МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

кафедра комп`ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Аналіз побудови корпоративної комп`ютерної мережі поштових відділень

Виконав студент групи: 1К-20

спеціальності: 123 «Комп`ютерна інженерія» Євгеній ЛИСЕНКО

Керівник: Маргарита МЕДОЛИЗ

Черкаси 2024

АННОТАЦІЯ

В цю роботу входить створення програмного інструменту для захисту корпоративної мережі, розкрито основні можливості корпоративних мереж та описується процес створення таких корпоративних інформаційних систем

ANNOTATION

This paper includes the creation of a software tool for corporate network security, reveals the main capabilities of corporate networks and describes the process of creating such corporate information systems

ЗМІСТ

ВСТУП

Актуальність дослідження. Однією з помітних тенденцій останнього часу є інтенсивний розвиток корпоративних мереж на виробничих підприємствах. Причому ці зміни видно не тільки у великих містах, але й у регіонах. Поняття «корпоративна мережа» можна визначити як групу організацій, яка, незалежно від організаційно-правової форми окремих одиниць або групи в цілому та деталей системи управління, об’єднана наявністю спільних організаційних, матеріальних і технологічних ресурсів. Інакше кажучи, всередині мережі відбувається вільний обмін інформацією, засобами, кадрами. У державних установах елементи мережевої структури можуть проявлятися у вигляді адміністративних та нормативних зв’язків між організаційними одиницями. Структура, що визначає характеристики мережі, є важливим параметром корпоративної мережі. Таким чином, структура мережі може розглядатися як об’єкт управління, вплив на який дозволяє контролювати потоки даних, що є основним завданням управління мережею.

На сьогоднішній день розроблено та використовується багато потужних систем управління захистом корпоративних мереж. Це дозволяє аналізувати їхню роботу та підкреслити їхні загальні позитивні й негативні сторони. Це пов’язано з необхідністю враховувати особливості функціонування корпоративної системи, що вимагає відповідних методів управління її роботою та налаштування корпоративної мережі. Таким чином, постійно поглиблюється розрив між зростаючими можливостями систем управління та реальними потребами в управлінні, орієнтованому на конкретні застосування.

Внаслідок цього розробляються нові концептуальні підходи до управління корпоративними мережами. Вони спрямовані на вирішення необхідного набору прикладних завдань, що при використанні універсальних багатофункціональних систем управління забезпечують потрібну якість їхнього розв’язання. Вирішення проблеми ґрунтується на розробці підходів до управління корпоративною мережею, що поєднує облік специфіки розв’язуваних завдань та можливості

діючих систем управління. Це дослідження стосується створення захищеної корпоративної мережі приватного підприємства на базі обладнання Cisco.

Актуальність те. Комплексному дослідженню сутності корпоративних мереж, розробці технологій реалізації та впровадження різних систем присвятили свої роботи такі вітчизняні та іноземні фахівці, як В. Г. Хоменко та М. П. Павленко [56], які запропонували новий аналітичний підхід до підготовки проєктів впровадження корпоративних інформаційних систем в організаціях. Питання створення захищеної корпоративної мережі вивчали як українські, так і зарубіжні вчені. Серед них можна виділити роботи В. М. Фурашев, Д. В. Ланде [55], І. Г. Тарахнов [50], В. І. Романчук, О. А. Лаврів, Р. І. Бак [41], К. В. Панфілов [37], Д. Куроуз, К. Рос [27], А. В. Зав'ялов [17], В. Л. Бурячок, А. О. Аносов [8].

Метою цього дослідження є створення програмного інструменту для захисту корпоративної мережі з можливістю реалізації як програмного, так і апаратного захисту передачі даних у мережі. Основою для цього є використання функцій ACL та протоколів NAT і PAT на базі обладнання Cisco.

Об'єктом нашого дослідження є сукупність необхідних умов, які забезпечують найкращий підхід до розуміння процесу створення захищеної корпоративної мережі.

Предметом дослідження є програмний захист корпоративної мережі на базі обладнання Cisco.

Для досягнення поставлених цілей використовувалися наступні **методи дослідження**:

1. Теоретичний аналіз наукової літератури.
2. Аналіз та узагальнення.
3. Статистичні дані та порівняння.
4. Класифікація теоретичного матеріалу та розробка рекомендацій.
5. Проєктування.

Завдання дослідження полягає в:

- розкрити основні можливості корпоративних мереж та описати процес створення таких корпоративних інформаційних систем;
- привести особливості віртуальної мережі передачі даних та назвати технології, що використовуються в корпоративних мережах;
- перелічити основні принципи захисту інформації при підключенні до мережі Інтернет;
- окремо навести особливості захисту інформації такими способами, як NAT-перетворення, можливість PAT, демілітаризована зона, антивірусний захист мережі, функція ACL та захист інформації за допомогою міжмережних екранів;
- детально дослідити основні етапи проєктування комп'ютерної мережі на базі обладнання Cisco;
- навести розрахунок необхідної кількості комп'ютерного устаткування корпоративної мережі, зробити вибір і обґрунтування програмного забезпечення корпоративної мережі, вибір серверного обладнання та комутаційного обладнання корпоративної мережі (Cisco C2911R, C819GW, C881G і т.д.);
- зробити побудову корпоративної мережі на основі вибраного обладнання та забезпечити захист створеної мережі;
- розробити програмний засіб захисту транспортування даних у мережі з використанням функції ACL та протоколів NAT і PAT.

Новизна дослідження. В ході дослідження було проведено всебічний літературний пошук та детальний аналіз наукових джерел. Отримані результати були систематизовані та адаптовані для використання. Також розроблено рекомендації для вдосконалення існуючої системи формування доходів від реалізації продукції сільськогосподарських підприємств.

Джерелами інформації для вирішення поставлених завдань стали збірники наукових праць, монографії, періодична література, підручники, довідники та спеціалізовані журнали.

РОЗДІЛ 1
ФУНКЦІЇ ТА ПРИНЦИПИ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Основні можливості корпоративних мереж

Як вже було сказано у вступі, корпоративна мережа – це складний комплекс взаємопов'язаних і узгоджено функціонуючих апаратних і програмних компонентів, що забезпечує передачу інформації між різними віддаленими додатками і системами, використовуваними на підприємстві. Через наявність декількох центрів обробки даних корпоративні мережі належать до децентралізованих (або розподілених) обчислювальним системам.

Корпоративну мережу необхідно розглядати з різних сторін: структурної, функціональної та системно-технічної. Із структурної точки зору корпоративна мережа – мережа змішаної топології, яка містить кілька локальних обчислювальних мереж. Корпоративна мережа об'єднує філії підприємства створюючи спільний інформаційний корпоративний простір. З цієї точки зору корпоративна мережа відображає структуру установи. З функціональної точки зору корпоративна мережа – це ефективне середовище передачі актуальної інформації необхідної для вирішення завдань [1, с. 45].

Сучасна корпоративна мережа – це не тільки мережа передачі даних, а складний комплекс, який здатний надавати різні сервіси з прогнозованими характеристиками. Завдяки корпоративним мережам результативно вирішуються завдання ключових процесів. Таких як:

- швидкий доступ до інформаційних масивів загального інформаційного простору;
- аналіз стану та управління бізнес-процесами з єдиного аналітичного центру;
- обмін інформаційними та розрахунковими документами;
- безперервне автоматизоване спостереження (моніторинг) і управління ресурсами інфокомунікаційної системи з Єдиного центру.

Основними перевагами впровадження корпоративних мереж є:

- отримання точної та оперативної інформації про роботу всіх підрозділів компанії;
- зростання ефективності управління організацією;
- скорочення витрат робочого часу на виконання робітниками певних процесів;
- зростання результатів роботи за рахунок більш доцільної її організації.

До найбільш суттєвих особливостей корпоративних мереж можна віднести наступні:

- масштабність системи, адже корпоративна мережа включає велику кількість комп'ютерів на великій території, які пов'язані між собою;
- гетерогенність – тобто неоднорідність обладнання, протоколів, операційних систем, додатків;
- використання глобальних зв'язків – корпоративна мережа для з'єднання віддалених локальних мереж і окремих комп'ютерів використовує всі типи глобальних зв'язків, в тому числі телефонні канали, радіоканали, супутниковий зв'язок, комерційні мережі з комутацією каналів і пакетів;
- Інтегрованість – неоднорідні частини і підмережі корпоративної мережі повинні працювати як єдине ціле, надаючи користувачам по можливості прозорий доступ до всіх необхідних ресурсів. Незалежно від того, яке обладнання придбано, корпоративна мережа повинна бути здатна інтегрувати вже наявні на підприємстві комп'ютерні системи [6, с. 210];
- підвищені вимоги до надійності – в корпоративній мережі виконуються стратегічно важливі для роботи підприємства додатки і зберігаються такі ж важливі дані, тому така мережа повинна мати мінімально можливий час простоїв основних компонентів через збої і відмови, а критична інформація не повинна втрачатися;
- підвищені вимоги до керованості мережі – масштабність мережі вимагає розвинених багатофункціональних засобів управління мережею, інакше

витрати експлуатації мережі з великим штатом фахівців набагато перевищать принесені вигоди. У корпоративних мережах користувачі висувають дуже жорсткі вимоги до часу усунення відмови обладнання, тому апаратна надмірність і планування відновлення після відмов є дуже важливими. Адміністратори корпоративних мереж потребують комплексних системах, що дозволяють їм не стільки оперативно реагувати на виникаючі відмови, скільки попереджати їх виникнення, наприклад, шляхом аналізу тенденцій в продуктивності мережі і виявлення проблем до того, як вони проявилися у вигляді відмов;

– універсальний характер розв’язуваних завдань – у той час як локальні мережі, як правило, мають спеціалізацію, для корпоративної мережі звичайним є наявність найрізноманітніших завдань, таких як автоматизація діловодства і автоматизація технологічних процесів, розробка програмних додатків і інформаційний пошук [20, с. 195];
– широта охоплення технічних проблем – при проєктуванні корпоративної мережі розробники мають справу з найширшим колом технічних питань (від мейнфреймів до ПК, від операційних систем до самих різних додатків, від вибору кабельної системи локальних мереж до вибору типу глобальних зв’язків, від питань сполучення різнорідних мережевих архітектур до проблем структуризації мережі з використанням всього різноманіття комунікаційного обладнання);
– потреба в наявності на підприємстві фахівців різних профілів високої кваліфікації – створення корпоративної мережі та управління нею вимагає наявності проєктувальників мережі, інсталяторів мережі та адміністраторів мережі.

1.2 Процес створення корпоративної інформаційної системи

Існує кілька способів об’єднання офісних локальних мереж в одну корпоративну мережу:

1. Використання бездротових мереж передачі даних. Застосовується для створення корпоративної мережі між робочими майданчиками, розташованими у близько розташованих будівлях.

2. Використання Інтернету як транспортного середовища передачі даних. Здійснюється за допомогою технології побудови VPN-тунелів.

3. Використання орендованих каналів передачі даних. Мережа може бути побудована як із застосуванням технології побудови VPN-тунелів, так і без неї.

Переваги об’єднання офісних мереж за допомогою бездротового обладнання [12, с. 58]:

- Швидке та просте розгортання локальної мережі.
- Низькі витрати на придбання обладнання.
- Низька вартість експлуатації та відсутність абонентської плати.
- Збереження інвестицій у локальну мережу при переїзді або зміні офісу.

Недоліки об’єднання офісних мереж за допомогою бездротового обладнання:

- Необхідність наявності прямої видимості між офісними майданчиками (в разі відсутності, необхідно проводити тестові випробування можливості підключення).

  Зниження швидкості передачі даних зі збільшенням відстані.

Використання Інтернету як транспортного середовища для передачі даних при створенні корпоративної мережі:

Переваги:

- Низька абонентська плата.
- Простота реалізації.

Недоліки:

- Невисока надійність.

– Відсутність гарантованої швидкості передачі даних.

Об’єднання локальних мереж підприємства в єдину корпоративну мережу на основі орендованих каналів передачі даних:

Переваги:

– Висока якість каналів передачі даних.
– Високий рівень послуг та сервісів, що надаються провайдером.
– Гарантована швидкість передачі даних.

Основна мета проєктування корпоративних мереж полягає в тому, щоб визначити структуру, склад апаратно-програмних засобів та організацію корпоративної мережі. І при заданих обмеженнях на витрати по проєктуванню, впровадженню та обслуговуванню вони будуть виконувати основні вимоги до якості інформаційних послуг, що надаються мережею [14, с. 33]. Процес будування відбувається на підставі характеристик корпоративних інформаційних потоків підприємства, параметрів споживачів і виробників інформації. Один з підходів до класифікації корпоративних мереж наведено в додатку А роботи.

Враховуючи масштабність, використання глобальних зв’язків, високий ступінь різнорідності проєктування корпоративних мереж є важко формалізуємими процесами. У сьогоднішній день відсутні універсальні методики проєктування корпоративних мереж. Тому необхідно сформулювати деякі типові етапи виконання мережевих проєктів. Процес проєктування корпоративної мережі складається з наступних етапів:

– аналіз вимог. На цьому етапі формулюються основні цілі підприємства (оперативний прийом замовлень, скорочення виробничого циклу, підвищення продуктивності праці). Аналізуються існуючі аналогічні системи, обґрунтовується необхідність у власних проєктах системи;
– розробка технічної моделі корпоративної мережі (структурний синтез). Технічна модель являє собою сукупність технічних засобів, необхідних для реалізації проєкту корпоративної мережі. На даному етапі

визначаються технічні параметри компонентів мережі, такі як повний функціональний набір необхідних програмних і апаратних засобів, але без конкретизації обладнання (марок і моделей);

- моделювання та оптимізація корпоративної мережі. Моделювання проводиться на даному етапі з метою оцінки характеристик функціонування корпоративної мережі та їх оптимізації [25, с. 420];
- установка і налагодження корпоративної мережі. На цьому етапі мається на увазі управління конфігураціями, координування поставок від субпідрядників, інсталяцію та налагодження обладнання, навчання персоналу;
- тестування корпоративної мережі. На цьому етапі повинні проводитися необхідні випробування, описані в контракті з інтегратором;
- супровід та експлуатація корпоративної мережі. Останній етап не має чітких часових меж, він передбачає безперервний процес.

В даний час набирає популярність багаторівнева архітектура, з огляду на те, що вона має багато таких переваг перед архітектурами файл-серверу і клієнт-серверу як:

- масштабованість;
- конфігурованість – ізольованість рівнів один від одного робить можливим миттєво і легкими засобами переконфігурувати систему при виникненні неполадок або при плановому обслуговуванні на одному з рівнів;
- високий рівень безпеки та ступінь надійності;
- невисокі вимоги до швидкості каналу (мережі) між терміналами і сервером додатків;
- невисокі вимоги до продуктивності і технічним характеристикам терміналів, тим самим відбувається зменшення їх вартості.

Але слід наголосити, що наведена архітектура мережі не змогла скласти конкуренцію іншим мережам завдяки:

- виникаючим труднощам під час розробки систем, адже складно узгодити різні модулі, через те, що вони були спроєктовані різними класами розробників. Як правило, зміна в одному плагіні призводить до обвальних змін в інших, виходячи з цього, неважко зробити висновок, що навіть саму елементарну систему, засновану на багаторівневій архітектурі, буде важче довести до ладу [30, с. 40];
- високим вимогам до ефективності роботи серверів додатків і сервера бази даних, що в свою чергу, збільшує вартість серверного обладнання;
- створеним завищеним умовам до забезпечення швидкості на лінії (мережі) між сервером бази даних і серверами додатків;
- існуванню великих труднощів по адмініструванню.

На даний час перспективною є технологія CASE (Computer Aided Software Engeneering). Початкове значення терміна CASE, яке було обумовлено питаннями автоматизації розробки виключно програмного забезпечення, в даний час отримало новий сенс, який охоплює процес розробки складних інформаційних систем. У порівнянні з традиційною технологією класичного проєктування CASE-технології володіють наступними перевагами:

- розвитком якості розроблюваного програмного продукту за рахунок засобів автоматичного контролю та генерації;
- можливістю використання елементів розробки повторно;
- підтриманням адаптивності та супроводу інформаційної системи;
- скороченням часу розробки системи – і це якраз те, що робить можливим на ранніх стадіях проєктування створення прототипу майбутньої системи.

1.3 Віртуальні мережі передачі даних

У 2012 році з’явилася технологія віртуалізації мережі (Network Virtualization, NV), що забезпечує можливість віртуалізації на принципово новому рівні – рівні мережевого сегменту. У випадку серверної віртуалізації з невеликими застереженнями операційна система (ОС) всередині віртуальних машин (ВМ) працює так, ніби була встановлена на фізичний сервер і була єдиною ОС на цьому обладнанні. За аналогією віртуалізація мережі призводить до того, що віртуальна, а точніше в даному контексті віртуалізована мережа, функціонує так, ніби вона була фізичною мережею [2, с. 205]. Даний рівень віртуалізації дозволяє створювати і використовувати кілька віртуальних мереж, можливо з перекриваємими або навіть повністю схожими просторами IP-адресів, на одній фізичній мережевій інфраструктурі. Ця мережева інфраструктура, може включати в себе довільну кількість фізичних серверів і мережевого обладнання. Схематичне зображення віртуальної мережі передачі даних наведено в додатку Б.

Штатні засоби платформи VMware vSphere не надають переваг масштабованості, гнучкості налаштування мережі і не реалізують функції, що необхідні для безпечної роботи мережі. Внаслідок чого необхідно використовувати додаткові сторонні засоби для створення нової системи роботи мережі. Віртуальна локальна мережа (VLAN) являє собою логічний домен циркулярної розсилки, який може охоплювати безліч фізичних локальних мережевих сегментів. За кожним портом комутатора може бути закріплена конкретна VLAN, яка може бути логічно сегментована відповідно до її функцій і завдань. Порти однієї VLAN мають спільний домен циркулярної розсилки. Порти, що відносяться до різних VLAN, не можуть здійснювати циркулярну розсилку.

Можна підвищити рівень безпеки шляхом сегментування мережі на окремі домени циркулярної розсилки. Крім того, можна регулювати розмір і структуру домену шляхом регулювання розміру і структури VLAN. Віртуальна корпоративна мережа з віддаленим доступом наведена в додатку В.

VLAN дозволяють групувати порти комутатора таким чином, щоб трафік обмежувався тільки членами тієї чи іншої групи. Ця функція обмежує циркулярну, одноадресну і багатоадресну розсилку (лавинна адресація) тільки портами, що включені в конкретну VLAN. VLAN дозволяє ефективно розділяти трафік, забезпечуючи більш високу пропускну здатність. Можливі такі типи VLAN:

- VLAN на базі порту, який не має стандарту;
- на базі тільки одного комутатора;
- VLAN на базі MAC, який не має стандарту;
- VLAN на базі ознаки (tag-based), IEEE 802.1 q;
- може бути між кількома комутаторами.

Внутрішньокорпоративні мережі VPN будуються з використанням Internet або мережевих інфраструктур, що розділяються між сервіс-провайдерами, які надають послугу. З'єднання вузлів мережі за допомогою технології Intranet VPN наведено в додатку Г. Основними перевагами Intranet VPN є:

- застосування потужних криптографічних протоколів шифрування даних для захисту конфіденційної інформації;
- надійність функціонування при виконанні таких критичних застосувань, як системи автоматизованого продажу і системи управління базами даних;
- гнучкість управління ефективним розміщенням швидко зростаючої кількості нових користувачів, нових офісів і нових програмних застосувань.
- Побудова Intranet VPN є найрентабельнішим способом реалізації VPN-технології. Проте в Internet рівні сервісу взагалі не гарантуються. Компанії, яким потрібно гарантовані рівні сервісу, повинні розглянути можливість розгортання своїх VPN з використанням мережевих інфраструктур, що розділяються між сервіс-провайдерами, які надають послугу [3, с. 16].

– Міжкорпоративна мережа VPN – це мережева технологія, яка забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії і, таким чином, сприяє підвищенню надійності зв’язку, підтримуваного в ході ділової співпраці. Міжкорпоративна мережа Extranet VPN наведена в додатку Д. Мережі Extranet VPN (ME) в цілому схожі на внутрішньокорпоративні віртуальні приватні мережі з тією різницею, що проблема захисту інформації є для них гострішою. VLAN на базі порту дозволяє створювати VLAN з різних портів одного моста. VLAN на базі MAC дозволяє об’єднувати в сегмент MAC адресу хост-машин, а VLAN на базі ознаки дозволяє створювати VLAN за якою-небудь ознакою. Ознака записується після MAC адреси джерела в кадрі Ethernet, що дозволяє ідентифікувати VLAN. На сьогодні рішення по віртуалізації мережі надають великі корпорації, а саме: VMware NSX – це платформа віртуалізації мережі для програмного ЦОД; Amazon Elastic Compute Cloud – Amazon EC2) – це веб-сервіс, що надає масштабовані обчислювальні ресурси в хмарі; Cisco Application Centric Infrastructure – ACI) – інфраструктура, що орієнтована на додатки.

OpenFlow – протокол управління процесом обробки даних, що передаються по мережі маршрутизаторами і комутаторами, що реалізує технологію SDN. Протокол використовується для управління мережевими комутаторами і маршрутизаторами з центрального пристрою-контролера мережі. Як елемент управління роботою мережі може бути використана віртуальна машина з встановленим на ній OpenFlow-контролером floodlight. Задля передачі даних між користувачами в кожному ESXi-хості встановлюють OpenvSwitch (реалізація OpenFlow switch). Ізоляція інформації між ESXi-хостами може бути реалізована за рахунок створення GRE-тунелів. Правила роботи OpenFlow switch описані в таблицях потоків, які містяться в його пам’яті. Таблиця потоків складається із записів, в кожній з яких містяться поля порівняння, лічильники та інструкції. Коли пакет надходить в OpenFlow switch

поля порівнянь записів таблиці потоків, то порівнюються з заголовком пакета в порядку пріоритету (одне з полів порівняння). Якщо знайдено схожий запис, то до пакету застосовуються інструкції, які асоційовані з цим записом, і при цьому, збільшується значення лічильника.

Таким чином, завдання зводиться до передачі таблиць потоків в відповідний Open vSwitch. Щоб визначити, який зміст таблиць повинен бути на кожному Open vSwitch-е, і яку необхідно зібрати інформацію про систему, (її MAC адресу, Vlan, на якому ESXi-хості і в якій зоні безпеки вона знаходитися). Для цього розроблений модуль збору інформації з vCenter з використанням засобів віддаленої командного рядка vSphere CommandLine Interface (програма на C++) [13, с. 185].

Xen – загальнодоступний гіпервізор, запропонований для роботи на товарних платформах апаратних засобів, які використовують метод паравіртуалізації. Xen дозволяє одночасно керувати багатофункціональними VMs на єдиній фізичній машині. Схематичне зображення архітектури Xen наведено в додатку Ж. Архітектура Xen складається з одного гіпервізора, розташованого вище фізичних апаратних засобів і кількох VMs по гіпервізору. У кожного VM може бути свій власний ОС і додатки. Гіпервізор керує доступом до апаратних засобів, а також наявними ресурсами, розділеними між VMs. Крім того, драйвери пристроїв збережені в ізольованому VM, названому Доменом 0 (dom0) для забезпечення надійної і ефективної апаратної підтримки. Оскільки dom0 має повний доступ до апаратних засобів фізичної машини, то у нього існують також спеціальні привілеї в порівнянні з іншими VMs, так званими користувацькими доменами (domUs).

Vmware – компанія, яка надає машинні платформи віртуалізації клієнтам центру обробки даних і кінцевого користувача. Платформи віртуалізації VMware засновані на понятті повної віртуалізації. Воно оцінює рівень платформи віртуалізації центру обробки даних VMware під назвою vmware сервер ESX. Ізоляція VM і частота представлення ресурсу на основі політики розподілу

ресурсів встановлюється системним адміністратором. Схематичне зображення архітектури Vmware наведено в додатку З.

Архітектура Vmware складається з компонентів інтерфейсу апаратних засобів, монітора віртуальної машини (VMM), VMkernel, менеджера ресурсів і сервісного управління. Компоненти інтерфейсу апаратних засобів відповідальні за здійснення визначених для апаратних засобів функцій і створюють надану VMs абстракцію апаратних засобів. Це робить незалежні апаратні засоби VM як VMM відповідальними за центральний процесор віртуалізації, надаючи vCPU кожному VM. VMkernel керує і стежить за основними апаратними засобами. VMM і VMkernel разом здійснюють шар віртуалізації. Управління ресурсами здійснюється VMkernel. Він ділить основні фізичні ресурси між VM, перерозподіляючи ресурси для кожного VM.

