ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка
до магістерської роботи
на тему:

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

Виконав: студент 6 курсу, групи БСДМ - 63
Спеціальності 125 «Кібербезпека»
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Завадський В.В.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ВСТУП

Актуальність дослідження. Комп'ютерні мережі в сучасну епоху є найпоширенішою річчю. Переважно все стає цифровим, і для виконання цих операцій на комп'ютері потрібна комп'ютерна мережа, а основою комп'ютерних мереж є компонент комп'ютерної мережі, який будує ці комп'ютерні мережі. Як і маршрутизатори, медіа тощо, без цього неможливо побудувати комп'ютерну мережу.

Щоб створити мережевий дизайн, який приносить цінність бізнесу та відповідає його цілям і напрямкам, розробники мереж повинні дотримуватися структурованого підходу. Цей підхід повинен починатися з верхнього рівня, зосереджуючись на бізнес-потребах, рушійних факторах і напрямках, щоб створити дизайн, орієнтований на бізнес. Крім того, за допомогою низхідного підходу розробники та архітектори мереж завжди можуть створювати керовану бізнесом мережеву архітектуру, яка полегшує на наступних етапах вибір бажаних апаратних платформ, технологічних функцій і протоколів для розгортання запланованого дизайну. Це робить мережевий дизайн більш чутливим до будь-яких нових вимог бізнесу або технологій. Крім того, розгляд різних принципів проектування, розглянутих у цьому розділі, і врахування різних вимог (бізнес, функціональні та критично важливих додатків) може допомогти розробникам мережі спланувати та зробити правильний вибір дизайну, який зрештою змусить мережу розглядатися як « сприяння розвитку бізнесу».

Ці вимоги обумовлюють потребу в уніфікованому наскрізному управлінні, яке дозволяє мережевим командам мати повну видимість середовища та здатність керувати ним більш ефективно. Наскрізна уніфікація також призведе до швидшого часу усунення несправностей, підвищення доступності, гнучкості та розширеного досвіду. Прикладом такої є об'єкт дослідження роботи Cisco AVVID.

Безпека корпоративної мережі - це не те, що можна організувати за загальною схемою, яка однаково підходить для будь-якої компанії. Вибір видів діяльності з

кібербезпеки має залежати від розміру компанії, її бюджету та сфери діяльності. Тому, метою даної роботи буде визначення проблеми вразливостей корпоративних мереж та створити безпечні умови з використанням Cisco AVVID.

Для забезпечення кіберзахисту невеликої корпоративної мережі, якщо немає необхідності захищати персональні або фінансові дані своїх клієнтів, цілком достатньо застосування брандмауера та антивірусів. Однак, якщо компанія займає відносно значне місце в регіоні, де вона працює, і може легко стати мішенню для кібератак, вона повинна бути готова розширити заходи кібербезпеки та застосувати безпеку електронної пошти, сегментацію мережі, безпеку кінцевих точок тощо. Встановлення DLP і Системи SIEM також можуть стати обов'язковими, особливо для організацій, які здійснюють свою діяльність у регульованих галузях за допомогою Cisco AVVID.

Забезпечення безпеки корпоративної інформаційної системи є пріоритетним завданням для керівництва компанії, оскільки від збереження конфіденційності, цілісності та доступності корпоративних інформаційних ресурсів багато в чому залежить оперативність прийняття рішень та ефективність діяльності компанії, тому забезпечення безпеки такої компанії буде практичним завданням в цій роботі, включаючи об'єкт дослідження Cisco AVVID.

Об'єкт дослідження – корпоративні мережі та Cisco AVVID.

Предмет дослідження – технології та засоби забезпечення безпеки корпоративних мереж.

Мета роботи – створити безпечні умови корпоративній мережі з використанням Cisco AVVID.

Завдання:

- визначити основні компоненти та властивості комп'ютерних мереж, вимоги до розробки великомасштабних мереж для задоволення сучасного динамічного бізнесу та IT-потреб і тенденцій;

- проаналізувати заходи безпеки для корпоративних мереж, найпоширеніші загрози мережевій безпеці з урахуванням сучасних тенденцій;

- дослідити надійність та відмовостійкість у корпоративній комп’ютерній мережі;

- розглянути компоненти мережевої інфраструктури Cisco AVVID та налаштування безпеки для корпоративної мережі;

- дослідити стратегії Cisco AVVID та SAFE для захисту корпоративних мереж.

Практичне значення одержаних результатів. Результат та рекомендації по налаштуванню безпеки в Cisco AVVID у межах корпоративної мережі. Стратегії Cisco AVVID та SAFE можуть бути використані як підхід глибокого захисту до проектування безпеки корпоративної мережі будь-якою організацією, зацікавленою у безпеці комп’ютерної мережі.

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

Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., ст. 69-70.

1 ПОБУДОВА КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ПІДПРИЄМСТВ ТА АНАЛІЗ КОРПОРАТИВНОЇ СТРУКТУРИ

1.1 Основні компоненти та властивості комп'ютерних мереж

Компонентами комп'ютерної мережі називають фізичні пристрої, програмне забезпечення, середовища тощо, які разом необхідні для успішного встановлення зв'язку між обчислювальними пристроями.

Перш ніж розуміти компоненти комп'ютерної мережі, спочатку зрозуміємо, що таке комп'ютерна мережа.

Комп'ютерна мережа – це взаємозв'язок двох або більше комп'ютерних пристроїв для зв'язку один з одним і обміну даними. Такими обчислювальними пристроями можуть бути пристрої Інтернету речей, смартфони, планшети, ноутбуки тощо, і спосіб їх підключення залежить від середовища, наприклад бездротового або дротового.

З точки зору програмного забезпечення, програми, які ми використовуємо щодня, як-от браузер, WhatsApp, електронна пошта тощо, — це все програмне забезпечення, яке використовує комп'ютерні мережі у фоновому режимі для обміну даними з іншими комп'ютерами. Апаратне та програмне забезпечення працюють разом, щоб забезпечити успішний зв'язок між комп'ютерами та утворити комп'ютерну мережу.

У сучасному світі Інтернет став дуже популярним. Це стає дуже важливим для спілкування. Отже, ІНТЕРНЕТ (міжнародна мережа) — це не що інше, як велика кількість обчислювальних пристроїв, з'єднаних для обміну даними між собою. Це може бути найкращим прикладом комп'ютерної мережі.

Мережа — це з'єднання обчислювальних пристроїв, з'єднаних через середовище для обміну даними.

