ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження методів захисту комп'ютерної мережі на всіх рівнях моделі TCP/IP»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

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

_____ *Денис МАТВІЄНКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-41
Денис МАТВІЄНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Ігор БУЧЕНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
_____Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Матвієнко Денис Кенанович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження методів захисту комп'ютерної мережі на всіх рівнях моделі TCP/IP
керівник кваліфікаційної роботи Ігор БУЧЕНКО,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024р. № 36
2. Строк подання кваліфікаційної роботи «3» червня 2024р.
3. Вихідні дані до кваліфікаційної роботи:
Програма-симулятор Cisco Packet Tracer, для моделювання мережі
Стандарти з побудови безпечних та надійних мереж
Існуючі протоколи стеку TCP/IP
Науково-технічна література з питань, пов'язаних з побудовою мереж.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження шляхів побудови корпоративної комп'ютерної мережі.
2. Дослідження способів захисту корпоративної мережі.
3. Реалізація корпоративної комп'ютерної мережі в Cisco Packet Tracer
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «27» лютого 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	28.02-16.04.2024	Виконано
2	Обробка матеріалу	23.03-05.04.2024	Виконано
3	Розробка теоретичної частини	06.04-10.04.2024	Виконано
4	Розробка проєкту мережі в симуляторі Cisco Packet Tracer	11.04-30.04.2024	Виконано
5	Впровадження деяких функцій захисту в проєкт мережі	01.05-03.05.2024	Виконано
6	Висновки за результатами аналізу	04.05-08.05.2024	Виконано
7	Розробка презентації	09.05-11.05.2024	Виконано
8	Передзахист	13.05-17.05.2024	Виконано
9	Здача в деканат	27.05-3.06.2024	Виконано

Здобувач вищої освіти _____ Денис МАТВІЄНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ігор БУЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 40 стор., 16 рис., 31 джерел.

Мета роботи – дослідження потенційних вразливостей при побудові мережі та захист від них.

Об'єкт дослідження – побудова захищеної мережі на всіх рівнях TCP/IP.

Предмет дослідження – корпоративна комп'ютерна мережа в симуляторі Cisco Packet Tracer.

Короткий зміст роботи: стек протоколів TCP/IP використовується в повсякденному житті, але його перші протоколи не передбачали шифрування трафіку. Коли почали з'являтися перші інциденти інформаційної безпеки, то компанії почали замислюватися про безпеку своїх даних. Саме тому потрібно захищатися не лише фізично, а і в мережі Інтернет. Витік будь-якої цінної інформації може поставити під загрозу існування компанії, так як це втрата великої кількості прибутку, клієнтів, адже їхня довіра до замовника різко втрачається.

КЛЮЧОВІ СЛОВА: кібербезпека, LAN, WAN, модель OSI, TCP/IP, WPA, IEEE, IETF, мережеві екрани, побудова мережі.

ЗМІСТ

ВСТУП

Кібербезпека передбачає захист даних від крадіжки та несанкціонованої зміни. Сюди входять: конфіденційні дані, інформація про здоров'я, особиста інформація, інтелектуальна власність, державні, галузеві й інформаційні системи. Без продуманого плану захисту мережі та сервісів ваша компанія не зможе захистити себе від інцидентів з витоку даних, що робить її вразливою перед кіберзлочинцями.

Дедалі більша залежність від технологій у сучасному світі зробила захист конфіденційної інформації більш важливим пріоритетом, ніж будь-коли раніше. Від особистих даних до фінансових операцій, кіберзагрози можуть порушити бізнес і вплинути на людей у всьому світі. Кібербезпека – це галузь, яка охоплює різноманітні заходи та практики, які захищають комп'ютерні системи та мережі від несанкціонованого доступу, пошкодження чи крадіжки, і передбачає впровадження надійних протоколів безпеки, складних методів шифрування та проактивних контрзаходів.

Як внутрішній ризик, так і залишковий ризик зростають через підключення та використання хмарних служб, таких як Amazon Web Services та Mircosoft Azure для зберігання конфіденційних даних і особистої інформації. Погане налашування хмарних служб у поєднанні з дедалі більш досвідченими кіберзлочинцями означає зростання ризику того, що ваша організація постраждає від успішної кібератаки або витоку даних.

Компанії більше не можуть покладатися лише на готові рішення кібербезпеки, такі як антивірусне програмне забезпечення та брандмауери, тому що кіберзлочинці стають розумнішими, а їхня тактика стає більш стійкою до традиційних засобів кіберзахисту. Важливо охоплювати всі аспекти потенційних атак, щоб залишатися добре захищеними.

Кіберзагрози можуть надходити з будь-якого рівня вашої організації. Для працівників має проводитися регулярне навчання з питань кібербезпеки, щоб ознайомити їх із поширеними кіберзагрозами, такими як шахрайство соціальна інженерія, фішинг, атаки програм-вимагачів (наприклад, WannaCry) та інше шкідливе програмне забезпечення, призначене для викрадення інтелектуальної власності чи особистих даних.

Поширення витоку даних означає, що кібербезпека актуальна не лише для суворо регульованих галузей, як-от охорона здоров'я. Навіть малі підприємства ризикують зазнати шкоди репутації внаслідок витоку даних.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Комп’ютерна мережа та її компоненти

Комп’ютерна мережа – це система, яка з’єднує два або більше обчислювальних пристроїв для передачі та обміну даними. Ці пристрої можуть бути мобільним телефоном, ноутбуком, сервером, стаціонарним персональним комп’ютером тощо. Ці пристрої підключаються або за допомогою фізичних кабелів, таких як оптоволоконних або мідних, або можуть використовувати бездротове з’єднання.

Мережеві пристрої або вузли — це обчислювальні пристрої, які необхідно об’єднати в мережу.

Комп’ютери, мобільні телефони та інші пристрої: це кінцеві пристрої, до яких користувачі мають прямий і частий доступ. Наприклад, користувачі отримують доступ до своєї електронної поштової скриньки та мають змогу листуватися швидкими повідомленнями.

Сервери – це обчислювальні апарати, які містять додатки або виступають у ролі сховища даних, де відбуваються основні обчислення та зберігання даних. Сервер отримує запит, які обробляє та віддає відповідь кінцевому користувачу, який робив запит.

Маршрутизація – це процес вибору мережевого шляху, через який проходять потоки даних. Маршрутизатори — це пристрої, які пересилають ці пакети між мережами, щоб досягти пункту призначення. Вони є необхідним компонентом для забезпечення виходу в Інтернет кінцевих користувачів.

Повторювачі для мереж, як трансформатори для електричних мереж — це електронні пристрої, які приймають мережеві сигнали, очищають та підсилюють їх. Концентратори — це повторювачі з декількома портами. Вони передають дані на будь-які доступні порти. Мости — це розумніші концентратори, які передають

дані лише до порту призначення. Комутатор — це багатопортовий міст. Кілька кабелів даних можна підключити до комутаторів, щоб увімкнути зв'язок із кількома мережевими пристроями.

Шлюзи – це апаратні пристрої, які діють як «шлюзи» між двома окремими мережами. Це можуть бути брандмауери, маршрутизатори або сервери.

Перша робоча мережа під назвою «ARPANET» була створена наприкінці 1960-х років і фінансувалася Міністерством оборони США. Урядові дослідники обмінювалися інформацією в той час, коли комп'ютери були великими та їх важко було переміщувати. Сучасний світ обертається навколо Інтернету, який є мережею мереж, що об'єднує мільярди пристроїв по всьому світу. Організації будь-якого розміру використовують мережі для підключення пристроїв своїх співробітників і спільних ресурсів, наприклад принтерів.

Прикладом комп'ютерної мережі є системи моніторингу руху в містах. Ці системи сповіщають офіційних осіб і служб екстреного реагування інформацією про рух транспорту та інциденти. Простішим прикладом є використання програмного забезпечення для спільної роботи, наприклад Google Drive, для обміну документами з колегами, які працюють віддалено. Кожного разу, коли ми з'єднуємося через відеодзвінок, транслюємо фільми, обмінюємося файлами, спілкуємося за допомогою миттєвих повідомлень або просто отримуємо доступ до чогось в Інтернеті, працює комп'ютерна мережа.

Комп'ютерні мережі — це галузь інформатики, яка займається розробкою ідей, архітектурою, створенням, обслуговуванням і безпекою комп'ютерних мереж. Це поєднання інформатики, комп'ютерної інженерії та телекомунікацій.[3][4]

1.2 Мережеві протоколи і галузеві стандарти

Протокол зв'язку — це набір правил, яких дотримуються всі вузли, що беруть

участь у передачі інформації. Деякі поширені протоколи включають набір протоколів Інтернету (TCP/IP), IEEE 802, Ethernet, бездротову локальну мережу та стандарти стільникового зв'язку. TCP/IP — це концептуальна модель, яка стандартизує зв'язок у сучасній мережі. Він пропонує чотири функціональні рівні цих зв'язків:

– канальний рівень визначає спосіб фізичної передачі даних. Він включає в себе те, як пристрій надсилає біти даних через середовище передачі даних;

– інтернет-рівень(мережевий) рівень відповідає за комлектування даних у зрозумілі пакети та дозволяє їх надсилати та отримувати;

– транспортний рівень дозволяє пристроям підтримувати комунікацію, забезпечуючи дійсне та стабільне з'єднання;

– рівень рівень визначає, як програми високого рівня можуть отримувати доступ до мережі для ініціювання передачі даних.

Більшість сучасної структури Інтернету базується на моделі TCP/IP, хоча все ще є сильні впливи подібної, але семирівневої моделі взаємозв'язку відкритих систем (OSI).[27]

Рисунок 1.1 – Порівняння мережевих двох моделей[26][28]

Деякі з найвідоміших галузевих стандартів в сфері інформаційних технологій

включають:

– *IEEE (Institute of Electrical and Electronics Engineers)* розробляє стандарти для широкого кола електронних пристроїв і систем, включаючи мережеві протоколи;

– *ISO (International Organization for Standardization)* розробляє стандарти для широкого кола продуктів і послуг, включаючи інформаційні технології, має свою мережеву модель: OSI (Open Systems Interconnection) – це концептуальна структура, що описує етапи та принципи взаємодії мережевих компонентів. Вона ділить мережу на чітко визначені рівні, кожен з яких відповідає за певну функцію в процесі передачі даних. Цей поділ робить роботу мережевих пристроїв та програмного забезпечення більш зрозумілою, прозорою та організованою;

– *IETF (Internet Engineering Task Force)* розробляє стандарти для Інтернету, включаючи протоколи TCP/IP.

IEEE 802 — це сімейство стандартів IEEE, що відносяться до локальних мереж (LAN) і міських мереж (MAN). Бездротова локальна мережа є членом сімейства IEEE 802 і більш відома як WLAN або Wi-Fi та має кодову назву 802.11.

IEEE 802.11 (1997) або перший Wi-Fi:

- діапазон 2.4 ГГц;
- швидкість 1-2 Мбіт/с;
- модуляція DSSS, FHSS.

IEEE 802.11b (1999):

- діапазон 2.4 ГГц;
- швидкість 11 Мбіт/с (до 5.5, 2 та 1 Мбіт/с);
- модуляція DSSS;
- переваги. Більш поширений, дешевший;
- недоліки. Менша пропускна здатність, схильність до перешкод.

IEEE 802.11a (1999):

- діапазон 5 ГГц;
- швидкість 54 Мбіт/с (до 48, 36, 24, 18, 12, 9 і 6 Мбіт/с);
- переваги. Менше перешкод, більша пропускна здатність;

- недоліки. Менш поширений, дорожчий.

IEEE 802.11ac (2013):

- діапазон 5 ГГц (6 ГГц з Wi-Fi 5+);
- швидкість до 6 Гбіт/с (8x MU-MIMO);
- технології MU-MIMO, Beamforming, канал до 160 МГц;
- переваги. Значно вища пропускна здатність, менші затримки;
- недоліки. Вища вартість, сумісність з пристроями Wi-Fi 5.

IEEE 802.11ax (2021): Wi-Fi 6 / Wi-Fi 6E

- діапазон 5 ГГц, 2.4 ГГц (додаткові смуги 1-7 ГГц);
- швидкість до 10 Гбіт/с;
- технології OFDMA, MU-MIMO, Color-Based Ranging, Target Wake Time;
- переваги. Значно вища пропускна здатність, менші затримки, краща ефективність в переповнених мережах;
- недоліки. Потребує нових пристроїв Wi-Fi 6 / 6E;[15]

Fast Ethernet (IEEE 802.3u). Цей стандарт розроблений для мереж Ethernet, яким потрібні вищі швидкості передачі даних. Він збільшує пропускну здатність з 10 Мбіт/с до 100 Мбіт/с, вносячи мінімальні зміни до існуючої кабельної інфраструктури. Fast Ethernet пропонує кращу продуктивність для відео, мультимедіа, графіки, вебсерфінгу, а також більш надійне виявлення та виправлення помилок.

Існує три типи Fast Ethernet:

- 100BASE-TX: Використовує кабель UTP 5-ї категорії;
- 100BASE-FX: Використовує оптоволоконний кабель;
- 100BASE-T4: Використовує два додаткових дроти в кабелі UTP 3-ї категорії.

100BASE-TX став найпопулярнішим завдяки сумісності зі стандартом 10BASE-T Ethernet.

Gigabit Ethernet: Цей тип мережі передає дані зі швидкістю 1000 Мбіт/с (1 Гбіт/с). Gigabit Ethernet - це модернізація Fast Ethernet, яка поступово витісняє її. У цій мережі всі чотири пари крученої пари в кабелі задіяні для передачі даних.

Gigabit Ethernet широко використовується у системах відеозв'язку з кабелями CAT5e або новішими. Для розширених мереж (до 500 м) можна використовувати оптоволоконні кабелі: 1000Base SX для багатомодових систем та 1000Base LX для одномодових.

Основні відмінності Gigabit Ethernet від Fast Ethernet:

- додаткова підтримка повнодуплексного режиму на рівні MAC;
- збільшена швидкість передачі даних.

10 Gigabit Ethernet: Це найновіший і найшвидший стандарт Ethernet. IEEE 802.3ae визначає номінальну швидкість 10 Гбіт/с, що у 10 разів швидше, ніж Gigabit Ethernet. На відміну від інших систем Ethernet, 10 Gigabit Ethernet використовує виключно оптоволоконні з'єднання. Цей стандарт відходить від дизайну LAN (широмовна розсилка) на користь системи з елементами глобальної маршрутизації.

Візьмемо для прикладу вебсервер і вебклієнт. Коли ви вводите адресу вебсайту в браузері, ваш вебклієнт надсилає запит до вебсервера. Цей запит і відповідь вебсервера ґрунтуються на цілій низці протоколів і стандартів, які гарантують, що ви отримаєте правильну сторінку. Різні протоколи працюють разом, як частини головоломки, щоб забезпечити чіткий і зрозумілий обмін інформацією.[8]

Мережеві протоколи – це набір правил і специфікацій, які визначають формат і правила обміну даними між комп'ютерними пристроями в мережі. Вони відіграють фундаментальну роль у забезпеченні сумісності, ефективності та надійності мережевих комунікацій.