OpenVZ – загальнодоступний інструмент віртуалізації рівня ОС. Кожне ізольоване навколишнє середовище називають Virtual Private Server (VPS). VPS схожий на фізичний сервер, маючи власні процеси, файли, адреси Internet Protocol (IP), системну конфігурацію і забезпечуючи повний доступ до кореня [11, с. 52]. Головне місце використання цієї технології віртуалізації є веб-хостинг, де надається кожному клієнту повне навколишнє середовище Linux, а так само вона використовується в освітніх інформаційних технологіях (IT). OpenVZ менш гнучкий, ніж інші інструменти віртуалізації, такі як VMware або Xen, тому що середовище для OpenVZ має бути Linux дистрибутивом, на основі того ж самого ядра ОС фізичного сервера. Схематичне зображення архітектури OpenVZ наведено в додатку Є.

Архітектура OpenVZ складається з зміненого ядра Linux, яке знаходиться вище апаратних засобів. OpenVZ – змінене ядро, що здійснює віртуалізацію та ізоляцію кількох підсистем, управління ресурсом і контрольно-пропускними пунктами. Крім того, механізми віртуалізації вводу / виводу забезпечені OpenVZ-зміненим ядром, у якого є драйвер пристрою для кожного пристрою введення / виводу. Це змінене ядро також здійснює дворівневий планувальник

процесу, який відповідальний за перший рівень, визначаючи який VPS буде здійснюватися, і хто буде керувати процесами VPS.

1.4 Технології, що використовуються в корпоративних мережах

Сучасні корпоративні мережі створюються за допомогою комплексного підходу, який довів свою ефективність і надійність. Цей підхід спрямований на забезпечення захищеного середовища для обробки інформації в корпоративних мережах. Він включає правові, морально-етичні, організаційні, програмні та технічні методи забезпечення інформаційної безпеки.

Основні технології, що використовуються для побудови корпоративних мереж, включають Ethernet, Token Ring і FDDI. Технологія Ethernet використовує дуже простий алгоритм доступу, який дозволяє вузлу мережі передавати дані тоді, коли він вважає, що спільне середовище вільне. Простота Ethernet обумовила низьку вартість і простоту обладнання для цієї технології. Однак, недоліком алгоритму доступу Ethernet є можливість зіткнення кадрів, що передаються різними станціями, в загальному середовищі. Це знижує ефективність використання спільного середовища та надає роботі з мережею непередбачуваного характеру.

Початковий варіант Ethernet був розроблений для використання з коаксіальним кабелем, який використовувався всіма вузлами мережі як загальна шина. Перехід на кабельні системи з використанням концентраторів (хабів) значно підвищив експлуатаційні характеристики мереж Ethernet [33, с. 302].

Технології Token Ring та FDDI використовують більш складні та ефективні алгоритми доступу до середовища, засновані на передачі спеціального кадру, відомого як токен. Цей механізм забезпечує контрольований доступ до мережі, однак ці переваги не забезпечили їм успішної конкуренції з технологією Ethernet.

Серед популярних мережевих технологій побудови локальних мереж виділяються Token Ring та FDDI, які є функціонально складнішими. Їхні розробники прагнули наділити корпоративні мережі низкою позитивних

якостей: забезпечити кероване та передбачуване розділення середовища, створити відмовостійкість мережі, та організувати пріоритетне обслуговування трафіку, чутливого до затримок, наприклад, голосового. Механізм доступу до середовища в мережах Token Ring та FDDI є більш детермінованим, ніж в Ethernet.

Зазвичай вузли в мережах Token Ring та FDDI з'єднані у кільце, де кожна станція отримує інформацію від попередньої і передає наступній по колу. Перші мережі Token Ring, розроблені IBM, мали швидкість передачі даних 4 Мбіт/с, яку згодом підвищили до 16 Мбіт/с. Основним середовищем передачі даних є вита пара.

Для адресації мереж Token Ring та FDDI використовуються MAC-адреси того ж формату, що і в Ethernet. Метод доступу в Token Ring полягає в передачі токену між вузлами. Лише вузол, що володіє токеном, може передавати свої кадри, що робить мережу розділеним середовищем. Існує обмеження на час монопольного використання середовища – так званий час утримання токену, по закінченню якого вузол передає токен сусідньому по кільцю вузлу. Це запобігає невизначеному часу очікування доступу до середовища, характерному для Ethernet.

Мережі FDDI (Fiber Distributed Data Interface, волоконно-оптичний розподілений інтерфейс даних) можна вважати вдосконаленим варіантом Token Ring. FDDI використовує той самий принцип доступу через передачу токену і кільцеву топологію зв'язків, але працює на вищих швидкостях і має більш досконалий механізм відмовостійкості. Технологія FDDI стала першою корпоративною мережею, яка використала оптичне волокно як спільне середовище передачі даних [36, с. 560].

Використання оптичних систем дозволило підвищити швидкість передачі даних до 100 Мбіт/с. Пізніше з'явилося обладнання FDDI на витій парі, що працює на аналогічній швидкості. Для забезпечення високої надійності в мережах FDDI використовували подвійне кільце. У звичайному режимі станції

використовують первинне кільце для передачі даних і токену доступу, тоді як вторинне кільце залишається в резерві. У разі відмови, наприклад, через обрив кабелю між станціями 1 і 2, первинне кільце об'єднується зі вторинним, створюючи єдине кільце. Цей режим роботи мережі називається режимом згортання кілець. Операція згортання здійснюється за допомогою повторювачів і мережевих адаптерів FDDI.

Для спрощення процедури згортання дані по первинному кільцю завжди передаються в одному напрямку, а по вторинному – у зворотному. Таким чином, при об'єднанні двох кілець передавачі станцій залишаються підключеними до приймачів сусідніх станцій, що дозволяє їм правильно передавати та приймати інформацію.

Однією з базових технологій локальних комп'ютерних мереж з комутацією пакетів є Ethernet. Ця технологія використовує протокол CSMA / CD (множинний доступ з контролем несучої та виявленням колізій), який дозволяє лише один сеанс передачі в логічному сегменті мережі в будь-який момент часу. При одночасній появі двох і більше сеансів передачі виникає колізія, яка фіксується станцією, що ініціює передачу.

Для передачі даних технологія Ethernet може використовувати:

- коаксіальний кабель з діаметром 0,5 дюйма (товстий коаксіал) – стандарт 10Base – 5;
- коаксіальний кабель з діаметром 0,25 дюйма (тонкий коаксіал) – стандарт 10Base – 2;
- неекрановану виту пару (UTP, Unshielded Twisted Pair) – стандарт 10Base-T;
- оптоволоконний кабель – стандарт 10Base-F.

Технологія Ethernet стала основою для кількох високошвидкісних технологій: Fast Ethernet (100 Мбіт/с), Gigabit Ethernet (1000 Мбіт/с), 10 Gigabit Ethernet (10 Гбіт/с). Порівняльна характеристика технологій побудови локальної мережі представлена в таблиці 1.1.

Таблиця 1.1

Порівняльна характеристика технологій побудови локальної мережі

Характеристика	FDDI	Token Ring	Ethernet
Топологія	Подвійне кільце дерев	Зірка, кільце	Загальна шина, зірка
Бітова швидкість	100 Мбіт/с	4, 16 Мбіт/с	10 (100) Мбіт/с
Середовище передачі даних	Оптичне волокно, неекранована вита пара 5 категорії	Екранована та неекранована вита пара, оптичне волокно	Товстий коаксіал, тонкий коаксіал, вита пара, оптичне волокно
Метод доступу	Доля від часу обороту маркера	Пріоритетна Система резервування	CSMA / CD
Максимальна відстань між вузлами	2 км (не більше 11 дБ втрат між вузлами)	100 м	2500 м
Максимальна довжина мережі (без мостів)	200 км (100 км на кільце)	4000 м	2500 м
Максимальна кількість вузлів	500 (1000 з’єднань)	260 – екранована витої пари 72 – неекранована вита пара	1024

Можна зробити такі висновки: технології Token Ring та Ethernet є економічнішими варіантами для підключення клієнтських комп’ютерів і невеликих серверів. Token Ring забезпечує гарантовану затримку передачі даних, чого не може забезпечити Ethernet, де затримка зростає зі збільшенням інтенсивності передачі. Розмір кадру в Token Ring становить 4500 байт, тоді як у Ethernet – 1500 байт, що робить Token Ring ефективнішим у передачі даних. Метод доступу Token Ring, заснований на маркерному підході, є складнішим порівняно з множинним доступом в Ethernet, тому мережеві адаптери для Token Ring коштують дорожче, що призводить до вищих витрат на встановлення мережі Token Ring. Ця технологія здебільшого використовується в технологічних процесах, де пріоритетом є не стільки швидкість, скільки надійність доставки інформації.

Висновки до розділу 1

Отже, у розділі розглянуто основні аспекти створення та функціонування корпоративних мереж, які є невід'ємною частиною сучасних інформаційних систем. Аналіз було проведено за такими ключовими напрямками:

Висвітлено основні функціональні можливості корпоративних мереж, які забезпечують ефективну комунікацію та обмін даними в межах організації. До основних можливостей відносяться підтримка великої кількості користувачів, висока швидкість передачі даних, надійність та безпека мережі. Корпоративні мережі дозволяють централізовано управляти ресурсами, що значно полегшує адміністрування та підтримку системи.

Розглянуто принципи функціонування віртуальних приватних мереж (VPN), які дозволяють забезпечити безпечну передачу даних між віддаленими підрозділами організації через Інтернет. Віртуальні мережі використовуються для шифрування даних та створення захищених каналів зв'язку, що мінімізує ризики несанкціонованого доступу до корпоративної інформації. Описані різні типи VPN (Site-to-Site, Remote Access) та їхні переваги для корпоративного середовища.

Розділ присвячений огляду сучасних технологій, які використовуються для побудови та підтримки корпоративних мереж. Серед них – комутація і маршрутизація, технології бездротових мереж (Wi-Fi), мережеві протоколи (TCP/IP), методи забезпечення якості обслуговування (QoS) та засоби захисту мережі (firewall, IDS/IPS). Зокрема, акцентовано увагу на важливості інтеграції цих технологій для забезпечення надійної та ефективної роботи корпоративної мережі.

У розділі детально проаналізовано ключові аспекти побудови та експлуатації корпоративних мереж. Вивчення основних можливостей, процесу створення інформаційної системи, використання віртуальних мереж передачі даних та сучасних технологій дозволяє розробити комплексний підхід до створення ефективної та безпечної корпоративної мережі. Це, у свою чергу, сприятиме підвищенню продуктивності та конкурентоспроможності організації.

РОЗДІЛ 2
КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ В КОРПОРАТИВНІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ ПОШТОВИХ ВІДДІЛЕНЬ

2.1. Основні принципи захисту інформації при підключенні до мережі Інтернет

Проблема забезпечення інформаційної безпеки є надзвичайно актуальною через наступні фактори:

1. Розвиток технологій інформаційної безпеки: швидкість розвитку цих технологій відстає від темпів росту інформаційних технологій. Це створює прогалину, яку можуть використовувати зловмисники для атак на інформаційні системи.

2. Зростання парка комп'ютерів: швидкість зростання числа комп'ютерів, які використовуються в різних галузях, зробила інформаційні системи ще більш вразливими перед можливими атаками.

3. Розширення кола користувачів: більша кількість людей має безпосередній доступ до обчислювальних ресурсів і масивів даних, що збільшує ризик витоку чутливої інформації.

Забезпечення інформаційної безпеки при підключенні до мережі Інтернет передбачає захист від можливих загроз, які можуть завдати збитку власникові або користувачеві. Ці загрози можуть бути спрямовані на порушення конфіденційності, цілісності або доступності інформації.

При побудові системи захисту необхідно враховувати, що кожен рівень захисту ускладнює використання мережі, обмежує функціональні можливості і вимагає фінансових та обчислювальних ресурсів. Тому, важливо підбирати рівень захисту, який був би пропорційним цінності ресурсу, що захищається [32, с. 613].

Firewall (Брандмауер). Одним з основних та широко визнаних засобів захисту є брандмауер (firewall). Брандмауер встановлюється між корпоративною

мережею та Інтернетом і діє як мережевий фільтр, який контролює та регулює потік даних (рис. 2.1).

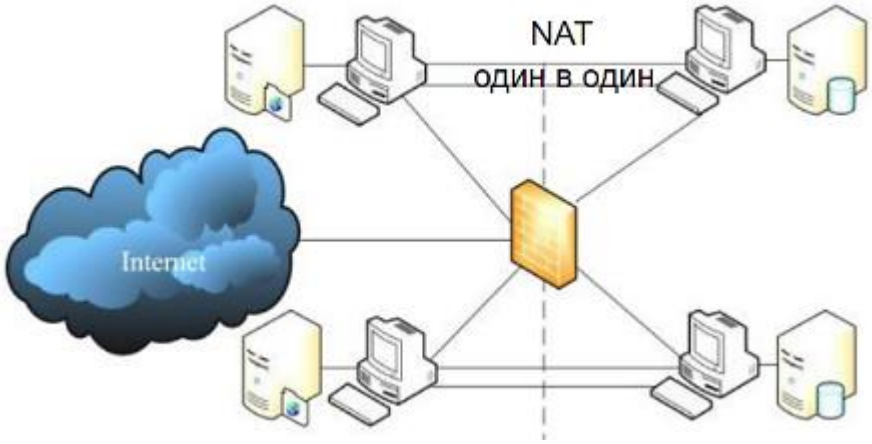


Рисунок – 2.1. Встановлення брандмауера у корпоративній мережі

Він конфігурується для пропуску допустимого трафіку від користувачів мережі до Інтернету і назад, а також обмеження трафіку з Інтернету до мережі, яка потребує захисту, лише на необхідні служби, такі як smtp, dns, ntp. Допустимість трафіку визначається мережним адміністратором відповідно до політики інформаційної безпеки організації. Наприклад, доступ може бути дозволений з деяких комп'ютерів мережі до web та ftp-серверів Інтернету, а також двонаправлений доступ між Інтернетом та поштовим сервером, але заборонені будь-які інші протоколи та напрями трафіку.

Таким чином, міжмережний екран фізично розташовується на місці мережного шлюзу (маршрутизатора) і логічно поєднує їх функції в одному пристрої. Це дозволяє захистити і локальну мережу, і безпосередньо сам шлюз одним засобом. Така можливість передбачена для маршрутизаторів компанії Cisco Systems (Firewall Feature Set). Однак це правило не є обов'язковим, і міжмережний екран може бути реалізований окремим пристроєм.

У простішому виконанні функції міжмережного екрана можна реалізувати за допомогою мережевого фільтру на основі списків доступу (access-lists). Списки доступу визначають правила, за якими дозволяється або забороняється проходження трафіку з певними характеристиками від одного мережного інтерфейсу маршрутизатора до іншого всередині самого маршрутизатора.

Характеристиками можуть бути IP-адреси або діапазон, IP-адреса джерела й приймача, тип протоколу, номер порту призначення або відправлення, та інші параметри IP-пакету.

Розглянемо комплексний підхід до забезпечення інформаційної безпеки корпоративної мережі поштових відділень. До основних способів забезпечення інформаційної безпеки відносяться: законодавчі (правові); морально-етичні; організаційні (адміністративні); технічні; програмні.

Законодавчі заходи захисту визначаються законодавчими актами країни, якими регламентуються правила використання, обробки і передачі інформації обмеженого доступу і встановлюються заходи відповідальності за порушення цих правил.

Організаційні (адміністративні) засоби захисту – це організаційно-технічні і організаційно-правові заходи здійснювані, у процесі створення і експлуатації апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють всі структурні елементи апаратури на всіх етапах їх життєвого циклу (будівництво приміщень, проєктування системи, монтаж і наладка устаткування, випробування і експлуатація).

Організаційні заходи передбачають встановлення правил і процедур, контроль за дотриманням цих правил, регулярне навчання персоналу з питань інформаційної безпеки, а також контроль за доступом до інформації і фізичну безпеку обладнання. Організаційні заходи також включають в себе планування заходів з реагування на інциденти і відновлення після них.

Технічні засоби захисту включають в себе використання шифрування для захисту даних під час їх передачі по мережі, використання брандмауерів для фільтрації трафіку, встановлення антивірусного програмного забезпечення для захисту від шкідливих програм тощо.

Програмні засоби захисту включають в себе використання спеціалізованих програмних продуктів для захисту від шкідливих програм, встановлення програм для моніторингу та аналізу трафіку, а також регулярне оновлення

програмного забезпечення для запобігання використанню вразливостей в програмах.

Комплексний підхід до забезпечення інформаційної безпеки передбачає використання всіх цих способів захисту для забезпечення максимального рівня безпеки корпоративної мережі поштових відділень:

1. Обмеження доступу в приміщення, де відбувається обробка конфіденційної інформації.

2. Допуск до вирішення завдань на комп'ютері з обробки секретної, конфіденційної інформації перевірених посадових осіб, визначення порядку проведення робіт на комп'ютері.

3. Зберігання магнітних носіїв в ретельно захищених шафах.

4. Призначення одного або кількох комп'ютерів для обробки цінної інформації і подальша робота тільки на цих комп'ютерах.

5. Установка дисплея, клавіатури і принтера так, щоб виключити перегляд сторонніми особами змісту оброблюваної інформації.

6. Постійне спостереження за роботою принтера та інших пристроїв виводу на носії цінної інформації; знищення фарбувальних стрічок або інших матеріалів, що містять фрагменти цінної інформації.

7. Заборона ведення переговорів про безпосередній зміст конфіденційної інформації особами, зайнятими її обробкою.

Організаційно-технічні заходи захисту корпоративної мережі поштових відділень включають:

1. Обмеження доступу всередину корпусу комп'ютера шляхом встановлення механічних пристроїв замикання.

2. Знищення всієї інформації на вінчестері комп'ютера при відправці в ремонт з використанням засобів низькорівневого форматування.

3. Організацію живлення комп'ютера від окремого джерела живлення або від загальної (міської) електромережі через стабілізатор напруги (мережевий фільтр) або мотор-генератор.

4. Використання для відображення інформації рідкокристалічних або плазмових дисплеїв, а для друку – струменевих або лазерних принтерів.

5. Розміщення дисплея, системного блоку, клавіатури і принтера на відстані не менше 2,5–3,0 метрів від пристроїв освітлення, кондиціонування повітря, зв’язку (телефону), металевих труб телевізійної і радіоапаратури, а також інших комп’ютерів, що не використовуються для обробки конфіденційної інформації.

6. У час обробки цінної інформації на комп’ютері рекомендується виключати пристрої, що створюють додатковий шумовий фон (кондиціонери вентилятори), а також обробляти іншу інформацію на комп’ютерах, що стоять поряд. Ці пристрої повинні бути розташовані на відстані не менше 2,5–3,0 метрів.

7. Знищення інформації безпосередньо після її використання.

Технічні засоби захисту корпоративної мережі поштових відділень реалізуються у вигляді механічних, електричних, електромеханічних і електронних пристроїв, призначених для перешкоди на можливих шляхах проникнення і доступу потенційного порушника до компонентів захисту. Програмні засоби представляють собою програмне забезпечення, що спеціально призначене для виконання функцій захисту інформації. Програмні засоби представляють собою програмне забезпечення, що спеціально призначене для виконання функцій захисту інформації. Програмні засоби складають основу механізмів захисту на першій фазі розвитку технології забезпечення безпеки зв’язку в каналах телекомунікацій.

2.2 NAT-Перетворення

На даному етапі захисту корпоративної мережі поштових відділень використання технології трансляції мережних адрес (Network Address Translation – NAT) відіграє важливу роль у забезпеченні безпеки. NAT дозволяє заховати діапазон внутрішніх IP-адрес від зовнішніх мереж і виконує цю функцію, транслюючи тільки той трафік, який має бути переданий між внутрішньою і

зовнішньою мережею. Варто зазначити, що NAT не фільтрує трафік, тому для блокування небажаних пакетів потрібно використовувати додаткові заходи, наприклад, списки доступу [44, с. 175].

На сьогоднішній день існують різні методи реалізації NAT:

- Статичний NAT: відображає конкретну внутрішню IP-адресу на конкретну зовнішню IP-адресу. Часто використовується, коли потрібно забезпечити доступ до вузла внутрішньої мережі з зовнішніх мереж за допомогою конкретних протоколів на рівні застосунків.
- Динамічний NAT: відображає адресу з блоку внутрішніх IP-адрес на одну з вільних адрес зовнішніх адрес. Цей метод рідко використовується через потребу у кількох зовнішніх IP-адресах та обмеженою масштабованістю.
- Перевантаження (Overload): форма динамічного NAT, яка відображає адресу з блоку внутрішніх IP-адрес на єдину зовнішню IP-адресу, використовуючи різні порти. Цей метод є найпоширенішим для підключення внутрішніх вузлів корпоративної мережі поштових відділень до Інтернету.
- Списки контролю доступу (ACL): містять набір правил, що визначають дію над пакетами та їх параметри для фільтрації (адреси відправників та отримувачів, номера портів протоколів на рівні транспортного рівня тощо).

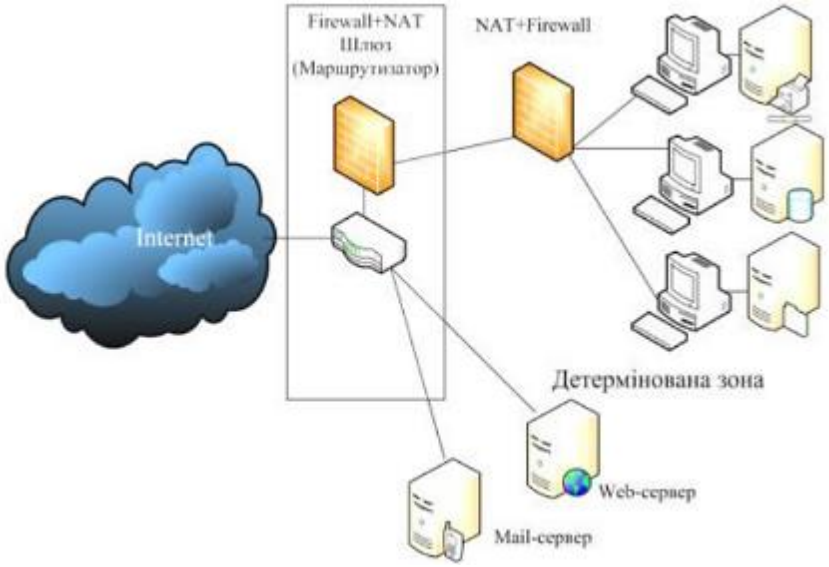


Рисунок – 2.2. Трансляція фіксованої внутрішньої адреси у фіксовану зовнішню мережу

Перевірка пакетів відбувається в порядку, вказаному в списку правил. Коли пакет надходить на інтерфейс, він перш за все перевіряється за першим правилом. Якщо параметри пакета відповідають першому правилу, подальша перевірка припиняється, і пакет або передається далі, або відкидається. Якщо параметри пакета не відповідають першому правилу, вони перевіряються за наступним правилом і так далі, поки не будуть перевірені всі правила (якщо пакет не відповідає вимогам жодного з правил вище). Якщо параметри пакета не відповідають жодному правилу списку, пакет просто відкидається (на кінці кожного списку є неявне правило, яке забороняє проходження всіх пакетів).

ACL можуть бути застосовані до різних об’єктів:

- фізичних або логічних інтерфейсів (включаючи інтерфейси VLAN-комутаторів 3-го рівня);
- термінальних ліній для обмеження доступу до пристрою по протоколам Telnet або SSH;
- VPN-тунелів (для шифрування пакетів);
- механізмів QoS (встановлення пріоритетів для різних типів трафіку);
- шейперів для обмеження швидкості трафіку користувачів;
- протоколу NAT (визначення адрес, які потрібно транслювати).

За допомогою списків доступу також розв’язується проблема захисту від атак, що спрямовані на зміну маршруту пакетів, наприклад, атаки на основі ICMP-повідомлення «Redirect». Такі атаки можуть призвести до розриву зв’язку вузла з мережею.

Другий вид NAT – трансляція групи внутрішніх адрес в одну зовнішню. Це дозволяє всім внутрішнім комп’ютерам працювати з Інтернетом одночасно, а маршрутизатор розрізняє, кому яка відповідь перетрансльовується за службовими даними TCP-з’єднання. Для зовнішньої мережі створюється враження, що до неї звертається лише один комп’ютер. Така трансляція

ускладнює життя зловмисникам, оскільки приховує внутрішні комп’ютери і перешкоджає визначенню їх адреси [46, с. 117].

Це також унеможливлює можливість встановлення ініціативного з’єднання з зовнішньої мережі до внутрішнього комп’ютера, оскільки для маршрутизатора не існує правила, яке б прив’язувало зовнішню адресу до внутрішньої. Це виключає можливість сканування внутрішньої мережі ззовні.

