Duo. Cisco Secure Access від Duo – зручний, масштабований спосіб тримати бізнес попереду постійно мінливих загроз безпеці завдяки реалізації частини моделі безпеки Zero Trust. Багатофакторна автентифікація від Duo захищає мережу за допомогою другого джерела перевірки, наприклад телефону або маркера, для перевірки особи користувача перед наданням доступу. Duo розроблено таким чином, щоб забезпечити простий і спрощений вхід для кожного віддаленого користувача. Як хмарне рішення, воно легко інтегрується з існуючою технологією та забезпечує адміністрування, видимість і моніторинг.

Cisco Secure Access by Duo інтегрується з Cisco FTD VPN, щоб додати двофакторну автентифікацію для входу в Secure VPN. Duo підтримує двофакторну аутентифікацію для FTD за допомогою аутентифікації RADIUS. Завдяки цій конфігурації кінцеві користувачі отримують автоматичний push або телефонний дзвінок для багатофакторної автентифікації після надсилання своїх основних облікових даних за допомогою Secure VPN Mobility Client. Користувачі можуть додати інший фактор до свого введення пароля[26].

Cisco Secure VPN. Cisco Secure VPN надає віддаленим працівникам безперешкодний, високозахищений доступ до корпоративної мережі з будь-якого пристрою, у будь-який час і в будь-якому місці, одночасно захищаючи організацію. Він забезпечує узгоджену взаємодію з користувачами на всіх пристроях, як на території, так і за її межами, не створюючи головного болю для ваших IT-команд. Спростіть керування за допомогою одного агента.

Модуль Cisco Umbrella Roaming Security. Модуль Cisco Umbrella Roaming Security для Cisco Secure VPN забезпечує постійну безпеку в будь-якій мережі, будь-де та будь-коли. Модуль безпеки роумінгу забезпечує безпеку через Secure Internet Gateway (SIG) Umbrella. Cisco Umbrella SIG об’єднує кілька функцій в одному рішенні, для якого традиційно потрібен набір локальних пристроїв безпеки (міжмережеві екрани, проксі-сервери, шлюзи) або однофункціональні хмарні рішення безпеки. Umbrella забезпечує видимість у режимі реального часу та контроль за всією діяльністю в Інтернеті як у вашій мережі, так і за її межами.

Cisco Secure Endpoint (AMP) Enabler. Модуль Cisco Secure VPN AMP Enabler використовується як середовище для розгортання Cisco Secure Endpoint, раніше — Advanced Malware Protection (AMP). Цей підхід надає роумінгу додатковий агент безпеки, який діє як система захисту від вірусів і зловмисного програмного забезпечення. Він виявляє потенційні загрози зловмисного програмного забезпечення, видаляє ці загрози та захищає пристрої від зламу. Cisco Secure Endpoint захищає користувача як у мережі, так і поза нею.

Cisco Secure Firewall. Захищений міжмережевий екран Cisco Secure Firewall, що використовує Firepower Threat Defense (FTD), допомагає запобігти зламам,

отримати видимість для швидкого припинення загроз і автоматизувати операції для економії часу. Брандмауер наступного покоління — це пристрій мережевої безпеки, який надає можливості, окрім традиційного брандмауера з контролем стану, додаючи такі можливості, як віртуальна приватна мережа (VPN), видимість і контроль програм (AVC), IPS наступного покоління (NGIPS), фільтрація URL-адрес і розширений захист від шкідливих програм. Cisco FTD доступний на апаратному забезпеченні та як віртуальний пристрій.

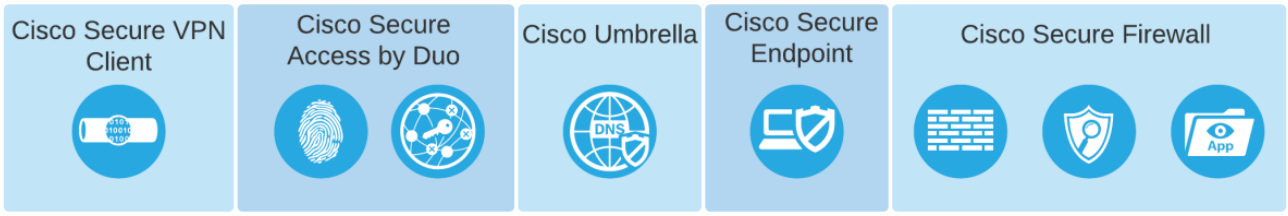

Рис.3.4. Інтеграція продуктів Cisco для безпечної роботи віддалених працівників

3.3. Налаштування політик безпеки для рішень Cisco

Перш ніж виконувати кроки щодо розгортання безпечного підключення віддалених працівників, спочатку потрібно налаштувати політики для модулів VPN.

Umbrella. Ця політика застосовуватиметься до всіх віддалених працівників, які перебувають у роумінгу.

Крок 1. Необхідно перейти до «Політики» - «Керування» - «Політики DNS» (рис.3.5).

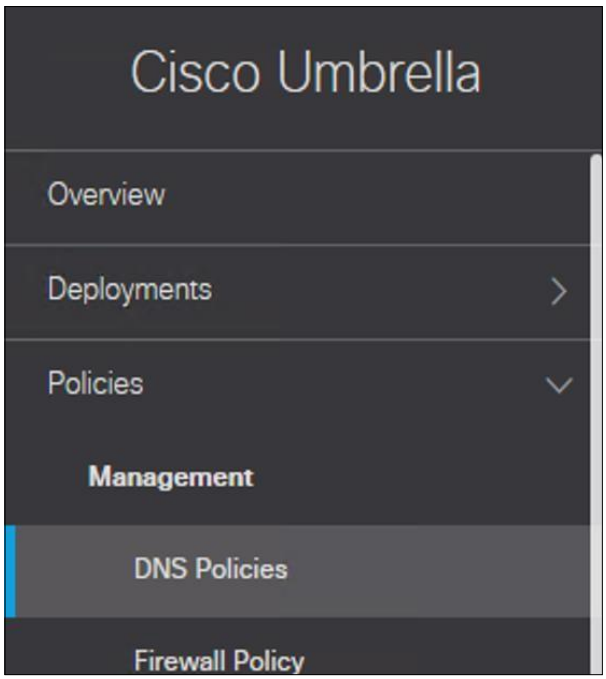

Рис.3.5. Налаштування політики DNS для Umbrella

Крок 2. Додати нову політику.

Крок 3. Залишити всі представлені вимоги за замовчуванням і натиснути «Далі» (рис.3.6).

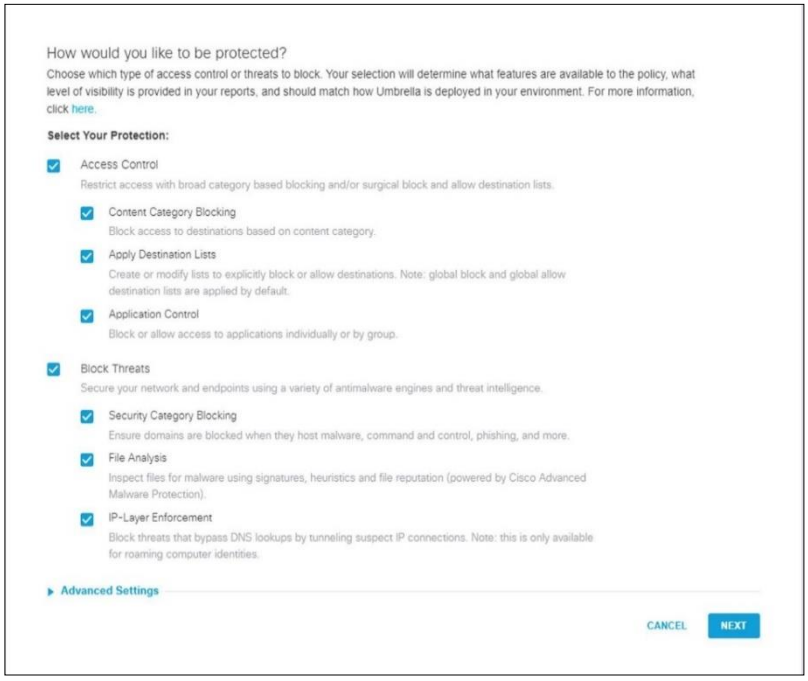

Рис.3.6. Налаштування Umbrella за замовчуванням

Крок 4. Додавання кінцевих пристроїв віддалених працівників до політики та натиснути «Далі».