Приклади протоколів:

– протокол прикладного рівня HTTP (HyperText Transfer Protocol) використовується для взаємодії між вебсерверами та вебклієнтами, визначаючи формат запитів і відповідей, якими вони обмінюються;

– транспортний протокол TCP (Transmission Control Protocol) керує сеансами зв'язку між серверами та клієнтами, розбиваючи повідомлення на дрібніші частини, гарантуючи їхню надійну передачу;

– інтернет-протокол IP (Internet Protocol) відповідає за адресацію та

маршрутизацію пакетів даних у мережі, забезпечуючи їхню доставку до адресата.

Протоколи мережевого доступу:

– зв'язок по каналу передачі даних: описує логічне з'єднання між двома точками в мережі;

– фізична передача даних по мережевому середовищу визначає правила передачі сигналів по фізичному каналу, наприклад, через кабель або Wi-Fi.

Важливість протоколів:

– сумісність. Завдяки спільним протоколам пристрої різних виробників можуть без проблем обмінюватися даними;

– ефективність. Протоколи оптимізують процес передачі даних, роблячи його швидшим і надійнішим;

– надійність. Протоколи гарантують, що повідомлення будуть доставлені без помилок і втрат.

Мережеві протоколи – це основа, на якій будуються сучасні комп'ютерні мережі. Вони роблять можливим те, що ми сприймаємо як Інтернет, безпроблемний обмін інформацією між мільярдами пристроїв по всьому світу.

Галузеві стандарти – це набори правил і специфікацій, які розробляються організаціями, що представляють певну галузь промисловості. Ці стандарти забезпечують сумісність продуктів і послуг різних виробників, що полегшує обмін інформацією та співпрацю.[16]

1.3 Типи комп’ютерних мереж

Комп’ютерні мережі можна класифікувати на основі кількох критеріїв, таких як середовище передачі, розмір мережі, топологія та організаційні наміри. Виходячи з географічного масштабу, існують різні типи мереж: PAN, LAN, SAN, CAN, MAN, WAN, EPN, VPN.

Персональна мережа (PAN) використовується лише однією особою за для

підключення кількох пристроїв, наприклад ноутбуків до сканерів тощо. Поширена технологія – Bluetooth.[9]

Локальна мережа (LAN) об’єднує пристрої в межах обмеженої географічної області, як-от школи, лікарні чи офісні будівлі.[10]

Мережа зберігання даних (SAN) – це виділена мережа, яка полегшує зберігання даних на рівні блоків. Це використовується в пристроях зберігання, таких як дискові масиви та стрічкові носії інформації.[14]

Кампусна мережа (CAN) – це набір взаємопов’язаних локальних мереж. Вони використовуються організаціями, такими як університети та уряди.[11]

Міська або муніципальна мережа (MAN) – це велика комп’ютерна мережа, яка охоплює все місто.[13]

Глобальна мережа (WAN) охоплює великі території, такі як великі міста, штати та навіть країни.[12]

Корпоративна приватна мережа (EPN) – це єдина мережа, яку велика організація використовує для з’єднання кількох офісів.

Віртуальна приватна мережа (VPN) – це віртуальна приватна мережа, розташована поверх загальнодоступної мережі.

Хмарна мережа – це WAN, інфраструктура якої надається через хмарні служби.

За організаційним призначенням мережі можна класифікувати як:

– інтранет – це набір мереж, які обслуговуються та контролюються однією організацією. Як правило, це найбезпечніший тип мережі з доступом лише для авторизованих користувачів. Інтранет зазвичай існує позаду маршрутизатора в локальній мережі;[5]

– Інтернет (або міжмережа) – це сукупність кількох мереж, з’єднаних маршрутизаторами та роз’єднаних мережевим програмним забезпеченням. Це глобальна система, яка об’єднує уряди, дослідників, корпорації, громадськість та окремі комп’ютерні мережі;

– екстранет схожий на інтранет, але має підключення до певних зовнішніх мереж. Зазвичай він використовується для обміну ресурсами з партнерами,

клієнтами або віддаленими співробітниками.[6]

1.4 Різновиди топологій

Структура мережі та спосіб підключення кожного компонента до інших визначаються топологією мережі. Топологія буває двох типів: логічна топологія та фізична топологія.

Топологія шини. Кожен комп'ютер і мережевий пристрій під'єднані до одного кабелю в мережі шинної топології. Топологія лінійної шини визначається як наявність рівно двох терміналів.

Переваги:

– просте налаштування;

– порівняно з сітчастою, зіркоподібною та деревоподібною топологіями шина використовує менше кабелів.

Недоліки:

– складність переналаштування та усунення несправностей;

– несправність або розрив кабелю шини перериває весь зв'язок.

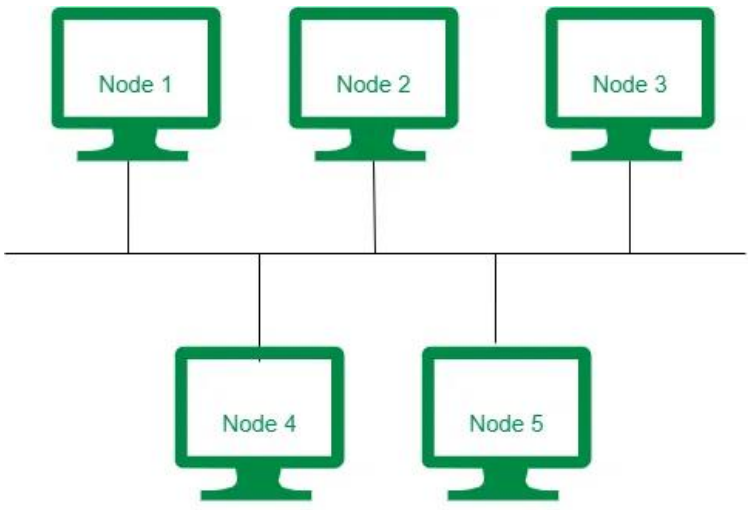


Рисунок 1.2 – Топологія шини

Кільцева топологія. Топологія називається кільцевою, тому що один комп'ютер з'єднаний з сусідніми, а останній з'єднаний з першим. Рівно два сусіди для кожного пристрою. Сигнал пропускається по кільцю в одному напрямку. Кожне кільце містить повторювач.

Переваги:

– передача даних відносно проста, оскільки пакети рухаються лише в одному напрямку;

– немає потреби звертатися до контролера керування для зв’язку між вузлами;

– легке провадження та переналаштування.

Недоліки:

– в однонаправленому кільці пакет даних повинен пройти через усі вузли;

– усі комп’ютери мають бути увімкнені, щоб вони мали змогу з’єднатися один з одним.

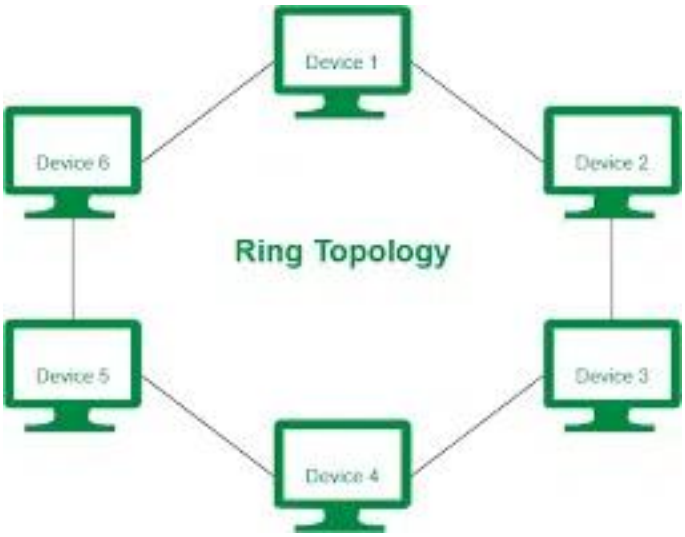


Рисунок 1.3 – Топологія кільця

Топологія “зірка”. Кожен пристрій у топології типу «зірка» має спеціальне з’єднання «точка-точка» з центральним контролером, який зазвичай називають концентратором. Прямого зв'язку між пристроями немає. Трафік між пристроями заборонений у цій топології.

Переваги:

– при підключенні або відключенні пристроїв немає перебоїв у мережі;

– його легко встановити та налаштувати;

– визначити та усунути несправності просто;

– менше, ніж “сітка”;

– легко встановити та налаштувати.

Недоліки:

– вузли, підключені до комутатора або концентратора, який раптово вийшов з ладу, не мають змоги комунікувати в мережі;

– через вартість концентраторів/комутаторів ця топологія дорожча, ніж топології лінійної шини;

– у порівнянні з шиною чи кільцем потрібно більше кабелю;

– надто сильна залежність від концентратора.

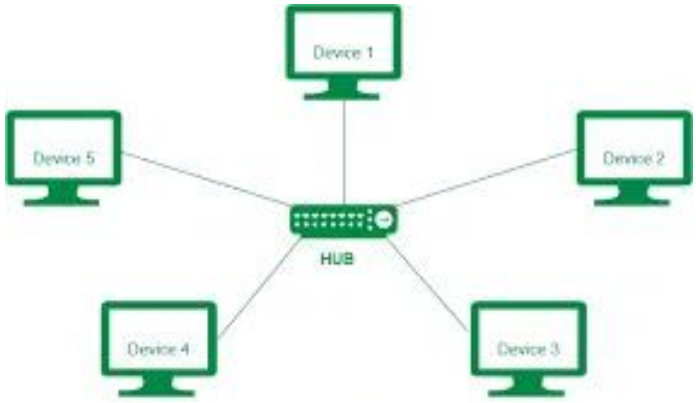


Рисунок 1.4 – Топологія “зірка”

Топологія сітки. Кожен пристрій у сітчастій топології підключений методом «точка-точка» до кожного іншого пристрою. Термін «виділений» стосується того факту, що канал передає дані виключно між двома пристроями, які він пов’язує. Щоб підключити n пристроїв, повністю підключена сітчаста мережа має містить n*(n-1)/2 фізичних каналів.

Переваги:

– дані можуть надсилатися з кількох пристроїв одночасно. Ця топологія може обробляти великий трафік;

– навіть якщо одне з підключень виходить з ладу, резервна копія завжди доступна. Як наслідок, передача даних продовжується;

– фізичні межі перешкоджають іншим користувачам отримати доступ до повідомлень;

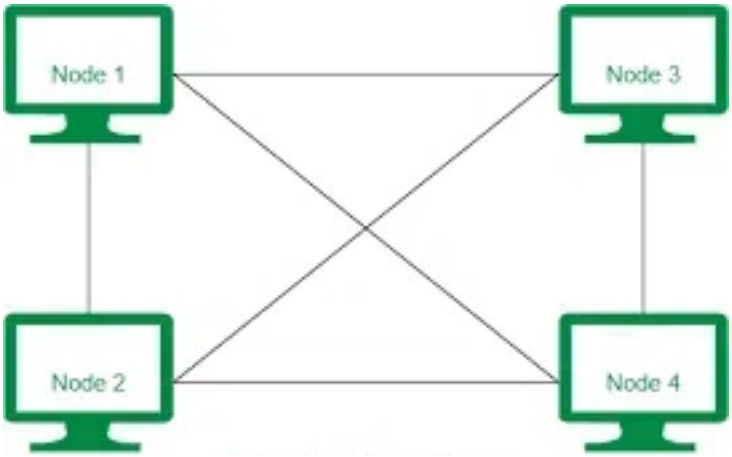
– зв'язки «точка-точка» спрощують передачу та усунення несправностей.

Недоліки:

– необхідна кількість кабелів і кількість портів введення/виведення;

– кількість проводів може бути більшою, ніж може вмістити доступний простір;

– її складно встановити і переналаштувати.



Рисисунок 1.5 – Топологія сітки[4]

1.5 Основи для побудови корпоративної мережі

Для підприємств мати власну мережу є важливим, тому що це покращує взаємодію з клієнтами, так і впроваджує підтримку нових моделей роботи співробітників. Незалежно від того, чи це ресторан швидкого обслуговування, який

пропонує клієнтам каси для самостійного замовлення, роздрібний продавець, який використовує штучний інтелект для перевірки наявності асортименту в режимі реального часу, або мінімагазин, який розробляє нову програму лояльності, щоб залучати клієнтів, поки вони заправляють свої транспортні засоби, безперебійне підключення є основою.

У той час як підприємства працюють, щоб не відставати від зростаючих очікувань і мінливих моделей роботи, вони визнають важливість підключення та даних для підвищення корпоративної стійкості. Інвестиції в безперебійне та гнучке підключення допоможуть підприємствам пристосуватися до поточних вимог ринку.

Однак створення перспективної мережі не відбувається відразу. Це вимагає створення гнучкої та швидкодіючої мережі, щоб допомогти підприємствам залишатися на випередженні. Щоб працювати над цією моделлю, підприємствам потрібні кілька ключових елементів.

1. *Універсальна та гнучка мережа.* Гнучкість є ключовою для підприємств, які хочуть йти в ногу з новими технологіями. Їм потрібні мережі, які можуть розвиватися та відповідати мінливим вимогам. SD-WAN є одним із найважливіших компонентів, що забезпечує таку універсальність, оскільки він може підтримувати різні з’єднання та мережі та зменшувати затримку.

SD-WAN може не тільки знизити витрати, але й підвищити продуктивність і оптимізувати мережеві можливості. Використовуючи широкосмуговий зв’язок для розвантаження некритичних бізнес-додатків, автоматизації завдань моніторингу та керування трафіком через централізований контролер, SD-WAN може збільшити гнучкість і зменшити розростання мережі.

Запровадження хмарних технологій також прискорюється, оскільки підприємства прагнуть гнучкості, операційної ефективності та економії коштів. Оскільки все більше організацій рухаються в такому напрямку, це стає ще більш важливою особливістю SD-WAN. Завдяки SD-WAN з підтримкою хмари клієнти та співробітники можуть отримати прямий доступ до хмарних програм незалежно

від місця розташування. Ця гнучкість є важливою для підтримки контролю над динамічними мережевими граничними середовищами.

2. *Автоматизована мережа з урахуванням додатків.* Автоматизація, як-от ШІ, стає основою у технологіях. Зараз це один із найважливіших чинників цифрової трансформації. Інтелектуальні мережі, зокрема мережі з підтримкою додатків, мають вбудовану інформацію та інтелектуальні дані про програми та шаблони трафіку, які допомагають визначити та керувати потребами підключення. Ця поглиблена функціональність дозволяє ефективніше працювати в мережі.