Мережею можна назвати це, коли відбувається зв'язок між мережевими пристроями за допомогою набору протоколів.

Компоненти комп’ютерної мережі — це частини (апаратні пристрої, програмне забезпечення або середовище) обчислювальних пристроїв, які допомагають формувати комп’ютерну мережу. Є 3 різні компоненти комп’ютерної мережі – вузол, медіа та послуги.

Вузол може бути комп’ютером, принтером або будь-яким іншим пристроєм, здатним надсилати та отримувати дані, створені іншими вузлами в мережі. Приклад – комп’ютери, маршрутизатори, концентратори/комутатори тощо.

Медіа — це середовище передачі, яке з’єднує різні вузли та допомагає передавати дані, що надсилаються від одного вузла до іншого в мережі. Приклад – WiredorWireless.

Послуги - це діяльність, яка може бути реалізована за допомогою комп'ютерної мережі. Приклад – веб-серфінг, електронна пошта, чат тощо.

Для побудови комп’ютерної мережі це надмножина основних компонентів. І вони пов’язані з обладнанням. І за допомогою цього можна побудувати комп’ютерну мережу. Тепер після створення з’єднання спільний доступ до ресурсів може відбуватися ефективно за допомогою програмних компонентів, які називаються протоколами.

Таким чином, термін «Протоколи» — це не що інше, як набір правил, які повинен узгодити кожен вузол мережі для успішної передачі даних.

А в реальному світі комп’ютерна мережа має низку протоколів, які дотримуються для передачі даних у мережі, як модель TCP/IP.

1. Вузол. Вузол — це обчислювальний пристрій, підключений для обміну даними через мережу. Вузлами можуть бути будь-які пристрої, які приймають і передають дані через мережу для успішного зв’язку. Приклад – ноутбук, смартфон, маршрутизатор тощо. Вузли також поділяються на два типи – кінцеві та проміжні.

Кінцеві вузли – це ті вузли, які є або початковою точкою зв’язку, або кінцевою точкою зв’язку. Якщо два пристрої A та B хочуть спілкуватися один з одним, то пристрій, який ініціює з’єднання, та інший пристрій, який отримує з'єднання є кінцевим вузлом. Ці пристрої спілкуються один з одним за допомогою проміжних вузлів [1].

Приклад – доступ до Інтернету. Таким чином, пристрій, з якого запитується веб-сайт, є кінцевим вузлом, а сервер, який відповідає веб-сторінкою, є кінцевим вузлом.

Комп’ютер також є кінцевим вузлом. Персональні комп'ютери є основоположниками мережі. Це вихідний вузол, який запитує дані, а на іншому кінці дані обробляються персональним комп’ютером.

Мережеві принтери – мережевий принтер також є кінцевим вузлом, оскільки він обробляє друк повідомлення, отриманого з комп’ютера.

Телефони VoIP – (протокол передачі голосу через Інтернет) перетворюють електричний сигнал у звук також є кінцевим вузлом. Можна назвати його новітнім мобільним телефоном, який підтримує послугу VoLTE (Voice Over Long term Evolution), яка використовується в мережах 4G для передачі дзвінка через Інтернет-протокол.

Кінцеві точки телеприсутності – цей пристрій також є кінцевим вузлом. І в основному він використовується для відеоконференцій. Здебільшого він використовується на зустрічах у великих компаніях, щоб учасники могли приєднатися до зустрічі віртуально.

Камери безпеки – вони безпосередньо займаються захопленням середовища та процесу, тому їх також можна розглядати як кінцевий вузол. Ці пристрої більш популярні та широко використовуються в реальному світі. Як-от банкомати, транспортні засоби, лікарні тощо.

Мобільні портативні пристрої – такі пристрої, як смартфони, КПК, планшети, пристрої для зчитування дебетових/кредитних карток тощо, також є кінцевим вузлом. Це звичайні пристрої, які зазвичай використовують користувачі. Це також кінцевий вузол, оскільки запит походить від нього, і отримані дані завершуються тут.

Проміжні вузли діють як посередники для передачі повідомлень або даних від одного вузла до іншого. Вони також називаються вузлами маршрутизації. Іншими словами, можна сказати, що проміжні вузли - це вузли, розміщені між кінцевими вузлами.

Якщо відкрити веб-сторінку в Інтернеті, пристрій і сервер вважаються кінцевими вузлами, а маршрутизатори, з яких надходить трафік, є проміжними вузлами

Повторювачі – має 2 порти, один для прийому сигналів, а інший – для надсилання сигналів, і він використовується для посилення потужності сигналу.

Є 2 різні вузли, і повторювач отримує сигнал від одного вузла, копіює сигнал з його початковою частотою та надсилає його до наступного вузла.

HUB – це не що інше, як багатопортовий повторювач. Це точно поводиться як повторювач. Але різниця лише в тому, що він копіює дані, які отримує з одного порту, і копіює їх на всі порти, які підключилися до нього.

Існує два типи HUB – I. Активний концентратор – має власне джерело живлення. I може більш точно копіювати сигнал на інші вузли, з якими він підключений. II. Пасивний концентратор – він не має власного джерела живлення, тому не може повторити сигнал, він просто передає сигнали.

Міст – це інтелектуальний пристрій, який може переглядати дані, які він отримує в сигналі, і може ідентифікувати, якому комп'ютеру належать дані. Він фільтрує дані на основі MAC-адрес. Це двопортовий пристрій, який використовується для підключення 2 локальних мереж (локальної мережі).

Існує два види мостів – 1. Прозорий міст – це простий міст, який просто передає дані з однієї локальної мережі в іншу. 2. Міст вихідної маршрутизації – він передає дані, враховуючи пакет даних, яким шляхом слідувати, щоб пакет досягнув місця призначення.

Комутатор – це не що інше, як багатопортовий міст. Комутатори - дуже розумні пристрої. Він має так званий буфер, який є нічим іншим, як тимчасовою пам'яттю. А також мають деяку обчислювальну потужність, яка є сьогодні

Він фільтрує дані на основі MAC-адрес і допомагає спрямувати пакет до вузла призначення.

Маршрутизатори – це найрозумніший пристрій, який широко використовується в наш час. Він зчитує дані про те, до якого мережевого розташування він належить. А потім передає дані на основі IP-адреси.

Він з’єднує кілька локальних і глобальних мереж. Це допомагає цим маршрутизаторам маршрутизувати пакет у мережі. Він направляє пакет до місця призначення, і досягає цього за допомогою таблиць маршрутизації. Він містить усі відомості про найближчі маршрутизатори, які допомагають передати пакет, щоб він міг досягти пункту призначення.