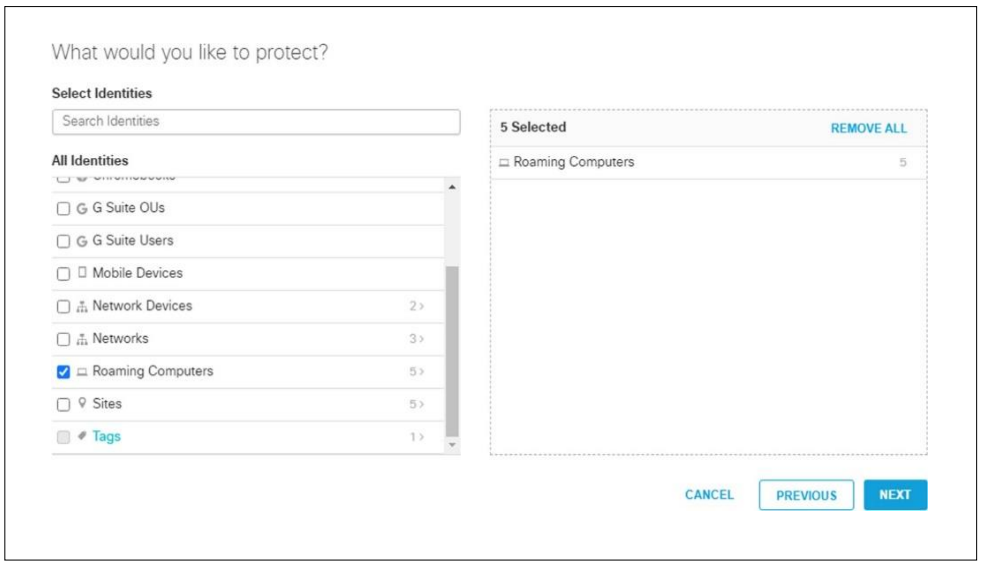

Рис.3.7. Додавання кінцевих пристроїв віддалених працівників до політики Umbrella

Крок 5. Всі параметри на наступній сторінці налаштування потрібно залишити без змін. Натиснути «Далі».

Крок 6. Змінити доступ до вмісту на «Moderate» та натиснути «Далі».

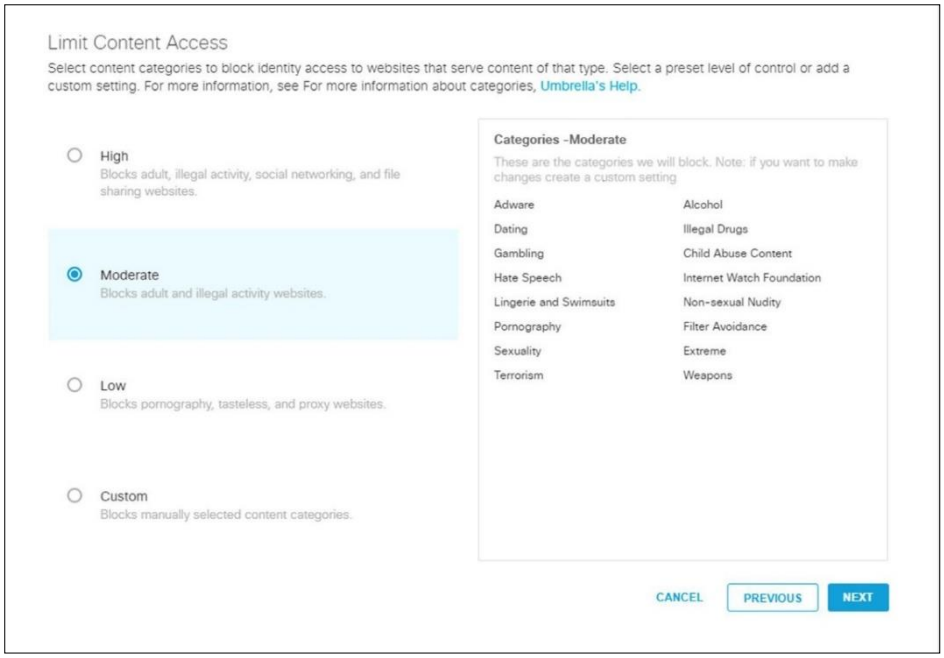

Рис.3.8. Зміна доступу до вмісту

Крок 7. Розділ «Control Applications» залишити без змін, та натиснути «Далі».

Крок 8. Застосувати список адресатів до користувачів у роумінгу. Натиснути «Далі».

Крок 9. Надати зрозумілу назву для політики безпеки та зберегти (рис.3.9). Налаштування завершені[27].

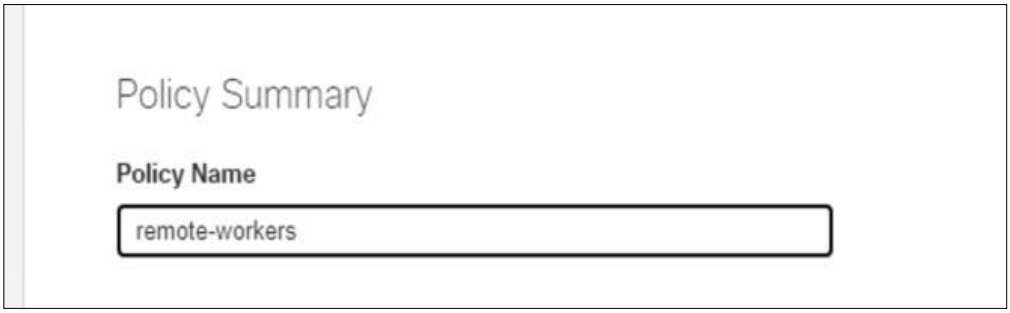

Рис.3.9. Збереження політики Umbrella

Secure Endpoint. Щоб створити модуль AnyConnect, потрібно створити групу Secure Endpoint. Наступні кроки описують створення цієї групи (рис.3.10)

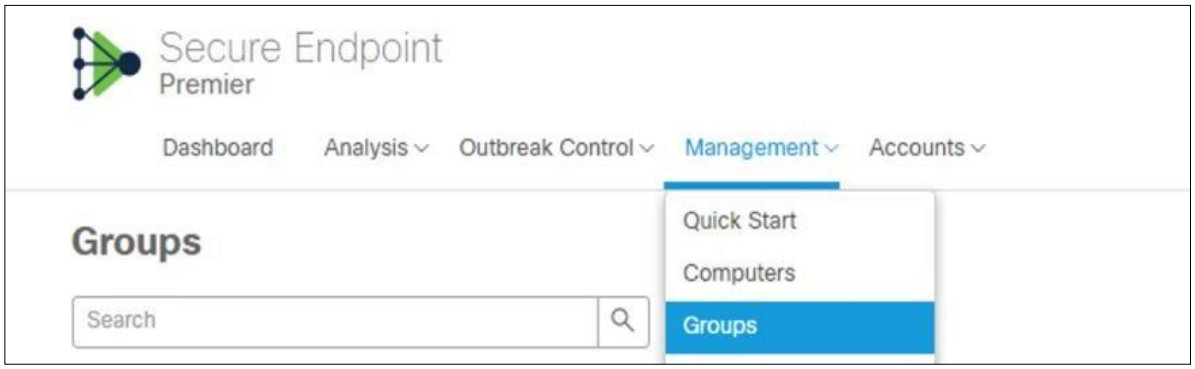

Рис.3.10. Створення налаштувань Secure Endpoint

Крок 1. Перейти до «Керування» - «Групи».

Крок 2. Натиснути «Створити групу» праворуч.

Крок 3. Надати новій групі нову назву та залишити всі налаштування як за замовчуванням, а потім зберегти.