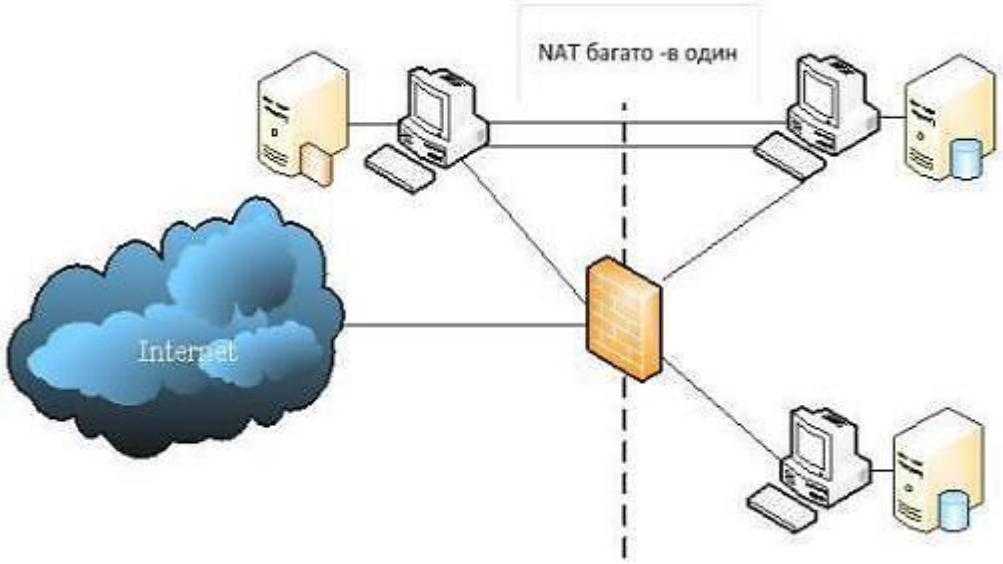


Рисунок – 2.3. Трансляція групи внутрішніх адрес в одну зовнішню

Третя форма NAT полягає в тому, що внутрішні адреси замінюються на будь-яку вільну адресу з пулу. Коли внутрішні комп’ютери виходять в Інтернет, вони отримують вільну адресу з динамічної бази даних. Кожне нове TCP-з’єднання може встановлюватись з іншою IP-адресою. Це також ускладнює завдання потенційному зловмиснику, оскільки він не може атакувати конкретний внутрішній комп’ютер. Те ж саме стосується і другої форми NAT. Якщо запит приходить ззовні, маршрутизатор не може встановити відповідність між адресою з бази даних і адресою внутрішньої мережі, тому такий запит буде невдалим [39, с. 48].

2.3 Демілітаризована зона

Зазвичай організаціям необхідно мати деякі мережні ресурси, до яких можна отримати доступ з Інтернету. Це, зазвичай, поштові, DNS та веб-сервери.

Оскільки їх робота передбачає вільний або обмежений доступ з мережі Інтернет, ймовірність їх компрометації вища, ніж у інших комп'ютерів мережі. Тому не доцільно розміщувати їх у зоні, яка захищається, оскільки вони можуть стати воротами для атак на внутрішні комп'ютери [40, с. 245]. Для зниження ризику та забезпечення функціональності такі сервери розміщують поза основним шлюзом мережі, але перед мережевим екраном, що захищає внутрішні комп'ютери. Цю область називають демілітаризованою зоною (рис. 2.4).

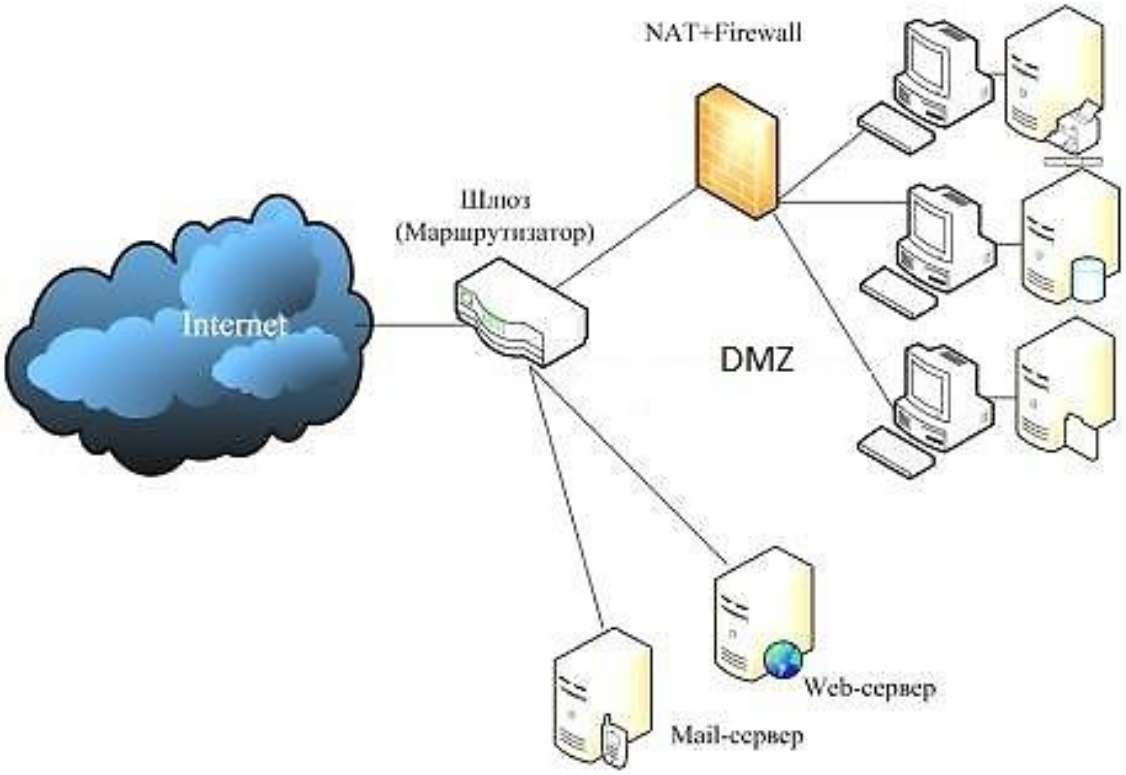


Рисунок – 2.4. Демілітаризована зона

З рисунку 2.4 видно, що можливо встановити другий мережевий екран (Firewall) на основному шлюзі корпоративної мережі поштових відділень. Це логічне рішення, яке дозволяє одночасно підвищити рівень захисту внутрішньої мережі і захистити сервери демілітаризованої зони. При належному налаштуванні обох мережевих екранів, користувачу, який намагається завдати шкоду корпоративній мережі, стане значно складніше проникнути у внутрішню мережу організації.

Проте, наявність другого мережевого екрана ускладнює конфігурацію мережевого обладнання та налаштування роботи всіх елементів мережі. Для додаткового підвищення захисту можна використовувати мережеві екрани різних виробників. Таким чином, якщо один з них має вразливість, інший не дозволить користувачу, що намагається завдати шкоду корпоративній мережі, безперешкодно проникнути у мережу, як це могло б статися при використанні мережевих екранів одного типу [42, с. 43].

Особливо важливо враховувати, що можливість мережного доступу до шлюзів і мережевих екранів повинна бути відключена, щоб запобігти можливому зловживанню. З точки зору безпеки, пристрої, які захищають мережу, повинні бути налаштовані та адмініструватися лише через консольний порт локально (рис. 2.5).

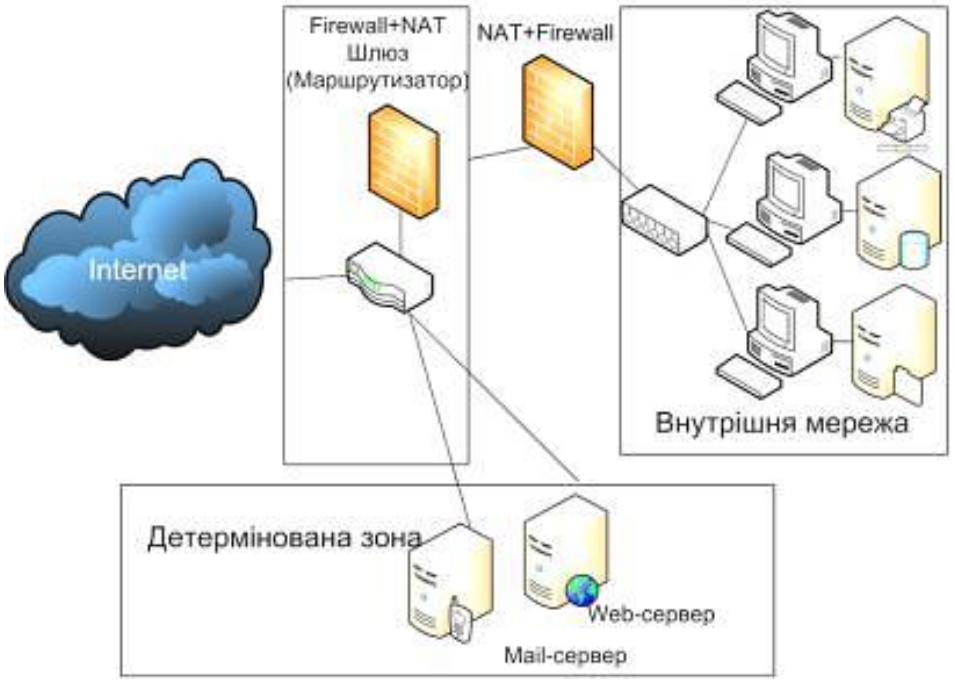


Рисунок – 2.5. Локально-консольний порт для серверів

Схема, запропонована на рис. 2.4, може бути дещо вдосконалена. Для цього необхідно використати граничний маршрутизатор із двома Ethernet-портами.

2.4 Антивірусний захист корпоративної мережі

На сьогодні відомі десятки тисяч різних комп'ютерних вірусів. Незважаючи на такий достаток, число типів вірусів, що відрізняються один від одного механізмом поширення і принципом дії, досить обмежено. Існують і комбіновані 241 віруси, які можна віднести одночасно до декількох типів [43, с. 268].

Рисунок – 2.6. Класифікація комп'ютерних вірусів за місцем існування

Мережеві віруси використовують для свого поширення протоколи або команди комп'ютерних мереж і електронної пошти. Іноді мережеві віруси називають програмами типу «черв'як». Мережеві черв'яки підрозділяються на Internet-черви (поширюються по Internet), LAN-черви (поширюються по локальній мережі), IRC-черви Internet Relay Chat (поширюються через чати). Існують також змішані типи, які поєднують в собі відразу кілька технологій.

Проблема антивірусного захисту – одна з пріоритетних проблем безпеки корпоративних інформаційних ресурсів організації. Її актуальність пояснюється:

– лавиноподібним зростанням числа комп'ютерних вірусів;
– незадовільним станом антивірусного захисту в існуючих корпоративних комп'ютерних мережах.

Сьогодні корпоративні мережі постійно розвиваються, але разом з цим збільшується число шляхів для вірусів проникнути в них через Інтернет.

Антивірусні програми завжди були основною зброєю у боротьбі з цим явищем. Вони виявляють віруси, що використовують різні методи маскування, і допомагають у їх видаленні. Існують різні види антивірусних програм, включаючи вакцини, детектори, ревізори, охоронці, монітори, поліфаги і евристичні аналізатори. Останнім часом розробники антивірусного програмного забезпечення пропонують комплексні рішення для антивірусного захисту, що охоплюють різні аспекти захисту. [38, с. 28].

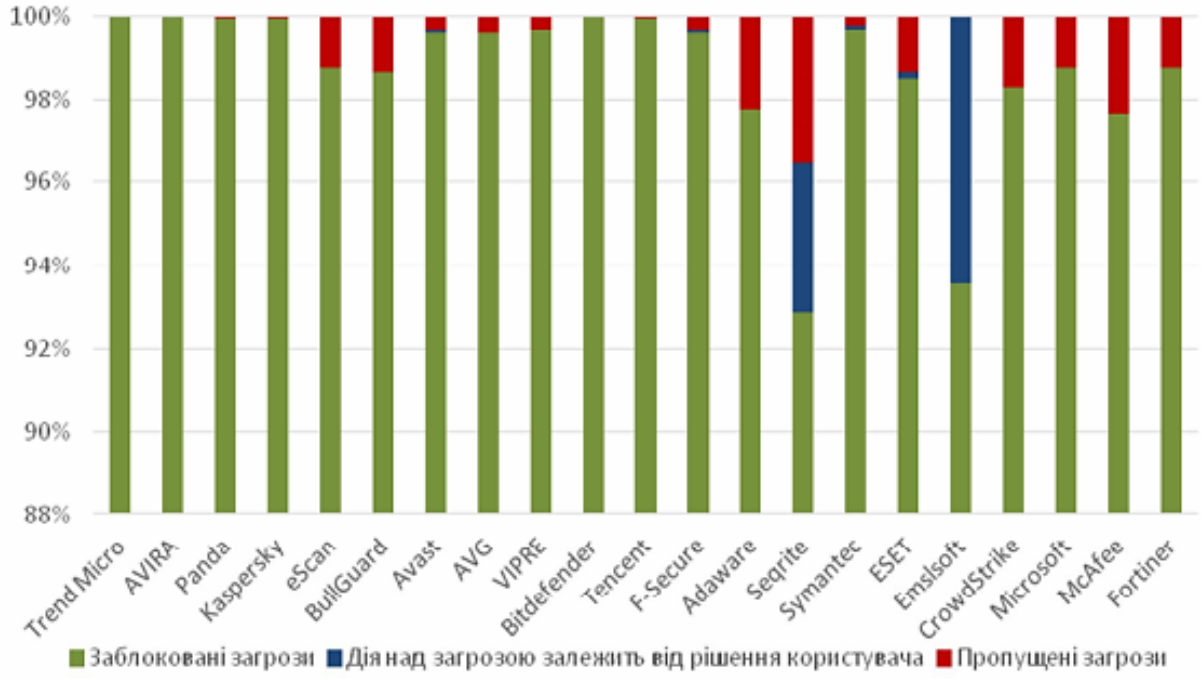


Рисунок – 2.7. Тест антивірусних засобів на захист від шкідливих програм

Як правило, такими точками є: шлюзи і сервери Інтернету, сервери файлових додатків, сервери групової роботи і електронної пошти, робочі станції. Для невеликих підприємств, які мають до 10 вузлів, оптимальними можуть бути антивірусні рішення зручним графічним інтерфейсом і можливістю локальної конфігурації без потреби централізованого управління. Для великих підприємств більш прийнятним може бути застосування системи антивірусного захисту з декількома консолями і менеджерами управління, які пов’язані з єдиним центром управління. Такі рішення дозволяють забезпечити ефективне централізоване управління локальними антивірусними клієнтами і можуть бути

інтегровані з іншими рішеннями в галузі безпеки корпоративних мереж, якщо це необхідно [35, с. 117].

На сьогоднішній день більшість заходів у сфері комп'ютерної безпеки корпоративних мереж реалізуються як комплекс декількох технологій. У класичних антивірусах сигнатурне виявлення часто поєднується з моніторингом системних подій та емуляцією. Важливо зауважити, що немає універсального або найкращого рішення. Кожна технологія має свої переваги і недоліки. Наприклад, моніторинг подій постійно вимагає процесорних ресурсів, але його важко обійти; емуляцію можна обманути за допомогою певних команд у коді, але вона виявляє шкідливий код в попереджувальному режимі, залишаючи систему захищеною.

Вибір технології – це пошук балансу з урахуванням конкретних потреб і обставин. Існує безліч методик виявлення невідомих шкідливих програм. Кожна з них має свої переваги, недоліки та особливості. Проте наразі немає методики, яка б повністю вирішувала проблему виявлення невідомих шкідливих програм з прийнятною ефективністю для всіх видів шкідливих програм і всіх вимог до системи виявлення. Теоретично комбінація кількох методик може вирішити цю проблему.

2.5 Захист інформації за допомогою міжмережних екранів

Серед засобів забезпечення інформаційної безпеки в корпоративних мережах особливе місце займають міжмережеві екрани (ММЕ), інструменти аналізу захищеності та системи виявлення атак [34, с. 358].

Міжмережевий екран (МЕ), також відомий як брандмауер або firewall, – це спеціалізований комплекс для мережевого захисту. МЕ розділяє загальну мережу на дві або більше частини, застосовуючи набір правил, що визначають умови проходження пакетів даних між цими частинами. Зазвичай цей поділ здійснюється між корпоративною (локальною) мережею підприємства та глобальною мережею Інтернет. МЕ переважно захищають внутрішню мережу

підприємства від загроз з Інтернету, але також можуть бути використані для захисту від атак всередині корпоративної інтрамережі. МЕ є однією з перших технологій захисту корпоративних мереж від зовнішніх загроз.

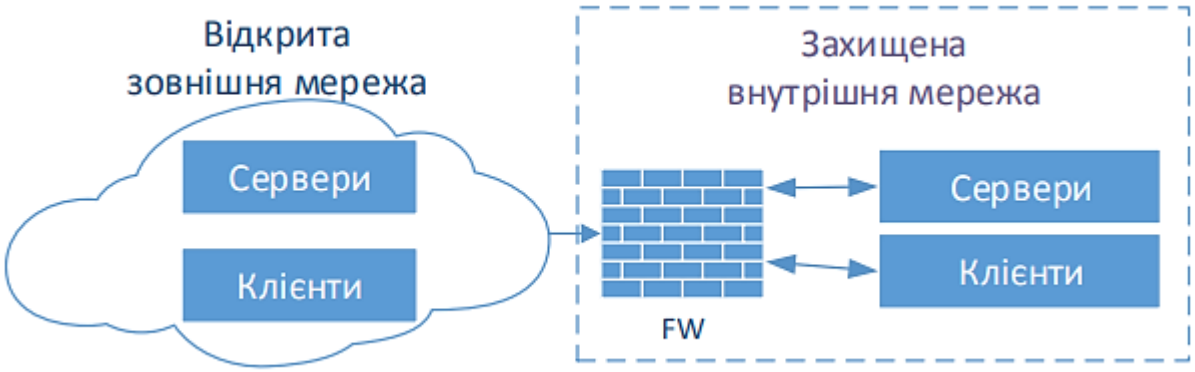


Рисунок – 2.8. Схема підключення міжмережевого екрану

Міжмережеві екрани (брандмауери, firewall) застосовують набір правил, які регулюють умови проходження пакетів даних з однієї частини розподіленої корпоративної мережі поштових відділень (відкритої) до іншої (захищеної). В залежності від рівня взаємодії мережевих об’єктів, основними видами ММЕ є фільтруючі маршрутизатори, а також шлюзи сеансового і прикладного рівнів. Фільтруючі маршрутизатори, що працюють на мережевому рівні еталонної моделі, виконують функцію фільтрації пакетів даних, які входять у захищену частину мережі або виходять з неї. Правила фільтрації визначають, чи буде дозволено або заблоковано проходження пакета через ММЕ на основі заданих параметрів.

Рисунок – 2.9. Структура міжмережевого екрану

Основними перевагами фільтруючих маршрутизаторів є простота їх створення, установки і налаштування; прозорість для користувацьких додатків у корпоративній мережі та мінімальний вплив на їх продуктивність; невисока вартість. Однак, ці пристрої мають такі недоліки [26, с. 180]:

1. Відсутність автентифікації на рівні користувачів мережі; вразливість до підміни IP-адреси у заголовку пакета;
2. Незахищеність від загроз порушення конфіденційності та цілісності переданої інформації;
3. Висока залежність ефективності набору правил фільтрації від рівня знань адміністратора ММЕ конкретних протоколів;
4. Відкритість IP-адрес комп’ютерів захищеної частини мережі.

Шлюзи сеансового рівня призначені для контролю віртуального з’єднання між робочою станцією захищеної частини мережі та хостом незахищеної частини, а також для трансляції IP-адрес комп’ютерів захищеної частини корпоративної мережі поштових відділень.

У процесі трансляції IP-адрес, виконуваного шлюзом сеансового рівня, відбувається перетворення їх в одну IP-адресу, асоційовану з ММЕ. Це усуває пряму взаємодію між хостами захищеної і відкритої мереж, що не дозволяє зловмиснику здійснити атаку шляхом підміни IP-адрес.

Перевагами шлюзів сеансового рівня є простота і надійність їх програмної реалізації. Недоліком є відсутність можливості перевіряти вміст переданої інформації, що дозволяє зловмиснику спробувати передати пакети зі шкідливим кодом і звернутися безпосередньо до одного з серверів корпоративної мережі поштових відділень [28, с. 75].

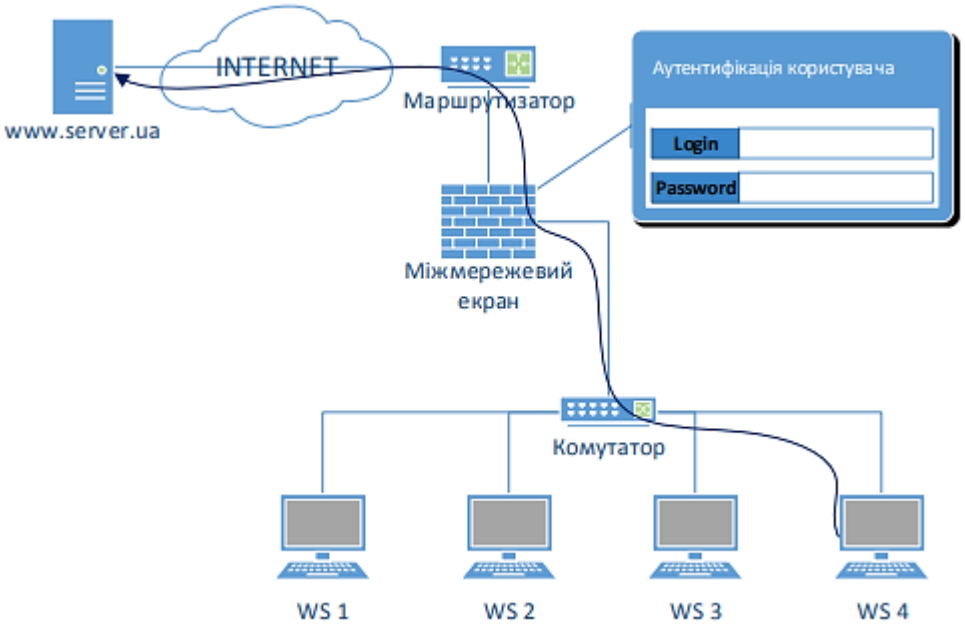


Рисунок – 2.10. Схема аутентифікації користувача по паролю

Шлюзи прикладного рівня не лише виключають пряму взаємодію між користувачами захищеної мережі та хостами відкритої частини, але й фільтрують усі вхідні та вихідні дані на прикладному рівні, аналізуючи зміст переданої інформації.

Основні функції шлюзів прикладного рівня:

1. Ідентифікація та автентифікація користувачів корпоративної мережі поштових відділень під час спроб встановлення з’єднань;
2. Перевірка цілісності переданих даних; контроль доступу до ресурсів захищеної та відкритої частин мережі; фільтрація та перетворення повідомлень (виявлення шкідливого коду, шифрування та розшифрування);
3. Реєстрація подій у спеціальному журналі; кешування зовнішніх запитів до внутрішніх даних для підвищення продуктивності мережі.

Переваги шлюзів прикладного рівня:

1. Приховування структури захищеної частини мережі від інших хостів [29, с. 67];
2. Надійна автентифікація та реєстрація проходження повідомлень;

3. Спрощені правила фільтрації пакетів на мережному рівні, де маршрутизатор пропускає лише трафік до шлюзу прикладного рівня, блокуючи інший;
4. Можливість реалізації додаткових перевірок.

Основні недоліки шлюзів прикладного рівня:

1. Вища вартість, складність розробки, установки та налаштування;
2. Зниження продуктивності корпоративної мережі поштових відділень, «непрозорість» для додатків користувачів мережі.

Міжмережеві екрани є основою для створення віртуальних приватних мереж (VPN), які приховують топологію внутрішніх мереж організацій, що обмінюються інформацією через Інтернет, і захищають трафік між ними, використовуючи спеціальні системи маршрутизації.

Загальний недолік будь-якого типу міжмережевих екранів полягає в тому, що вони не можуть запобігти багатьом видам атак, таким як несанкціонований доступ до інформації через підроблений DNS-сервер, аналіз мережевого трафіку, атаки відмови в обслуговуванні. Порушнику може бути навіть простіше здійснити атаку на корпоративну мережу, яка використовує MME, адже для цього достатньо атакувати хост з MME, що фактично відключить від зовнішньої мережі всі комп’ютери захищеної частини мережі [21, с. 44].

2.6 Можливості адресного перетворення (PAT)

Порт адресного перетворення (PAT), також відомий як NAT overload або маскування адрес, є одним з методів мережевого трансляції мережних адрес. PAT є розширенням технології мережевої адресації (NAT), яка дозволяє приватним мережам з внутрішніми IP-адресами отримувати доступ до Інтернету через одну або кілька публічних IP-адрес.

PAT використовується для маскування внутрішніх IP-адрес з приватних мереж (наприклад, з діапазону IP-адрес 10.0.0.0 / 8, 172.16.0.0 / 12 або 192.168.0.0 / 16) і надання доступу до Інтернету для всіх пристроїв в цих мережах через одну

або кілька публічних IP-адрес. Це досягається шляхом переписування інформації про порт та IP-адресу пакетів, що проходять через мережевий пристрій, який виконує PAT.