Оскільки автоматизація стає більш масовою, багато компаній звертаються до штучного інтелекту для IT-операцій (AIOps) і машинного навчання для збору даних із багатьох компонентів IT-інфраструктури, вимог до програм, інструментів моніторингу ефективності та систем продажу квитків на обслуговування. Тоді AIOs може розширити можливості автоматизації за допомогою прогнозованої аналітики та реагування.

Оскільки технології продовжують розвиватися, складність мережі також зростає, тому важливо розуміти та впроваджувати сучасні функції.

3. *Мультитранспорт і висока пропускна здатність.* Важливо мати надійне підключення до інтернету, тому що воно є необхідною умовою успішного та вчасного виконання задач. Корпоративні мережі потребують кількох варіантів підключення, як-от: широкосмугове з’єднання, конвергентне оптоволокно та кабель, 5G і приватне бездротове з’єднання. Підприємствам зазвичай необхідна висока пропускна здатність, щоб оптимізувати продуктивність і швидкість реагування, забезпечуючи реакцію в режимі реального часу та швидкий розвиток для кращої підтримки технологій, таких як ШІ.

4. *Інтегрований підхід до вирішення.* Кожен бізнес різний. Від ресторанів до охорони здоров’я та роздрібної торгівлі підприємства мають унікальні потреби. Ці потреби, що постійно змінюються, вимагають кількох режимів підключення та відповідних рішень. Завдяки інтегрованим рішенням або моделям «як послуга» компанії отримують численні переваги. По-перше, час отримання вигоди зменшується, оскільки програмне забезпечення вже встановлено та налаштовано.

Це скорочує час налаштування та підвищує ефективність. Інтегровані моделі також максимізують продуктивність і якість обслуговування організацій. Програми постійно оновлюються, щоб зменшити час простою, підвищити продуктивність і забезпечити ефективний моніторинг. По-друге, такий підхід також економить гроші на операційному, сервісному обслуговуванні, програмному забезпеченні та витратах на інфраструктуру.

5. *Безпечна та надійна мережа.* На безпеку часто не звертають уваги, але всі компанії повинні мати план з реагування на інциденти. Зростаючий цифровий простір і складність мереж ставлять перед підприємствами багато загроз інформаційній безпеці. Оскільки загрози безпеці розвиваються, організаціям потрібно вдосконалювати захист мережі. Особливо з віддаленими та гібридними моделями роботи, мережі повинні захищати себе за допомогою численних заходів кібербезпеки.[7]

РОЗДІЛ 2. ЗАХИСТ МЕРЕЖІ НА ВСІХ РІВНЯХ МОДЕЛІ TCP/IP

2.1 Захист рівнів мережі

Захист мережі – це багаторівневий процес, який потребує комплексного підходу до забезпечення безпеки на всіх рівнях мережевої моделі. Ось деякі з методів захисту на кожному рівні.

Фізичний рівень:

- захист мережевих пристроїв від несанкціонованого доступу за допомогою фізичних бар'єрів, таких як охорона та камери відеоспостереження;
- захист даних, що зберігаються на жорстких дисках, від несанкціонованого доступу у разі крадіжки або втрати пристрою використовуючи шифрування диску.

Рівень доступу:

- застосування методів аутентифікації, таких як паролі, двофакторна аутентифікація (2FA) або біометрія, для перевірки особистості користувачів перед наданням їм доступу до мережі;
- надання користувачам лише тих дозволів, які їм необхідні для виконання своїх завдань, обмежуючи доступ до конфіденційних даних та ресурсів, тобто контроль доступу на основі ролей (RBAC – role based access);

Рівень мережі:

- виявлення та блокування підозрілих мережевих дій, які можуть свідчити про кібератаку, тобто використовувати IPS;
- сегментація мережі на логічні групи для обмеження доступу до певних ресурсів та підвищення безпеки, тобто використовувати технологію VLAN.

Транспортний рівень:

- використання брандмауерів для блокування несанкціонованого доступу до мережі та регулювання трафіку;

– використання протоколів, таких як TLS/SSL, для шифрування даних та забезпечення конфіденційності під час комунікацій в Інтернеті та відкритих мереж;

– блокування невикористовуваних портів для зменшення ризику атак, тобто фільтрація портів.

Рівень прикладного програмного забезпечення:

– брандмауери вебдодатків (WAF – web application firewall) захисту вебдодатків від атак, таких як SQL-ін'єкції та міжсайтові скрипти (XSS);

– антивірусне програмне забезпечення забезпечує захист від шкідливого програмного забезпечення, яке може бути завантажене з Інтернету або з інших джерел;

– регулярне оновлення програмного забезпечення та операційних систем для усунення вразливостей.

Важливо пам'ятати, що захист мережі – це тривалий та постійний процес, який потребує постійної уваги та зусиль. Регулярно оцінюйте ризики, оновлюйте методи захисту та навчайте співробітників основам кібербезпеки, щоб гарантувати, що ваша мережа буде максимально захищена.

2.2 Захист фізичного доступу до мережі

1. Захист периметра. Рівень фізичної безпеки мережі має на меті тримати сторонніх осіб якнайдалі від вашого центру обробки даних**.** Але навіть якщо ЦОД не знаходиться в окремій будівлі, для отримання конфіденційної інформації потрібен лише один викрадений корпоративний ноутбук, пошкоджений сервер або несправний флеш-накопичувач. Важливо розглядати фізичний захист периметра мережі як фізичний «брандмауер».

2. Контроль доступу до об'єкту. Потрібно визначити можливість обмеження входів виходів до будівлі. Маючи один головний вхід, ви змушуєте всіх

проходити через нього, контактувати з особою на рецепції та потрапляти на відеокамери (якщо вони встановлені на вході).

Якщо за протоколом необхідні додаткові виходи, розгляньте встановлення дверей без зовнішніх ручок. Їх можна використовувати для безпечного виходу з об'єкта, але їх дуже важко відкрити ззовні. Ці двері також повинні бути підключені до сигналізації, яка спрацює та надішле повідомлення про потенційне порушення.

Контроль входів до об'єкта та центру обробки даних є необхідністю. Це дозволить вам дистанційно проводити моніторинг та керувати тим, хто має доступ до об'єкта, коли і до яких його частин. Ви також зможете відстежувати, хто входив і скільки часу вони перебували в тій чи іншій частині ЦОДу. Щоб гості чи відвідувачі могли пройти, вони повинні зареєструватися та отримати тимчасову перепустку. Підрядникам, яким потрібен доступ до центру обробки даних, можна видавати картки доступу з певними термінами дії, щоб вони могли потрапити до приміщення лише тоді, коли ви будете готові їх прийняти, і не зможуть без вашого відому повернутися назад в ЦОД після його відвідування.

3.Відеоспостереження. Відеокамери можна використовувати будь-де: зовнішній периметр, входи до об'єкта та центру обробки даних, на сходах, на окремих рядах усередині центру обробки даних тощо. Відеозапис можна зберігати в архіві, що дозволить легко його отримати та переглянути за потреби.

Переконайтеся, що система відеоспостереження може забезпечувати якісне зображення за умов поганого освітлення, аби можна було чітко розпізнати, хто входить і виходить, побачити, що вони несуть, зафіксувати номери транспортних засобів, застосувати розпізнавання облич тощо.[17]

2.3 Захист рівня доступу до мережі

Зі стрімким зростанням IP-мереж за останні роки, високопродуктивні комутатори відіграли одну з найважливіших ролей у надійній, ефективній та безпечній передачі даних по мережах.

Рівень каналу даних (2 рівень моделі OSI) забезпечує функціональні засоби передачі даних між мережевими пристроями із взаємодією з іншими рівнями, але з точки зору безпеки рівень каналу даних має свої власні проблеми. Захист мережі настільки на 2 рівні є не менш важливим, ніж будь-який інший рівень. Застосування сильних заходів безпеки до верхніх рівнів (рівні 3 і вище) не приносить користі мережі, якщо рівень 2 не достатньо захищено.

Функції *керування трафіком* на рівні портів можуть використовуватися для забезпечення захисту на рівні портів. Комутатори можуть пропонувати такі функції: Storm Control (контроль великого потоку трафіку), Protected Ports (захист портів), Private Virtual Local Area Network (PVLAN – Віртуальна Локальна Мережа), Port Blocking (блокування портів) та Port Security (безпека портів).

«Шторм» в локальній мережі (LAN) зазвичай виникає, коли сегмент LAN переповнюється зайвими пакетами, що створює непотрібний та надмірний трафік, який призводить до зниження продуктивності мережі. Існує декілька факторів, які можуть спричинити великий обсяг пакетів у мережі: помилки у реалізації протокольного стека або проблеми у вигляді помилок коду, що були знайдені в конфігурації пристрою.

Функція Storm Control запобігає порушенню звичайного мережевого трафіку штормом пакетів широкого мовлення (broadcast), групового мовлення (multicast) або одиничного мовлення (unicast) на будь-якому з фізичних інтерфейсів.

Керування великим потоком трафіку (також відома, як функція пригнічення трафіку) відстежує вхідні пакети протягом 1 секунди та порівнює їх із налаштованим рівнем пригнічення контролю шторму, використовуючи один із таких методів для вимірювання активності:

– відсоток загальнодоступної пропускної здатності порту, виділений для трафіку широкого мовлення, групового мовлення або одиничного мовлення;

– швидкість трафіку за інтервал 1 секунди, за який пакети широкого мовлення, групового мовлення або одиничного мовлення отримуються на інтерфейсі.

За будь-яким із цих методів порт блокує трафік, коли досягається поріг, відсіюючи всі наступні пакети. Оскільки порт залишається заблокованим, трафік продовжує скидатися, доки швидкість трафіку не знизиться нижче рівня порогу, після чого порт відновлює звичайну переадресацію трафіку.

Захищені порти (PVLAN Edge). В деяких мережевих середовищах виникає необхідність, щоб жоден трафік не був видимий або переадресований між хостами в одному сегменті LAN, тим самим запобігаючи широкомовного трафіку. Функція PVLAN edge забезпечує цю ізоляцію, створюючи бар'єр, схожий на брандмауер, тим самим блокуючи будь-який трафік одиничного, широкого або групового мовлення між захищеними портами на комутаторі. Але варто зазначити, що функція захищеного порту обмежена комутатором, на якому це налаштовано, і функція PVLAN edge не передбачає ізоляції трафіку між двома "захищеними" портами, розташованими на різних комутаторах.

Протокол кістякового дерева (Spanning Tree Protocol, STP) призначений для запобігання утворенню петель у мережі. Коли комутатори з'єднані між собою кількома каналами, STP гарантує відсутність петель. Петля STP може виникнути у випадках через апаратний збій, помилку конфігурації або мережну атаку. Петлі STP можуть призвести до серйозних перебоїв у роботі мережі. STP потрібно використовувати для покращення стабільності мереж на 2 рівні.

802.1X IEEE – це промисловий стандарт безпеки, який передбачає високу ступінь захисту бездротової мережі, за рахунок аутентифікації користувачів з використанням генерації і розподілу динамічних ключів шифрування.

Стандарт IEEE 802.1X забезпечує регулярну заміну сеансових ключів і моніторинг мережевого доступу (з метою обліку використання мережевих ресурсів). Управління доступом здійснюється на основі ідентифікаторів (user name)

і паролів користувачів або їх цифрових сертифікатів. Стандартом передбачається можливість аутентифікації користувачів з використанням спеціального RADIUS сервера, на якому зберігаються облікові записи (логіни та паролі) всіх користувачів мережі.[18]

Для захисту невеликої бездротової мережі, де немає сенсу встановлювати сервер RADIUS, адміністратор може використовувати майстер ключ, який вводиться в клієнтський бездротовий пристрій і базову бездротову точку доступу вручну. Точка доступу створює WEP-ключ і відсилає його клієнтському пристрою, попередньо зашифрувавши за допомогою майстер ключа. Стандарт IEEE 802.1X використовується в специфікаціях – Wireless Protected Access (WPA) асоціації Wi-Fi Alliance і IEEE 802.11i.

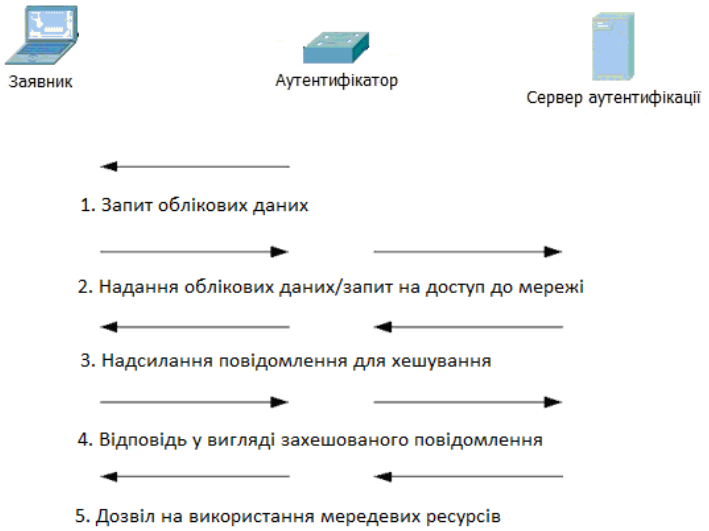


Рисунок 2.1 – Процес аутентифікації клієнта на RADIUS сервері

2.4 Захист мережевого рівня

Рівень мережі в моделі TCP/IP відповідає за маршрутизацію пакетів даних між мережами. Він використовує протокол IP (Internet Protocol) для адресації та OSPF (Open short path first) маршрутизації пакетів, а також інші протоколи, такі як

ICMP (Internet Control Message Protocol) та IGMP (Internet Group Management Protocol) для управління мережею.

Існує ряд методів, які можна використовувати для захисту рівня мережі:

1. Маршрутизація та фільтрація:

- використовуйте брандмауери та списки доступу (ACL) для блокування небажаного трафіку;
- налаштуйте маршрутизатори для фільтрації трафіку на основі IP-адрес, портів та інших критеріїв;
- використовуйте VPN (Virtual Private Network) для створення безпечних тунелів для передачі даних через загальнодоступні мережі.

2. *Шифрування:*

- шифруйте трафік IP за допомогою протоколів, таких як IPSec (Internet Protocol Security) або SSL/TLS (Secure Sockets Layer/Transport Layer Security);[30]
- використовуйте VPN з шифруванням для додаткового рівня безпеки.

3. *Протоколи безпеки:*

- використовуйте протоколи безпеки, такі як IKEv2 (Internet Key Exchange Protocol version 2) та DH (Diffie-Hellman key exchange), для встановлення безпечного з'єднання між двома пристроями;
- використовуйте протоколи аутентифікації, такі як RADIUS (Remote Authentication Dial-In User Service) та TACACS+ (Terminal Access Controller Access Control System Plus), для перевірки автентичності користувачів.

Система запобігання вторгненням (IPS) – це інструмент мережевої безпеки (апаратний пристрій або програмне забезпечення), який постійно слідкує за периметром мережі на наявність шкідливої активності та вживає заходів для її запобігання. Ці заходи можуть включати звітування або блокування підозрілого трафіку.