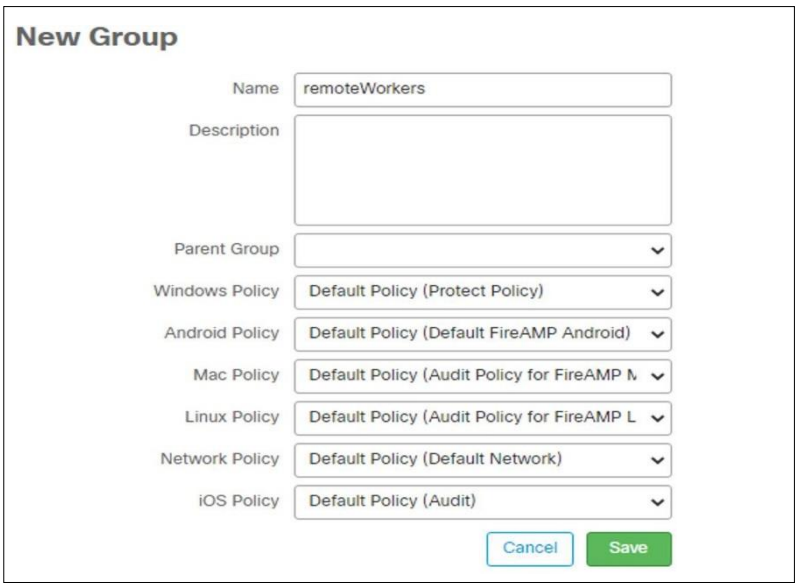

Рис.3.11. Збереження налаштувань Secure Endpoint

3.4. Налаштування рішень для безпечної роботи віддалених працівників в корпоративній мережі

3.4.1. Налаштування інтерфейсів

Як правило, необхідно налаштувати щонайменше два інтерфейси, щоб мати систему, яка пропускатиме необхідний для роботи віддалених працівників трафік.

У загальному випадку, мережева архітектура включає зовнішній інтерфейс, орієнтований на вихідний маршрутизатор або Інтернет, а також один або кілька внутрішніх інтерфейсів, призначених для мереж всередині організації.

У контексті проектування мережі, зовнішній інтерфейс часто використовується як вхідний інтерфейс для VPN-з'єднань, тоді як внутрішній інтерфейс вказує на з'єднання з рештою корпоративної мережі. Для детального розуміння налаштування цих інтерфейсів важливо звернутися до відповідних ресурсів у Центрі керування брандмауером. Це може включати інструкції або керівництва з налаштування мережевих параметрів, конфігурації забезпечення безпеки, а також рекомендації щодо оптимального використання апаратних ресурсів для ефективного керування мережевим трафіком.

Налаштування захисту зовнішнього інтерфейсу

Крок 1. Перейти до «Пристрої» - «Керування пристроями в FMC». Натиснути назву пари FTD або HA (High Availability).

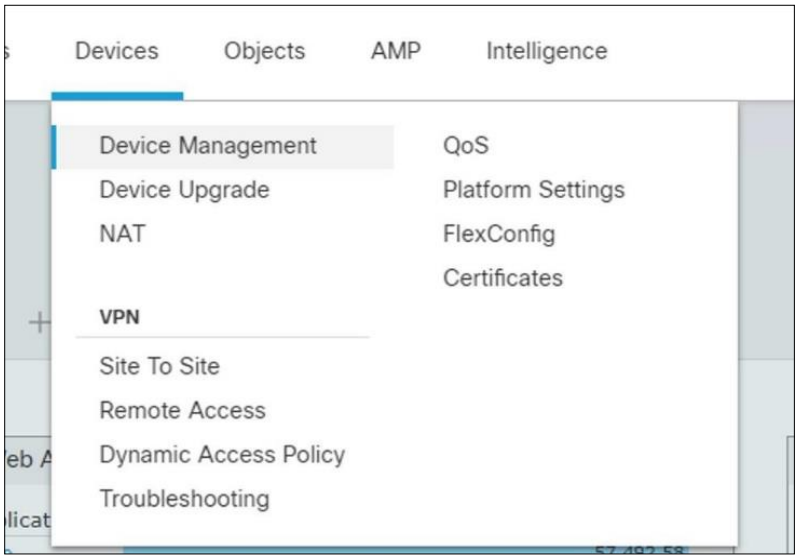

Рис.3.12. Керування пристроями в FMC

Крок 2. Перейти на вкладку «Інтерфейси». Відредагувати інтерфейс, який відповідає за надсилання запитів назовні, використовуючи піктограму олівця з правого боку. У цьому випадку це port-channel1. Змінити назву.

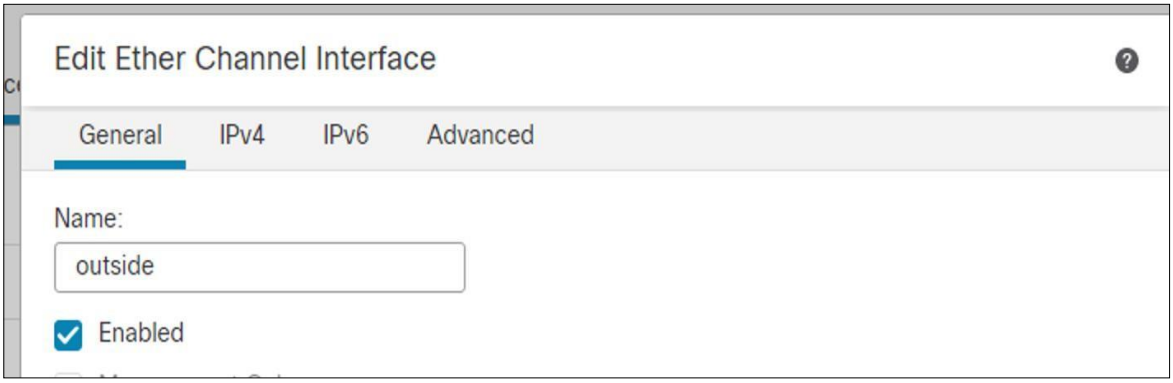

Рис.3.13. Налаштування інтерфейсів

Крок 3. Створіть нову зону. Змінити назву, та переконатися, що зону було створено та заповнено в спадному списку.

Крок 4. Перейти на вкладинку з налаштуваннями IPv4. Заповнити загальнодоступну IP-адресу організації з маскою мережі 255.255.255.254. Натиснути «OK» та переконатися, що інформація про інтерфейс є на сторінці

інтерфейсу пристрою. Натиснути «Зберегти» у верхньому правому куті, для збереження конфігурації внутрішнього інтерфейсу[28].

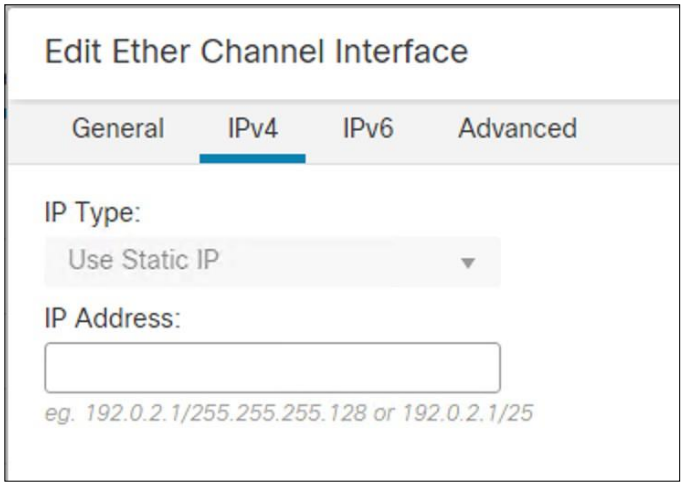

Рис.3.14. Налаштування IPv4

Налаштування захисту внутрішнього інтерфейсу

Крок 1. Для внутрішнього інтерфейсу необхідно повторити аналогічні дії, що й для зовнішнього інтерфейсу.

Крок 2. Встановити внутрішню IP-адресу як шлюз для всіх внутрішніх IP-адрес. Натиснути «ОК», та переконатися, що інформація є на вкладинці «Інтерфейси». Зберегти конфігурацію у верхньому правому куті.

3.4.2. Налаштування маршрутизації

Cisco FTD підтримує кілька Інтернет-протоколів для маршрутизації, а саме:

- Розширений внутрішній протокол маршрутизації шлюзу (EIGRP);
- Спочатку відкрити найкоротший шлях (OSPF);
- Протокол інформації про маршрутизацію (RIP);
- Протокол прикордонного шлюзу (BGP).

Для налаштувань маршрутизації необхідно:

Крок 1. Перейти до «Пристрої» - «Керування пристроями в FMC», та натиснути «FTD» або «HA».