Бмаршрутизатори (Brouters) – це комбінація Bridge + Routers. Оскільки маршрутизатори працюють на мережевому рівні моделі TCP/IP, а міст працює на рівні каналу даних моделі TCP/IP. Таким чином, маршрутизатори працюють на обох цих рівнях і можуть виконувати завдання обох пристроїв.

Інші – Існують інші проміжні вузли, наприклад – вежа стільникового зв’язку, брандмауери (пристрої безпеки), точки бездротового доступу тощо.

2. Медіа. Його називають середовищем, через яке передається сигнал між вузлами. Його також можна назвати ланкою між вузлами. Медіа є основою, яка забезпечує підключення вузлів. Його поділяють на два різні типи:

Дротове медіа має фізичний дріт, який забезпечує зв’язок між вузлами. Його також називають керованим середовищем. Для передачі сигналів використовувалися різні види дротових носіїв.

Кабель з витою парою – він винайдений для телефонних ліній. А раніше більшість комп’ютерних мереж побудовані на самій телефонній мережі, і це робиться за допомогою модемів. Кабелі з витою парою дуже тонкі, дешеві та легко ламаються. Він містить кілька скручених проводів.

В основному він призначений для невеликих відстаней. Зазвичай на відстані менше 100 метрів.

Екранована вита пара – це покращений кабель вита пара, який використовувався в основному для передачі даних через телефонні лінії. Скручені дроти екрановані алюмінієвим екраном, який допомагає уникнути втрати даних і допомагає передавати дані на великі відстані. Хоча він також не здатний обробляти дані великого розміру та не може охопити велику відстань. Він може працювати на відстані до 100 метрів.

Коаксіальний кабель – має один провід з дуже високою ємністю. Він має провідник, загорнутий в ізоляцію, яка, у свою чергу, покрита дротяною сіткою, яка запобігає електричним перешкодам. Коаксіальний кабель дозволяє передавати багато каналів одночасно, що усуває потребу в тисячах окремих проводів. Більшість компаній кабельного телебачення використовують коаксіальний кабель для передачі багатьох каналів передплатного телевізійного програмування в помешкання. Коаксіальний кабель також популярний у локальних мережах, які постачальники послуг Інтернету також використовують для підключення до Інтернету. Це дорожче, а також може подолати відстань майже в 1 кілометр.

Волоконно-оптичний кабель. Оптоволоконний кабель або OFC має вищу пропускну здатність і може передавати великі дані. Він використовував світловий промінь для передачі даних від джерела до місця призначення. Це в основному використовується в наш час. Інтернет-кабелі, які йдуть до моря, мають оптоволоконний кабель. Він має дуже мало магнітних перешкод. Це дуже дорого і може становити від 1 км до 10 км.

У бездротовому середовищі дані передаються без фізичного проводу. Можна сказати, що дані передаються по повітрю. Його також називають некерованим середовищем. Використовувались різні типи бездротових носіїв:

Інфрачервоне випромінювання – це тип електромагнітного сигналу, який здебільшого використовується в системах дистанційного керування, таких як телевізор, система змінного струму тощо. Вони охоплюють невелику відстань, і сигнал переривається, якщо між ними з’явиться будь-яка перешкода. Це означає, що він не може пробити стіни. Він містить інфрачервоний передавач і приймач.

Мікрохвильова (радіочастота) – це також бездротове середовище передачі, яке використовується для передачі сигналів від одного вузла до іншого. Він використовує сигнал радіохвиль для передачі сигналу. Він широко використовується в багатьох місцях, наприклад перевірка Fastag. Радіочастота також використовується мобільними вежами для зв'язку. Його радіус дії може варіюватися від 10 км до 100 км залежно від частоти.

Радіо (Wi-Fi) – WiFi означає точність бездротового зв’язку. Здебільшого він використовується для спільного доступу до Інтернету. Він також використовував радіохвилі у формі сигналу, який використовується для передачі даних. Це канал зв’язку на короткій відстані, який використовується в будівлі чи кампусі.

Супутник – супутниковий зв’язок використовує штучні супутники для забезпечення зв’язку між різними точками на Землі. Супутниковий зв'язок відіграє життєво важливу роль у глобальній телекомунікаційній системі. Супутниковий зв’язок складається з двох основних компонентів – наземного передавача та приймача та супутника, який обертається навколо Землі з космосу. Зв'язок встановлюється від відправника до одержувача за допомогою супутника.

3. Послуги. Комп’ютерні мережі пропонують багато послуг, якими широко користуються користувачі у повсякденному житті. Такі послуги як:

Електронна пошта – Електронна пошта (Електронна пошта) – це служба, яку підтримує комп’ютерна мережа. Користувачі можуть надсилати або отримувати текстові повідомлення, вкладення тощо від різних користувачів за допомогою служби електронної пошти. Деякі з найпопулярніших постачальників послуг електронної пошти – Gmail (Google Mail), Outlook (Microsoft Mail), Yahoo Mail тощо.

Зберігання – Зберігання також є послугою, яка активується за допомогою операційної системи. Це також можна назвати це хмарним сховищем. При цьому користувачі можуть зберігати свої дані в Інтернеті на платформі, наданій компаніями. Деякі з компаній, які надають хмарне сховище, – Google Drive, MEGA, OneDrive тощо.

Обмін файлами – комп’ютерна мережа дозволяє обмінюватися файлами. Це можна зробити за допомогою різних протоколів, які запущено для цього.

Обмін миттєвими повідомленнями – можна часто спілкуватись за допомогою різних програм, таких як WhatsApp. Месенджер і т.д. це послуги, які можливі за допомогою концепції комп’ютерної мережі.

Онлайн-ігри – не кожна комп’ютерна система задовольняє вимогам апаратного забезпечення для гри. Таким чином, послуги онлайн-ігор також

створюються за допомогою концепції комп’ютерних мереж. Гра працює на стороні сервера, а контент доставляється користувачеві за допомогою комп’ютерної мережі.

Відеоконференції. Зараз відеоконференції є найпоширенішою послугою комп’ютерної мережі. Не тільки для особистого спілкування, а й для офіційних ділових зустрічей використовується відеоконференція. І це досягається за допомогою концепції комп'ютерної мережі.

World Wide Web – WWW також є найпоширенішим сервісом. У сучасному світі більшість речей робиться за допомогою Інтернету. А Інтернет (Міжнародна мережа) формується за допомогою комп’ютерної мережі.