Він є більш сучасним рішенням, ніж система виявлення вторгнень (IDS), яка лише виявляє підозрілу активність, але не може вживати жодних заходів проти неї, окрім оповіщення адміністратора. Системи запобігання вторгненням іноді входять до складу рішення next-generation firewall (NGFW) або об'єднаного керування

загрозами (UTM). Як і багато технологій мережевої безпеки, вони повинні бути достатньо потужними, щоб сканувати великий обсяг трафіку, не знижуючи продуктивності мережі.

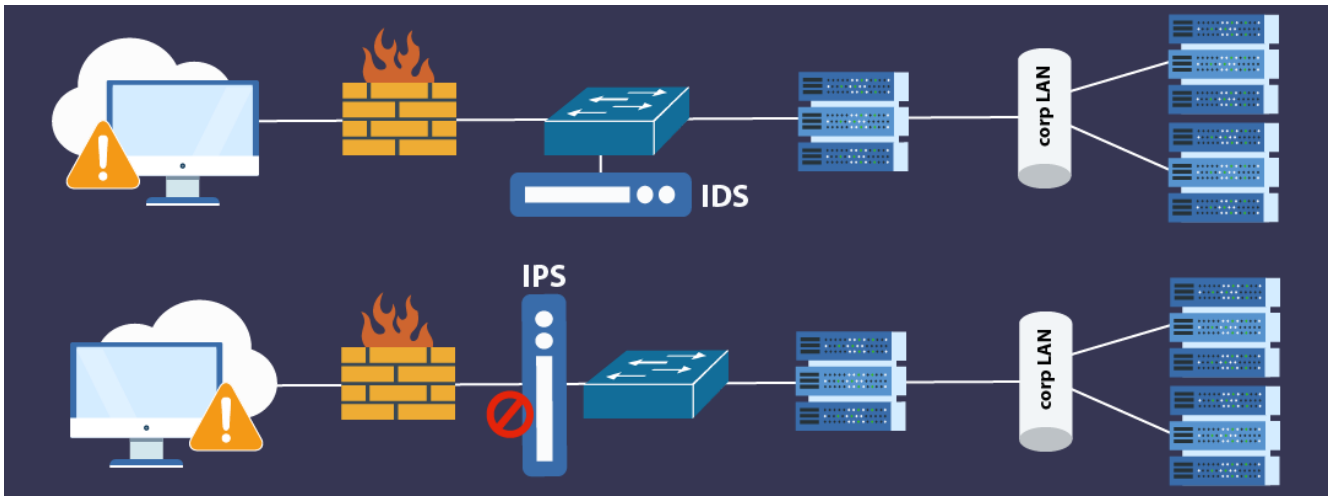


Рисунок 2.2 – Системи виявлення та запобігання вторгненням

Система запобігання вторгненням (IPS) встановлюється безпосередньо в потік мережевого трафіку між джерелом та призначенням, зазвичай розміщуючись одразу за брандмауером. Для виявлення загроз системи запобігання вторгненням використовують декілька методів:

– *базовані на сигнатурах.* Цей метод порівнює активність із сигнатурами відомих загроз. Недоліком цього методу є те, що він може зупинити лише раніше виявлені атаки і не зможе розпізнати нові;

– *базовані на аномаліях.* Цей метод здійснює моніторинг на предмет аномальної поведінки, порівнюючи випадкові зразки мережевої активності з базовим стандартом. Він є більш надійним, ніж моніторинг на основі сигнатур, але іноді може давати помилкові спрацювання. Деякі новіші та більш досконалі системи запобігання вторгненням використовують штучний інтелект та машинне навчання для підтримки моніторингу на основі аномалій;

– *базовані на політиках.* Цей метод менш поширений, ніж моніторинг на основі сигнатур або аномалій. Він використовує політики безпеки, визначені

підприємством, і блокує дії, які порушують ці політики. Це потребує від адміністратора налаштування та конфігурації політик безпеки.

Після того, як IPS виявляє підозрілу активність, вона може вжити багато автоматичних дій, включаючи оповіщення адміністраторів, відкидання пакетів, блокування трафіку з адреси джерела або переривання з'єднання. Деякі системи запобігання вторгненням також використовують "honeypot" (пастку для зловмисників) або підроблені цінні дані, щоб привабити атакуючих і не дозволити їм дістатися до цілей.

Існує декілька типів IPS, кожен з яких має трохи інше призначення:

- *система запобігання вторгненням в мережу (NIPS).* Цей тип IPS встановлюється лише в стратегічних точках для моніторингу всього мережевого трафіку та активного сканування на наявність загроз;
- *система запобігання вторгненням на хості (HIPS).* На відміну від NIPS, HIPS встановлюється на кінцевій точці (наприклад, на ПК) і аналізує лише вхідний та вихідний трафік з цієї машини. Він працює найкраще в поєднанні з NIPS, оскільки служить останньою лінією захисту від загроз, які пройшли повз NIPS;
- *аналіз мережевої поведінки (NBA).* Цей метод аналізує мережевий трафік для виявлення незвичайних потоків трафіку, таких як атаки DDoS (Distributed Denial of Service);
- *безпровідна система запобігання вторгненням (WIPS).* Цей тип IPS просто сканує мережу Wi-Fi на наявність несанкціонованого доступу та відключає неавторизовані пристрої від мережі.[29][19]

VPN – віртуальна приватна мережа, встановлює з'єднання між вашим комп'ютером і віддаленим сервером, створюючи тунель «точка-точка», який шифрує ваші особисті дані, маскує вашу IP-адресу і дозволяє вам обходити блокування вебсайтів і брандмауери в Інтернеті. Це гарантує, що ваша робота в Інтернеті є приватною, захищеною та більш безпечною.

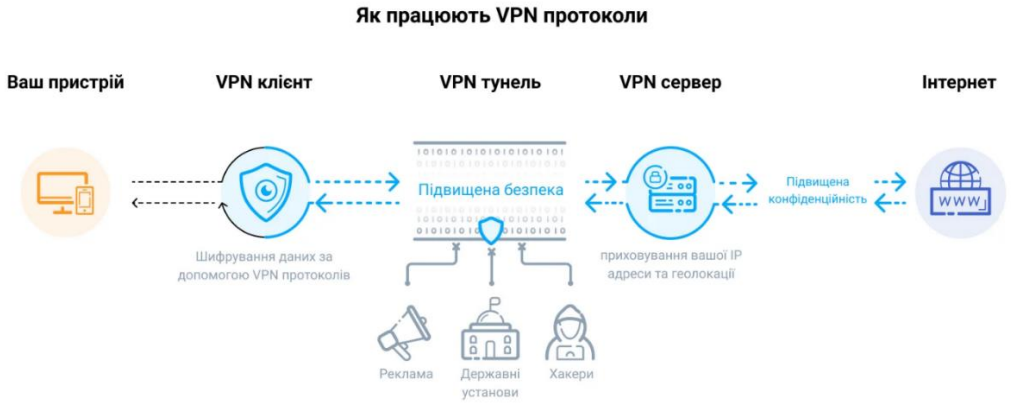


Рисунок 2.3 – Процес комунікації через VPN тунель

Існує кілька видів VPN: Site-to-Site VPN, IPsec, SSL, MPLS VPN.

VPN між декількома сайтами (Site-to-Site VPN), також відомий як маршрутизатор-маршрутизатор (Router-to-Router VPN), використовується переважно в корпоративних операціях. Багато компаній мають офіси як в межах країни, так і за її межами. Site-to-Site VPN використовується для підключення мережі головного офісу до кількох офісів. Цей тип VPN також відомий як VPN в межах мережі (intranet VPN). За допомогою Site-to-Site VPN можна зробити і навпаки. Компанії використовують Site-to-Site VPN для з'єднання з іншими компаніями у такий же спосіб, що і зовнішню мережу VPN. Іншими словами, Site-to-Site VPN створює віртуальний міст, який з'єднує мережі з різних місць, для підключення їх до Інтернету та забезпечення безпечного та приватного зв'язку між цими мережами.

IPsec - це скорочення від англійської назви Internet Protocol Security (безпека інтернет-протоколу). Цей VPN використовується для захисту зв'язку в IP-мережі. IPsec тунель на віддаленому сайті дозволяє отримати доступ до вашого центрального сайту. Щоб забезпечити безпеку комунікації з інтернет-протоколом, IPsec перевіряє кожен сеанс та індивідуально шифрує пакети даних протягом всього періоду з'єднання. IPsec VPN працює в двох режимах: транспортування та тунелювання. Обидва режими створені для захисту передачі даних між двома різними мережами. У режимі транспортування повідомлення в пакеті даних шифрується, а в режимі тунелювання - шифрується весь пакет даних.

Використання IPsec VPN має перевагу в тому, що можна використовувати різні протоколи захисту, для забезпечення більш сильної системи безпеки при користуванні послугами мережі. [20]

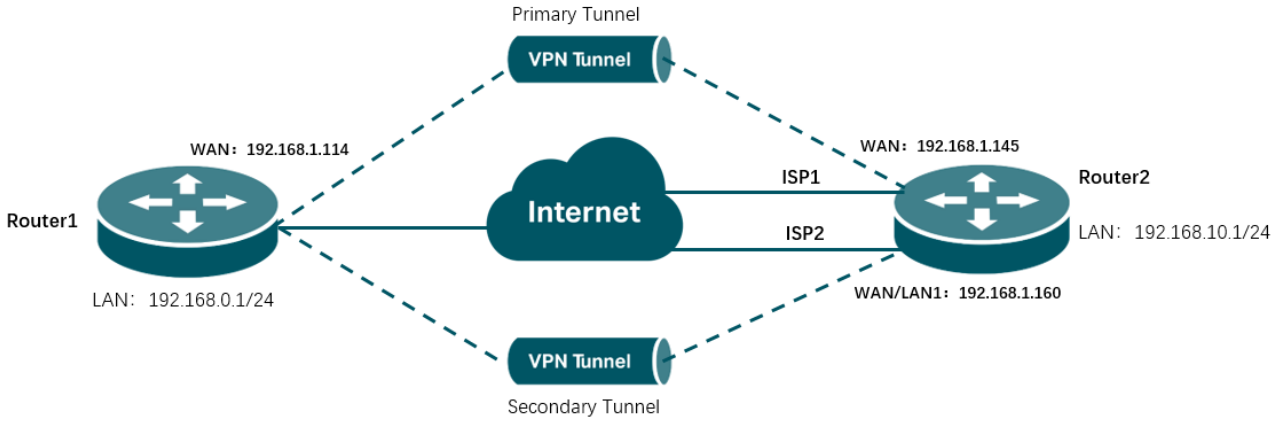


Рисунок 2.4 – Як відбувається комунікація в IPsec тунелі

SSL і TLS є абревіатурами від Secure Sockets Layer (рівень захищених гнізд) та Transport Layer Security (безпека транспортного рівня) відповідно. Ці протоколи працюють як один протокол і використовуються для встановлення VPN-з'єднання. Це VPN-з'єднання, де веб-браузер виконує роль клієнта і користувацький доступ обмежується лише певними програмами, а не цілою мережею. Протоколи SSL і TLS використовуються передусім сайтами онлайн-магазинів і провайдерами послуг. SSL та TSL VPN забезпечують безпечний сеанс між вашим ПК та сервером додатків через веб-браузер. Це можливо завдяки тому, що браузери легко переходять на SSL і не вимагають практично ніяких дій від користувача. SSL та TSL вже вбудовані в браузери. SSL-з'єднання мають на початку URL-адреси префікс https, а не http.[30][31]

MPLS VPN є скороченням від англійської фрази Multi-Protocol Label Switching, який є ще одним варінтом для з'єднання типу Site-to-Site. Це пов'язано з тим, що MPLS найбільш гнучкий та легко адаптується. MPLS є стандартним ресурсом, який використовується для прискорення розподілу мережевих пакетів за допомогою кількох протоколів. MPLS VPN є системами, які налаштовані на ISP VPN, який підключає два або більше сайтів, щоб створити VPN з використанням

того самого інтернет-провайдера. Однак, найбільшим недоліком використання MPLS VPN є те, що, порівняно з іншими VPN-послугами, мережу не так просто налаштовувати та вносити зміни, тому ціна на MPLS VPN, як правило, вища. [31]

2.5 Захист транспортного та прикладного рівнів

Транспортний рівень та прикладний – це два нерозривно пов'язаних рівня в моделі TCP/IP, які спільно роблять можливим представлення даних на кінцевих пристроях.

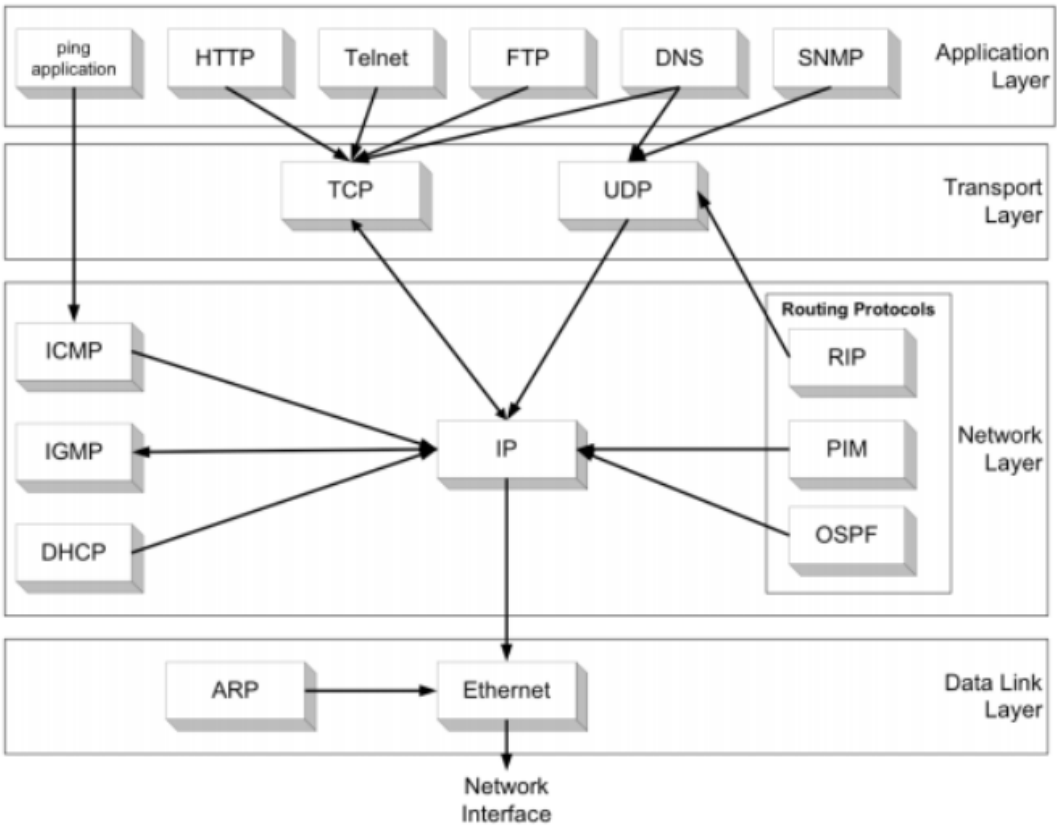


Рисунок 2.5 – Основні протоколи всіх рівнів TCP/IP

Брандмауер – це перший рубіж захисту вашої мережевої безпеки зі сторони Інтернету. Це інструмент кібербезпеки, який використовується для моніторингу та фільтрації вхідного та вихідного мережевого трафіку – зовнішніх джерел, внутрішніх джерел та навіть певних програм. Основна мета брандмауера –

блокувати шкідливі запити та пакети даних, дозволяючи при цьому легітимний трафік.