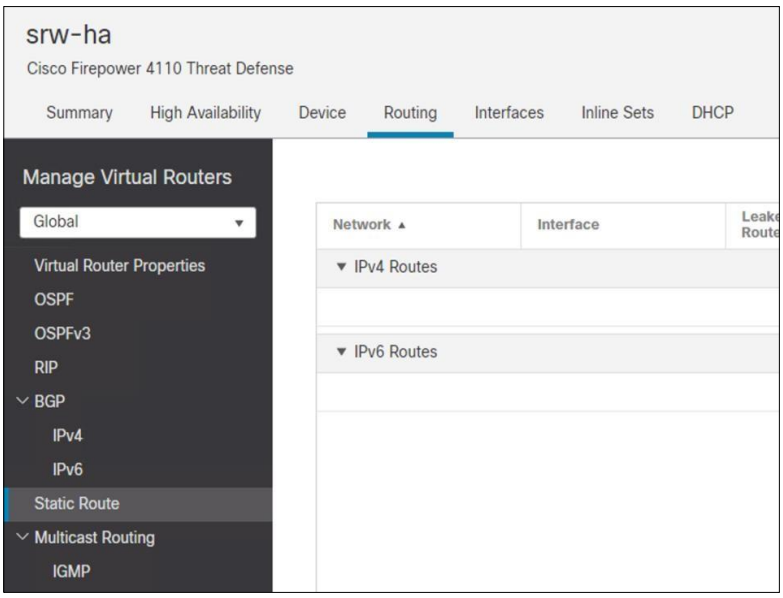

Рис.3.15. Налаштування маршрутизації

Крок 2. Перейти на вкладинку «Маршрутизація», а потім у розділ «Статичний маршрут», та натиснути «Додати маршрут».

Крок 3. Обрати зовнішній інтерфейс, а потім створити нову доступну мережу. Після чого, необхідно назвати її. Для використання мережі Інтернет, необхідно внести зміну мережі на 0.0.0.0/0 і зберегти.

Крок 4. Додати щойно створену мережу до розділу «Вибрана мережа» за допомогою меню «Додати» та створити новий шлюз, натиснувши символ (+).

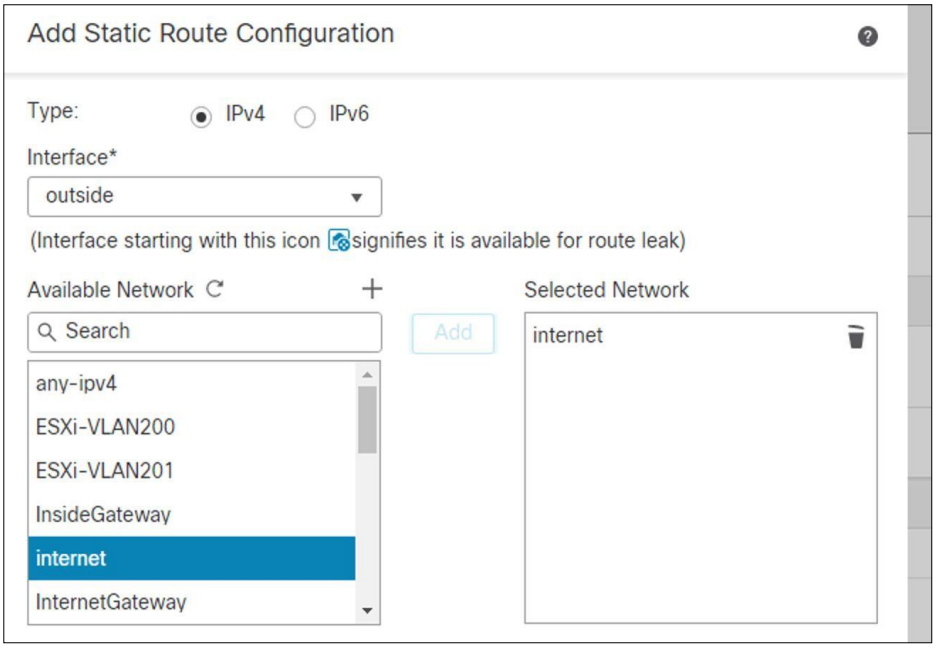

Рис.3.16. Внесення змін в конфігурування маршрутизації

Крок 5. Додати нову назву. Заповнити поле хоста інформацією щодо зовнішнього інтерфейсу та натиснути «Зберегти». Необхідно також переконатися, що інформація є на сторінці статичного маршруту, і зберегти конфігурацію у верхньому правому куті FMC (рис.3.17) [29].

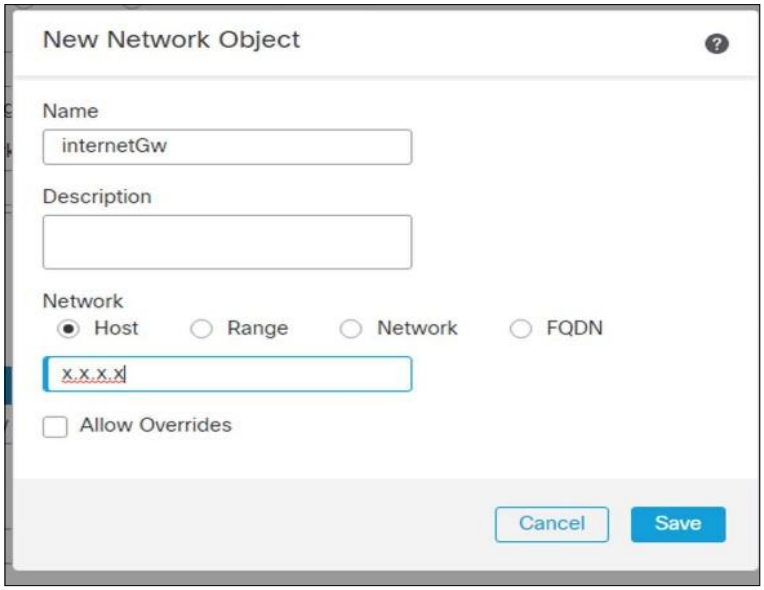

Рис.3.17. Збереження оновлень щодо маршрутизації

3.4.3. Налаштування NAT

Cisco Firepower Threat Defense (FTD), яке використовується для доступу до VPN, служить також межею Інтернету для мережі. Для ефективного забезпечення доступу внутрішньої мережі до Інтернету необхідно реалізувати мережеву адресну трансляцію (NAT).

NAT використовується для забезпечення доступу внутрішніх хостів до Інтернету, що важливо для оновлень програмного забезпечення, виконання завдань на місці, використання Firepower Management Center (FMC) та задоволення інших потреб програм, які потребують доступу до Інтернету. У випадку, коли межа Інтернету розташована в іншій частині мережі, слід пропустити налаштування NAT на Cisco FTD і встановити маршрутизацію між брандмауером VPN та крайовим маршрутизатором або маршрутизаторами. Це забезпечить коректне спрямування трафіку між внутрішньою мережею та Інтернетом через визначені мережеві вузли.

Крок 1. Перейти до «Пристрої» - «NAT» (рис.3.18).

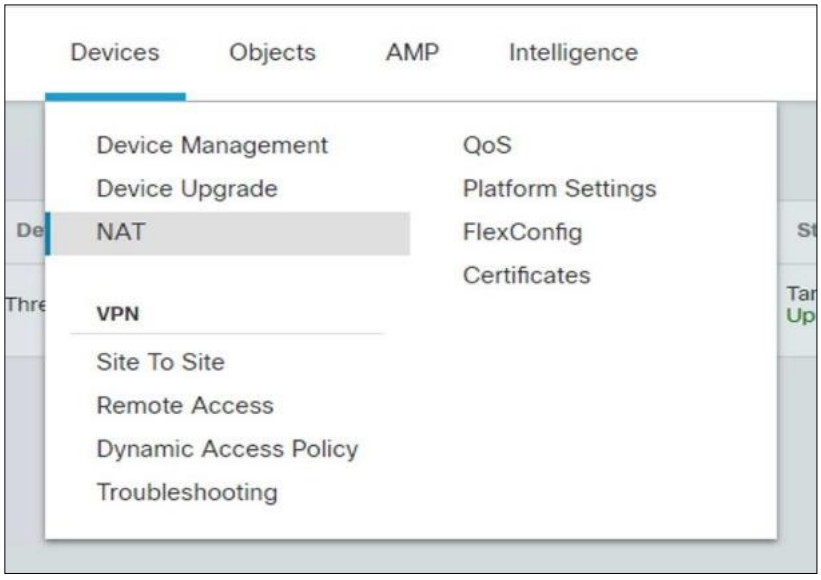

Рис.3.18. Налаштування NAT

Крок 2. Створити нову політику за допомогою параметра NAT захисту від загроз. Додати нову назвудо політики, додати пристрій FTD у розділ «Вибрані пристрої» та натиснути «Зберегти» (рис.3.19).