1.2 Аналіз вимог до розробки мережі

Розробка великомасштабних мереж для задоволення сучасного динамічного бізнесу та IT-потреб і тенденцій є складним завданням, незалежно від того, чи це мережа корпоративного типу чи мережі постачальника послуг. Це особливо вірно, коли мережа була розроблена для технологій і вимог, відповідних багато років тому, і компанія вирішила застосувати нові IT-технології, щоб полегшити досягнення своїх цілей, але існуюча мережа компанії не була розроблена відповідно до вимог цих нових технологій. Тому, щоб досягти бажаної мети даного дизайну, розробник мережі повинен прийняти підхід, який розглядає проект у структурований спосіб [2].

Існує два поширених підходи до аналізу та проектування мереж:

■ Низхідний підхід: Низхідний підхід до проектування спрощує процес проектування, розділяючи завдання проектування, щоб зробити їх більш зосередженими на масштабах проектування та виконувати більш контрольованим способом, що зрештою може допомогти розробникам мереж переглядати рішення для проектування мережі. з бізнес-підходу.

■ Підхід «знизу вгору». Навпаки, підхід «знизу вгору» фокусується на виборі мережевих технологій і моделей проектування. Це може призвести до високого

ризику помилок у проектуванні, оскільки мережа не відповідатиме вимогам бізнесу чи додатків.

Щоб досягти успішного стратегічного дизайну, необхідно зробити додатковий акцент на бізнес-підхід. Це означає, що основна увага приділяється бізнес-цілям і технічним завданням на додаток до існуючих і майбутніх послуг і програм. Насправді в сучасних мережах бізнес-вимоги керують IT-і мережевими ініціативами.

Наприклад, хоча відповідність може здатися обмеженням дизайну, а не рушійною силою, сьогодні багато організацій прагнуть відповідати певним стандартам щодо своєї IT-інфраструктури та послуг, щоб отримати певні бізнес-переваги, наприклад відповідність вимогам ISO/IEC 27001 «Інформаційна безпека» [3]. Керівництво допоможе таким підприємствам, як організації, що надають фінансові послуги, продемонструвати свій авторитет і довіру. Зрештою це допоможе цим організаціям отримати більше конкурентних переваг, оптимізувати час безвідмовної роботи та зменшити операційні витрати (менша кількість інцидентів у результаті зменшення кількості порушень інформаційної безпеки).

Технічні вимоги до мережі можна розуміти як технічні аспекти, які мережева інфраструктура повинна забезпечувати з точки зору безпеки, доступності та цілісності [4].

Ці вимоги часто називають нефункціональними вимогами. Технічні вимоги відрізняються, і їх потрібно використовувати для обґрунтування вибору технології. Крім того, технічні вимоги вважаються найбільш динамічним типом вимог порівняно з іншими вимогами, такими як бізнес-вимоги, оскільки вони часто змінюються внаслідок технологічних змін. Технічні вимоги включають наступне:

- Підвищений рівень доступності мережі (наприклад, за допомогою протоколу резервування першого переходу)
- Підтримка інтеграції з мережевими інструментами та службами (наприклад, NetFlow Collector або система автентифікації та авторизації «сервери RADIUS»)

■ Забезпечення методів безпеки мережевої інфраструктури (наприклад, механізми захисту рівня керування або списки контролю доступу до інфраструктури)

1.3 Принципи проєктування мережі

Проектування мережі можна визначити як філософію, яка керує тим, як різні компоненти, протоколи та технології повинні бути інтегровані та розгорнуті на основі певних підходів і принципів для побудови згуртованого середовища мережевої інфраструктури, яке може сприяти досягненню тактичних або стратегічних бізнес-цілей [5].

Надійність і стійкість. Надійна мережа доставляє майже кожен прийнятий мережею пакет до потрібного пункту призначення протягом розумного періоду часу. У сучасних конвергентних мережах підтримка високонадійної мережі є надзвичайно важливою, оскільки сучасні підприємства значною мірою покладаються на IT-послуги для досягнення своїх бізнес-цілей. Для цих підприємств (особливо постачальників послуг і сучасних фінансових установ) може бути ще важливішим, щоб їхня мережа розглядалася як організація, що генерує дохід. Наприклад, п’ятихвилинний збій мережі, який може вплинути на кількість клієнтів, може коштувати компанії сотні тисяч доларів. Таким чином, наявність високонадійної та доступної мережевої архітектури, яка може вижити під час відмови будь-якого мережевого компонента без втручання оператора (також відома як відмовостійкість), є ключовим принципом проектування. Це вважається головним пріоритетом більшості сучасних компаній. Щоб мережа досягла бажаного рівня відмовостійкості, має існувати надлишковий компонент, щоб взяти на себе роль несправного компонента після події збою.

Модульність. Модульний дизайн зазвичай використовується в розробці програмного забезпечення, де додаток може бути створено з кількох блоків коду, які разом інтегруються, щоб сформувати потрібний додаток. Ці «будівельні блоки» модульної структури покращують і спрощують загальну архітектуру програми.

Наприклад, якщо проблема існує в одному блоці чи модулі цього програмного забезпечення, її можна легко відокремити від інших модулів і виправити окремо, не впливаючи на інші частини. Крім того, з точки зору поточних удосконалень легше додавати додаткові модулі або блоки до цієї структури, якщо потрібні нові функції. Це робить загальну архітектуру програми більш структурованою та керованою.

Подібним чином модульність є одним із фундаментальних принципів структурованої мережі. У структурованій мережі архітектуру мережі можна розділити на кілька функціональних модулів, причому кожен модуль виконує певну роль у мережі та представлений окремою фізичною мережею. Індивідуальна фізична мережа також відома як місця в мережі (PIN-код), наприклад кампус підприємства, WAN або центр обробки даних.

Отже, ці функціональні модулі легко відтворити, перепроектувати та розширити [6].

Дослідження показують, що при побудові IT-мережі близько 20 відсотків бюджету йде на придбання обладнання, а 80 відсотків — на експлуатаційні витрати. Наприклад, якщо мережа розроблена таким чином (наприклад, плоска), що не може ізолювати порушення безпеки, оновлення системи або збої в певних частинах мережі, вона не буде «достатньо швидкою», щоб адаптуватися до майбутніх бізнес-вимог, таких як як масштабованість і швидка мережева конвергенція [7].