Існує багато типів архітектур розгортання брандмауерів, включаючи мережеві (програмне забезпечення), на базі хоста (апаратне забезпечення) та хмарні. Кожен брандмауер працює на основі визначених заздалегідь правил, щоб визначити, яким зовнішнім мережам та програмам можна довіряти. Таким чином, брандмауери є ключовим компонентом будь-якої архітектури мережевої безпеки.

Брандмауер захищає вашу мережу від підозрілих даних, перевіряючи вхідні пакети даних на наявність загроз. Брандмауери аналізують мережевий трафік на вміст даних, порти брандмауера (або точки входу), які дані намагаються використовувати, та звідки ці дані надходять.

Різні типи брандмауерів використовують різні методи або комбінації методів – для оцінки потенційно шкідливих джерел.

До цих інструментів брандмауера належать фільтрація пакетів, перевірка TCP, глибокий аналіз та проксі-контрольні точки. Брандмауери наступного покоління (NGFW) йдуть ще далі, застосовуючи превентивні заходи, такі як машинне навчання для виявлення незвичайної поведінки даних.

Існує три основних типи брандмауерів: програмні, апаратні або комбіновані, залежно від їхньої структури. Кожен тип брандмауера має різні функціональні можливості, але служить одній і тій же цілі – захисту. Однак для досягнення максимально можливої безпеки рекомендується використовувати обидва типи:

- апаратний брандмауер – це фізичний пристрій, який підключається між комп'ютерною мережею та шлюзом. Наприклад, широкосмуговий маршрутизатор. Іноді апаратний брандмауер називають апаратним пристроєм безпеки;
- програмний брандмауер – це звичайна програма, встановлена на комп'ютері, яка працює через номери портів та інше встановлене програмне забезпечення. Цей тип брандмауера також називають брандмауером хоста.

Крім того, існує багато інших типів брандмауерів залежно від їхніх функцій та рівня безпеки, який вони забезпечують. Нижче наведені типи технологій брандмауерів, які можуть бути реалізовані як програмно, так і апаратно:

- брандмауери з фільтрацією пакетів;
- проксі-сервери програмового рівня;
- брандмауери наступного покоління (NGFW);
- NGFW орієнтовані на загрози;
- брандмауери трансляції мережевих адрес (NAT).

Брандмауер з фільтрацією пакетів є найпростішим типом брандмауера. Він діє як програма керування, яка контролює мережевий трафік і фільтрує вхідні пакети на основі налаштованих правил безпеки. Ці брандмауери призначені для блокування мережевого трафіку за протоколами IP, IP-адресами та номерами портів, якщо пакет даних не відповідає встановленому набору правил.

Хоча брандмауери з фільтрацією пакетів можна вважати швидким рішенням без особливих вимог до ресурсів, вони також мають певні обмеження. Оскільки такі брандмауери не запобігають вебатакам, вони не є найбезпечнішими.

Проксі-сервери (брандмауери рівня додатків) працюють на рівні додатків як проміжний пристрій для фільтрації вхідного трафіку між двома кінцевими системами (наприклад, мережевими та трафік-системами). Саме тому ці брандмауери називаються "шлюзами рівня додатків".

На відміну від базових брандмауерів, ці брандмауери передають запити від клієнтів, видаючи себе за оригінальних клієнтів на вебсервері. Це захищає ідентифікаційну інформацію клієнта та іншу підозрілу інформацію, зберігаючи мережу захищеною від потенційних атак. Після встановлення з'єднання проксі-сервер перевіряє пакети даних, що надходять із джерела. Якщо вміст вхідного пакета даних захищений, проксі-сервер передає його клієнту. Такий підхід створює додатковий рівень безпеки між клієнтом та багатьма різними джерелами в мережі.

Багато з останніх випущених брандмауерів зазвичай визначаються як *"брандмауери наступного покоління" (NGFW).* Проте, чіткого визначення NGFW не існує. Цей тип брандмауера, як правило, визначається як пристрій безпеки, що поєднує функції та можливості інших брандмауерів. До таких функцій належать глибокий аналіз пакетів (DPI), поверхневий аналіз пакетів та тестування рукости TCP тощо.

NGFW забезпечує вищий рівень безпеки порівняно з брандмауерами з фільтрацією пакетів та перевіркою стану. На відміну від традиційних брандмауерів, NGFW відстежує всю транзакцію даних, включаючи заголовки пакетів, вміст пакетів та джерела. NGFW розроблені таким чином, що вони можуть запобігати більш складним та еволюційним загрозам безпеки, таким як атаки шкідливих програм, зовнішні загрози та складні вторгнення.

NGFW орієнтовані на загрози поєднують усі функції традиційного NGFW. Крім того, вони також забезпечують розширене виявлення та усунення загроз. Ці типи брандмауерів здатні швидко реагувати на атаки. Завдяки інтелектуальній автоматизації безпеки NGFW орієнтовані на загрози встановлюють правила та політики безпеки, що додатково підвищує безпеку загальної оборонної системи.

Більше того, ці брандмауери використовують системи ретроспективної безпеки для постійного моніторингу підозрілих дій. Вони продовжують аналізувати поведінку кожної активності навіть після початкової перевірки. Завдяки цій функціональності NGFW орієнтовані на загрози значно скорочують загальний час, необхідний від виявлення загрози до її усунення.[21][22]

РОЗДІЛ 3. ПОБУДОВА МЕРЕЖІ В СИМУЛЯТОРІ CISCO PACKET TRACER ТА ВПРОВАДЖЕННЯ ЗАХИСТУ ДЛЯ НЕЇ

3.1 Умови створення мережі

Працюючи мережевим інженером, доводиться спілкуватися із замовником, домовлятися з ним про вибір обладнання, терміни виконання задач, налаштування будь-якої технології або апаратної частини, адже всі мають різне бачення налаштування мережевого обладнання, маршрутів трафіку, відкриті порти, місце зберігання конфіденційних даних тощо. На етапі розробки має передбачатися майбутнє розширення мережі, безпека, тобто, надлишковість та безпека від злоякісних дії.

Отже, замовник – компанія-інтегратор безпекових рішень. Було отримано наступне завдання:

- розробити мережу, яка здатна вмістити та обробити запити від 150 до 200 користувачів;
- налаштувати VPN тунель між двома офісами в різних містах;
- впровадити мінімальні системи захисту(в даному випадку в межах програми Packet Tracer).

3.2 Створення фізичної та логічної топології мережі

Фізична та логічна топологія мережі відіграють важливу роль у проєктуванні, реалізації та керуванні мережевими системами. Розуміння цих двох концепцій є ключовим для створення ефективної та надійної мережі, яка відповідає вашим потребам.

Фізична топологія описує фізичне розташування мережевих пристроїв (комп'ютерів, маршрутизаторів, комутаторів тощо) та їх з'єднання один з одним. Це включає тип кабелів, що використовуються, розташування пристроїв та методи підключення.

Логічна топологія, з іншого боку, описує, як дані передаються через мережу. Це не залежить від фізичного розташування пристроїв, а описує логічні шляхи, якими дані переміщуються між ними.[23]

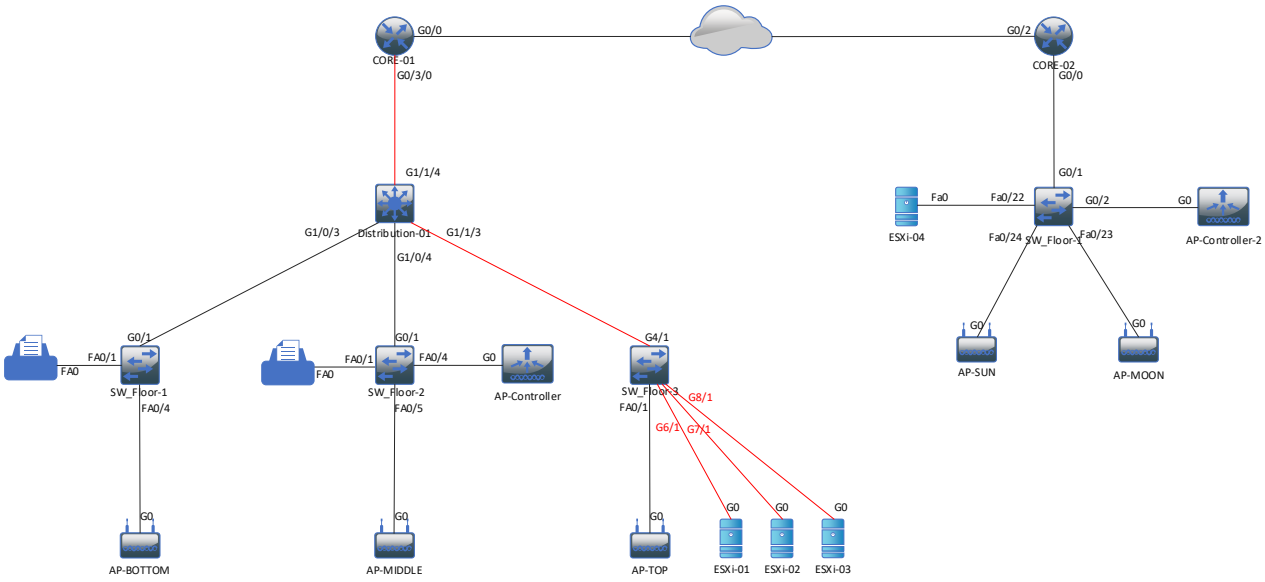


Рисунок 3.1 – Фізична топологія мережі

Виходячи з топології, можна побачити класичну, на сьогодні, модель мережі від компанії Cisco, яка містить:

– рівень доступу;

– рівень розподілу;

– рівень ядра.

Рівень доступу містить 3 комутатори, які рівномірно розподілені між поверхами в офісі, що знаходиться зліва, в той же час в правому офісі один єдиний комутатор виступає в ролі доступу та розподілу. Рівень доступу включає в себе комутатори доступу, які підключені до кінцевих пристроїв (комп'ютерів,

принтерів, серверів тощо). Також вони забезпечують доставку пакетів до кінцевих пристроїв.

На рівні розподілу було вирішено як тимчасовий варіант використати один L3 комутатор, адже на це вплинув бюджет компанії. Але на майбутнє заплановано додати ще один комутатор 3 рівня, задля протидії аварійним інцидентам на рівні розподілення. Мета цього рівня – забезпечити визначення меж шляхом реалізації списків доступу та інших фільтрів. Таким чином, рівень розподілу визначає політику для мережі. Рівень розподілу включає в себе високоякісні комутатори рівня 3. Рівень розподілу забезпечує правильну маршрутизацію пакетів між підмережами та віртуальними локальними мережами на вашому підприємстві.

Рівень ядра складається з найбільших, найшвидших і найдорожчих маршрутизаторів з найвищими номерами моделей і вважається основою мережі. Маршрутизатори Core Layer використовуються для об'єднання географічно розділених мереж. Маршрутизатори Core Layer переміщують інформацію в мережі максимально швидко. В даній топології маємо по одному потужному маршрутизаторі на рівні ядра.

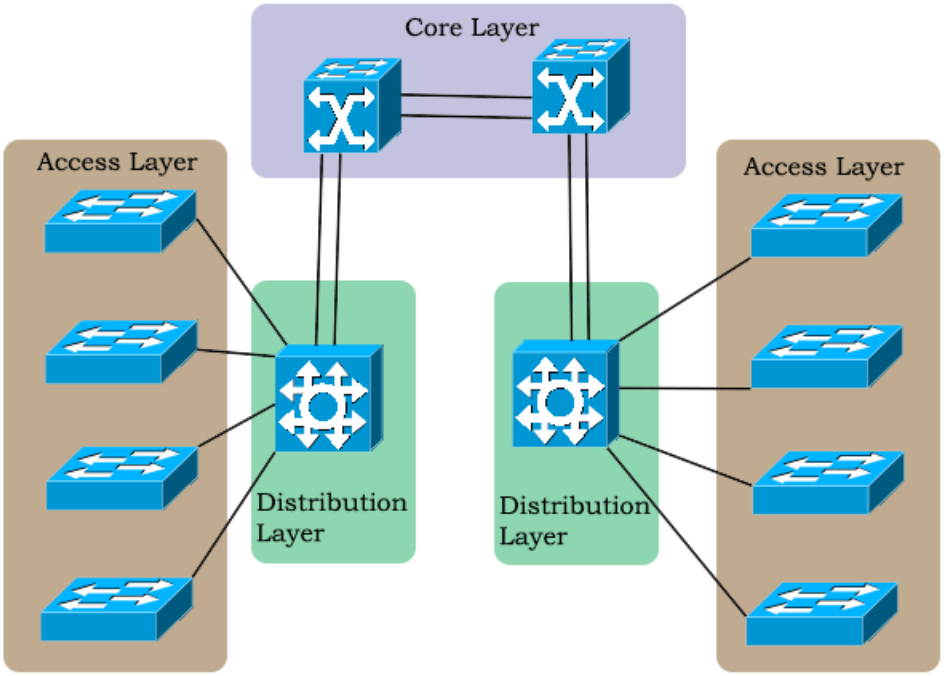


Рисунок 3.2 – Приклад трирівненої моделі компанії Cisco

Перевагу трирівневій ієрархічній моделі було надано тому, що вона допомагає проєктувати, розгортати і підтримувати масштабовану, надійну, економічно ефективну ієрархічну інтернет-мережу.

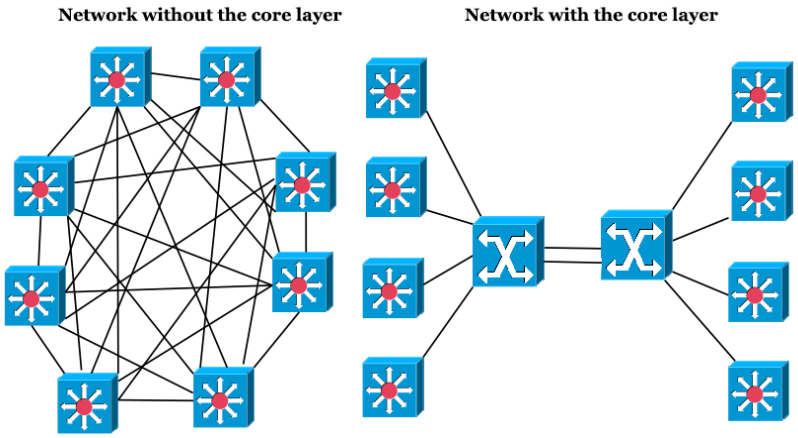


Рисунок 3.3 – Порівняння архітектури з без рівня ядра(зліва) та з ним(справа)

Продуктивність. Трирівнева мережева модель дозволяє створювати високопродуктивні мережі.