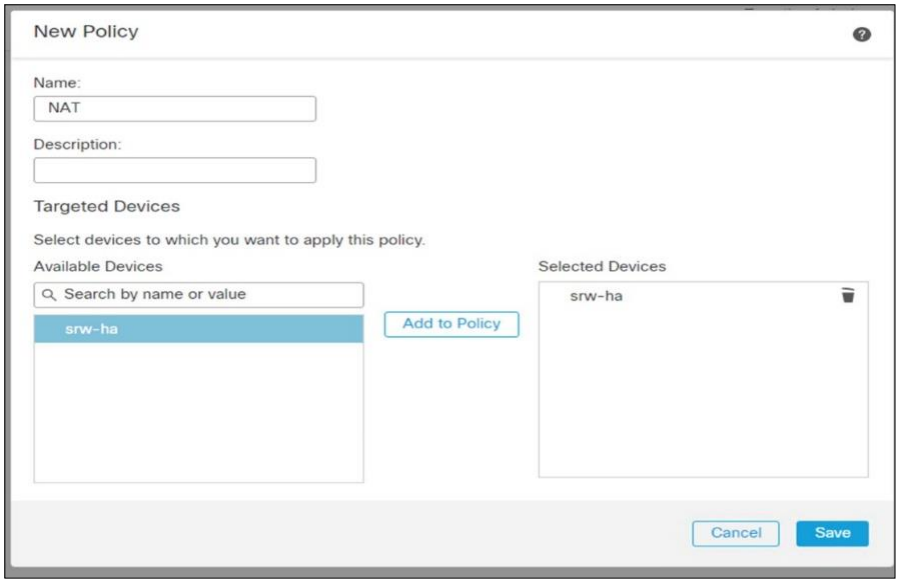

Рис.3.19. Додавання політики до NAT

Крок 3. При необхідності, внести правки до нової політики NAT за допомогою значка олівця та створити нове правило.

Крок 4. На вкладинці «Переклад» прибрати «Оригінальне джерело», «Оригінальне призначення» на «Адреса» і IP-адресу інтерфейсу до призначення

Крок 5. На вкладинці «Об’єкти інтерфейсу» додати всередину до об’єктів вихідного інтерфейсу та зовні до «Цільові інтерфейсні об’єкти». Натиснути «Зберегти». Переконатися, що правило є в списку (рис.3.20).

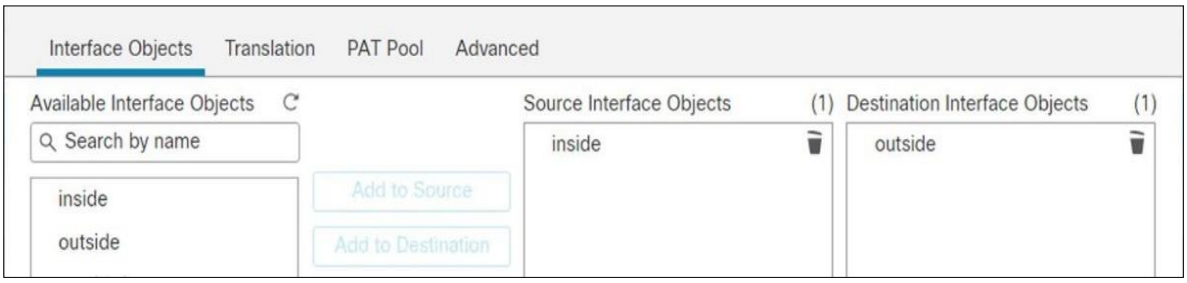

Рис.3.20. Об’єкти інтерфейсу

3.4.4. Налаштування Cisco Secure Access від Duo

Для встановлення проксі-сервера автентифікації, необхідно дотримуватися вимог Cisco Firepower Threat Defense VPN with AnyConnect.

Для уникнення необхідності ручного створення нового користувача при кожній потребі входу в систему можна застосувати Duo Directory Sync. Цей інструмент дозволяє автоматично синхронізувати користувачів і групи з сервера Active Directory (AD) через проксі-сервер автентифікації. Для налаштування Directory Sync необхідно слідувати відповідним інструкціям. Якщо проксі-сервер автентифікації вже встановлено, існує можливість додавання нового розділу для хмарних служб до існуючої конфігурації замість встановлення другого проксі-сервера. Файл конфігурації для проксі-сервера автентифікації повинен бути відповідно оновлений та налаштований для відображення цих змін (рис.3.21).

```
[ad_client]
host=10.22.1.50
service_account_username=administrator
service_account_password=*********
search_dn=DC=srwlab03,DC=com

[radius_server_auto]
ikey=DIxxxxxxxxxxx
skey=Dbxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-XXXXXXXX.duosecurity.com
radius_ip_1=0.0.0.0/0
radius_secret_1=**********
failmode=safe
client=ad_client
port=1812

[cloud]
ikey=DXXXXXXXXXXXXXXXXX
skey=iAXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXXX.duosecurity.com
service_account_username=administrator
service_account_password=*********
```

Рис.3.21. Файл конфігурації проксі-сервера автентифікації

Це забезпечить інтеграцію між Duo Directory Sync та сервером AD, що дозволить автоматично керувати користувачами та групами без потреби в ручному втручанні[30].

Алгоритм налаштування політики безпеки Duo. Необхідно змінити політику для програми FTD VPN, створеної в Duo, щоб вона дозволяла підключення лише з певних IP-адрес і блокувала всі інші.

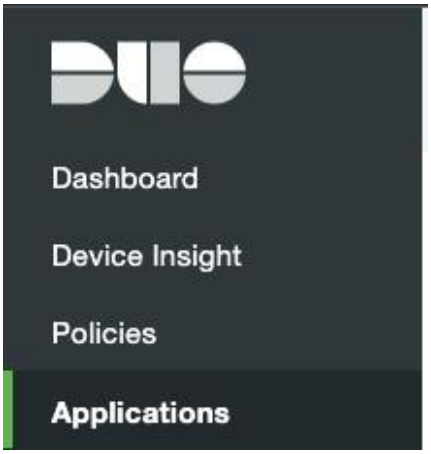

Рис.3.22. Внесення змін до політики безпеки Duo

Крок 1. На інформаційній панелі адміністрування Duo необхідно перейти до «Програми».

Крок 2. Обрати програму, яка використовується для захисту VPN-підключення до FTD.

Крок 3. Перейти до «Політика» та в розділі «Політика програми» натиснути «Редагувати».

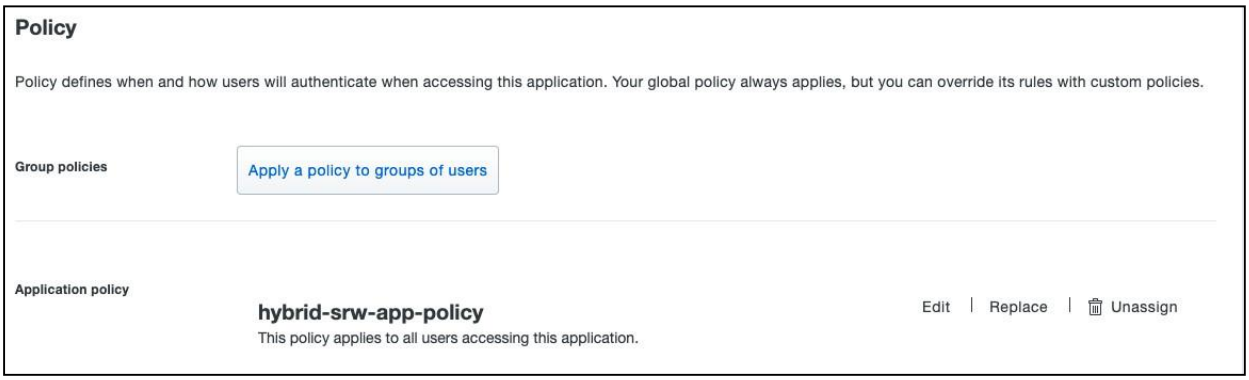

Рис.3.23. Редагування політики безпеки Duo

Крок 4. У розділі «Розташування користувача» необхідно клацнути на рядок пошуку та обрати країни, для яких буде ввімкнено доступ до VPN. Біля «Усі інші країни» обрати «Заборонити доступ» та натиснути «Зберегти політику».