У той час як за модульного підходу до проектування, якщо будь-який модуль стикається з проблемою, такою як порушення безпеки або додавання або видалення модулів, не повинно бути необхідності перепроектувати мережу або вносити будь-який вплив на інші модулі. Крім того, розбиття складних частин мережі на основі модульного підходу на керовані блоки оптимізує загальну керованість мережі. Іншими словами, з точки зору проектування мережі, модульність може сприяти простоті дизайну, гнучкості, ізоляції помилок і масштабованості.

Ізоляція несправностей і простота. Межі ізоляції несправності зазвичай розроблені для забезпечення поведінки безвідмовної зупинки для бажаної моделі

несправності. Термін «відмовна зупинка» означає, що неправильна поведінка не поширюється через межу ізоляції несправності. Іншими словами, проектування мережі має враховувати те, як запобігти повідомленню про збій в одному домені або поширенню на всі інші домени в мережі. Це необхідно, щоб уникнути непотрібної обробки та затримок у всій мережі через збій зв'язку або пристрою в одному домені мережі.

Наприклад, у проектуванні маршрутизації можна використовувати домени підсумовування та логічного перетоку, щоб пом'якшити цю проблему, де завжди рекомендується, щоб складні мережі (фізично або на рівні рівня керування) були логічно обмежені, кожна у своєму домені помилки.

Таким чином, буде більш стабільна, надійна та швидша конвергентна мережа.

Крім того, ця концепція спрощує загальну архітектуру та зменшує складність експлуатації. Загалом ізоляція помилок запобігає поширенню інформації про помилки мережі в кількох мережевих областях або доменах, що сприяє досягненню стабільнішого дизайну мережі та оптимізації часу відновлення мережі після будь-якої події збою мережі. Після цієї помилки може виникнути велика кількість непотрібної обробки [8].

Цьому обмеженому впливу сприяє розділення принципу «доменів помилок», якого зазвичай можна досягти шляхом логічного розділення (наприклад, приховування інформації про доступність і топологію Open Shortest Path First [OSPF] між доменами або блоками затоплення). Отже, дизайн зможе запропонувати вищий рівень масштабованості, стабільності та керованості.

1.4 Важливість уніфікованого керування мережею

Організації швидко розгортають високорозподілені сучасні середовища додатків, щоб підвищити гнучкість і здатність краще обслуговувати своїх клієнтів. Цей зсув відбувається завдяки ініціативам цифрової трансформації, які впливають на людські процеси та технології. Справді, «Опитування намірів щодо витрат на

технології у 2022 році» ESG показує, що понад дев’ять із 10 організацій (91%) починають, перебувають у процесі або мають зрілі ініціативи цифрової трансформації [9].

Дійсно, організації створюють розподілене хмарне середовище, розгортаючи сучасні програми в приватних центрах обробки даних, численних публічних хмарних службах – IaaS і SaaS – і периферійних місцях. У результаті загальнодоступний Інтернет швидко перетворюється на корпоративну мережу, а організації використовують програмно визначену WAN (SD-WAN) і широкосмугові підключення до цих розподілених середовищ.

У той же час мережеві команди повинні боротися з гібридними моделями роботи, які вимагають безпечного підключення з дому чи інших віддалених місць. Ці з’єднання мають бути не тільки безпечними, але й ефективними та забезпечувати постійний позитивний досвід, незалежно від того, де працівники вирішать працювати в той чи інший день.

Це дуже розподілене та динамічне середовище створює кілька проблем для мережі.

Складність впливає на здатність передавати позитивні враження

Незважаючи на те, що ці високорозподілені середовища є більш швидкими та чутливими, вони також є більш складними. Згідно з дослідженням Enterprise Strategy Group (ESG), більше половини респондентів (54%) сказали, що вважають, що мережеве середовище стало більш або значно складнішим, ніж два роки тому.

Складність мережі спричиняє не лише розподілений характер. Продукти керування мережею також сегментовано за їх роллю в організації та навіть за технологією. До них відносяться наступні сегменти.

Кілька доменів. Мережеві команди та технології були сегментовані на основі їх функцій. Мережі та команди центрів обробки даних часто відокремлюються від команд кампусу, філії, хмари та глобальної мережі. Традиційно ці сегменти можуть мати різні інструменти керування навіть від одного постачальника.

Мультивендор. Часто організація не хоче бути прив’язаною до певного постачальника технологій, натомість віддає перевагу найкращому підходу для

кожного домену мережі. Однак це вимагає від мережевих операційних груп вивчення додаткових інструментів керування та вручну кореляції інформації під час усунення несправностей. Також важко знайти команди з мережевих операцій, які мають навички від кількох різних постачальників.

Динамічні сучасні прикладні середовища. Зміни неминучі для мережевого середовища, і тенденція віртуалізації лише зростає з додатками на основі мікросервісів. Тепер мережеві служби потрібно вмикати та вимикати за лічені секунди, а не години, дні чи тижні.

Підтримка надомників. У той час, коли спалахнула пандемія COVID-19, мережеві команди відповідали за підключення до десятків або сотень — можливо, тисяч для великих організацій — віддалених сайтів. Однак, коли гібридні моделі роботи стають звичним явищем, ці мережеві команди тепер повинні забезпечити безпечне підключення до сотень, тисяч або навіть десятків тисяч віддалених працівників. Вони часто використовували застарілі служби VPN, які вимагали транспортування всього трафіку через центр обробки даних, що впливає на продуктивність [10].

Керування декількома різними інструментами керування впливає на ефективність роботи, оскільки вимагає від операторів використання поворотного крісла (перевертання для перегляду кількох екранів) і вручну кореляції подій. Це призводить до обмеження видимості всієї наскрізної мережі.

Раніше технологія керування мережею розгорталася локально, що все ще може бути вимогою для певних секторів. Локальне керування мережею може вплинути на можливість використання інструментів ШІ та машинного навчання (ML) і обмежити обсяг даних, що зберігаються для історичного аналізу.

Оскільки організації переходять на хмару, додається додаткова складність, оскільки вони повинні набути досвіду та навчитися керувати службами керування хмарними мережами для кожного постачальника хмар.

Загалом, ці фактори створюють значні проблеми для мережевих операційних груп, які працюють над тим, щоб не тільки підтримувати роботу існуючих мережевих середовищ, але й безперешкодно масштабувати мережу для розміщення

нових корпоративних сайтів, загальнодоступних хмарних служб або віддалених співробітників, забезпечуючи позитивний досвід і безпечне підключення.