Краще управління та усунення несправностей. Дана модель дозволяє краще керувати мережею та знаходити або ізолювати причину не справності.

Легше *створення та застосування фільтрів/політик.* Трирівнева мережева модель дозволяє краще створювати фільтри/політики.

Масштабованість. Дозволяє ефективно адаптуватися до майбутнього зростання.

Надмірність. Трирівнева мережева модель забезпечує кращу надмірність. Кілька каналів зв'язку між кількома пристроями забезпечують кращу надмірність. Якщо один комутатор вийшов з ладу, у нас є інший альтернативний шлях, щоб дістатися до місця призначення. Але це поки не реалізовано, та планується на майбутнє.[25][24]

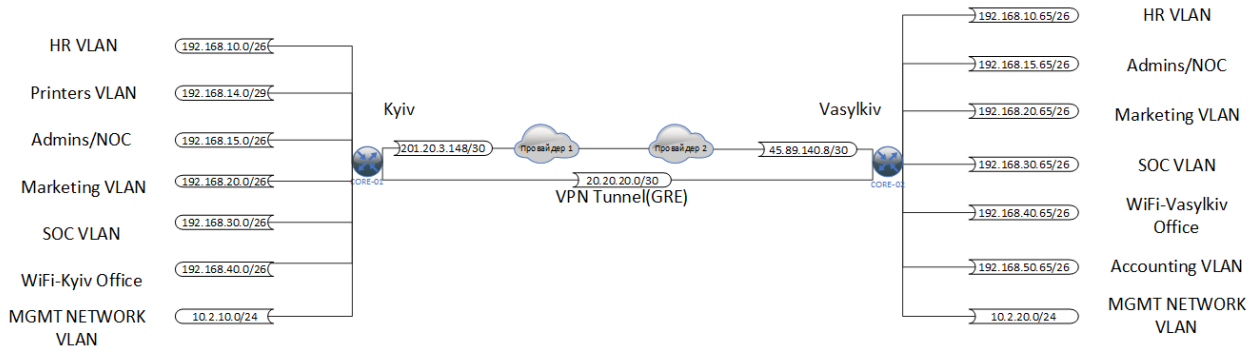


Рисунок 3.4 – Логічна топологія мережі

3.3 Налаштування мережевих пристроїв

Для роботи комутатора рівня доступу потрібно налаштувати:

– пароль до консольного порту;

– перевести всі віртуальні лінії комутатора режим транспорту SSH;

– задати параметри для менеджмент порту(порт підключення до комутатора для його конфігурації);

– опціонально увімкнути RSTP, але за умовчуванням функцію STP увімкнено на всіх L2 комутаторах;

– налаштувати AAA сервер, а саме видати ключ цьому комутатору;

– налаштувати необхідні VLAN;

– налаштувати VLAN на всі порти доступу(access mode), або увімкнути технологію IEEE 802.1x.

Приклад налаштувань на комутаторі рівня доступу продемонстровано у додатку А.

Для підключення до безпровідної корпоративної мережі також використовуємо IEEE 802.1x, який спирається на логін та пароль користувача.

Налаштовуємо менеджмент інтерфейс для контролера безпровідними точками доступу (рис.3.3).

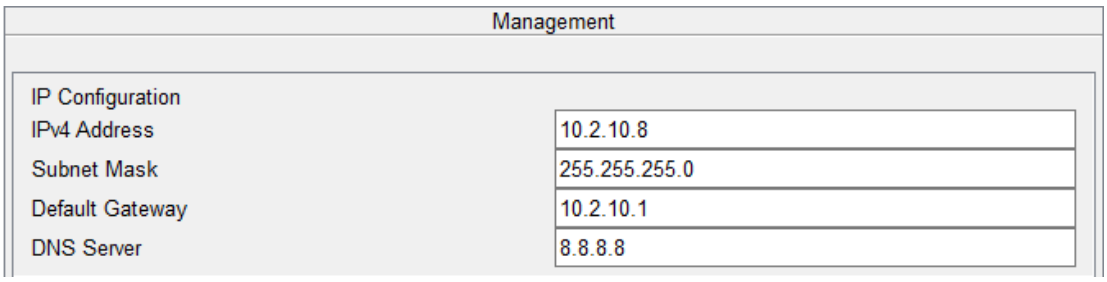


Рисунок 3.5 – Приклад налаштування менеджменту на контролері точок доступу

Також налаштовуємо тип аутентифікації, IP адресу AAA сервер, тип шифрування трафіку підчас процесу аутентифікації та авторизації клієнта:

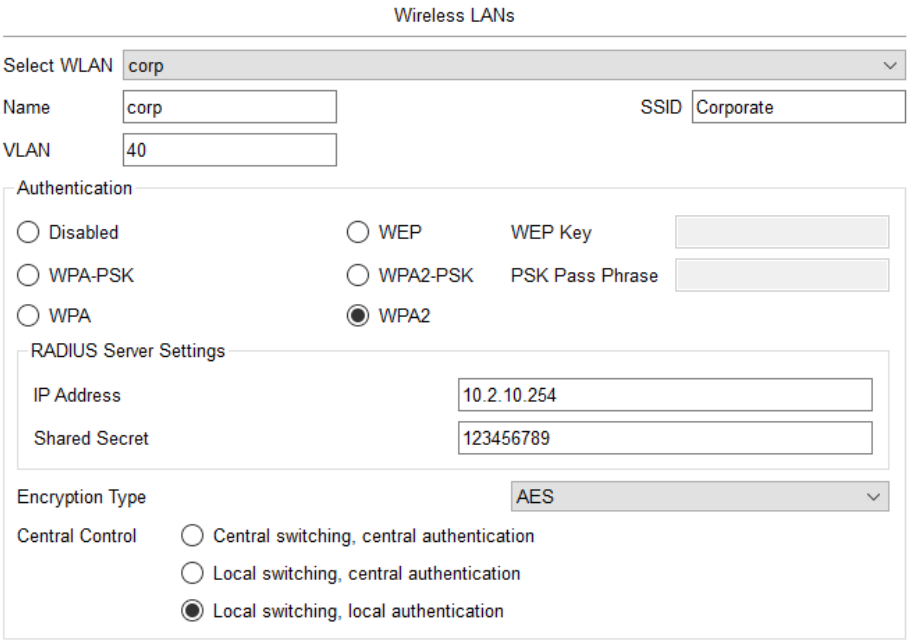


Рисунок 3.6 – Приклад налаштування аутентифікації на контролері точок доступ

Налаштувавши рівень доступу в мережі, потрібно налаштувати рівень розподілення, адже від цього рівня залежить швидкість комутації трафіку всередині мережі. В основному на ньому можуть комутуватися всі мережі та навіть деякі можуть бути затерміновані.

Зазвичай для такого рівня використовують потужний L3 комутатор, який загалом налаштовується як і пристрій рівня доступу. Але відмінність в тому, що рівень розподілення може працювати з IP адресацією та маршрутизацією.

Приклад налаштувань на комутаторі рівня розподілу продемостровано в додатку Б.

Рівень ядра – основа будь-якої мережі. Це шлюз який, дозволяє або забороняє трафік з внутрішньої мережі та всередину неї. Налаштування пристроїв цього рівня схожа на налаштування пристроїв іншого рівня, але є відмінності такі як:

– обов’язкова IP адресація та маршрутизація;

– NAT, який слугує брандмауером;

– ACL, яким можна заборони відповідний трафік з середині мережі, ззовні в мережу або з мережі;

– VPN, для безпечної передачі трафіку між офісами компанії, які розташовані географічно далеко.

Приклад налаштування роутера рівня ядра продемонстровано в додатку В.

ВИСНОВКИ

Отже, у світі, де кіберзагрози стають все більш складними та розповсюдженими, захист корпоративної комп’ютерної мережі стає критично важливим завданням для будь-якої компанії. Недбале ставлення до кібербезпеки може призвести до серйозних фінансових втрат, втрати довіри клієнтів та партнерів, а також до правових наслідків. Інвестування в комплексні заходи з кібербезпеки, впровадження передових технологій та вдосконалення політик та процедур безпеки – є важливим кроком для забезпечення надійного захисту корпоративної мережі. Тільки шляхом постійного підтримання та удосконалення заходів кібербезпеки компанії можуть ефективно протистояти зростаючим загрозам в цифровому середовищі та забезпечити свою стійкість та успішність у сучасному бізнес-середовищі.

Головна проблема будь-якої мережі – це люди. Саме вони спричиняють багато проблем, які потім доводиться вирішувати системному адміністратору або мережевому інженеру. Тому дуже важливо навчати працівників компанії, адже зловмисники використовують дуже велику площу атаки на компанію, починаючи від будь-яких сервісів в загальному доступі й закінчуючи користувачами та внутрішніми ресурсами.

Також варто підкреслити, що в Інтернеті немає нічого задарма, і якщо воно безкоштовне, то доводиться розплачуватися особистими даними. Тому важливо подбати про безпеку своїх даних та, перед використанням безкоштовних сервісів, переконатися в тому, що все безпечно або можливо варто купити платну версію, яка в тій чи іншій мірі має важіль на розробників, що ви є їх дорогоцінним клієнтом, якого вони боятимуться проґавити, через якийсь безпековий інцидент.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бученко І. А., Матвієнко Д. К. Чому протокол Ethernet такий популярний? «Проблеми комп'ютерної інженерії» : IV науково-практ. конф., м. Київ, 1 груд. 2023 р. С. 109–111. URL: https://duikt.edu.ua/uploads/p_2626_33497568.pdf.
2. Бученко І. А., Матвієнко Д. К. Проблеми сучасних фаєрволів. «Проблеми комп'ютерної інженерії» : IV науково-практ. конф., м. Київ, 1 груд. 2023 р. С. 112–113. URL: https://duikt.edu.ua/uploads/p_2626_33497568.pdf.
3. Mohanakrishnan R. What Is a Computer Network? Definition, Objectives, Components, Types, and Best Practices. *spiceworks*. URL: https://www.spiceworks.com/tech/networking/articles/what-is-a-computer-network/#_001 (дата звернення: 02.03.2024).
4. What is Computer Networking? – GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/what-is-computer-networking/ (дата звернення: 02.03.2024).
5. Учасники проєктів Вікімедіа. Інтранет – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Інтранет (дата звернення: 02.03.2024).
6. Учасники проєктів Вікімедіа. Екстранет – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Екстранет (дата звернення: 03.03.2024).
7. Nascimento C. Five Essentials for Building a Future-Ready Enterprise Network. *The Fast Mode | International Telecoms News, Analysis & Trends*. URL: https://www.thefastmode.com/expert-opinion/32791-five-essentials-for-building-a-future-ready-enterprise-network (дата звернення: 03.03.2024).
8. Що таке Ethernet - енциклопедія lanmarket.ua. *Магазин мережевого обладнання Lanmarket - роздрібний та оптовий продаж мережевого обладнання.* URL: https://lanmarket.ua/ua/entsiklopediya/telekommunikatsionnye-tekhnologii/ethernet.html (дата звернення: 03.03.2024).
9. Учасники проєктів Вікімедіа. PAN – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/PAN (дата звернення: 04.03.2024).

10. Учасники проєктів Вікімедіа. Локальна мережа – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Локальна_мережа (дата звернення: 04.03.2024).

11. Учасники проєктів Вікімедіа. Campus Area Network – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Campus_Area_Network (дата звернення: 04.03.2024).

12. Учасники проєктів Вікімедіа. WAN – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/WAN (дата звернення: 04.03.2024).

13. Учасники проєктів Вікімедіа. MAN (мережа) – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/MAN_(мережа) (дата звернення: 04.03.2024).

14. Учасники проєктів Вікімедіа. Мережа зберігання даних – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Мережа_зберігання_даних (дата звернення: 04.03.2024).

15. Учасники проєктів Вікімедіа. IEEE 802.11 – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/IEEE_802.11 (дата звернення: 07.03.2024).

16. Олещенко Л. *DSpace :: ELAKPI :: Репозитарій КПІ ім. Ігоря Сікорського*. URL:https://ela.kpi.ua/server/api/core/bitstreams/245d8d52-1715-4f2e-9e6a-e4bd17db7d4d/content (дата звернення: 16.03.2024).

17. Masucci M. 4 Ways to Ensure Network Physical Security. *Belden*. URL: https://www.belden.com/Blogs/Smart-Building/2020/05/06/ensuring-network-physical-security (дата звернення: 17.03.2024).

18. Технології мереж. *Nettech.ua* URL: https://nettech.ua/news/802-1x-ieee (дата звернення: 23.03.2024).

19. What is Intrusion Prevention System? | VMware Glossary. *VMware*. URL: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html (дата звернення: 27.03.2024).

20. How to Configure IPsec Failover on Omada Router in Standalone mode. *TP-Link Deutschland - Netzwerklösungen für Privat- und Businessanwender*. URL: https://www.tp-link.com/ru/support/faq/3575/ (дата звернення: 27.03.2024).

21. Types of Firewall – javatpoint.*www.javatpoint.com*. URL: https://www.javatpoint.com/types-of-firewall (дата доступу: 08.05.2024).

22. Dosal E. What is a Firewall? The Different Firewall Types & Architectures. *Cybersecurity Solutions | Enterprise IT Security Services | Compuquip*. URL: https://www.compuquip.com/blog/types-firewall-architectures (дата доступу: 30.03.2024).

23. STUDY.COM. *study.com*. URL: https://study.com/academy/lesson/physical-logical-topology-definition-characteristics.html (дата звернення: 03.04.2024).

24. Cisco Three Layer / Three-tier Hierarchical Network Model. *Free Networking tutorials, System Administration Tutorials and Security Tutorials - omnisecu.com*. URL: https://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php (дата звернення: 07.04.2024).

25. ComputerNetworkingNotes. Access, Distribution, and Core Layers Explained. *ComputerNetworkingNotes*. URL: https://www.computernetworkingnotes.com/ccna-study-guide/access-distribution-and-core-layers-explained.html (дата звернення: 11.04.2024).

26. Мікуляк С. *duikt.edu.ua*. URL: https://duikt.edu.ua/repozitorii/tsm/2020/Мікуляк%20С.В.pdf (дата звернення: 13.04.2024).

27. Еталонна модель OSI. *learn.ztu.edu.ua*. URL: https://learn.ztu.edu.ua/pluginfile.php/309890/mod_resource/content/1/Еталонна%20модель%20OSI.pdf (дата звернення: 14.04.2024).