3.4.5. Налаштування модуля безпеки Cisco Umbrella Roaming Security

Модуль Cisco Umbrella Roaming Security використовуватиметься для захисту користувачів під час увімкнення або вимкнення VPN. Алгоритм налаштування наступний:

Крок 1. Необхідно увійти у обліковий запис Cisco Umbrella на dashboard.umbrella.com

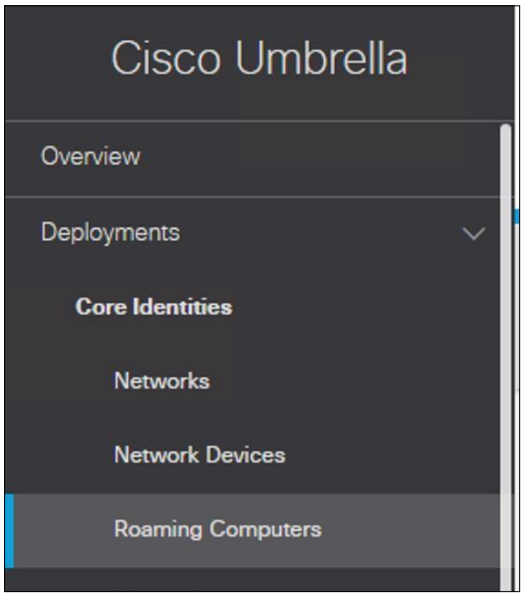

Рис.3.24. Підключення облікового запису Cisco Umbrella

Крок 2. Перейти до «Розгортання» - «Переміщені ПК», та натиснути кнопку «Завантаження клієнта роумінгу». Після чого, необхідно «Завантажити профіль модуля». Його слід завантажити як OrgInfo.json. Далі - додати профіль до профілю VPN (рис.3.25).

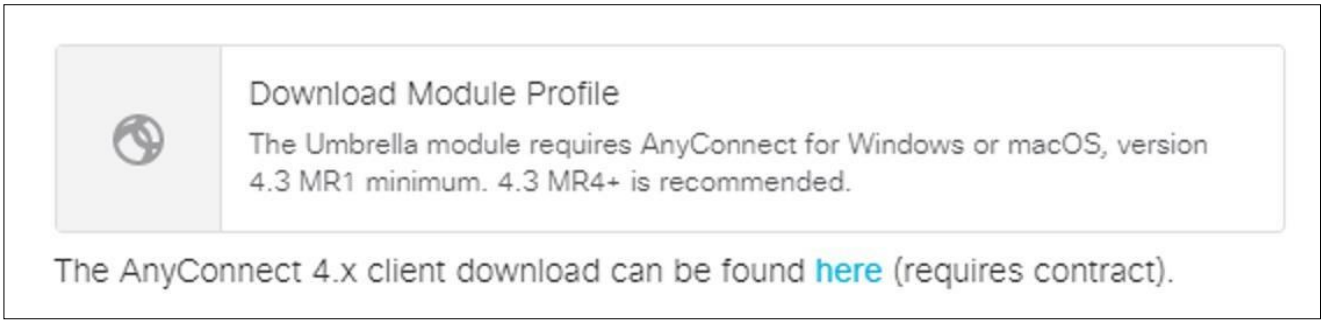

Рис.3.25. Завантаження профілю модуля

Крок 3. У FMC перейти до «Пристрої» - «VPN віддаленого доступу» та відредагувати створену політику VPN. Також необхідно внести правки до профілю підключення, та відредагувати групову політику (рис.3.26)

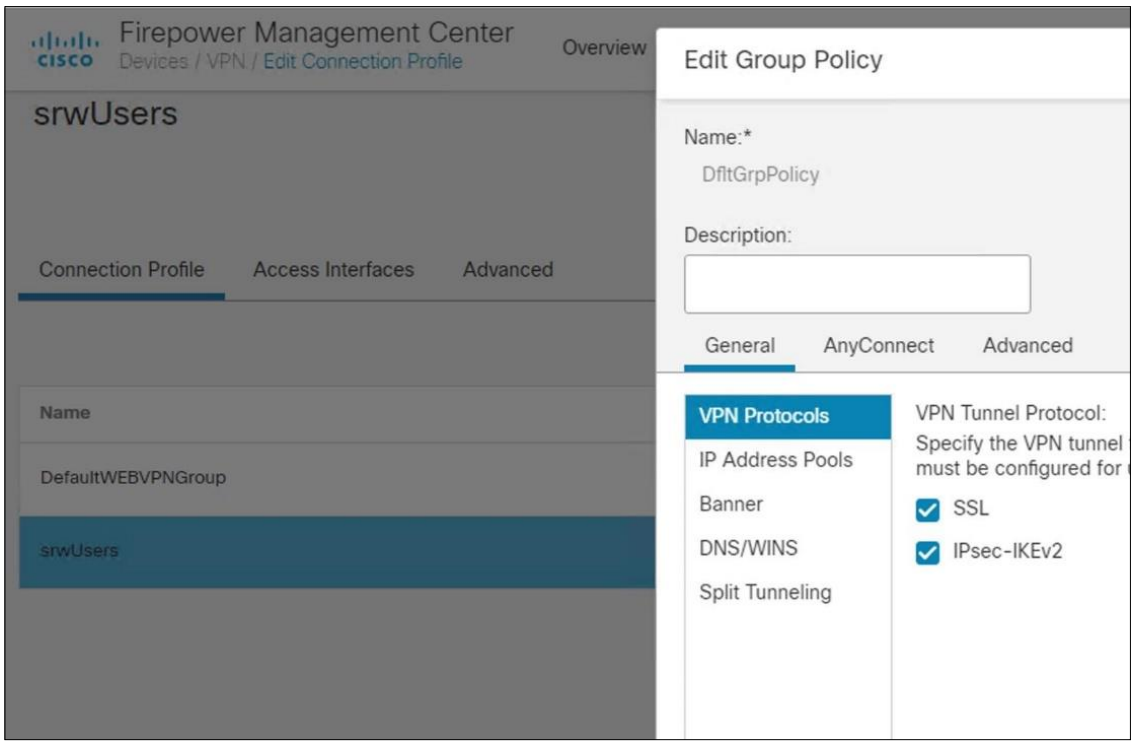

Рис.3.26. Редагування групової політики

Крок 4. У вкладинці «AnyConnect» додати новий модуль.

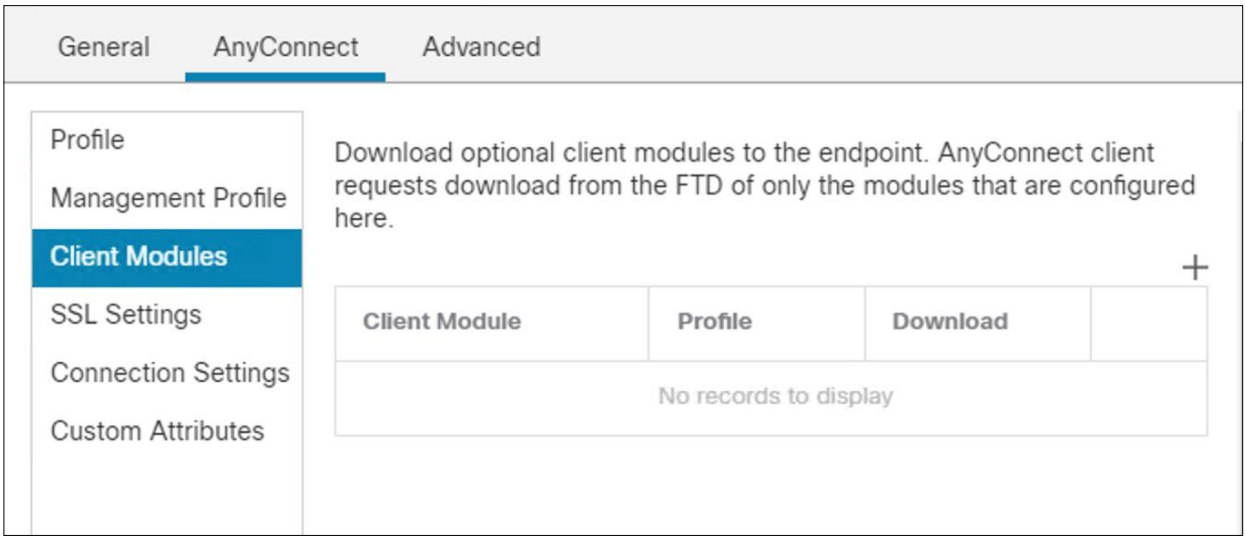

Рис.3.27. Додавання нового модулю в AnyConnect

Крок 5. Змінити клієнтський модуль на Umbrella Roaming Security. Додати новий профіль (рис.3.28).