Незважаючи на труднощі, пов’язані з традиційним або застарілим дизайном, майбутнє виглядає світлим. Постачальники мережевих технологій були свідками тих самих проблем зі своїми клієнтами та працюють над їх подоланням. Багато хто працює над наданням уніфікованих пропозицій для керування мережею. Ця концепція перегукується з організаціями, оскільки дослідження ESG підкреслило, що практично всі організації (99%) вважають, що уніфіковане наскрізне керування мережею є критичним, дуже важливим або дещо важливим. Більше чотирьох п'ятих (84%) респондентів сказали, що це критично або дуже важливо.

Постачальники реагують на це шляхом уніфікації частин мережі, причому найпоширенішими є уніфіковані дротові та бездротові мережі для розміщення кампусів. Дослідження ESG підтверджує цю тенденцію: 40% респондентів зазначили, що наразі мають уніфіковані дротові та бездротові мережі, а ще 48% планують об’єднати. Що стосується філії, постачальники, які мають технологію SD-WAN, йдуть ще далі й об’єднують дротові, бездротові та глобальні мережі, щоб підвищити ефективність роботи. Деякі постачальники створюють пропозиції, щоб поширити їх на домашніх працівників і зберегти їх у тій самій системі керування мережею.

Хмарні мережі — або, точніше, багатохмарні мережі — також спостерігають сплеск активності, коли кілька нових компаній пропонують можливість абстрагуватися від складності керування кількома загальнодоступними хмарами за допомогою єдиної уніфікованої консолі керування.

Іншим важливим досягненням для досягнення уніфікованого наскрізного управління є розширення використання хмарних служб керування мережею. Не плутати з наведеним вище хмарним або багатохмарним мережевим керуванням, хмарне мережеве керування — це концепція розгортання керування для локальних або навіть хмарних служб керування мережею в публічному чи приватному хмарному середовищі. Завдяки централізації керування мережею в загальнодоступній хмарі постачальники можуть отримати кілька переваг, зокрема:

полегшений доступ для віддалених співробітників; можливість консолідувати анонімні дані та створити репозиторій для технологій AI та ML; практично необмежене зберігання даних для історичного аналізу; єдине вікно для забезпечення наскрізної видимості; єдине розташування для інтеграції безпеки або обміну мережевою інформаціє; і використання AI та ML для підвищення ефективності роботи та автоматизації.

1.5 Топології комп'ютерних мереж

Топологія мережі – це схема з'єднання комп'ютерних систем або мережевих пристроїв між собою. Топології можуть визначати як фізичний, так і логічний аспект мережі. Як логічна, так і фізична топології можуть бути однаковими або різними в одній мережі [11].

Точка-точка. Мережі «точка-точка» містять рівно два хости, такі як комп'ютер, комутатори або маршрутизатори, сервери, з'єднані один до одного за допомогою одного кабелю. Часто приймальна сторона одного хоста з'єднана з відправною стороною іншого і навпаки.

Якщо хости з'єднані точка-точка логічно, то можуть мати кілька проміжних пристроїв. Але кінцеві хости не знають про базову мережу та бачать один одного так, ніби вони підключені напряму.

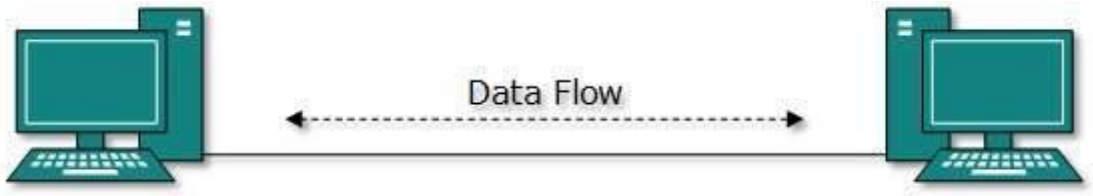

Рис.1.1. Точка-точка

Топологія шини. У випадку топології шини всі пристрої спільно використовують одну лінію зв'язку або кабель. Топологія шини може мати проблеми, коли кілька хостів надсилають дані одночасно. Тому для вирішення проблеми топологія шини або використовує технологію CSMA/CD, або розпізнає

один хост як головний. Це одна з простих форм мережі, коли збій пристрою не впливає на інші пристрої. Але збій спільної лінії зв'язку може призвести до припинення роботи всіх інших пристроїв.

Обидва кінці спільного каналу мають кінцеву лінію. Дані надсилаються лише в одному напрямку, і як тільки вони досягають крайнього кінця, термінатор видаляє дані з лінії.

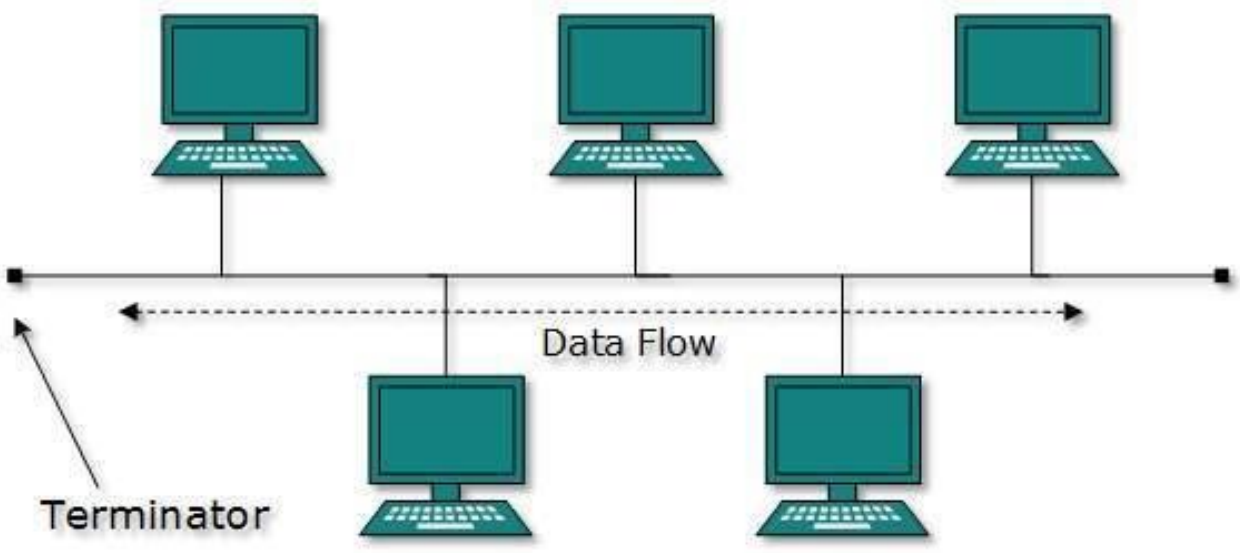

Рис.1.2. Топологія шини

Зоряна топологія. Усі хости в топології Star підключені до центрального пристрою, відомого як пристрій-концентратор, за допомогою з’єднання «точка-точка». Тобто між хостами та концентратором існує з’єднання «точка-точка». Пристроєм-концентратором може бути будь-який із наведених нижче пристроїв.