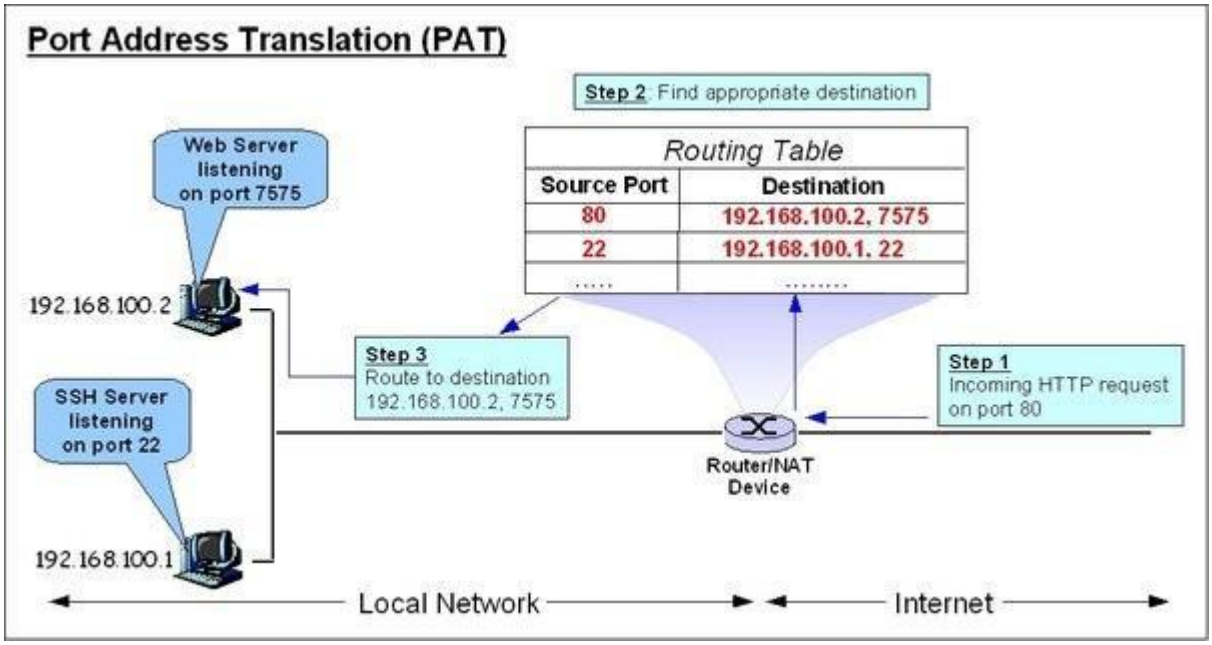


Рисунок – 2.11. Функціональність PAT

Основні переваги використання PAT включають:

1. Економія публічних IP-адрес: Завдяки PAT можна використовувати одну або кілька публічних IP-адрес для доступу до Інтернету для багатьох пристроїв в приватній мережі. Це економить кількість доступних публічних IP-адрес і дозволяє більш ефективно використовувати їх.

2. Захист приватної мережі: При використанні PAT внутрішні IP-адреси пристроїв в приватній мережі не відкриті для прямого доступу з Інтернету. Зовнішні пристрої бачать лише публічну IP-адресу маршрутизатора або мережевого пристрою, що виконує PAT. Це забезпечує певний рівень безпеки для внутрішніх пристроїв, ховаючи їхні IP-адреси від зовнішніх загроз.

3. Доступ до Інтернету для багатьох пристроїв: PAT дозволяє багатьом пристроям в приватній мережі одночасно використовувати Інтернет через одну або кілька публічних IP-адрес. Він використовує унікальні порти для ідентифікації пристроїв, що забезпечує правильну доставку пакетів з Інтернету до відповідних пристроїв в приватній мережі.

Використання PAT може бути особливо корисним для невеликих офісів або домашніх мереж, де кількість публічних IP-адрес обмежена або дорога. Він дозволяє об’єднувати декілька пристроїв в одну публічну IP-адресу, забезпечуючи їм доступ до Інтернету [21].

Cisco – це серія мережевих пристроїв, що використовуються для створення локальних корпоративних мереж та надання доступу до Інтернету. Деякі моделі пристроїв Cisco підтримують функцію порт адресного перетворення (PAT) для ефективного маскування адрес у внутрішніх мережах.

За допомогою функції PAT на обладнанні Cisco можна налаштувати перетворення IP-адрес та портів, що дозволяє використовувати одну або кілька публічних IP-адрес для доступу до Інтернету для всіх пристроїв у приватній мережі. Основна ідея полягає в тому, що пристрої з приватними IP-адресами в мережі Cisco використовують одну публічну IP-адресу під час взаємодії з Інтернетом.

Існує кілька кроків для налаштування PAT на пристроях Cisco:

1. Встановлення публічної IP-адреси: Почніть з призначення публічної IP-адреси, яку ви будете використовувати для доступу до Інтернету. Цю інформацію вам надасть ваш Інтернет-провайдер.

2. Встановлення внутрішньої мережі: Налаштуйте внутрішню мережу на пристрої Cisco, використовуючи приватні IP-адреси. Ви можете налаштувати статичну IP-адресу для кожного підключеного пристрою або використовувати DHCP для автоматичного призначення IP-адрес.

3. Налаштування правил порт переадресації: Встановіть правила переадресації портів (port forwarding), які пересилають вхідний трафік з публічної IP-адреси до конкретного пристрою або служби у внутрішній мережі. Це дозволить зовнішнім пристроям отримувати доступ до внутрішніх ресурсів.

4. Активація PAT: Включіть функцію порт адресного перетворення (PAT) на пристрої Cisco та налаштуйте правила перетворення IP-адрес та портів. Це

забезпечить правильну маршрутизацію пакетів і забезпечить доступ до Інтернету для всіх підключених пристроїв.

Точність процесу налаштування PAT на пристроях Cisco може змінюватися в залежності від моделі та версії програмного забезпечення пристрою. Рекомендується використовувати документацію та ресурси, надані виробником, для отримання детальнішої інформації про налаштування PAT на конкретній моделі Cisco [21].

2.7 Засоби функціоналу ACL

Функція Access Control List (ACL) (Список керування доступом) є важливим елементом налаштування безпеки в локальних корпоративних мережах. ACL використовується для контролю доступу до ресурсів мережі, таких як пристрої, служби або сегменти мережі, шляхом встановлення правил для фільтрації трафіку.

ACL може бути налаштований на різних мережевих пристроях, включаючи комутатори, маршрутизатори або файєрволи. Він працює на рівні мережевого рівня (рівень 3 моделі OSI) та здатен контролювати трафік на основі різних параметрів, таких як IP-адреси джерела та призначення, номери портів, протоколи і т. д [21].

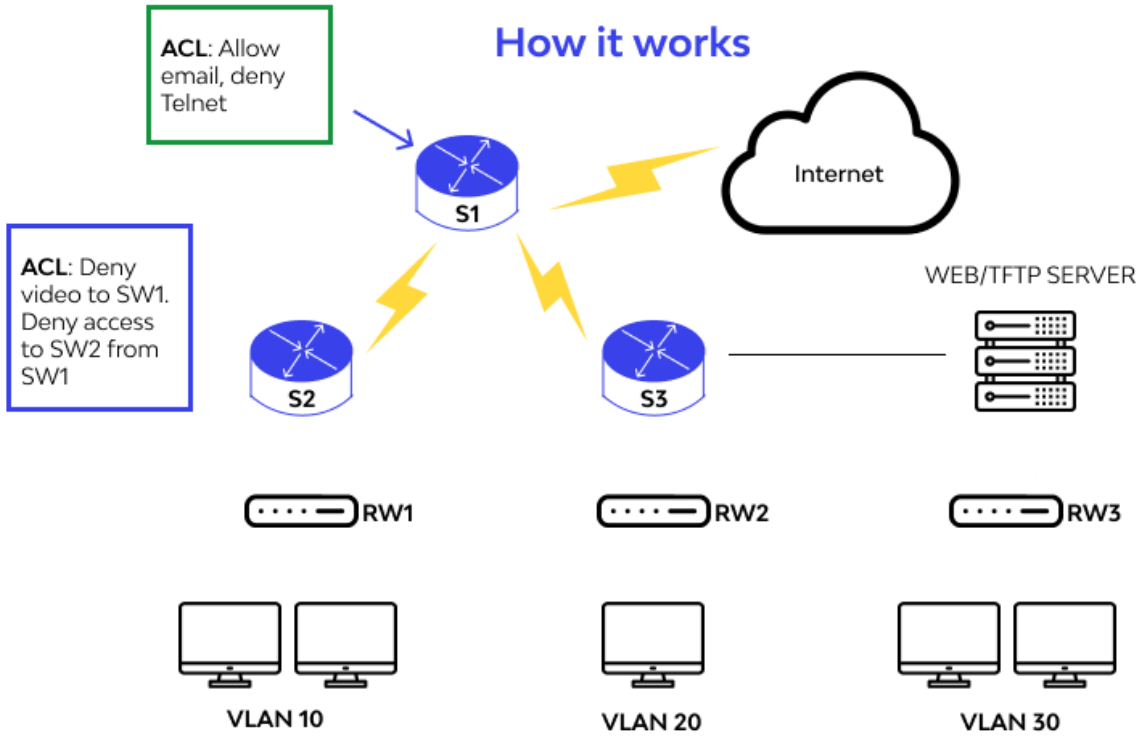


Рисунок – 2.12. Функціонал ACL

Основні аспекти функції ACL включають:

1. Фільтрація трафіку: ACL дозволяє встановлювати правила, які визначають, який тип трафіку може проходити через мережевий пристрій, а який повинен бути відхилений. Наприклад, ви можете налаштувати ACL, щоб дозволити лише певні IP-адреси або діапазони IP-адресів отримувати доступ до певних ресурсів мережі, а забороняти решту.

2. Керування безпекою: ACL використовується для забезпечення безпеки мережі шляхом контролю доступу до різних ресурсів. Ви можете налаштувати ACL для блокування небажаних або потенційно шкідливих підключень до мережі, запобігаючи атакам, шпигунству або несанкціонованому доступу.

3. Керування політикою: ACL дозволяє встановлювати політику доступу до мережі відповідно до вимог організації. Ви можете налаштувати ACL, щоб обмежити доступ до конкретних ресурсів або служб, встановити рівні пріоритету для різних типів трафіку або виконувати інші політики безпеки.

4. Маршрутизація: ACL може використовуватися для керування маршрутизацією трафіку в мережі. Ви можете налаштувати ACL, щоб вказати,

які маршрути повинні бути використані для певних типів трафіку або які маршрути повинні бути виключені.

5. Контроль бандвітду: ACL може бути використаний для керування пропускною здатністю мережі шляхом обмеження або пріоритезації певних типів трафіку. Наприклад, ви можете налаштувати ACL для обмеження шириною смуги для певних пристроїв або додатків, щоб забезпечити рівномірний розподіл ресурсів мережі.

Настройка ACL може варіюватися в залежності від типу обладнання та виробника. Рекомендується детально ознайомитися з документацією вашого пристрою Cisco або звернутися до підтримки виробника для отримання конкретної інформації про налаштування ACL на вашому пристрої.

ACL є потужним інструментом для керування доступом та забезпечення безпеки в корпоративних мережах. Правильне використання ACL допомагає контролювати трафік та забезпечувати безпеку вашої мережі.

Висновки до розділу 2

Отже, у цьому розділі розглянуто комплексні системи захисту інформації в корпоративній комп'ютерній мережі поштових відділень. Особливу увагу приділено різним методам та технологіям забезпечення безпеки даних. Нами проаналізовано основні принципи захисту інформації при підключенні до мережі Інтернет. Підкреслено важливість застосування багаторівневих методів захисту, що включають використання шифрування, автентифікації, контроль доступу та моніторинг мережевої активності. Акцент зроблено на необхідності постійного оновлення безпекових систем для протидії новим загрозам.

Проведено аналіз механізму Network Address Translation (NAT), який використовується для зміни IP-адрес при передачі даних через Інтернет. Описано переваги використання NAT для приховування внутрішніх адрес від зовнішніх користувачів та забезпечення додаткового рівня безпеки.

Розглянуто концепцію демілітаризованої зони (DMZ), яка створює ізольовану мережеву зону між внутрішньою корпоративною мережею та Інтернетом. DMZ використовується для розміщення серверів, що повинні бути доступними з Інтернету, але ізольовані від основної мережі, щоб запобігти можливим атакам.

Проаналізовано питання забезпечення антивірусного захисту в корпоративній мережі. Розглянуто різні типи антивірусних програм, їх принципи роботи та методи виявлення шкідливого ПЗ. Описано важливість регулярного оновлення антивірусних баз даних та впровадження багаторівневого захисту для максимального зниження ризиків зараження.

Розглянуто міжмережеві екрани (firewalls) як одного з основних інструментів захисту корпоративної мережі. Описано різні типи міжмережних екранів, їх функції та конфігурації. Акцент зроблено на важливості налаштування політик доступу для забезпечення захисту від несанкціонованих доступів.

Розглянуто механізм Port Address Translation (PAT), який дозволяє кільком пристроям у внутрішній мережі використовувати одну зовнішню IP-адресу для зв'язку з Інтернетом. Описано переваги PAT для ефективного використання IP-адрес та забезпечення додаткового рівня захисту.

Проаналізовано засоби Access Control Lists (ACL), які використовуються для контролю доступу до мережевих ресурсів. Описано принципи створення та налаштування ACL, а також їх важливість для забезпечення безпеки корпоративної мережі.

У розділі детально проаналізовано різні методи та технології захисту інформації в корпоративній комп'ютерній мережі поштових відділень. Застосування комплексних підходів до захисту, включаючи NAT, DMZ, антивірусний захист, міжмережні екрани, PAT та ACL, дозволяє забезпечити високий рівень безпеки та захисту даних в корпоративній мережі. Це є важливим

аспектом для забезпечення надійної та безперебійної роботи поштових відділень та захисту конфіденційної інформації.

РОЗДІЛ 3
ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПОШТОВИХ ВІДДІЛЕНЬ З ПРОГРАМНИМ ЗАСОБОМ ЗАХИСТУ ТРАНСПОРТУВАННЯ ДАНИХ НА БАЗІ ОБЛАДНАННЯ CISCO

3.1 Вибір серверного обладнання для роботи програмного засобу

Так як в корпоративній мережі використовується один сервер, необхідно підібрати продуктивне, сучасне обладнання яке забезпечить режим багатозадачності для роботи проєктованого програмного засобу [5, с. 61].

Таблиця 3.1

Технічні характеристики сервера для корпоративної мережі

Найменування	Комплектуючі	Характеристики/модель
Сервер ProLiant ML150G9 834607–421	Центральний процесор	Intel Xeon E5–2609v4
	Оперативна пам'ять	8 Т6 / DDR4 / 2400 МГц
	Підтримка RAID	0 / 1 / 10 / 5
	Блок живлення	1х550 Вт
	HDD	2х2 ТБ

Мобільна робоча станція в проєктуємій корпоративній мережі – ноутбук, призначений для керівника часто перебувають у відрядженнях або на ділових зустрічах.

Таблиця 3.2

Технічна характеристика ноутбуку для корпоративної мережі

Найменування	Комплектуючі	Характеристики/модель
Ноутбук HP Pavilion x360 13-u002ur	Центральний процесор	Core I5–6200U
	Оперативна пам'ять	4 г6 / DDR4 / 2133 МГц
	HDD	SSD 256 ГБ
	Дисплей	13,3

Таблиця 3.3

Технічні характеристики стаціонарного комп'ютера

Найменування	Комплектуючі	Характеристики/модель
Комп'ютер HP ProDesk 400 G2 K8K74EA	Центральний процесор	Intel Core I3 7100
	Оперативна пам'ять	4 г6 / DDR4 / 2133 МГц
	HDD	SATA 500 ГБ
	Відеосистема	Intel HD Graphics

Стаціонарна робоча станція в проєктованій корпоративній мережі - комп’ютер, призначений для рядових співробітників, розташовані практично у всіх кабінетах офісу.

3.2 Вибір комутаційного обладнання для створення програмного засобу в інфраструктурі корпоративної мережі

Для офісу був обраний роутер Інтернет-центр Cisco C819GW II. Він служить перш за все для підключення Інтернету, мережі провайдера і його сервісів. Вбудований міжмережевий екран Інтернет-центру захищає всі пристрої мережі від атак з Інтернету та має можливості налаштування функцій ACL та протоколів NAT і PAT.

Крім того, Cisco C819GW II обладнаний багатофункціональним 2-портовим хостом USB, завдяки якому можна організувати постійне підключення до Інтернету через USB-модем оператора мобільного зв’язку 3g / 4g, відкрити мережевий доступ до USB-накопичувача по FTP з Інтернету або з домашньої мережі по DLNA, а також забезпечити загальний доступ до USB-принтера з декількох мережевих пристроїв. Інтернет-центр Cisco C819GW II призначений для доступу в Інтернет по виділеній лінії Ethernet через провайдерів, що використовують будь-які типи підключення: VPN (PPTP і L2TP), PPPoE, 802.1 X, VLAN 802.1 Q, IPv4 / IPv6. Фірмова технологія ZyXEL Link Duo дозволяє комп’ютерам домашньої мережі отримати одночасно доступ і в Інтернет, і до локальних сервісів провайдера по одній виділеній лінії [7, с. 118].

Інтернет-центр дозволяє організувати високошвидкісну бездротову мережу для спільної роботи в Інтернеті і робочої мережі з ноутбуків, смартфонів і інших пристроїв Wi-Fi стандарту IEEE 802.11 n. Дві антени з коефіцієнтом посилення 5 дбі забезпечують широку зону покриття мережі Wi-Fi і висока бездротового зв’язку на швидкості до 300 Мбіт/с. Для гостьових пристроїв

можна включити окрему мережу Wi-Fi, призначену для виходу в Інтернет без доступу до інформації в мережі.

Для філій і сервісного центру обрані Інтернет центри Cisco C819GW та C881G. Ці пристрої мають ті ж самі функції, що і Cisco C819GW II, але володіють меншим радіусом дії Wi-Fi. На роботу філій це не позначиться, оскільки площа приміщень по перевищує 20 м, проте дозволить скоротити витрати на покупку мережевого та Інтернет обладнання.

Контролер в корпоративній мережі працює на всіх нових моделях Cisco (з індексом C-XXXX) від початку до ультра і на пристроях попереднього покоління, для яких доступний реліз Cisco IOS 2.0 (C819GW III, C2911R II). Для роботи не потрібно підключення Інтернету і хмарних сервісів.

Ретранслятором в корпоративній мережі може виступати будь-яка з нових моделей Cisco (з індексом C-XXXX) від початку до ультра, а також деякі моделі попереднього покоління, для яких доступний офіційний реліз CiscoOS 2.0 і вище (C819GW III, C2911R II).

Cisco C2911R. Апаратна конфігурація роутера частково збігається з Cisco C819GW: процесор MediaTek MT7621AT (два ядра MIPS1004Kc, 880 МГц, вбудовані контролери USB і гігабітний мережевий комутатор), 256 МБ оперативної пам’яті DDR3, 128 МБ Флеш-пам’яті NAND. Але є і важлива (втім, і єдина) відмінність – замість одного радіо MediaTek MT7615DN, обслуговуючого і діапазон 2,4 ГГц і діапазон 5 ГГц в режимі 2T2R кожен, тут встановлені дві мікросхеми MT7615N, так що обидва діапазони отримали схему 4T4R.

Рисунок – 3.1. Зовнішній вигляд Cisco C2911R

1. Антени бездротової мережі Wi-Fi, 2. Кнопка управління бездротовою мережею Wi-Fi, 3. Кнопка «скидання» (скидання налаштувань Користувача), 4. Мережеві порти «0... 4»

П’ять портів Ethernet для підключення домашніх пристроїв та інтернет-кабелю. 5. Вимикач і роз’єм «живлення». 6. Універсальні порти USB 2.0 і 3.0-і порти для підключення сумісних USB-пристроїв, таких, як Модеми 3G / 4G, принтери і зовнішні жорсткі диски з інтерфейсом USB 2.0 або USB 3.0. 7. Кнопки з призначуваними функціями «FN1» і «FN2».

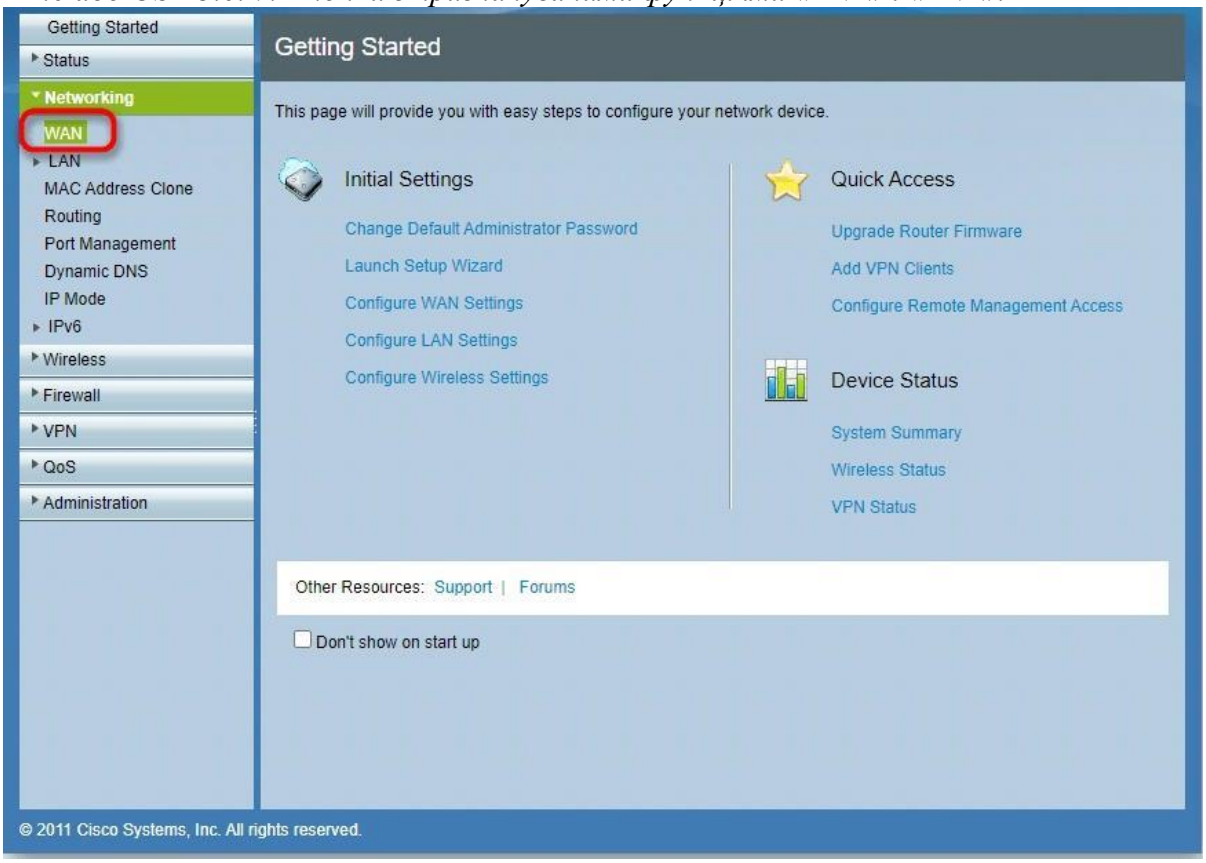


Рисунок – 3.2. Основні налаштування та підключення до бездротового інтернету Cisco C2911R

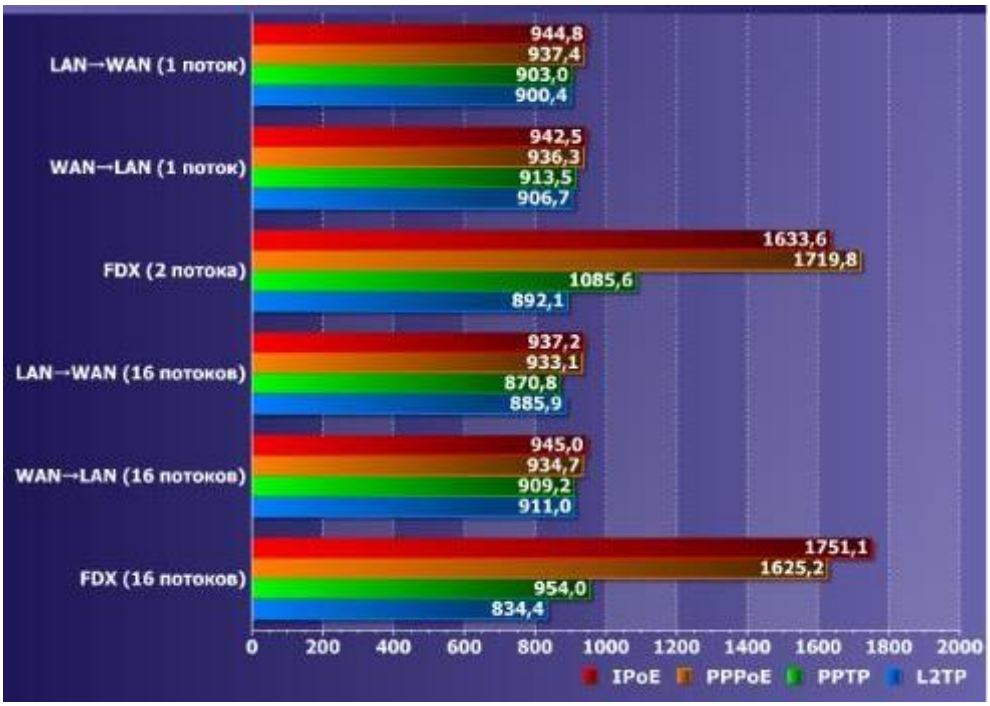


Рисунок – 3.3. Маршрутизації інтернет-трафіку для різних типів підключення Cisco C2911R

Пристрій здатний максимально ефективно працювати у всіх режимах – в разі передачі даних в одну сторону реальна швидкість становить близько 900 Мбіт/с. у дуплексі для PPTP і L2TP використовується тільки програмне прискорення, так що тільки в IPoE і PPPoE, де є і апаратний прискорювач, ми бачимо тут швидкість помітно вище гігабіта [9, с. 120].