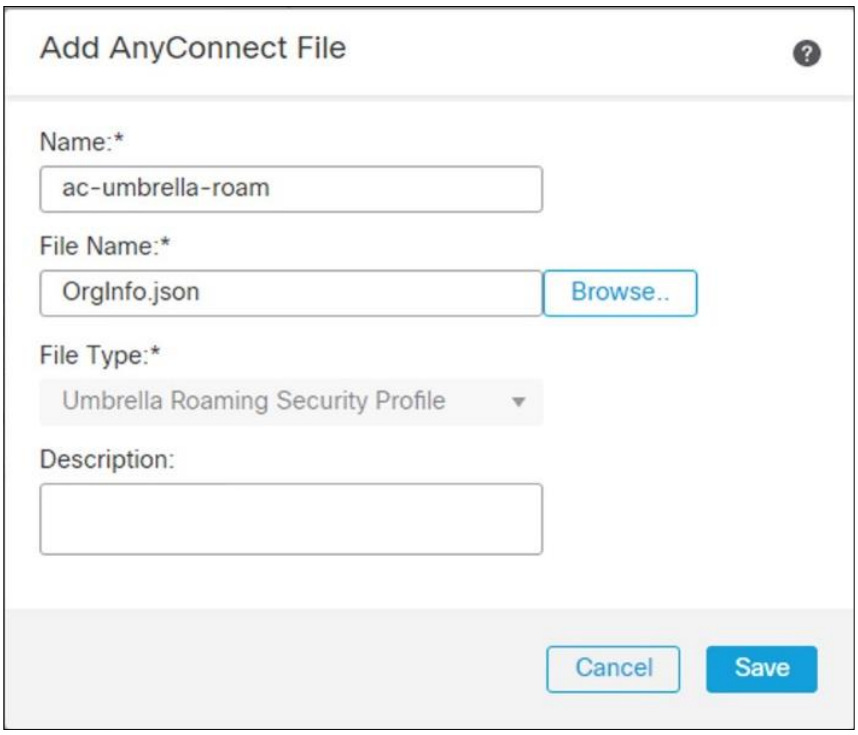

Рис.3.28. Зміна клієнтського модулю на Umbrella Roaming Security

Крок 6. Зімнити назву та знайти файл OrgInfo.json. Натиснути «Зберегти». Після чого, варто переконатися, що профіль є новим, створеним за допомогою файлу Umbrella orgInfo, і поставити відмітку «Увімкнути завантаження модуля» (рис.3.29). Натиснути «Додати» [31].

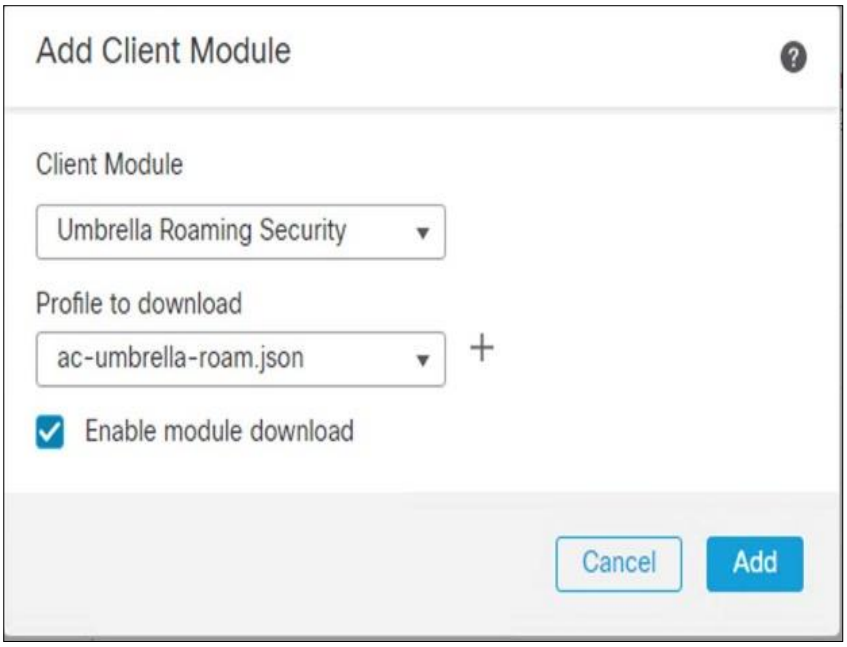

Рис.3.29. Ввімкнення завантаження модуля

3.4.6. Налаштування профілю AMP

Крок 1. Встановити редактор профілю AnyConnect, який було завантажено під час створення файлу «AnyConnect». Відкрити редактор профілів AMP Enabler (рис.3.30).

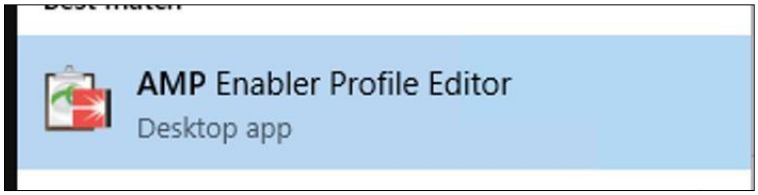

Рис.3.30. Редактор профілів AMP Enabler

Крок 2. Залишити Install AMP Enabler і розмістити дві URL-адреси (уніфіковані покажчики ресурсів) для роз'ємів у відповідних полях (рис.3.31). Якщо перевірка не вдається, необхідно встановити URL-адресу в браузер і перевірити, чи відбувається завантаження. Якщо так, конфігурацію зберегти.

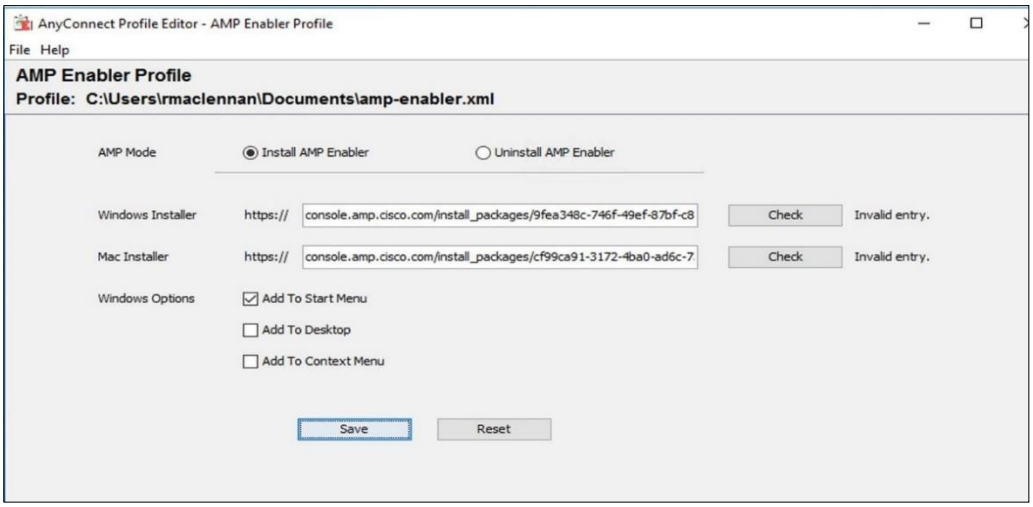

Рис.3.31. Додавання URL-адрес

Крок 3. Зберегти профіль і прийняти повідомлення про недійсність URL-адрес (уніфікованих покажчиків ресурсів). Після чого файл має бути збережено як amp-enabler.xml у папці документів (рис.3.32)

Рис.3.32. Збереження файлу конфігурації

3.5. Перевірка працездатності налаштувань рішень для забезпечення безпеки віддалених працівників

Двофакторна автентифікація Cisco Duo (2FA)

Крок 1. На пристрої в роумінгу необхідно відкрити AnyConnect Secure Mobility Client (рис.3.33)

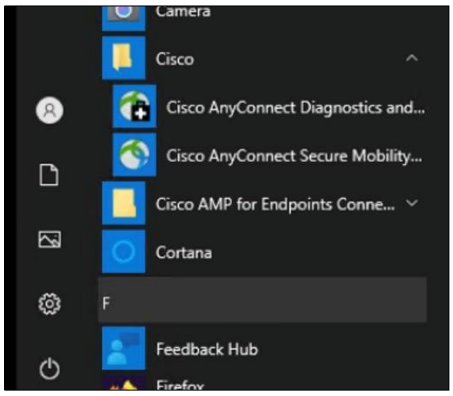

Рис.3.33. AnyConnect Secure Mobility Client

Крок 2. Необхідно обрати мережу, до якої потрібно підключитися, і натиснути «Connect». Після чого, необхідно ввести облікові дані для дійсного користувача та натиснути «OK».