Пристрій рівня 1, наприклад концентратор або повторювач

Пристрій рівня 2, наприклад комутатор або міст

Пристрій рівня 3, наприклад маршрутизатор або шлюз

Як і в топології шини, концентратор діє як єдина точка відмови. Якщо концентратор виходить з ладу, підключення всіх хостів до всіх інших хостів не вдається. Будь-яке спілкування між хостами відбувається лише через концентратор. Топологія «зірка» не дорога, оскільки для підключення ще одного хоста потрібен лише один кабель, а конфігурація проста.

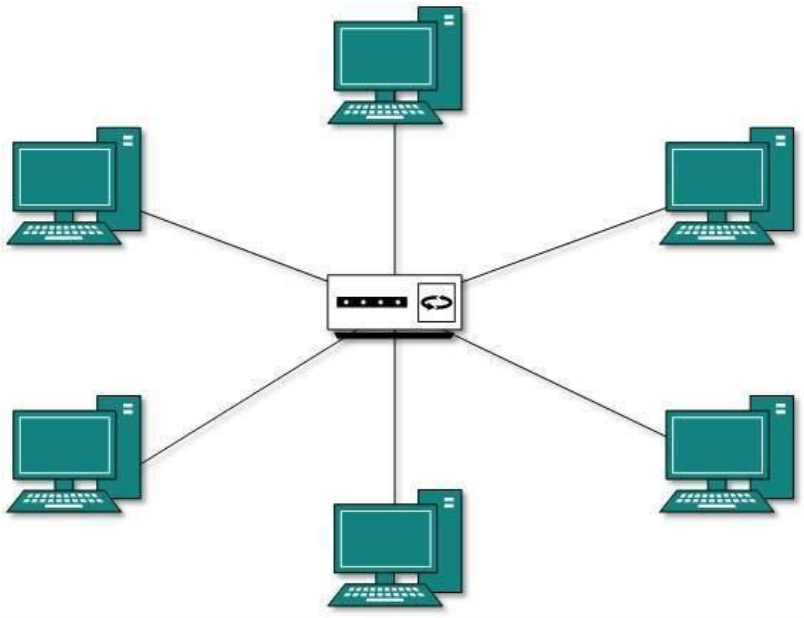

Рис.1.3. Зоряна топологія

Кільцева топологія. У кільцевій топології кожна хост-машина підключається рівно до двох інших машин, створюючи кільцеву структуру мережі. Коли один хост намагається зв’язатися або надіслати повідомлення хосту, який не суміжний з ним, дані проходять через усі проміжні хости. Щоб підключити ще один хост до існуючої структури, адміністратору може знадобитися ще один додатковий кабель.

Відмова будь-якого хоста призводить до відмови всього кільця. Таким чином, кожне з’єднання в кільці є точкою відмови. Є методи, які використовують ще одне резервне кільце.

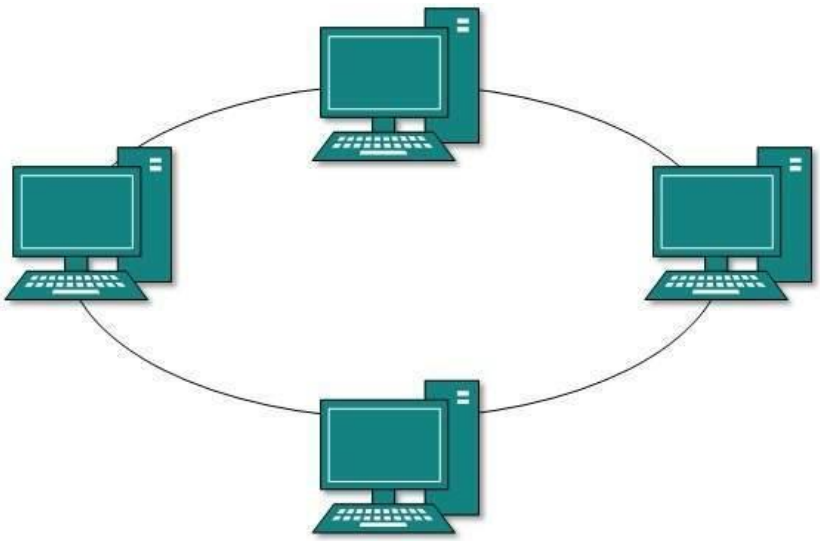

Рис.1.4. Кільцева топологія

Топологія сітки. У цьому типі топології хост підключений до одного чи кількох хостів. Ця топологія має хости, які мають з'єднання «точка-точка» з усіма іншими хостами, або також можуть мати хости, які підключаються лише до кількох хостів.

Хости в топології Mesh також працюють як ретранслятори для інших хостів, які не мають прямих зв'язків «точка-точка». Сітчаста технологія буває двох видів:

Повна мережа: усі хости мають з'єднання «точка-точка» з усіма іншими хостами в мережі. Таким чином, для кожного нового хоста потрібно n(n-1)/2 підключення. Він забезпечує найнадійнішу мережеву структуру серед усіх мережевих топологій.

Частково сітка: не всі хости мають з'єднання «точка-точка» з усіма іншими хостами. Хости підключаються один до одного довільним чином. Ця топологія існує там, де потрібно забезпечити надійність деяким із усіх хостів.