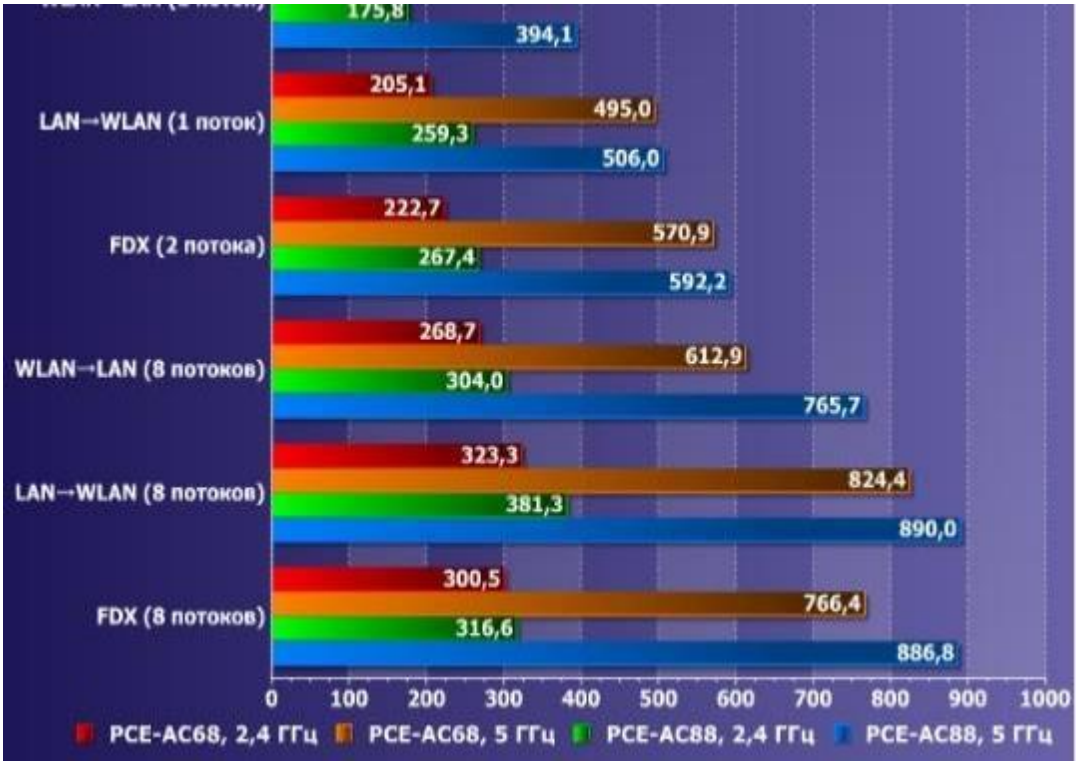


Рисунок – 3.4. Маршрутизації інтернет-трафіку (бездротового) для різних типів підключення Cisco C2911R

Маршрутизатор Cisco C2911R підтримує приблизно 150 Мбіт/с для режимів PPTP і L2TP та до 300 Мбіт/с для IPSec. Програмно реалізовані сервери SSTP і OpenVPN демонструють продуктивність близько 25 Мбіт/с.

Маршрутизатор Cisco C819GW призначений для стабільного та повнофункціонального підключення до Інтернету та IP-телебачення через виділену Ethernet-лінію, підтримуючи різноманітні типи з'єднань: IPoE, PPPoE, PPTP, L2TP, 802.1X, VLAN 802.1Q, IPv4 / IPv6. Він забезпечує максимальну швидкість до 1000 Мбіт/с за тарифом незалежно від типу підключення і

навантаження, а для IPoE / PPPoE – до 1800 Мбіт/с у дуплексі. Додатково, Cisco C819GW може підключатися до Інтернету через численні популярні 3G / 4G USB-модеми, DSL-модем або провайдерський Pon-термінал з Ethernet-портом, а також через провайдерський або приватний Wi-Fi хот-спот.

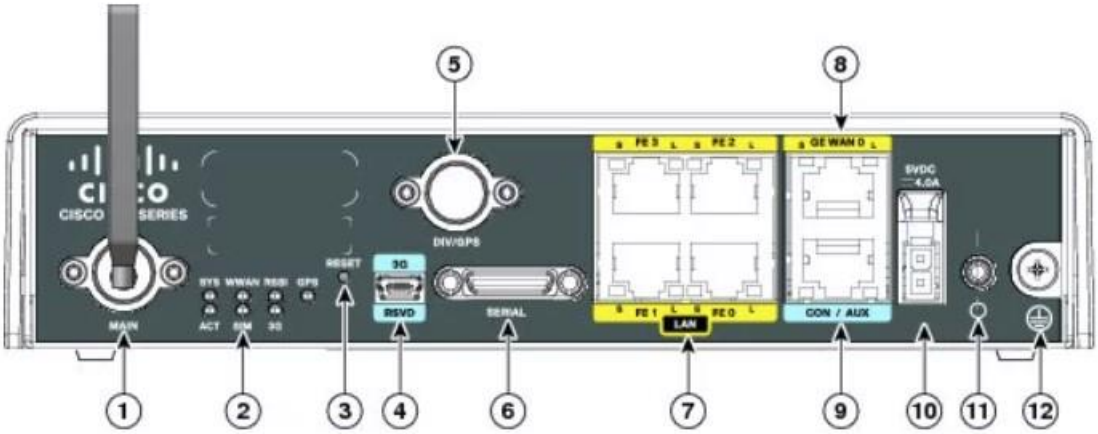


Рисунок – 3.5. Функціональне призначення основних виходів та індикаторів на пристрої Cisco C819GW III

1–3G main antenna. 2 – LEDs. 3 – Reset button. 4–3G mini-USB diagnostic port. 5 – Diversity / GPS antenna. 6–12-in – 1 serial port. 7 – FE ports. 8 – GE WAN port. 9 – Console / Aux port. 10–5 VDC molex power input. 11 – Power switch. 12 – Ground.

При першому підключенні Інтернет-центр створює двохдіапазонну Wi-Fi мережу 802.11 n / ac з максимальним захистом за стандартом WPA2 для ноутбуків, смартфонів, планшетів та інших бездротових пристроїв. Поворотні антени та спеціальні підсилювачі Wi-Fi сигналу забезпечують широку зону покриття і високу якість бездротового з'єднання зі швидкістю до 867 + 300 Мбіт/с незалежно від розташування Інтернет-центру. Окрема мережа Wi-Fi для гостьових пристроїв надає доступ лише до Інтернету, без доступу до домашньої мережі. Робочий канал вибирається автоматично на основі регулярного аналізу радіоефіру.

Окрім підключення до Інтернету через 3G / 4G USB-модеми, USB-порти можуть використовуватись для підключення мережевих USB-накопичувачів, USB-принтерів, DECT-станції Cisco Plus DECT, або ADSL2+/VDSL2-модему Cisco Plus DSL. Швидкість читання з USB 3.0 дисків становить не менше 40

Мбайт/с. Максимальна швидкість з’єднання в бездротовій мережі (867 Мбіт/с для діапазону 5 ГГц і 300 Мбіт/с для 2,4 ГГц) досягається за умови використання пристроїв Wi-Fi стандарту IEEE 802.11 ac або 802.11 n, що підтримують два просторові потоки та ширину каналу 80 МГц або 40 МГц відповідно.

Маршрутизатор Cisco C881G можна розглядати як спрощену версію C819GW.

Рисунок – 3.6. Зовнішній вигляд маршрутизатора Cisco C881G

Якщо звернути увагу на ціни, зазначені на сайті розробника, різниця між моделями C881G і C819GW становить 1 600 грн: 8 190 грн проти 6 590 грн. У нашому проєкті ми вибрали Cisco C819GW III та Cisco C881G, оскільки їхня вартість незначно відрізняється від Cisco C2911R. Основна перевага C881G полягає в її менших габаритах. Наприклад, вона значно компактніша за C819GW і C2911R – 159 × 110 × 29 мм проти 214 × 154 × 33 мм – і майже вдвічі легша. Проте цей пристрій має тенденцію до сильнішого нагрівання через іншу форму корпусу. Розміри були зменшені завдяки відмові від SFP-порту і перенесенню одного USB-роз’єму: тепер вони розташовані на протилежних бічних гранях. Однак загальний дизайн корпусу залишився незмінним. Блок живлення у C881G інший, трохи компактніший і менш потужний (18 Вт) [19, с. 73].

Таблиця 3.4

Порівняння характеристик Cisco C819GW та Cisco C881G

	Cisco C881G	Cisco C819GW
Чіпсет	MediaTek MT7621A (2 x MIPS1004KC 880 МГц)	
Стандарти	IEEE 802.11 a / b / g / n / ac (2,4 ГГц + 5 ГГц); 802.11 k / r	
Контролер	MT7615D	
	-	Realtek RTL8211FS
ROM	128 Мбайт	
RAM	128 Мбайт	256 Мбайт
Антени	4 x зовнішні 5 dBi; довжина 175 мм	
	-	Підсилювачі прийому / передачі
Шифрування Wi-Fi	WPA / WPA2, WEP, WPS	
Апаратні кнопки	Відключення Wi-Fi / запуск WPS, перезагрузка/скидування налаштувань, 2 x FN (програмовані)	
Макс, швидкість	802. Пас: до 867 Мбіт/с; 802.11п: до 400 Мбіт/с	
	5 x 10 / 100 / 1000 Мбіт/с RJ–45	
Інтерфейси	-	1 x 100 / 1000 Мбіт/с SFP
	2 x USB 2.0	1 x USB 2.0; 1 x USB 3.0
Індикатори	4 x на верхній кришці	6 x на верхній кришці (2 x FN)
	-	У кожного мережевого порту
Розміри (ШхДхВ)	159 x 110 x 29 мм	214 x 153 x 33 мм

Таблиця 3.5

Можливості Cisco C819GW та Cisco C881G

Сервіси	Сервер DLNA, FTP, SMB, AFP; TimeMachine; прінт-сервер; BitTorrent-клієнт Transmission; VLAN; VPN-сервер (IPSec / L2TP, PPTP, Open VPN, SSTP); Entware; модулі Cisco Plus; автообновлення прошивки; Captive-портал; NetFlow / SNMP; SSH-доступ
Доступ в Інтернет	Static IP, DHCP, PPPoE, PPTP, L2TP, SSTP, 802. lx; VLAN; KABiNET; DHCP Relay; IPv6 (6in4); Multi-WAN; пріоритети підключення (policy-based routing); резервне підключення + Ping checker; MSP; майстер налаштування NetFriend
Проброс портів	Інтерфейс / VLAN +порт+протокол+IP; UPnP, DMZ; IPTV / VoIP LAN-Port, VLAN, IGMP / PPPoE Proxy, udpxy
Захист	Батьківський контроль, фільтрація, захист від телеметрії і реклами: «Яндекс. DNS», SkyDNS, AdGuard, Norton ConnectSafe; HTTPS-доступ до веб-інтерфейсу
Режим роботи	Маршрутизатор, MSP-клієнт/медіа-адаптер, точка доступа, повторювач
QoS / Шейпинг	WMM, IntelliQoS; вказання пріоритету інтерфейсу / VLAN + DPI; шейпер
Сервіси Dynamic DNS	DNS-master (RU-Center), DynDns, NO-IP; KeenDNS
Брандмауер	Фільтрація по порт / протокол / IP; Packet Capture; SPI; захист від DoS
Проброс VPN, ALG	PPTP, L2TP, IPSec; (T) FTP, H. 323, RTSP, SIP

Через обмеження версії порту 2.0 у Cisco C881G швидкість роботи буде нижчою: заявлена швидкість становить до 40 Мбайт/с. Стендовий накопичувач Kingston SSDNow V+200 з одним розділом NTFS у зовнішньому корпусі LanShuo INIC–3609 показав саме ці результати. Як при передачі по FTP, так і по SMB швидкість читання становила трохи більше 40 Мбайт/с, а швидкість запису – трохи менше 40 Мбайт/с.

Таблиця 3.6

Результати тестування маршрутизатора Cisco C881G

Потоки	1	2	4	8	16	32	64
Середня швидкість Wi-Fi 802.11ac 5 ГГц, Мбіт/с							
R →A	268	537	607	669	681	658	627
A → R	415	546	559	671	673	657	607
A↔R	520	547	573	644	683	681	661
Середня швидкість Wi-Fi 802.1Ш 2,4 ГГц, Мбіт/с							
R →A	173	195	202	211	226	190	193
A → R	171	209	193	214	169	141	151
A↔R	167	186	206	209	210	198	170

Базові налаштування Cisco C881G залишилися незмінними: шифрування WPA2, 802.11 n з шириною каналу 20 / 40 МГц для 2,4 ГГц, 802.11 n / ac з шириною каналу 20 / 40 / 80 МГц для 5 ГГц, і всі основні опції MU-MIMO, Beamforming, 256-QAM, TxBurst ввімкнені за замовчуванням. Конфігурація стендів також залишилася колишньою.

Перша машина: Intel Core i7–3770, 16 ГБ RAM, ASUS PCE-AC88 на базі чіпсета Broadcom 4366, Realtek RTL8168, Windows 7 SP1 x64.

Друга: Intel Xeon D – 1540, 32 ГБ ECC RAM, 2 x Intel I210 (позначений як R у таблиці), 2 x Intel I350, Devuan Jessie.

Загалом, умови тестування залишилися ті самі, змінювався лише стан навколишнього ефіру. Кількість видимих сусідських точок доступу зростає поступово, але важливо те, що все більше з них переходять у діапазон 5 ГГц. Через це, зокрема, довелося примусово вибрати 64-й канал, оскільки він був далі від сторонніх точок доступу.

Рисунок – 3.7. Схематичне зображення результатів тестування маршрутизаторів

Сам же роутер при автовиборі каналу стабільно йшов у верхню частину діапазону (за сотий канал). Cisco C819GW III та Cisco C881G знаходилися в прямій видимості один від одного на відстані чотирьох метрів. В обох діапазонах істотних відмінностей між C819GW і C881G немає. В 2,4 ГГц з C881G набагато рідше було видно швидкість 400 Мбіт/с і набагато частіше з'єднання йшло до 200 Мбіт/с [47, с. 205]. Cisco C819GW III, в свою чергу давала якщо вже не 400, то 300 Мбіт/с.

3.3 Розрахунок адресного простору IP-адрес

План IP-адресації є основою для будь-якого мережного проєкту. Його правильна структура допомагає зменшити навантаження на обладнання у великих мережах і спрощує їхнє адміністрування, що зменшує ймовірність помилок через людський фактор.

IP-адреси – це унікальні числові ідентифікатори, які присвоюються мережним адаптерам і використовуються для передачі даних у мережі. Вони можуть бути унікальними (Unicast), груповими (Multicast) або широкомовними (Broadcast). У повідомленнях IP-пакетів унікальні IP-адреси можуть бути як адресами відправника, так і отримувача, а групові і широкомовні адреси можуть бути тільки адресами отримувача. Існують два підходи до поділу IP-адреси версії 4: класовий і безкласовий.

Наприклад, у корпоративній мережі може бути використана IP-адреса 172.205.14.1. Для цієї адреси можна визначити різні параметри, такі як клас IP-адреси, маска мережі, IP-адрес мережі, IP-адрес вузла, широкомовна IP-адреса та інші.

Таблиця 3.7

IP-адресація проєктованої корпоративної мережі поштових відділень

Назва відділу	Кількість хостів	IP-адрес підмережі або діапазон
Директор поштового відділення	2	172.205.0.0 / 24
Відділ закупок	4	172.205.2.0 / 24
Приймальня	2	172.205.3.0 / 24
IT-відділ	5	172.205.4.0 / 24
Відділ обслуговування	2	172.205.5.0 / 24
Відділ сортування	4	172.205.6.0 / 24
Відділ управління	5	172.205.7.0 / 24
Склад	1	172.205.9.0 / 24 172.205.10.0 / 24

IP-адреса складається з номера мережі і номера вузла. Кількість байтів, виділених під мережу та вузол, визначається за таблицею класів. Наприклад, IP-адреса 172.205.14.1 належить до класу B, де маска мережі 255.255.0.0, інверсна маска 0.0.255.255, а префікс мережі / 16.

Для класу B перші два байти відводяться під номер мережі, тому IP-адрес мережі виглядає як 172.205.0.0, а для номеру вузла і самого вузла – як 0.0.14.1.

Мінімальна IP-адреса для вузлів – 172.205.0.1, максимальна – 172.205.255.254. Широкомовна IP-адреса мережі – 172.205.255.255.

Кількість вузлів (IP-адрес вузлів), які можуть входити в мережу, розраховується за формулою: $K_{вузлів} = 2^{(32-Класовий\ префікс)} - 2$

У нашому випадку кількість вузлів становить:

$$K_{вузлів} = 2^{(32-16)} - 2 = 2^{16} - 2 = 65536 - 2 = 65534 \text{ вузли.}$$

3.4 Побудова корпоративної мережі на основі вибраного обладнання для створення програмного засобу захисту транспортування даних

На початку нашого дослідження перелічимо основні етапи розробки проєктованого програмного засобу для корпоративної мережі поштових відділень (таб. 3.8).

Таблиця 3.8

Основні етапи розробки корпоративної мережі

Етап розробки мережі	Назва роботи	Зміст роботи
1	Планування та стратегія мережі	Визначення мети мережі, визначення бізнес-вимог, вивчення існуючої інфраструктури.
2	Аналіз потреб користувачів та вимоги до мережі	Вивчення потреб користувачів у доступі до мережі та обміні даними, визначення вимог до пропускної здатності та надійності мережі.
3	Вибір технологій та обладнання	Вибір оптимальних технологій та обладнання для відповідності вимогам до мережі.
4	Проєктування топології мережі	Створення схеми топології мережі, визначення маршрутів з'єднання між пристроями.
5	Вибір кабельної та бездротової інфраструктури	Вибір типу кабелю та бездротових технологій для підключення мережних пристроїв.
6	Розгортання мережі	Установка та налаштування мережного обладнання, прокладка кабелю та налаштування бездротової точки доступу.
7	Тестування та налагодження	Перевірка працездатності мережі, виявлення та виправлення помилок, налагодження швидкості та надійності мережі.
8	Захист та безпека мережі	Встановлення заходів безпеки для захисту мережі від несанкціонованого доступу та атак.
9	Документація та звітність	Підготовка технічної документації та звітів про розгортання мережі для майбутнього супроводження та аналізу.
10	Тренінг та навчання користувачів	Проведення навчання користувачів з використання мережі та її компонентів.
11	Підтримка та обслуговування	Забезпечення постійної підтримки та обслуговування мережі для її ефективної роботи.
12	Моніторинг та	Постійний моніторинг роботи мережі та вдосконалення її

	оптимізація	роботи шляхом впровадження нових технологій та методів.

Виконується моделювання комп’ютерної мережі в програмі Packet Tracer, що є емулятором мереж передачі даних, розробленим компанією Cisco Systems. Цей інструмент дозволяє створювати реалістичні моделі мережі, налаштовувати маршрутизатори і комутатори за допомогою команд Cisco IOS, а також взаємодіяти між користувачами через Інтернет. Packet Tracer включає в себе широкий спектр обладнання, включаючи маршрутизатори Cisco 1800, 2600, 2800 і комутатори 2950, 2960, 3560, а також сервери DHCP, HTTP, TFTP, FTP, робочі станції, різні модулі для комп’ютерів і маршрутизаторів, пристрої WiFi та різні типи кабелів.

У моделі мережі використовуються стаціонарні комутатори Cisco C881G. Різні типи пристроїв з’єднуються прямими кабелями, як показано на прикладі з’єднання комутатора з ПК, комутатора з сервером та комутатора з точкою доступу. Однакові пристрої з’єднуються перехресними кабелями.

У мережевій схемі працюють три сервери: DHCP, DNS, FTP. Сервер DHCP (протокол динамічної конфігурації) надає комп’ютерам IP-адреси та інші необхідні параметри для роботи в мережі TCP / IP. Сервер DNS (доменна система імен) встановлює відповідність між символьним ім’ям хоста та його IP-адресою. Сервер FTP (протокол передачі даних) дозволяє клієнтським комп’ютерам зберігати та отримувати доступ до файлів, що знаходяться на сервері.

Рисунок 3.8 ілюструє масштабовану модель локальної мережі, яка розробляється.

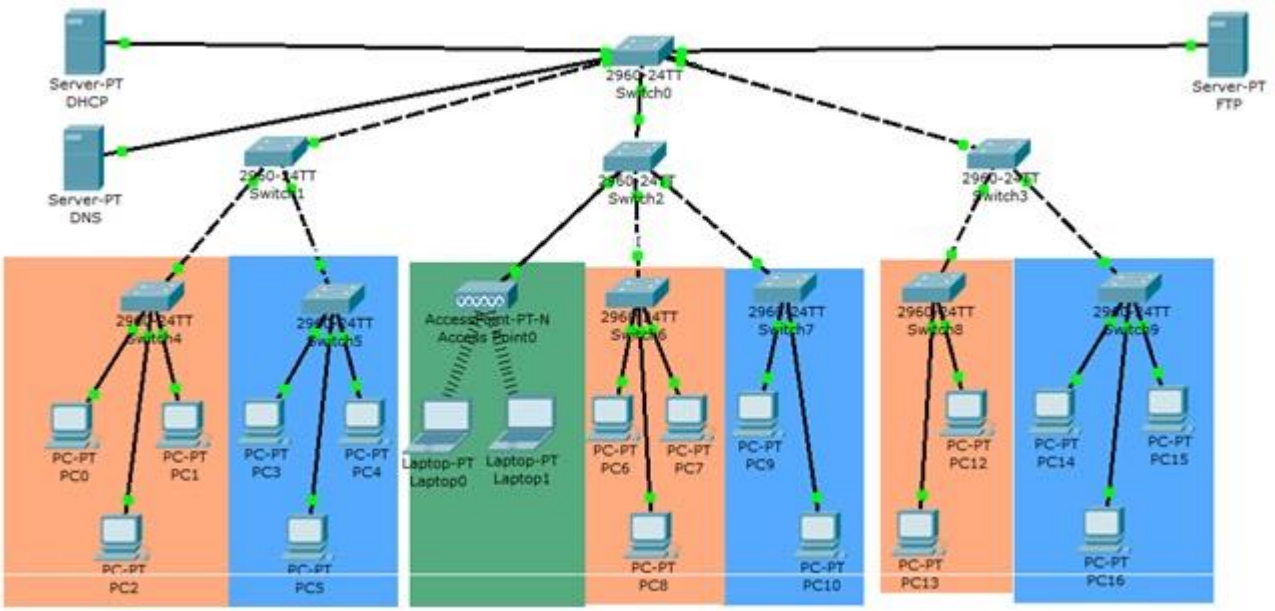


Рисунок – 3.8. Модель корпоративної мережі поштових відділень в Packet Tracer

При аналізі послідовності побудови корпоративної мережі поштових відділень з використанням вибраного обладнання варто відзначити, що контролер автоматично визначить версію операційної системи ретранслятора та, у разі наявності оновлення, під час додавання до Wi-Fi-системи, виконає оновлення операційної системи пристрою до останньої актуальної версії. Для додавання ретранслятора до системи Wi-Fi необхідно натиснути кнопку «захопити» та зачекати завершення процесу [54, с. 77].