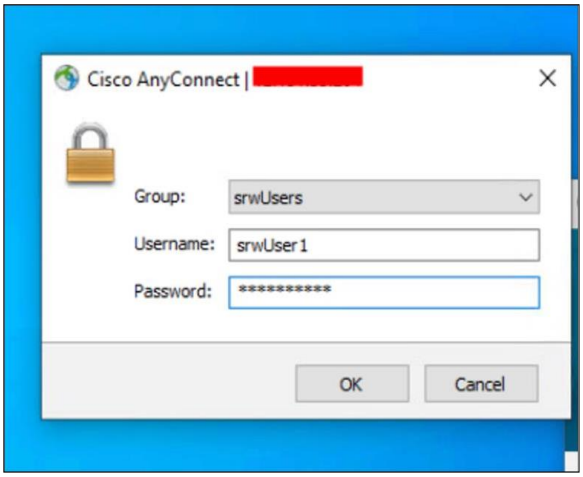

Рис.3.34. Введення облікових даних для дійсного користувача

Крок 3. Якщо налаштування були коректними, то користувач повинен отримати push-сповіщення від Duo. Підтвердити запит і завершити підключення.

Рис.3.35. Приклад push-сповіщення від Duo

Модуль безпеки роумінгу Cisco Umbrella (захист рівня DNS)

Крок 1. Відкрити AnyConnect Secure Mobility Client і переконатися, що модуль Roaming Security активний

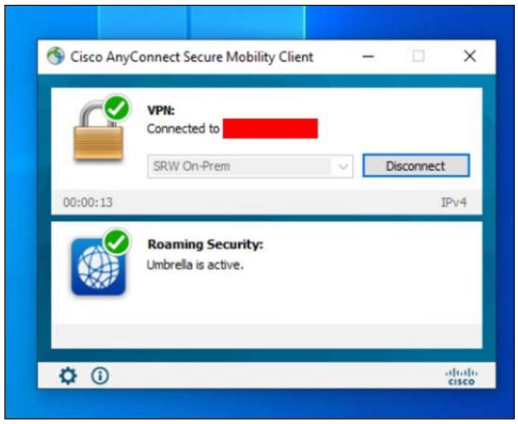

Рис.3.36. Ативний статус модуля Roaming Security

Крок 2. Після чого, необхідно відкрити будь-який браузер і здійснити підключення до 4shared.com. Переконатися, що його заблоковано.

Активатор Cisco Secure Endpoint AMP (блокування файлів)

Крок 1. Перевірити, чи встановлено активатор AMP

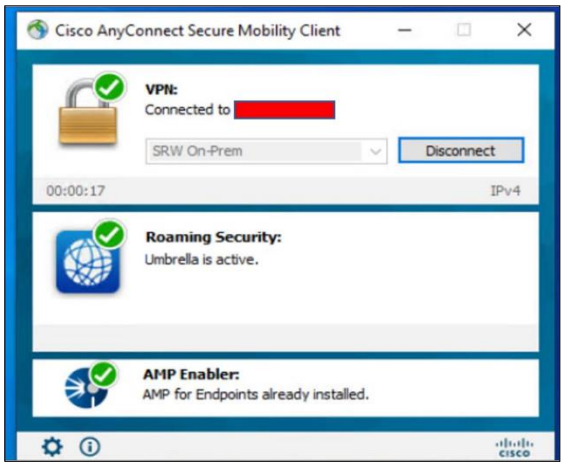

Рис.3.37. Перевірка встановлення активатора Cisco Secure Endpoint AMP

Крок 2. Перейти на eicar.org та завантажити файл eicar.com. Після збереження файлу він повинен бути заблокований або бути негайно видаленим (рис.3.38)

Рис.3.38. Блокування завантаженого файлу з eicar.com.

Крок 3. На інформаційній панелі Secure Endpoint Dashboard необхідно перейти на сторінку «Analysis» - «Event». У подіях має бути блок для зазначеного файлу.

Блокування геолокації. Цей тест підтвердить, що геоблок у Duo успішно блокує спроби підключення з пристроїв за межами географічного діапазону, встановленого в Duo.

Крок 1. Підключення до VPN з регіону, якому дозволено підключатися та авторизуватися.

Крок 2. Потрібно надіслати на пристрій запит Duo та надати доступ. Після чого, перевірити сторінку звітів Duo. Має бути підключення, схвалене користувачем.

Крок 3. Відключитися та спробувати підключитися з регіону, який не ввімкнено організацією.

Крок 4. Duo буде продовжувати запитувати інформацію для входу, на сторінці звітів має бути блок із причиною обмеження розташування (рис.3.39) [32].

Рис.3.39. Блокування Duo

Висновки до розділу 3

Досліджено важливість безпечного віддаленого доступу працівників до корпоративних ресурсів, що стає ключовим аспектом для сучасних підприємств у розподіленому робочому середовищі.

Зазначено, що ефективні рішення для безпеки віддалених працівників включають використання надійних VPN-з'єднань, систем ідентифікації та аутентифікації, а також політик кібербезпеки.

Описано роль Cisco Secure Access від Duo у реалізації багатофакторної автентифікації, забезпечуючи додатковий рівень безпеки для віддалених користувачів. Виявлено, що Cisco Secure VPN забезпечує безперешкодний та безпечний доступ віддалених працівників до корпоративної мережі.

Охарактеризовано функціональність модуля Cisco Umbrella Roaming Security у поєднанні з Cisco Secure VPN для захисту в будь-якій мережі.

Зіставлено налаштування політик безпеки для різних рішень Cisco, включаючи Umbrella, Secure Endpoint та інші, забезпечуючи гнучке управління безпекою.

Вказано на важливість детального налаштування мережевих інтерфейсів, маршрутизації та NAT для оптимальної роботи системи безпеки в корпоративній мережі.

ВИСНОВКИ

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

1. Проаналізовано корпоративні мережі та основні питання безпеки, що наразі висуваються до них.

2. Досліджено методи та рішення безпеки, що активно використовуються при проєктуванні та використанні компонентів корпоративної мережі.

3. Особливу увагу приділено питанням безпеки та стабільності ключових послуг, таких як Mail, Web, DNS, які розміщені у периферійній мережі та доступні через Інтернет.

4. Проаналізовано виклики, пов'язані з тестуванням сегментів мережі, зокрема проблеми з програмним забезпеченням впровадження мережевих пристроїв (GNS3) на операційній системі MS Windows. Зазначено, що незважаючи на виниклі проблеми, тести мережі були успішно виконані, демонструючи відсутність невідомих відкритих портів та інших серйозних проблем із безпекою, як підтверджено скануванням програмного забезпечення.

5. Досліджено важливість безпечного віддаленого доступу працівників до корпоративних ресурсів, що стає ключовим аспектом для сучасних підприємств у розподіленому робочому середовищі.

6. Описано роль Cisco Secure Access від Duo у реалізації багатофакторної автентифікації, забезпечуючи додатковий рівень безпеки для віддалених користувачів. Виявлено, що Cisco Secure VPN забезпечує безперешкодний та безпечний доступ віддалених працівників до корпоративної мережі.

7. Охарактеризовано функціональність модуля Cisco Umbrella Roaming Security у поєднанні з Cisco Secure VPN для захисту в будь-якій мережі.

8. Зіставлено налаштування політик безпеки для різних рішень Cisco, включаючи Umbrella, Secure Endpoint та інші, забезпечуючи гнучке управління безпекою.