28. Мережева взаємодія. *Мережева взаємодія*. URL: https://vlplk.blogspot.com/2017/12/osi.html (дата звернення: 14.04.2024).

29. Що таке IPS/IDS і де застосовується - Блог - HostZealot. *HostZealot*. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 15.04.2024).

30. What is SSL/TLS Encryption?. *F5, Inc.* URL: https://www.f5.com/glossary/ssl-tls-encryption (дата звернення: 16.04.2024).

31. Амос М. Різновиди мереж VPN та коли потрібно ними користуватися. *vpnMentor*. URL: https://uk.vpnmentor.com/blog/різновиди-мереж-vpn-та-коли-потрібно/ (дата звернення: 16.04.2024).

Додаток А

КОНФІГУРАЦІНИЙ ФАЙЛ КОМУТАТОРА ДОСТУПУ

```
Current configuration : 1857 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime
msec
service password-encryption
!
hostname SW_1Floor
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m
0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
!
username admin privilege 1 password 7
080148435817
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 14
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/4
switchport trunk native vlan 12
switchport trunk allowed vlan 10,12,14-
15,20,30,40
switchport mode trunk
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,12,14-
15,20,30,40
switchport mode trunk
!
interface GigabitEthernet0/2
switchport trunk allowed vlan
10,12,15,20,30,40
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan12
ip address 10.2.10.5 255.255.255.0
!
ip default-gateway 10.2.10.1

line con 0
password 7 0822455D0A16
login
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
end
```

Додаток Б

КОНФІГУРАЦІНИЙ ФАЙЛ КОМУТАТОРА РОЗПОДІЛУ

```
Current configuration : 2187 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Distribution-01
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
no ip cef
no ipv6 cef
!
username admin password 7 080148435817
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
!
spanning-tree mode pvst
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan
10,12,15,20,30,40
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport trunk allowed vlan 10,12,14-
15,20,30,40
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 10,12,14-
15,20,30,40
switchport mode trunk
!
interface GigabitEthernet1/1/3
switchport trunk allowed vlan 10,12,14-
15,20,30,40
switchport mode trunk
!
interface GigabitEthernet1/1/4
switchport trunk allowed vlan 10,12,14-
15,20,30,40
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 0002.17d2.e801
no ip address
!
interface Vlan12
mac-address 0002.17d2.e802
ip address 10.2.10.3 255.255.255.0
!
ip default-gateway 10.2.10.1
ip classless
!
ip flow-export version 9
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
!
transport input ssh
!
end
```

Додаток В

КОНФІГУРАЦІНИЙ ФАЙЛ РОУТЕРА ЯДРА

```
Current configuration : 4206 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime
msec
service password-encryption
!
hostname CORE-01
!
!
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m
0
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7
080148435817
!
!
license udi pid CISCO2911/K9 sn
FTX1524VS8Q-
!
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
!
spanning-tree mode pvst
!
interface Tunnel1
ip address 20.20.20.1 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0
tunnel destination 45.89.140.10
!
!
interface GigabitEthernet0/0
ip address 201.20.3.150
255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/3/0
no ip address
!
interface GigabitEthernet0/3/0.10
encapsulation dot1Q 10
ip address 192.168.10.1
255.255.255.192
ip access-group 101 in
!
interface GigabitEthernet0/3/0.12
encapsulation dot1Q 12
ip address 10.2.10.1 255.255.255.0
ip access-group 100 out
!
interface GigabitEthernet0/3/0.14
encapsulation dot1Q 14
```

```
ip address 192.168.14.1
255.255.255.248
!
interface GigabitEthernet0/3/0.15

encapsulation dot1Q 15
ip address 192.168.15.1
255.255.255.192
!
interface GigabitEthernet0/3/0.20
encapsulation dot1Q 20
ip address 192.168.20.1
255.255.255.192
ip access-group 102 in
!
interface GigabitEthernet0/3/0.30
encapsulation dot1Q 30
ip address 192.168.30.1
255.255.255.192
ip access-group 102 in
!
interface GigabitEthernet0/3/0.40
encapsulation dot1Q 40
ip address 192.168.40.1
255.255.255.192
ip helper-address 10.2.10.8
ip access-group 104 in
!
interface Vlan1
no ip address
shutdown
!
interface Vlan12
mac-address 000c.8593.2801
no ip address
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface
GigabitEthernet0/3/0
no passive-interface
GigabitEthernet0/3/0.10

no passive-interface
GigabitEthernet0/3/0.12
no passive-interface
GigabitEthernet0/3/0.14
no passive-interface
GigabitEthernet0/3/0.15
no passive-interface
GigabitEthernet0/3/0.20
no passive-interface
GigabitEthernet0/3/0.30
no passive-interface
GigabitEthernet0/3/0.40
network 192.168.10.1 0.0.0.0 area 0
network 192.168.15.1 0.0.0.0 area 0
network 192.168.20.1 0.0.0.0 area 0
network 192.168.30.1 0.0.0.0 area 0
network 192.168.40.1 0.0.0.0 area 0
network 10.2.10.1 0.0.0.0 area 0
network 201.20.3.150 0.0.0.0 area 0
network 20.20.20.1 0.0.0.0 area 0
!
ip classless
ip route 192.168.15.64 255.255.255.192
20.20.20.2
ip route 192.168.10.64 255.255.255.192
20.20.20.2
ip route 192.168.20.64 255.255.255.192
20.20.20.2
ip route 192.168.30.64 255.255.255.192
20.20.20.2
ip route 192.168.40.64 255.255.255.192
20.20.20.2
ip route 192.168.50.64 255.255.255.192
20.20.20.2
```

```
ip route 10.2.20.0 255.255.255.0
20.20.20.2
!
ip flow-export version 9
!
access-list 101 deny tcp 192.168.20.0
0.0.0.63 host 10.2.10.1
access-list 101 deny udp 192.168.10.0
0.0.0.63 host 10.2.10.1 range 22 telnet
access-list 101 deny tcp 192.168.10.0
0.0.0.63 host 10.2.10.1 range 22 telnet
access-list 100 deny udp 192.168.20.0
0.0.0.63 host 10.2.10.254 range 20 30
access-list 100 deny udp 192.168.10.0
0.0.0.63 host 10.2.10.254 range 20 30
access-list 102 deny udp 192.168.20.0
0.0.0.63 host 10.2.10.1 range 22 telnet
access-list 102 deny tcp 192.168.20.0
0.0.0.63 host 10.2.10.1 range 22 telnet
access-list 103 deny tcp 192.168.30.0
0.0.0.63 host 10.2.10.1 range 22 telnet
access-list 103 deny udp 192.168.30.0
0.0.0.63 host 10.2.10.1 range 22 telnet
access-list 104 deny udp
192.168.40.0 0.0.0.63 host 10.2.10.1
range 22 telnet
access-list 104 deny tcp 192.168.40.0
0.0.0.63 host 10.2.10.1 range 22 telnet
!
banner motd ^CVyjdy rozbijnyk!!!^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
End
```

Додаток Г

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

на тему: «Дослідження методів захисту комп'ютерної мережі на всіх рівнях моделі TCP/IP »

Виконав студент групи КІД-41
Матвієнко Денис Кенановчи

Керівник кваліфікаційної роботи :
Бученко Ігор Анатолійович ,
старший викладач кафедри КІ

Київ – 2024

Мета роботи – дослідження потенційних вразливостей при побудові мережі та захист від них

Об'єкт дослідження – побудова захищеної мережі на всіх рівнях TCP/IP

Предмет дослідження – корпоративна комп'ютерна мережа в симуляторі Cisco Packet Tracer

2

Актуальність обраної теми

Стек протоколів TCP/IP використовується в повсякденному житті, але його перші протоколи не передбачали шифрування трафіку. Коли почали з’являтися перші інциденти інформаційної безпеки, то компанії почали замислюватися про безпеку своїх даних. Саме тому потрібно захищатися не лише фізично, а і в мережі Інтернет. Витік будь-якої цінної інформації може поставити під загрозу існування компанії, так як це втрата великої кількості прибутку, клієнтів, адже їхня довіра до замовника різко втрачається.

3

Мережеві пристрої

Хаб

Маршрутизатор

Комутатор

Брандмауер

Сервер

4

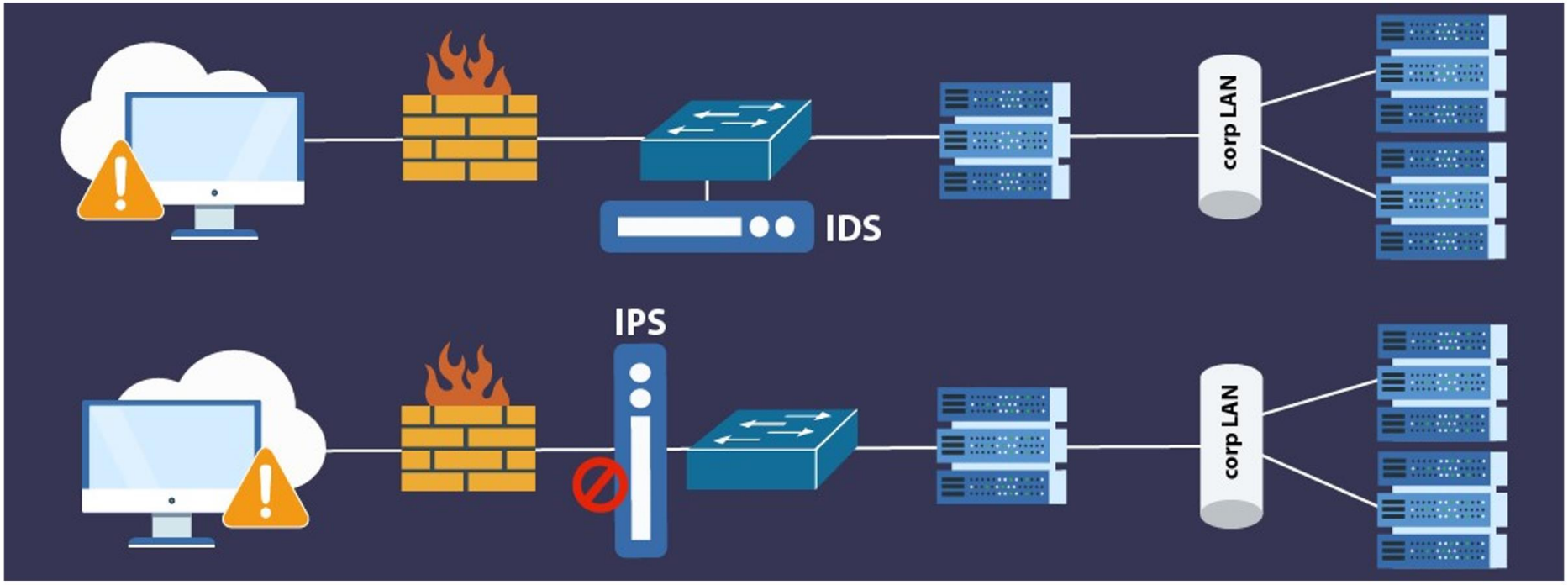
Порівняння різних мережевих моделей

5

Стандарти протоколу Ethernet

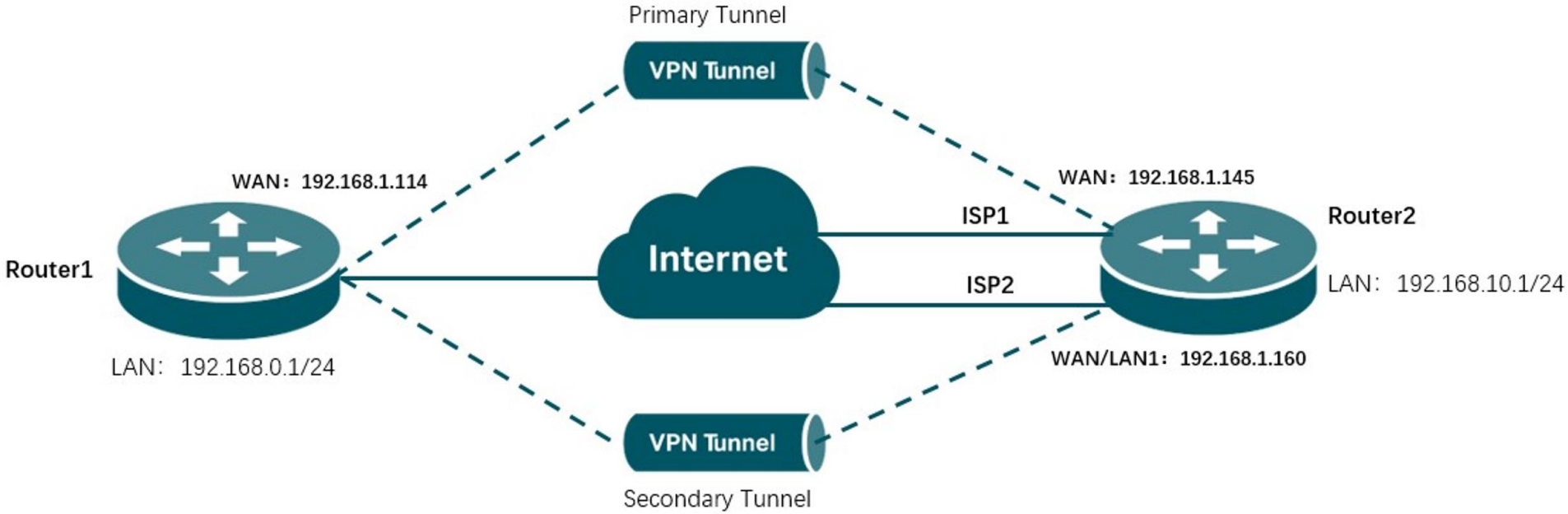
Тип Ethernet	IEEE Standard	Швидкість	Тип протоколу	Максимальна відстань
Ethernet	802.3	10 Mbps	10Base-T	100 метрів
Fast Ethernet/100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 – 2000 метрів
Gigabit Ethernet/GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 метрів 275/550 метрів 550/5000 метрів
10 Gigabit Ethernet	802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 метрів 300м / 10км 10км/40км 300м/10км/40км