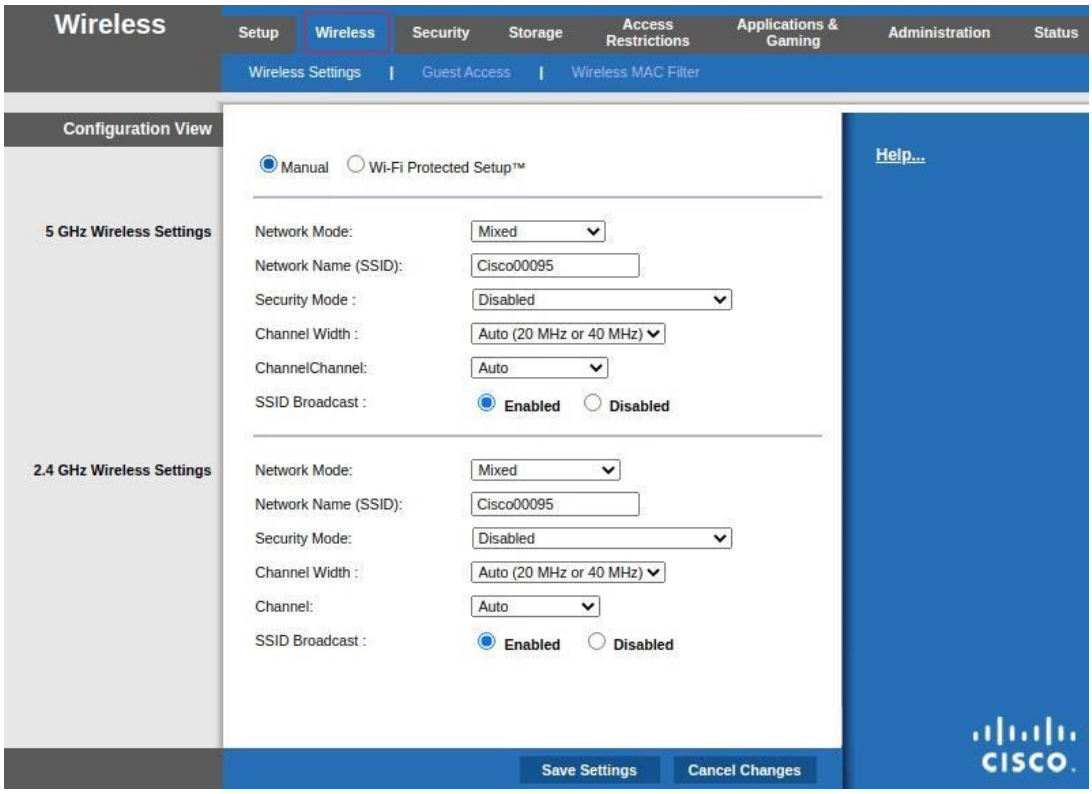


Рисунок – 3.9. Початок побудови мережі за допомогою обладнання Cisco C881G

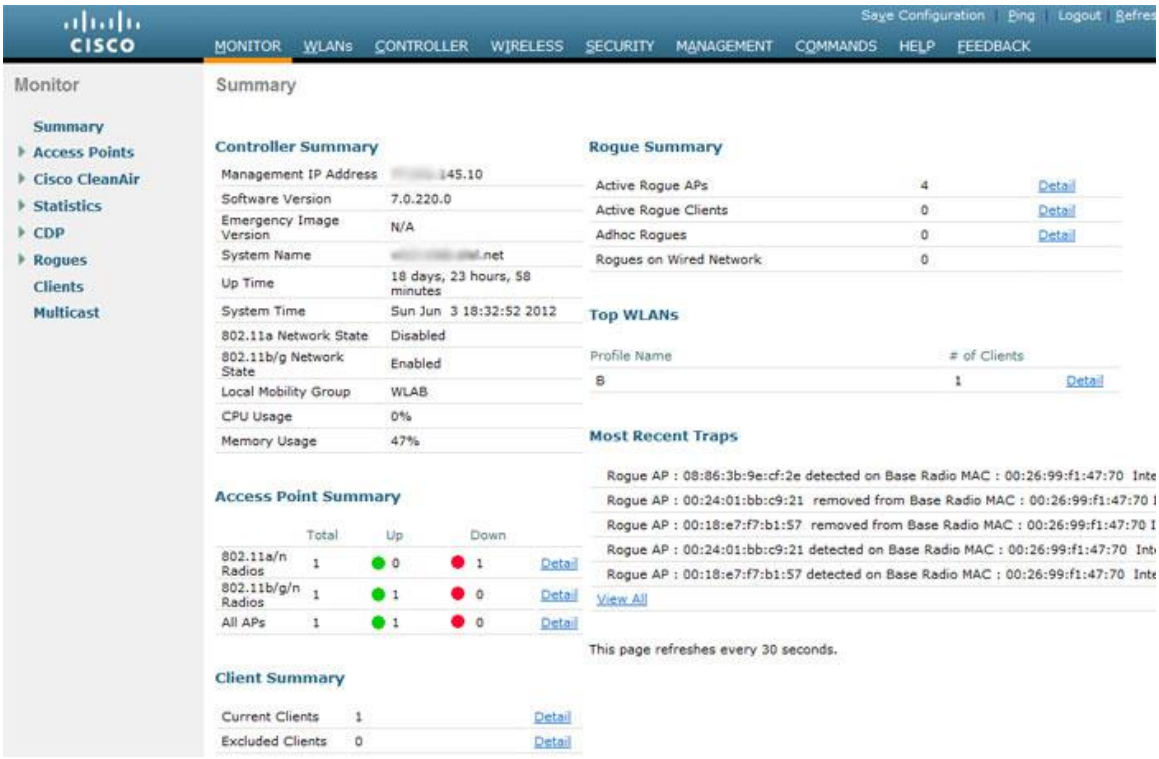


Рисунок – 3.10. Ідентифікація обладнання ОС

Після захоплення пристрою з’явиться в списку «Ретранслятори, що входять в Wi-Fi-систему» [61].

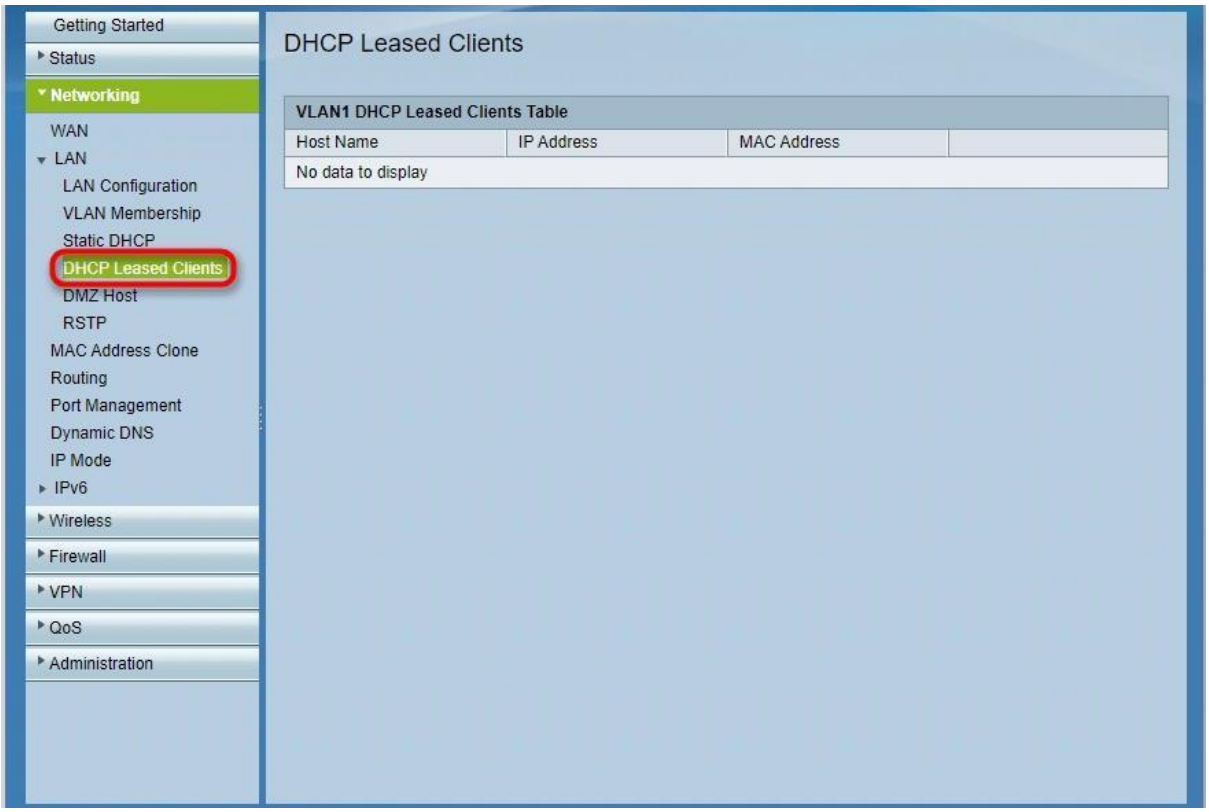


Рисунок – 3.11. Виявлення Wi-Fi-системою наявного підключеного обладнання

Якщо з якоїсь причини ретранслятор не з'являється в списку доступних для додавання або не захоплюється в Wi-Fi-систему, то потрібно виконати скидання налаштувань на заводські і потім повторити підключення. Після додавання ретранслятора в Wi-Fi-систему можна перейти до його веб-конфігуратору. Натисніть по посиланню в назві ретранслятора.

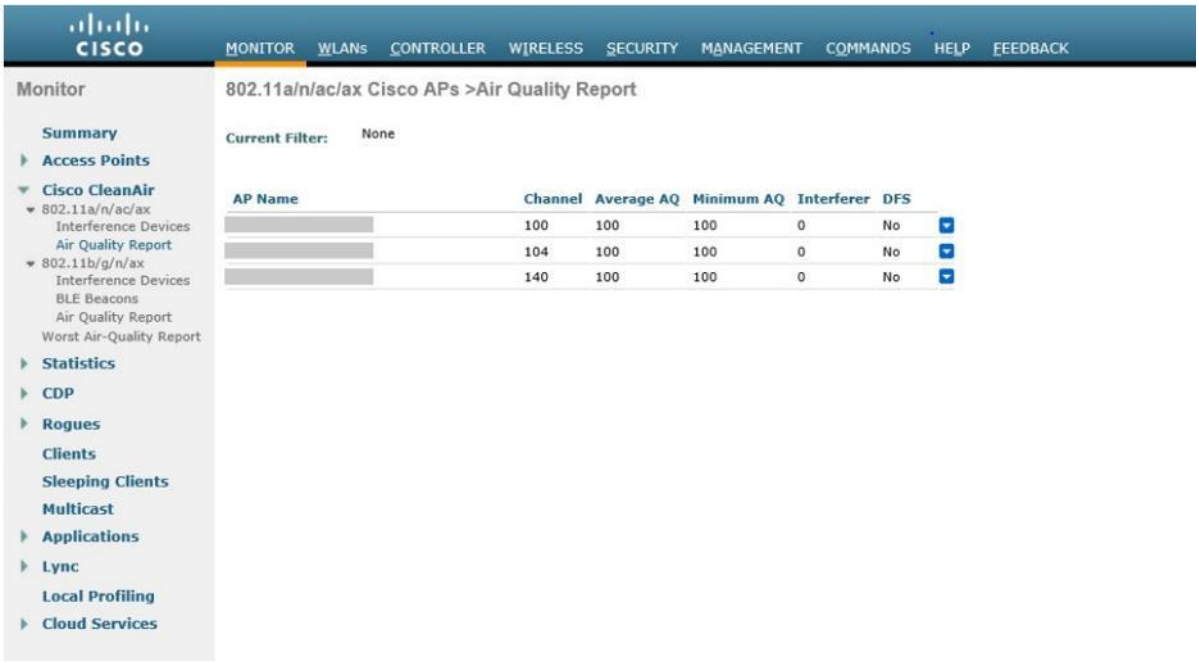


Рисунок – 3.12. Веб-конфігурація наявного підключеного обладнання

При з’єднанні з інтерфейсом ретранслятора необхідно використовувати пароль адміністратора, який був встановлений на контролері. Після встановлення з’єднання з веб-інтерфейсом ретранслятора може з’явитися повідомлення «Цей пристрій керується контролером Wi-Fi-системи».

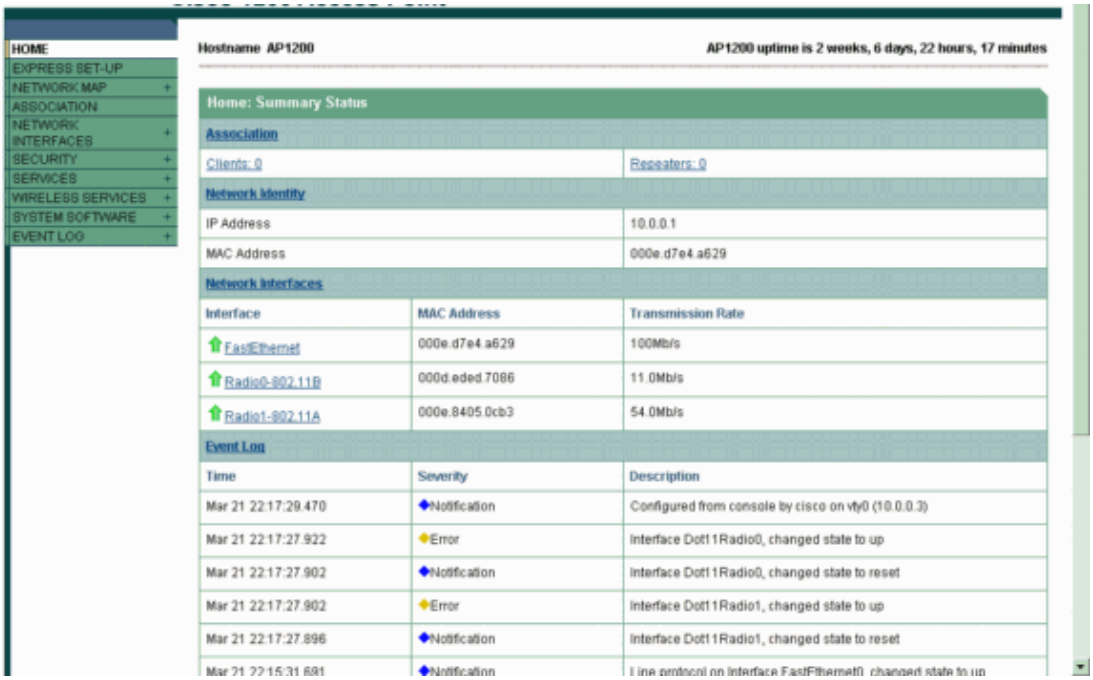


Рисунок – 3.13. Результат підключення до веб-інтерфейсу ретранслятора

На пристрої, який керується контролером Wi-Fi-системи, основні налаштування бездротової мережі, такі як ім’я мережі (SSID), захист мережі (протокол безпеки) і пароль (ключ безпеки), налаштування безшовного роумінгу, параметри IP та списки контролю доступу (білий / чорний) будуть недоступні для редагування. Їх можна змінити лише на контролері (головному інтернет-центрі).

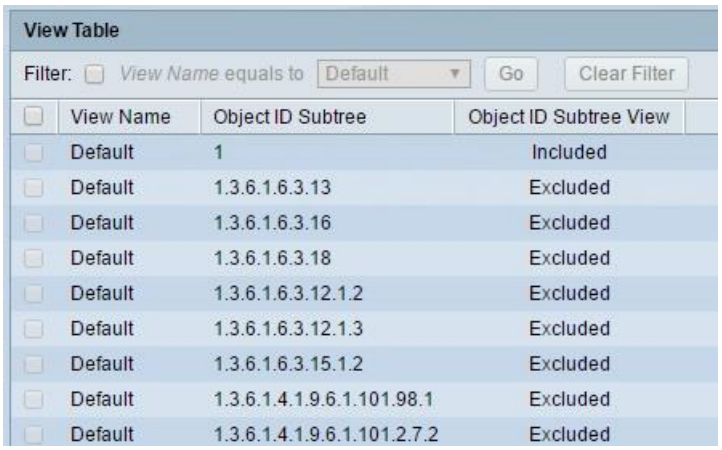


Рисунок – 3.14. Результат виявлення підключених користувачів

На вкладці «Пристрої» модульної Wi-Fi-системи відображаються всі доступні для додавання ретранслятори, які входять до складу Wi-Fi-мережі.

На вкладці «Переходи» показуються бездротові переходи між вузлами Wi-Fi-мережі. У журналі фіксуються такі події: підключення, відключення, стандартний перехід без «прискорювачів» (коли клієнт просто відключається від однієї точки доступу і підключається до іншої), перехід по PMK-кешу (швидкий перехід з використанням pmkid-кешу, ідентифікатора спарених майстер-ключів Pairwise Master Key Identifier) і швидкий перехід (найшвидший перехід з використанням 802.11 r і режиму Ft – Fast Transition). При надмірній кількості записів у журналі можна використовувати фільтр.

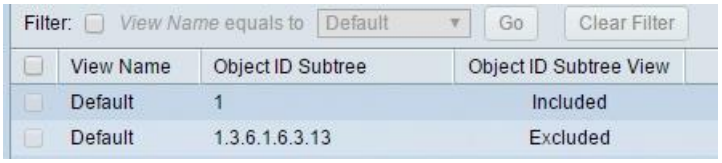


Рисунок – 3.15. Використання фільтрів для пошуку необхідних користувачів мережі

Якщо для підключення ретрансляторів використовується проміжний комутатор, то він має абсолютно прозоро пропускати трафік на рівні L2. При роботі Wi-Fi-системи використовується протокол STP, і якщо комутатор підтримує MSTP / RSTP / STP, то ці налаштування слід вимкнути на портах, які використовуються для Wi-Fi-системи. Для коректної роботи гостьової мережі на ретрансляторах необхідно додаткове налаштування Інтернет-центрів.

3.5 Технологічний засіб захисту транспортування даних у мережі

Розробимо програмний код, який демонструє, як можна використовувати JavaScript для налаштування захисту транспортування даних у мережі з використанням функції ACL, NAT і PAT на мережевому обладнанні Cisco:

```
// налаштування ACL
function configureACL {
// Підключення до мережевого пристрою Cisco
const Cisco = connectToCisco;

// Налаштування правил ACL
Cisco. configureACL({
sourceIP: '192.168.0.0 / 24',
destinationIP: '10.0.0.0 / 24',
protocol: 'tcp',
action: 'allow',
});

// Збереження налаштувань
Cisco. saveConfiguration;
}

// Налаштування NAT
function configureNAT {
// Підключення до мережевого пристрою Cisco
const Cisco = connectToCisco;

// Налаштування правил NAT
Cisco. configureNAT({
internalIP: '192.168.0.100',
externalIP: '1.2.3.4',
});

// Збереження налаштувань
Cisco. saveConfiguration;
}

// Нналаштування PAT
function configurePAT {
// Підключення до мережевого пристрою Cisco
const Cisco = connectToCisco;

// Налаштування правил PAT
Cisco. configurePAT({
internalIP: '192.168.0.100',
internalPort: 8080,
externalPort: 80,
});
```

```
// Збереження налаштувань
Cisco. saveConfiguration;
}

// Виклик функцій для налаштування захисту
configureACL;
configureNAT;
configurePAT;
```

Наведемо опис кожної функції з коду на JavaScript:

1. `*configureACL*`: Ця функція відповідає за налаштування правил ACL (Списку керування доступом). Вона викликає функцію `connectToCisco`, яка встановлює з'єднання з обладнанням Cisco. Потім вона викликає метод `configureACL` об'єкта `Cisco`, щоб налаштувати правила ACL, такі як діапазони IP-адрес, протоколи та дії (дозволити або заборонити).

2. `*configureNAT*`: Ця функція відповідає за налаштування правил NAT (Network Address Translation). Вона також викликає функцію `connectToCisco` для підключення до обладнання Cisco. Потім вона викликає метод `configureNAT` об'єкта `Cisco`, щоб налаштувати правила NAT, вказавши внутрішню IP-адресу та зовнішню IP-адресу для перетворення адрес.

3. `*configurePAT*`: Ця функція відповідає за налаштування правил PAT (Port Address Translation). Вона також викликає функцію `connectToCisco` для підключення до обладнання Cisco. Потім вона викликає метод `configurePAT` об'єкта `Cisco`, щоб налаштувати правила PAT, вказавши внутрішню IP-адресу, внутрішній порт та зовнішній порт для перетворення адрес.

4. `*connectToCisco*`: Ця функція відповідає за підключення до обладнання Cisco. У цьому прикладі вона може бути функцією, яка створює з'єднання з обладнанням Cisco і повертає об'єкт `Cisco`, який представляє підключення до пристрою.

5. `*Cisco. configureACL*`: Цей метод викликається на об'єкті `Cisco` і використовується для налаштування правил ACL на пристрої Cisco. Він отримує параметри, такі як діапазони IP-адрес, протоколи та дії, і встановлює відповідні налаштування на пристрої.

6. `*Cisco. configureNAT*`: Цей метод викликається на об’єкті `Cisco` і використовується для налаштування правил NAT на пристрої Cisco. Він отримує параметри, такі як внутрішню IP-адресу та зовнішню IP-адресу, і встановлює відповідні налаштування на пристрої.

7. `*Cisco. configurePAT*`: Цей метод викликається на об’єкті `Cisco` і використовується для налаштування правил PAT на пристрої Cisco. Він отримує параметри, такі як внутрішню IP-адресу, внутрішній порт та зовнішній порт, і встановлює відповідні налаштування на пристрої.

8. `*Cisco. saveConfiguration*`: Цей метод викликається на об’єкті `Cisco` і використовується для збереження налаштувань на пристрої Cisco після внесення змін. Він забезпечує збереження налаштувань, щоб вони були активними після перезавантаження або відновлення пристрою.

3.6 Особливості запуску програмного засобу та підключення інтернет-центру на базі обладнання Cisco

Інтернет-центр Cisco C819GW III, підключається до мережі Інтернет через встановлення компоненту серверу PPTP. У проєктуємій корпоративній мережі вихід в інтернет відбувається за допомогою Cisco C819GW 2 і Cisco C881G. До VPN-сервера на Cisco C819GW 2 інтернет-центр автоматично встановлює з’єднання (в якості клієнта PPTP), що дозволяє користувачам в домашній мережі (доступ як безпосередньо на Cisco (підключення до USB-накопичувачів і принтерів), так і до ресурсів, розташованим в його мережі комп’ютерів, серверів NAS [57, с. 65].

Для запуску програмного коду на налаштованому мережевому обладнанні Cisco потрібно використовувати спеціальний інтерфейс.

Особливості налаштування Cisco C819GW III. У меню «Networking → Wan» встановлюють користувача, від імені якого буде виконуватися PPTP-підключення до сервера, права доступу-vpn.

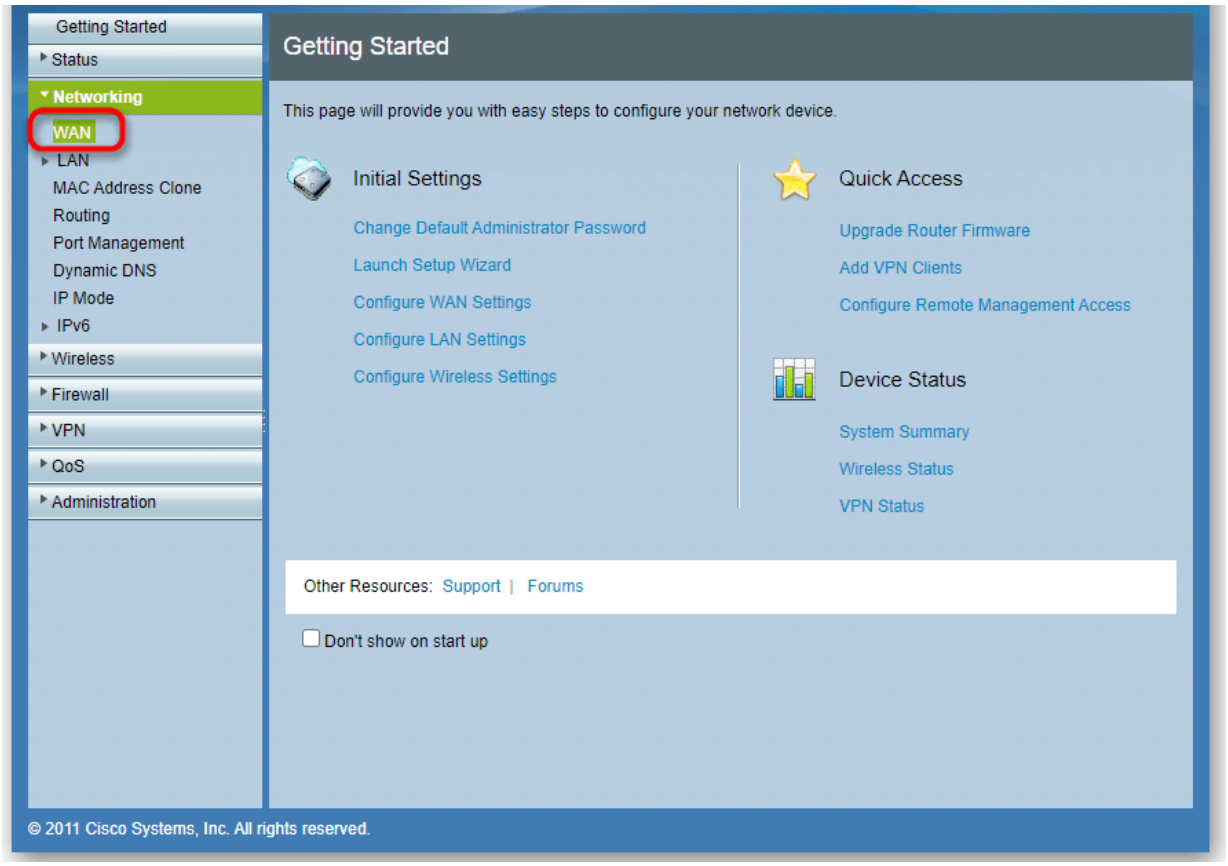


Рисунок – 3.16. Налаштування маршрутизатора Cisco C819GW

При роботі пристрою в даній схемі не слід встановлювати від імені цього ж користувача підключення з інших розташувань (тобто обліковий запис з ім’ям net_2 буде використовуватися виключно для PPTP-підключень).