Порівняння роботи IPS та IDS



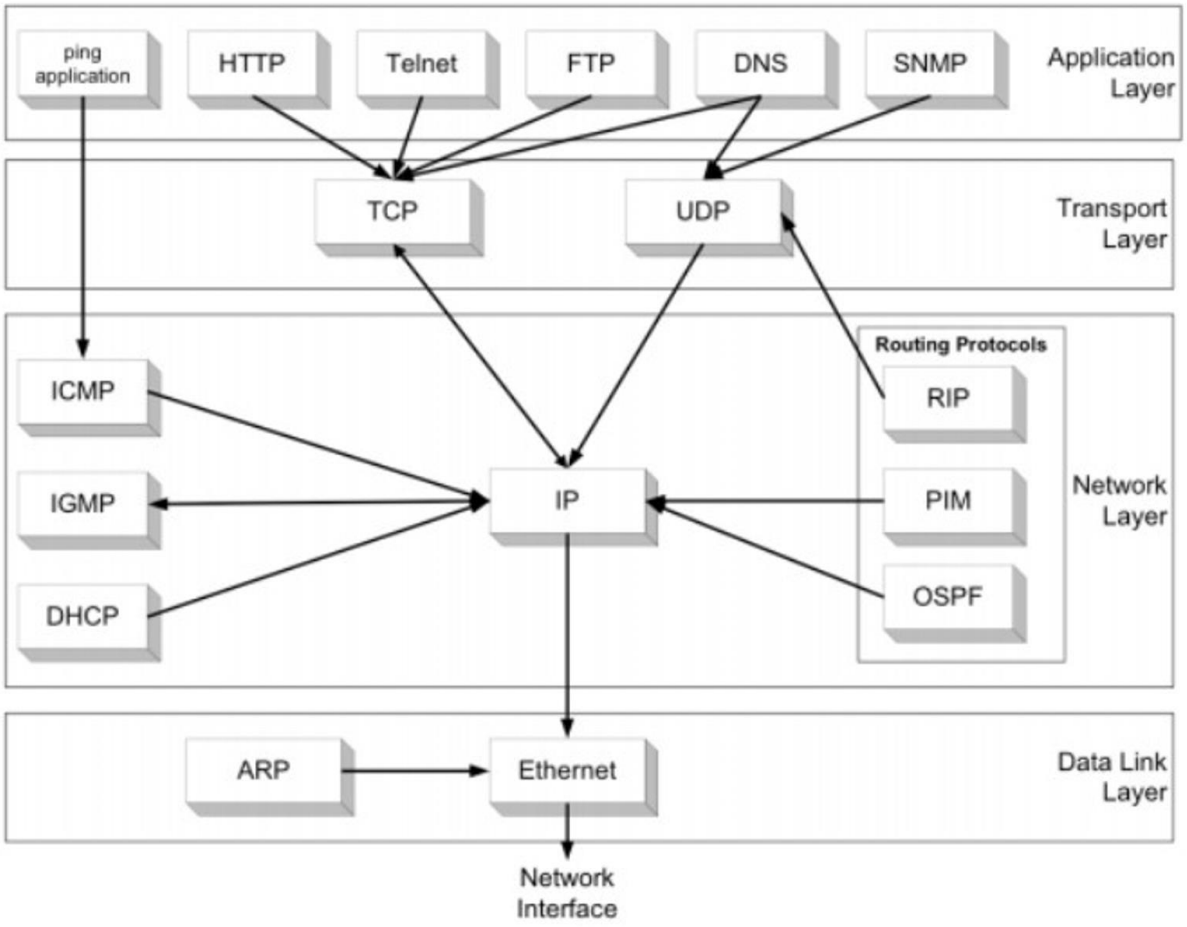
7

Принцип побудови тунелю IPSec

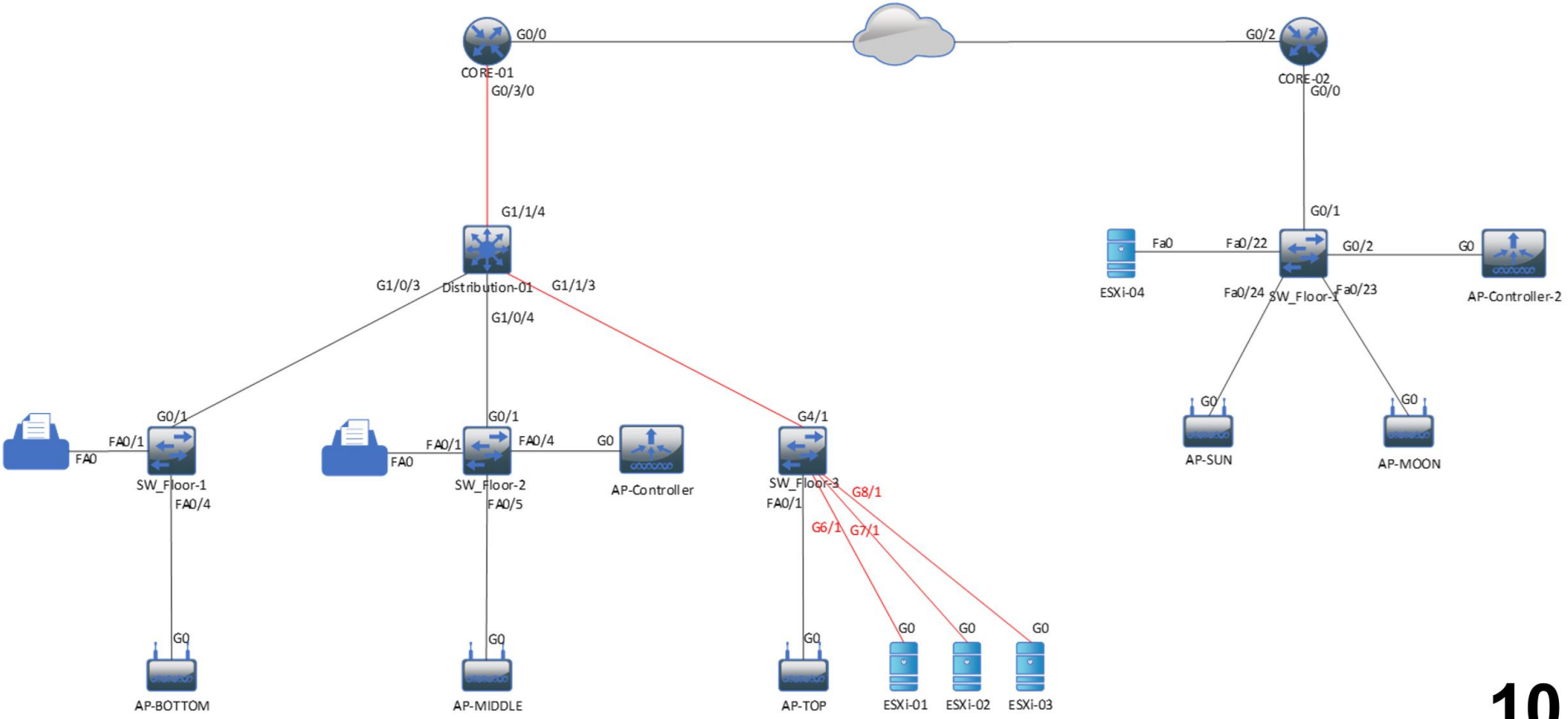


8

Основні протоколи моделі TCP/IP

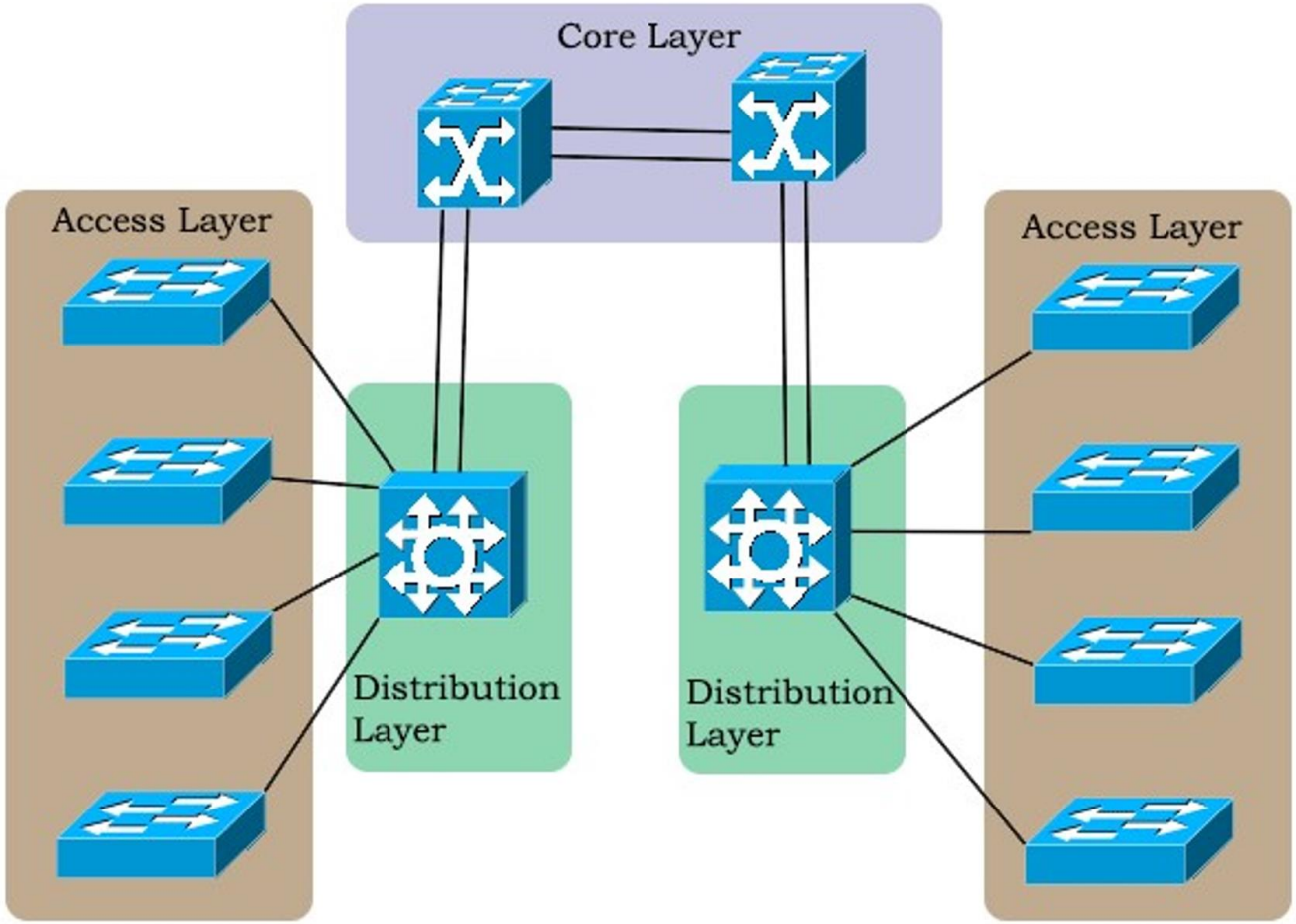


Фізична топологія мережі



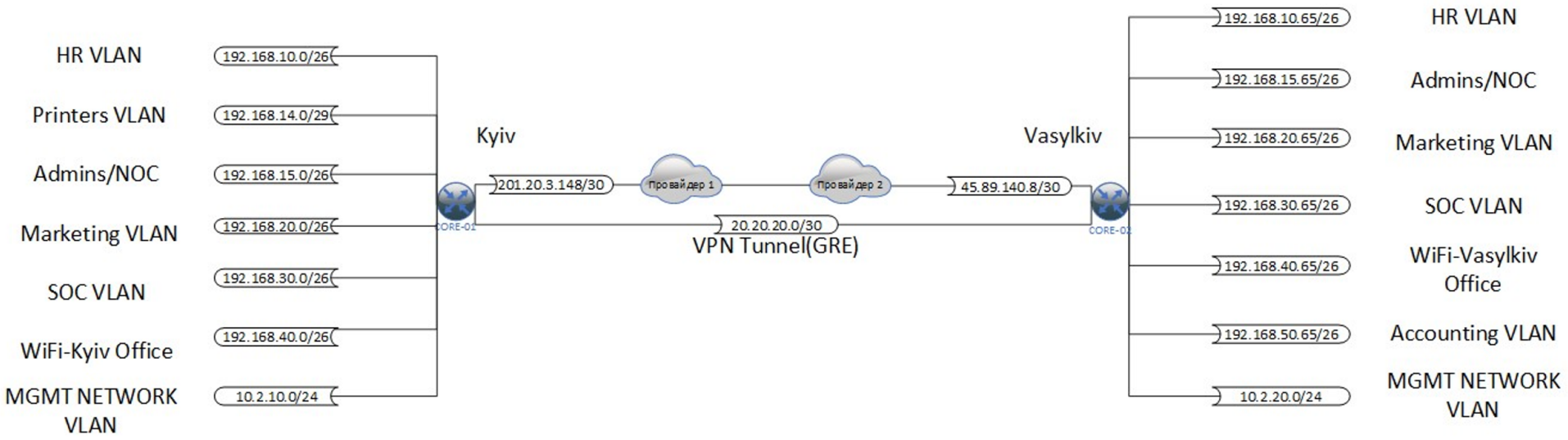
10

Трирівнева модель мереж компанії Cisco



11

Логічна топологія мережі



12

ВИСНОВКИ

Отже, у світі, де кіберзагрози стають все більш складними та розповсюдженими, захист корпоративної комп'ютерної мережі стає критично важливим завданням для будь-якої компанії. Недбале ставлення до кібербезпеки може призвести до серйозних фінансових втрат, втрати довіри клієнтів та партнерів, а також до правових наслідків. Інвестування в комплексні заходи з кібербезпеки, впровадження передових технологій та вдосконалення політик та процедур безпеки – є важливим кроком для забезпечення надійного захисту корпоративної мережі. Тільки шляхом постійного підтримання та удосконалення заходів кібербезпеки компанії можуть ефективно протистояти зростаючим загрозам в цифровому середовищі та забезпечити свою стійкість та успішність у сучасному бізнес-середовищі.

13

ПРОДОВЖЕННЯ ВИСНОВКІВ

Головна проблема будь-якої мережі – це люди. Саме вони спричиняють багато проблем, які потім доводиться вирішувати системному адміністратору або мережевому інженеру. Тому дуже важливо навчати працівників компанії, адже зловмисники використовують дуже велику площу атаки на компанію, починаючи від будь-яких сервісів в загальному доступі й закінчуючи користувачами та внутрішніми ресурсами.

Також варто підкреслити, що в Інтернеті немає нічого задарма, і якщо воно безкоштовне, то доводиться розплачуватися особистими даними. Тому важливо подбати про безпеку своїх даних та, перед використанням безкоштовних сервісів, переконатися в тому, що все безпечно або можливо варто купити платну версію, яка в тій чи іншій мірі має важіль на розробників, що ви є їх дорогоцінним клієнтом, якого вони боятимуться проґавити, через якийсь безпековий інцидент.

14

Результати впровадження

1. Бученко І. А., Матвієнко Д. К. Чому протокол Ethernet такий популярний? «Проблеми комп'ютерної інженерії» : IV науково-практ. конф., м. Київ, 1 груд. 2023 р. С. 109–111. URL: https://duikt.edu.ua/uploads/p_2626_33497568.pdf.

2. Бученко І. А., Матвієнко Д. К. Проблеми сучасних фаєрволів. «Проблеми комп'ютерної інженерії» : IV науково - практ. конф., м. Київ, 1 груд. 2023 р. С. 112–113. URL: https://duikt.edu.ua/uploads/p_2626_33497568.pdf .

15