Потім в меню «програми > сервер VPN» потрібно включити прив’язку сервера до інтерфейсу «Мережа». Початковий IP-адрес пулу слід вибрати таким, щоб не виникало перекриття з діапазонами IP-адрес робочих мереж. Рекомендується залишити в цьому полі значення за замовчуванням, а для клієнтського пристрою, що бере участь в схемі, вказати в списку користувачів статичну IP-адресу з цієї ж підмережі.

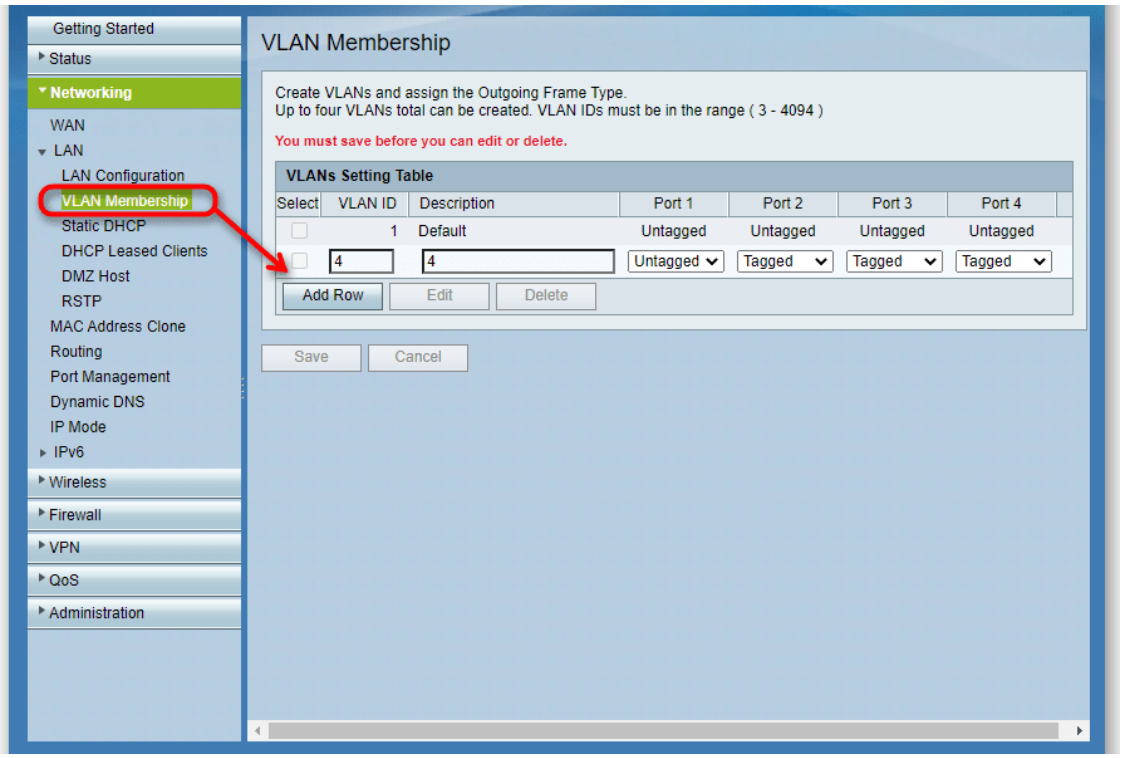


Рисунок – 3.17. Налаштування VPN для маршрутизатора Cisco C819GW III

Користувач net_2 буде при підключенні до VPN-сервера отримувати IP-адресу 172.205.1.2. Для настройки потрібно клацнути мишкою по потрібній облікового запису і в поле IP-адреса вказати адресу.

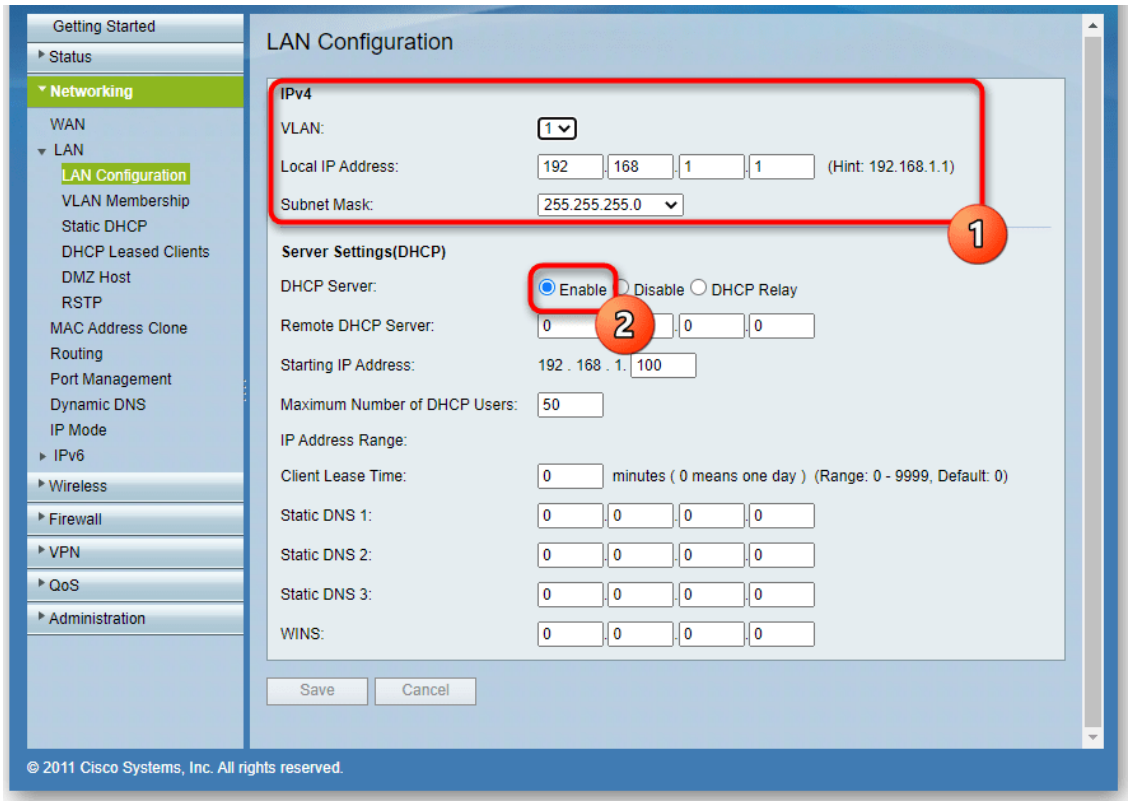


Рисунок – 3.18. Налаштування локальної мережі Cisco C819GW III

Для того щоб клієнтам мережі офісу були доступні ресурси мережі сервісного центру, в меню Інтернет > маршрути потрібно створити статичний маршрут, із зазначенням розташування мережі і сервісного центру. Локальна мережа 192.168.2.0 / 255.255.255.0 стане доступна через IP-адресу, видану сервером підключився Клієнту (в нашому випадку це клієнт с ім'ям net_2 і з IP-адресою 172.205.0.0). При налаштуванні маршруту слід вказати опцію додавати автоматично і вибрати в полі інтерфейс будь-яке значення.

Проведемо аналіз порядку налаштування Cisco C881G. На цьому пристрої потрібно виконати дві основні налаштування.

1. Об'єднувані мережі мають різні адресні простори – 192.168.1.0 / 24 і 192.168.2.0 / 24 (маска 255.255.255.0) – мережа сервера і клієнта відповідно, оскільки в локальній мережі клієнта потрібно використовувати адресацію, відмінну від мережі сервера. Налаштувати параметри локальної адреси пристрою можна в меню «Мережа > параметри IP».

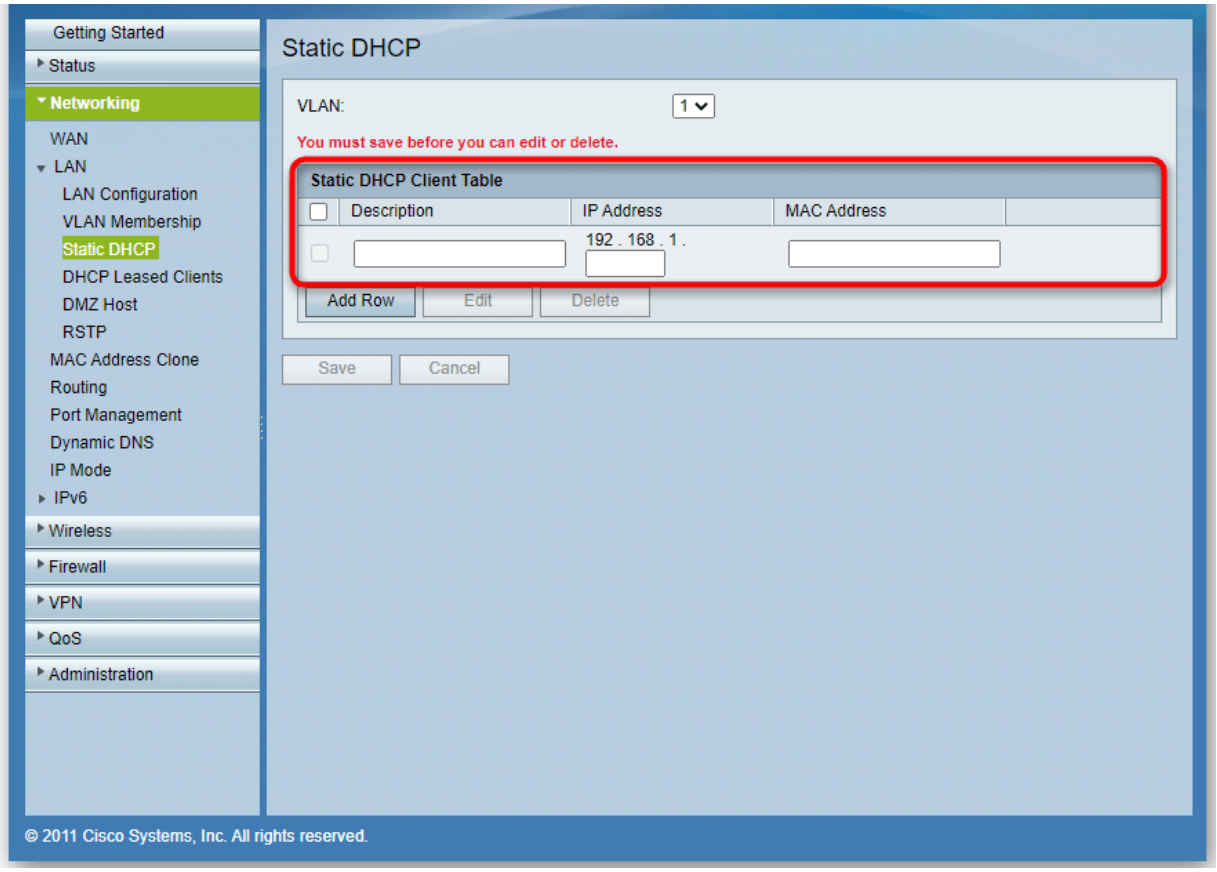


Рисунок – 3.19. Налаштування VLAN на маршрутизаторі Cisco C881G

2. Інтернет-центр Cisco C881G буде працювати в якості PPTP-клієнта. Необхідне PPTP-підключення до VPN-сервера потрібно створювати в меню Інтернет > PPPoE / VPN.

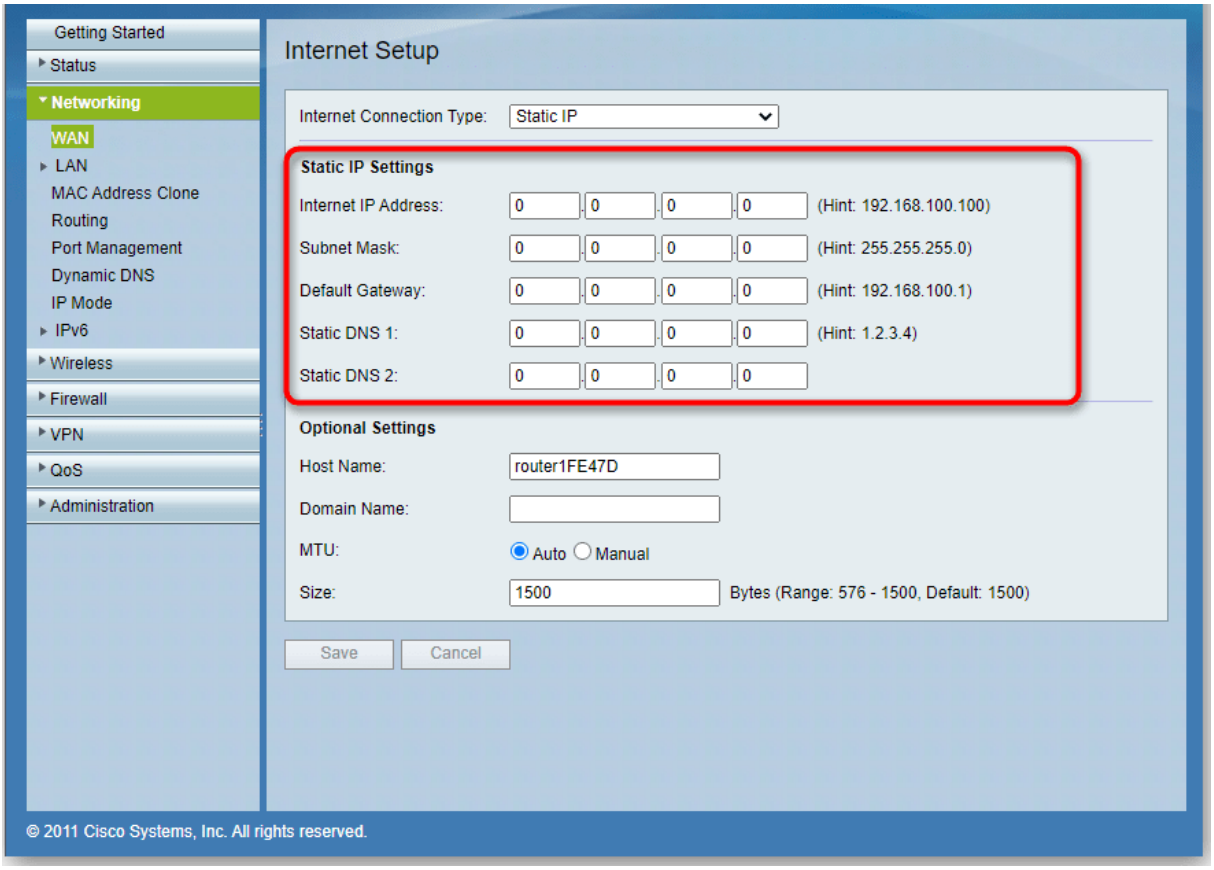


Рисунок – 3.20. Налаштування Internet-підключення до VPN-сервера

На маршрутизаторі для блокування доступу до Інтернету для користувачів з бухгалтерії і декількох робочих станцій у відділі сортування в діапазоні адрес 172.205.1.3–172.205.1.8 можна використати наступні команди:

```bash
enable
configure terminal
access-list 1 deny 172.205.1.3 0.0.0.5
access-list 1 permit any
interface [інтерфейс, через який йде доступ в Інтернет]
ip access-group 1 out
exit
exit
write memory
```

Ці команди створюють списки доступу, що блокують певні IP-адреси (бухгалтерія і маркетинг), і застосовують їх до виходу з вказаного інтерфейсу.

Список `access-list 1` блокує діапазон адрес 172.205.1.3–172.205.1.8, а команда `ip access-group 1 out` застосовує цей список до трафіку, що виходить з маршрутизатора. Пам’ятайте, що виконання цих команд може змінити доступність до Інтернету для вказаних користувачів.

Для налаштування пароля на з’єднання та створення підінтерфейсів у маршрутизаторі можна використати такі команди:

```bash
Router>enable
Router#configure terminal
Router (config)#hostname R0
Router (config)#ip domain-name some-dmn
Router (config)#crypto key generate rsa
Router (config)#line vty 0 4
Router (config-line)#transport input ssh
Router (config-line)#password secret password1
Router (config-line)#exit
Router (config)#interface FastEthernet0 / 0
Router (config-if)#no shutdown
Router (config-if)#interface FastEthernet0 / 0.10
Router (config-subif)#encapsulation dot1q 10
Router (config-subif)#ip address 172.205.6.14 255.255.255.240
Router (config-subif)#exit
Router (config)#exit
Router#write memory
```

Ці команди налаштовують пароль для з’єднання, генерують RSA ключі для SSH, створюють підінтерфейс з вказаними параметрами та зберігають зміни в конфігураційному файлі маршрутизатора.

1. Налаштування інтерфейсу на комутаторі:

```
Switch>enable
Switch#config terminal
Switch (config)#interface fastethernet 3 / 1
Switch (config-if)#switchport mode trunk
Switch (config-if)#switchport trunk allowed vlan 10, 20, 30, 40, 50, 60, 100, 101
```

2. Для з’єднання з центральним офісом через магістральний кабель, який матиме IP-адресу в локальній мережі 0.0.0.0, буде створений наступний список доступу на маршрутизаторі:

```
Router (config)#access-list 101 deny ip 172.18.6.0 0.0.0.15 any
```

```
     Router (config)#access-list 101 deny ip 172.205.6.16 0.0.0.15
any
     Router (config)#access-list 101 permit ip 172.205.6.32 0.0.0.7
any
     Router (config)#access-list 101 deny ip 172.205.6.48 0.0.0.7
any
     Router (config)#access-list 101 deny ip 172.205.6.56 0.0.0.7
any
     Router (config)#access-list 101 deny ip 172.205.6.64 0.0.0.7
any
     Router (config)#access-list 101 permit ip 172.205.6.72 0.0.0.7
any
     Router (config)#access-list 101 deny ip 172.205.6.76 0.0.0.7
any
     ```
```

3. При налаштуванні з’єднання не потрібно встановлювати прапорець «Використовувати для виходу в Інтернет», тоді клієнт отримає інформацію про локальну мережу офісу, розташованої за сервером, автоматично. Це усуває необхідність у статичній маршрутизації. В поле «Тип (протокол)» вкажіть значення PPTP, а в поле «Підключатися через» залиште значення за замовчуванням. В поле «Адреса сервера» вкажіть публічну IP-адресу Інтернет-центру Cisco C819GW3 [58, с. 405].

**Висновки до розділу 3**

Отже, у розділі розглянуто процес проектування комп'ютерної мережі поштових відділень із застосуванням програмного засобу захисту транспортування даних на базі обладнання Cisco. Аналіз проведено за такими основними напрямками:

Проведено опис процесу вибору серверного обладнання для забезпечення функціонування програмного засобу захисту даних. Обговорюються критерії відбору, зокрема продуктивність, надійність та масштабованість серверів. Наголошується на важливості вибору серверного обладнання, яке відповідає вимогам корпоративної мережі та здатне забезпечити ефективну роботу програмного засобу.

Проаналізоване комутаційне обладнання, необхідне для інтеграції програмного засобу в інфраструктуру корпоративної мережі. Розглядаються
```

різні типи комутаторів, їх характеристики та можливості. Підкреслюється важливість надійного та високопродуктивного комутаційного обладнання для забезпечення безперебійної роботи мережі.

Нами розглядається процес розрахунку адресного простору IP-адрес для корпоративної мережі. Описуються методи планування та розподілу IP-адрес, що забезпечують ефективне використання адресного простору та підтримують масштабованість мережі. Описано процес побудови корпоративної мережі з використанням вибраного обладнання Cisco. Розглядаються етапи проектування мережі, включаючи вибір топології, налаштування обладнання та інтеграцію програмного засобу захисту даних. Описано ключові аспекти, які забезпечують надійну та безпечну роботу мережі.

Виконано розробку програмного засобу захисту транспортування даних, його функціональних можливостей та методів забезпечення безпеки. Описано процес інтеграції програмного засобу в корпоративну мережу та його налаштування для забезпечення захисту передавання даних. Наголошується на важливості використання сучасних методів шифрування та захисту даних для забезпечення конфіденційності та цілісності інформації.

Розглянуто особливості запуску програмного засобу та підключення інтернет-центру з використанням обладнання Cisco. Описано етапи налаштування інтернет-центру, підключення до мережі та забезпечення безпечного доступу до Інтернету.

У розділі детально проаналізовано процес проектування комп'ютерної мережі поштових відділень із застосуванням програмного засобу захисту транспортування даних на базі обладнання Cisco. Використання надійного серверного та комутаційного обладнання, правильний розрахунок адресного простору, побудова безпечної мережі та інтеграція програмного засобу захисту даних забезпечують високу ефективність та безпеку корпоративної мережі. Це дозволяє забезпечити захист конфіденційної інформації та надійну роботу поштових відділень.

ВИСНОВКИ

У дослідженні висвітлено різноманітні можливості корпоративних мереж та процес їх створення. Корпоративна мережа функціонує як об'єднуюча структура, що поєднує філії підприємства в спільний інформаційний простір, відображаючи його внутрішню організацію. Сучасні корпоративні мережі виконують не лише роль передавача даних, але й надають широкий спектр сервісів з передбачуваними характеристиками, що сприяє вирішенню стратегічних завдань підприємства.

Досліджено особливості віртуальних мереж передачі даних та використані технології в корпоративних мережах. Головна мета проєктування корпоративних мереж полягає у визначенні структури, складу апаратно-програмних засобів та організації їх функціонування.

Значною є необхідність захисту інформації при підключенні до мережі Інтернет. Під час розробки заходів захисту варто бути обережним, оскільки вони можуть ускладнювати користування мережею та зменшувати зручність для користувачів. Обрані методи захисту, такі як NAT-перетворення, PAT, ACL, демілітаризована зона та інші, мають свої обмеження та області ефективного застосування.

У практичній частині досліджено основні етапи проєктування комп'ютерної мережі на базі обладнання Cisco. Визначено необхідне обладнання та оптимальні способи його конфігурування для забезпечення програмного захисту транспортування даних у мережі.

Також розглянуто практичні аспекти налаштування з'єднання з Інтернетом через встановлення серверу PPTP. Використання Cisco C819GW 2 і Cisco C881G дозволяє користувачам безпечно отримувати доступ до ресурсів у мережі, забезпечуючи високий рівень безпеки та зручності використання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абдулов Ф. З. Побудова IP-мережі на базі обладнання Cisco / Ф. З. Абдулов; наук. кер. Л. Р. Чупахіна. Київ: Комп'ютер юніті, 2019. 73 с.
2. Азаров О. Д. Комп'ютерні мережі: навчальний посібник. О. Д. Азаров, С. М. Захарченко, О. В. Кадук. Вінниця: Вінницький Національний Технічний Університет, 2013. 371 с.
3. Альтман Е. А. Проєктування корпоративної мережі. Е. А. Альтман, А. Г. Малютин. Донецьк: 2014. 22 с.
4. Альтман Е. А. Комп'ютерні мережі на базі обладнання компанії Cisco. Е. А. Альтман. Донецк: 2013. 32 с.
5. Бабаш А. В. Інформаційна безпека. Лабораторний практикум: підручник / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. Київ: КноРус, 2013. 136 с.
6. Білов Т. А. Безпека корпоративних мереж. Т. А. Білов. Харків: 2018. 512 с.
7. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. В. Л. Бурячок, Г. М. Гулак. Київ: ДУТ, 2015. 449 с.
8. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. В. Л. Бурячок, А. О. Аносов. Київ: КУБГ, 2019. 218 с.
9. Волков І. О. Економіка підприємства: підручник. І. О. Волков. Київ: ІНФРАМ, 2015. 416 с.
10. Білов П. В. Організація захисту мережі від мережевих загроз. П. В. Білов; наук. кер. А. Ю. Криштофович. Київ: Комп'ютер юніті, 2019. 99 с.
11. Виханов Д. А. Організація захисту корпоративної мережі підприємства. Д. А. Виханов; науч. рука. А. Ю. Криштофович. Київ: Комп'ютер юніті, 2019. 81 с.
12. Гатчин Ю. А. Теорія інформаційної безпеки та методологія захисту інформації. Ю. А. Гатчин. Донецьк, 2010. 98 с.
13. Гафнер В. В. Інформаційна безпека: підручник. В. В. Гафнер. Рн. Донецьк: Фенчкс, 2010. 324 с.
14. Гіленберг О. С. Розробка системи аналізу та підвищення захищеності корпоративної мережі. О. С. Гіленберг. Київ: Комп'ютер юніті, 2019. 82 с.

15. Громов Ю. Ю. Інформаційна безпека та захист інформації: підручник. Ю. Ю. Громов. Київ: ТНТ, 2010. 384 с.
16. Дятибратов А. П.; Гудино, Л. П.; Кириченко, А. А. Обчислювальні системи, мережі та телекомунікації. Фінанси і статистика. Київ, 2013. 512 с.
17. Зав'ялов А. В. Моделювання мереж пакетної комутації на основі обладнання Cisco. А. В. Зав'ялов. Київ: Комп'ютер юніті, 2018. 48 с.
18. Зегжда Д. П. Основи безпеки інформаційних систем. Д. П. Зегжда, А. М. Івашко. Київ: Гаряча лінія – телеком, 2009. 452 с.
19. Ідіятулліна А. С. Застосування критеріїв згоди при аналізі мережевого трафіку. А. С. Ідіятулліна. Київ: Комп'ютер юніті, 2018. 94 с.
20. Комп'ютерні мережі. Навчальний курс: Офіційний посібник Microsoft із самостійного темпу навчання: [пер. з англ.] – 5-е вид. Корпорація Майкорософт. Київ, 2015. 410 с.
21. Корнєв В. А. Проєктування захищеності фрагмента корпоративної мережі Ethernet. В. А. Корнєв. Київ: Комп'ютер юніті, 2019. 73 с.
22. Кравець С. В. Розробка методу захисту корпоративної мережі від використання користувачем глобальних ресурсів не за призначенням. Вінниця: ВНТУ, 2014. 80 с.
23. Кузін А. В. Комп'ютерні мережі. А. В. Кузін. Київ: 2015. 256 с.
24. Кузьменко Н. Г. Комп'ютерні мережі та мережеві технології. Н. Г. Кузьменко. Київ: Наука і техніка, 2013. 368 с.
25. Кульгін М. В. Корпоративні мережеві технології. М. В. Кульгін. Донецьк: ДОННТУ, 2009. 704 с.
26. Кульгін М. В. Технологія корпоративних мереж. М. ВБ. Кульгін. Київ: Мережі, 2014. 541 с.
27. Куроуз Д. Комп'ютерні мережі. Спадний підхід. Д. Куроуз, К. Росс. Київ: Освіта, 2016. 912 с.
28. Курушин В. Д. Комп'ютерна злочинність та інформаційна безпека. В. Д. Курушин. Київ: Новий юрист, 2012. 256 с.

29. Малюк А. А. Впровадження в інформаційну безпеку в автоматизованих системах. А. А. Малюк, С. В. Пазинин. Київ: Освіта. 2001. 148 с.
30. Нугман М. Розробка методики аналізу трафіку локальної обчислювальної мережі. М. Нугман; науч. рука. В. Г. Карташевський. Київ: Освіта, 2018. 70с.
31. Оліфер В. Г. Стратегічне планування загальнокорпоративних мереж. В. Г. Оліфер, Н. А. Оліфер та ін., 3 вид. Київ: Освіта. 2010. 680 с.
32. Оліфер В. Г. Комп'ютерні мережі: принципи, технології, протоколи. В. Г. Оліфер, Н. А. Оліфер та ін., 4 вид., Київ: Освіта, 2012. 958 с.
33. Оліфер В. Г. Нові технології та обладнання IP-мереж. В. Г. Оліфер, Н. А. Оліфер. Київ: Освіта, 2012. 512 с.
34. Оліфер В. Г. Мережеві операційні системи. В. Г. Оліфер. Київ: Освіта, 2016. 544 с.
35. Основи комп'ютерних мереж. Б. Д. Виснадул, С. А. Лупин. С. В. Сидоров, П. Ю. Чумаченко. Під ред. Л. Г. Гагаріної. Київ: Програміст. 2007. 272 с.
36. Палмер М. Проєктування та впровадження комп'ютерних мереж. М. Палмер, Р. Б. Синклер. Київ: Програміст, 2004. 752 с.
37. Панфілов К. В. Аналіз систем моніторингу мережевого обладнання мережі передачі даних. К. В. Панфілов. Київ: Комп'ютер юніті, 2019. 96 с.
38. Прончук П. Б. Комп'ютерні комунікації. Найпростіші обчислювальні мережі: Навчальний посібник. П. Б. Прончук. Київ: Програміст, 2009. 64 с.
39. Редько В. Н.; Басараб, І. А. Бази даних та інформаційні системи; Знання, 2013. 150 с.
40. Ретана А. Принципи проєктування корпоративної IP-мережі. А. Ретана, Д. Слайс, Р. Уайт, пер. з анг. Київ: Освіта, 2012. 368 с.
41. Романчук В. І. Дослідження імовірнісних властивостей трафіку корпоративної мультисервісної мережі. В. І. Романчук, О. А. Лаврів, В. В. Червенець, Р. І. Бак. Радіоелектроніка та телекомунікації. Львів: Видавництво Львівської політехніки, 2011. С. 128–134.

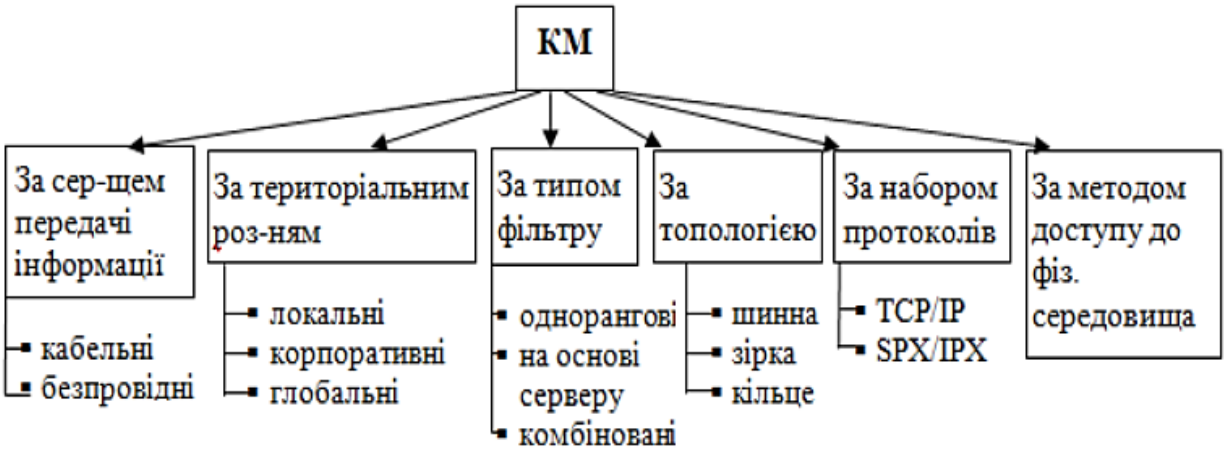
42. Севастьянов Е. Н. Проєктування захищених мереж зв’язку. Е. Н. Севастьянов. Київ: Комп’ютер юніті, 2019. 71 с.
43. Семенів А. Б. Проєктування та розрахунок структурованих кабельних систем та їх компонентів. А. Б. Семенів. Київ: Освіта, 2014. 416 с.
44. Семенів А. Б. Структуровані кабельні системи. А. Б. Семенів та ін. вид. 3 перероб. і доп. Київ: Освіта, 2013. 607 с.
45. Семенів А. Б. Волоконна оптика в локальних і корпоративних мережах. А. Б. Семенів. Київ: Програміст, 2016. 327 с.
46. Семенів А. Б. Структуровані кабельні системи Айті-СКС. А. Б. Семенів. Київ: Програміст, 2014. 269 с.
47. Семенів М. І. Автоматизовані інформаційні технології в економіці: Підручник. М. І. Семенів. Донецьк: Фінанси і статистика, 2014. 476 с.
48. Соколов А. В. Захист від комп’ютерного тероризму. А. В. Соколов. Донецьк: ДОННТКУ, 2015. 380 с.
49. Таненбаум Е. Комп’ютерні мережі. 5-е видання. Е. Таненбаум. Донецьк: Свічадо, 2012. 992 с.
50. Тарахнов І. Г. Проєктування і побудова бюджетної структурованої комп’ютерної мережі. І. Г. Тарахнов; наук. кер. І. В. Ротенштейн. Київ: Комп’ютер юніті, 2018. 84 с.
51. Титаренко Г. А. Автоматизовані інформаційні технології в економіці: Підручник. Г. А. Титаренко. Київ: Комп’ютер юніті, 2013. 400 с.
52. Шиндер Л. Д. Основи комп’ютерних мереж. Л. Д. Шиндер. Київ: Комп’ютер юніті: 2015. 152 с.
53. Федотов Е. Д. Аналіз характеристик сенсорних мереж. Е. Д. Федотов; наук. кер. Б. Я. Ліхтциндер. Донецьк: Свічадо, 2019. 135 с.
54. Філімонов А. Ю. Побудова мультисервісних мереж Ethernet: підручник. А. Ю. Філімонов. Київ: Програміст, 2015. 248 с.

55. Фурашев В. М. Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів. В. М. Фурашев, Д. В. Ланде. *Правова інформатика.* 2009. № 2 (22). С. 49–57.
56. Хоменко В. Г., Павленко М. П. Комп'ютерні мережі: Навчальний посібник. В. Г. Хоменко, М. П. Павленко. Донецьк: ЛАНДОН-ХХІ, 2011. 316 с.
57. Шаньгін В. Захист інформації в комп'ютерних системах та мережах. Шаньгін Донецьк: Свічадо, 2013. С. 65.
58. Експлуатація об'єктів мережевої інфраструктури: підручник для школярів. А. В. Назаров, В. П. Мельников; під кер. А. В. Назарова. Київ: Освіта, 2014. 538с.
59. Sukhov A. M. Active flows in diagnostic of troubleshooting on backbone links. A. A. Galtsev, A. M. Sukhov. *Journal of High Speed Networks*. 2011. Vol. 18. №. 1. P. 69–81.
60. Бездротова точка доступу. URL: https: // uk. wikipedia. org / wiki / Бездротова точка доступу. (дата звернення: 05.06.2024).
61. Cisco – Центр підтримки URL: https: // help. Cisco. net / (дата звернення: 05.06.2024).

ДОДАТКИ

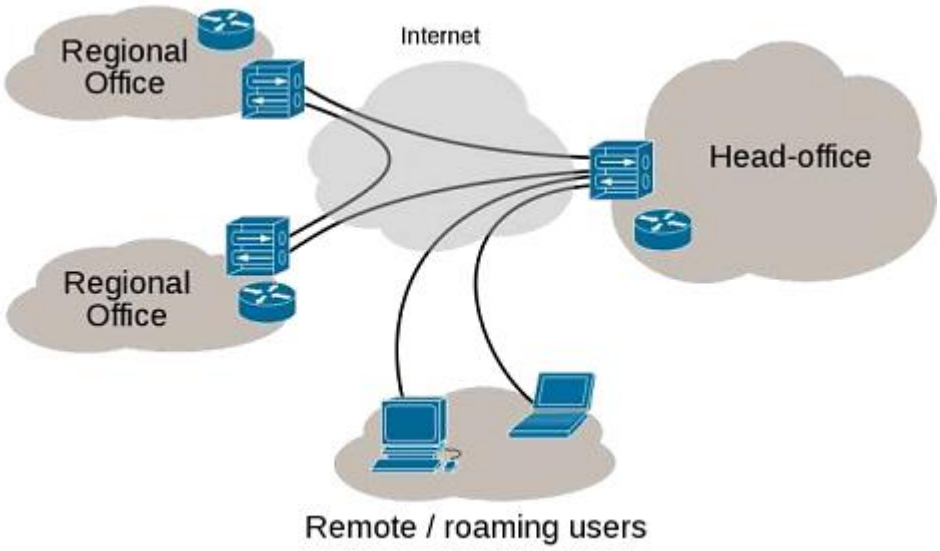
Додаток А

Класифікація корпоративних мереж



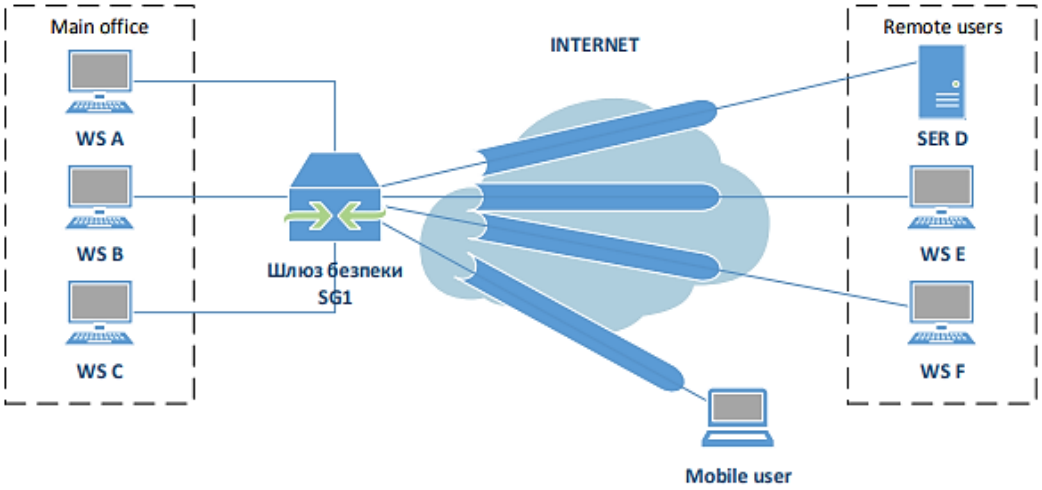
Додаток Б

Схематичне зображення віртуальної мережі передачі даних



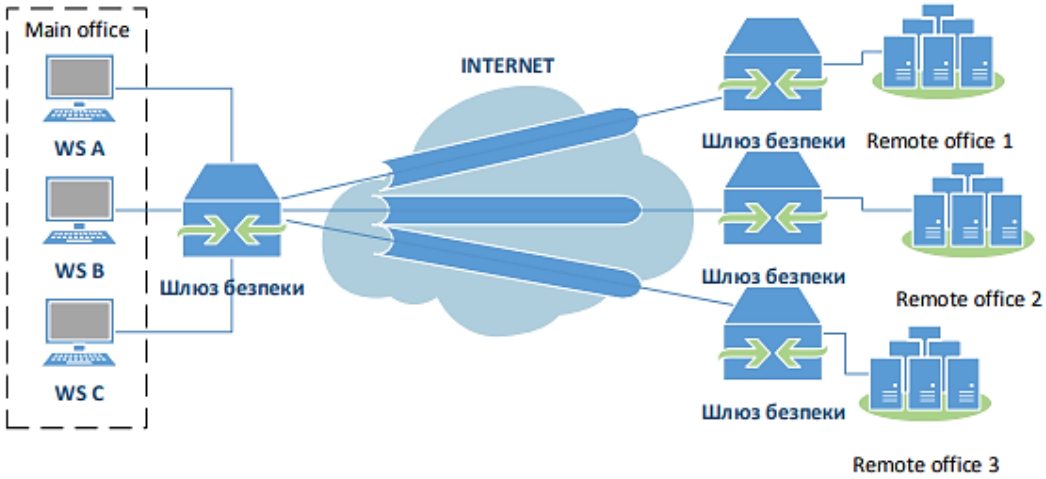
Додаток В

Віртуальна корпоративна мережа з віддаленим доступом



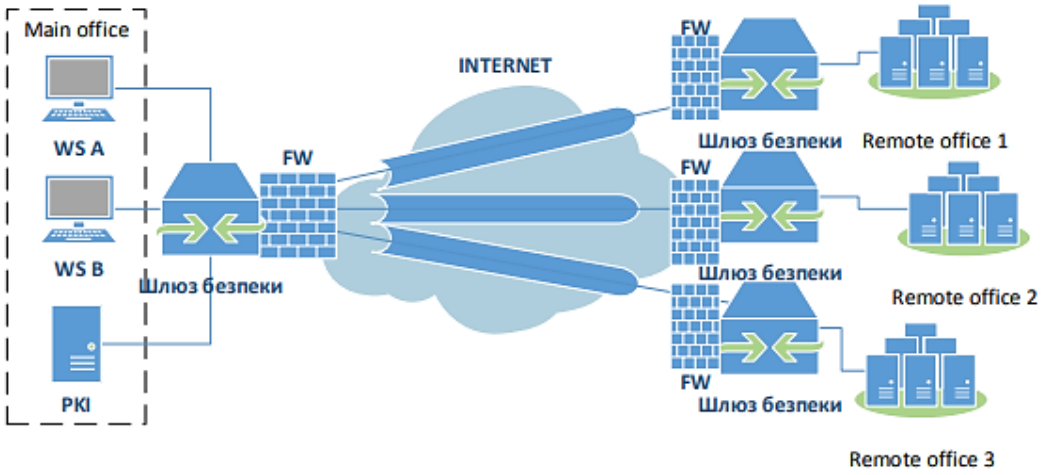
Додаток Г

З’єднання вузлів мережі за допомогою технології Intranet VPN



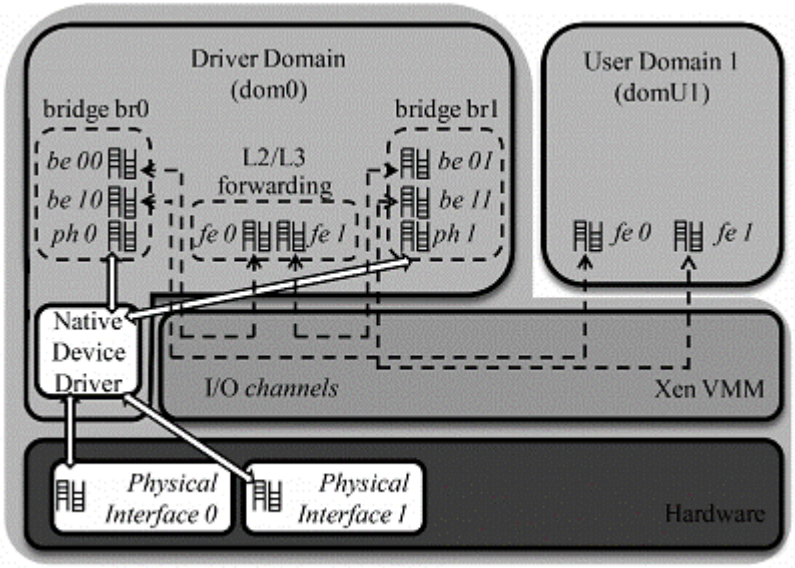
Додаток Д

Міжкорпоративна мережа Extranet VPN



Додаток Ж

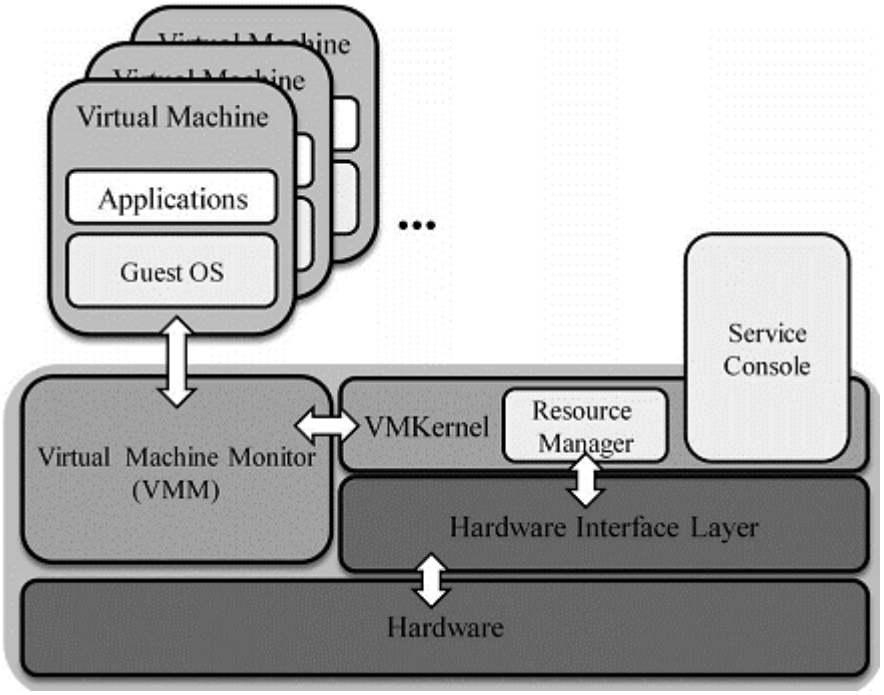
Схематичне зображення архітектури Xen



fe – front-end interface , be – back-end interface , ph – physical interface

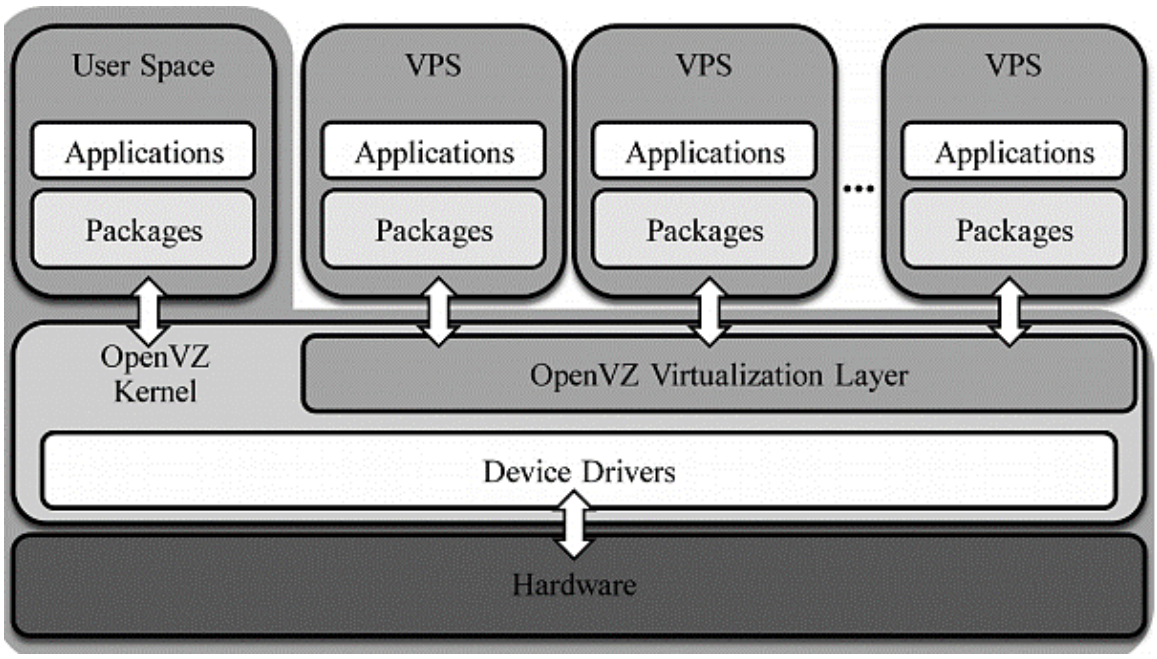
Додаток З

Схематичне зображення архітектури VMware



Додаток Є

Схематичне зображення архітектури OpenVZ



Додаток Е

Програмний код для налаштування захисту транспортування даних у мережі на обладнанні Cisco

```
// налаштування ACL
function configureACL {
// Підключення до мережевого пристрою Cisco
const Cisco = connectToCisco;
// Налаштування правил ACL
Cisco. configureACL({
sourceIP: '192.168.0.0 / 24',
destinationIP: '10.0.0.0 / 24',
protocol: 'tcp',
action: 'allow',
});
// Збереження налаштувань
Cisco. saveConfiguration;
}
// Налаштування NAT
function configureNAT {
// Підключення до мережевого пристрою Cisco
const Cisco = connectToCisco;
// Налаштування правил NAT
Cisco. configureNAT({
internalIP: '192.168.0.100',
externalIP: '1.2.3.4',
});
// Збереження налаштувань
Cisco. saveConfiguration;
}
// Нналаштування PAT
function configurePAT {
// Підключення до мережевого пристрою Cisco
const Cisco = connectToCisco;
// Налаштування правил PAT
Cisco. configurePAT({
internalIP: '192.168.0.100',
internalPort: 8080,
externalPort: 80,
});
// Збереження налаштувань
Cisco. saveConfiguration;
}
// Виклик функцій для налаштування захисту
configureACL;
configureNAT;
configurePAT;
```