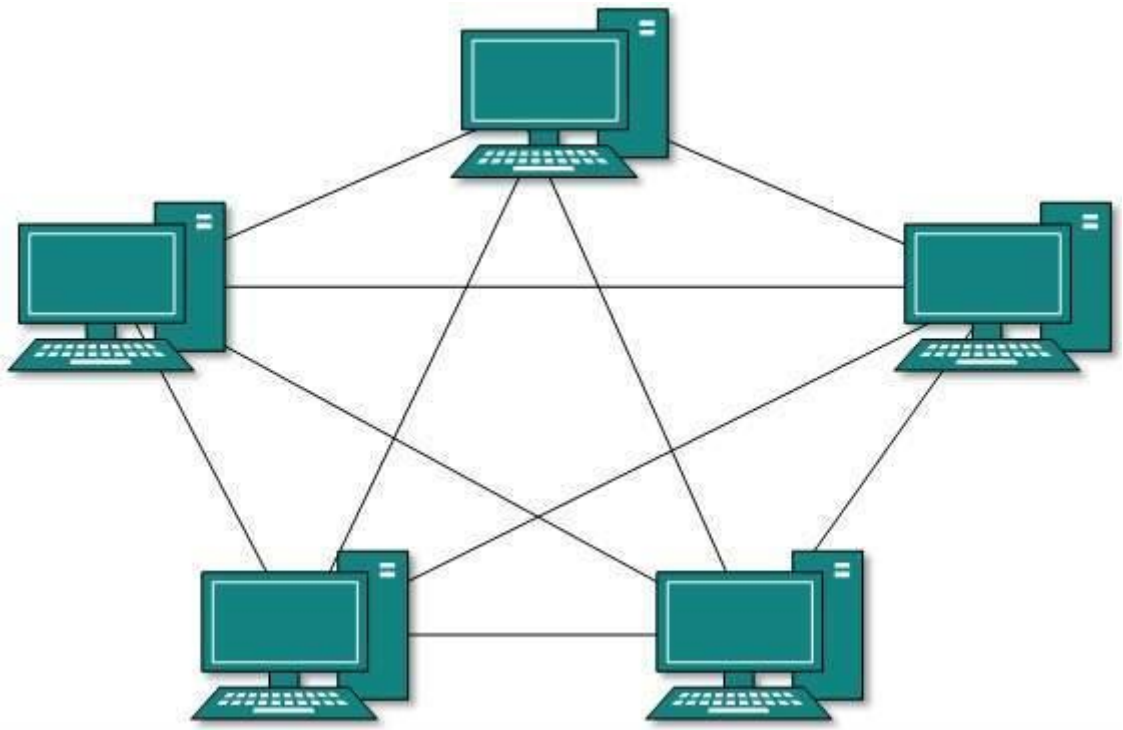

Рис.1.5. Топологія сітки

Топологія дерева. Також відома як ієрархічна топологія, це найпоширеніша форма мережевої топології, яка використовується на даний момент. Ця топологія імітує розширену топологію «зірка» та успадковує властивості топології шини.

Ця топологія поділяє мережу на кілька рівнів/рівнів мережі. В основному в локальних мережах мережа поділена на три типи мережевих пристроїв. Найнижчий — це рівень доступу, до якого підключаються комп’ютери. Середній шар відомий як шар розподілу, який працює як посередник між верхнім шаром і нижнім шаром. Найвищий рівень відомий як базовий рівень і є центральною точкою мережі, тобто коренем дерева, від якого розгалужуються всі вузли.

Усі сусідні хости мають з’єднання «точка-точка» між собою. Подібно до топології шини, якщо корінь не працює, страждає навіть уся мережа. Хоча це не єдина точка збою. Кожне з'єднання служить точкою збою, збій якого ділить мережу на недоступний сегмент.

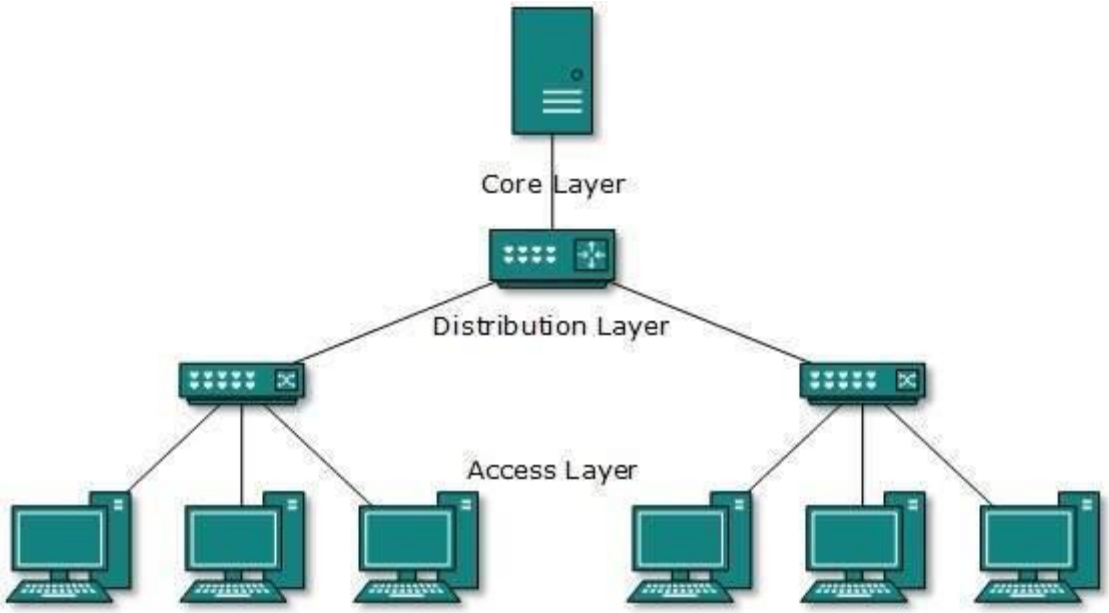

Рис.1.6. Топологія дерева

Послідовна топологія. Ця топологія з’єднує всі хости лінійним способом. Подібно до кільцевої топології, усі хости підключені лише до двох хостів, за винятком кінцевих хостів. Це означає, що якщо кінцеві хости підключено послідовно, це означає кільцеву топологію.

Кожна ланка в топології послідовного ланцюга представляє єдину точку відмови. Кожен збій зв’язку розділяє мережу на два сегменти. Кожен проміжний хост працює як ретранслятор для своїх безпосередніх хостів.

Рис.1.7. Послідовна топологія

Гібридна топологія. Структура мережі, проект якої містить більше однієї топології, називається гібридною топологією. Гібридна топологія успадковує переваги та недоліки всіх об’єднаних топологій.

Наведене нижче зображення представляє довільно гібридну топологію. Комбіновані топології можуть містити атрибути зіркової, кільцевої, шинної та послідовної топології. Більшість глобальних мереж підключено за допомогою топології подвійного кільця, а мережі, підключені до них, переважно є мережами топології Star. Інтернет є найкращим прикладом найбільшої гібридної топології.

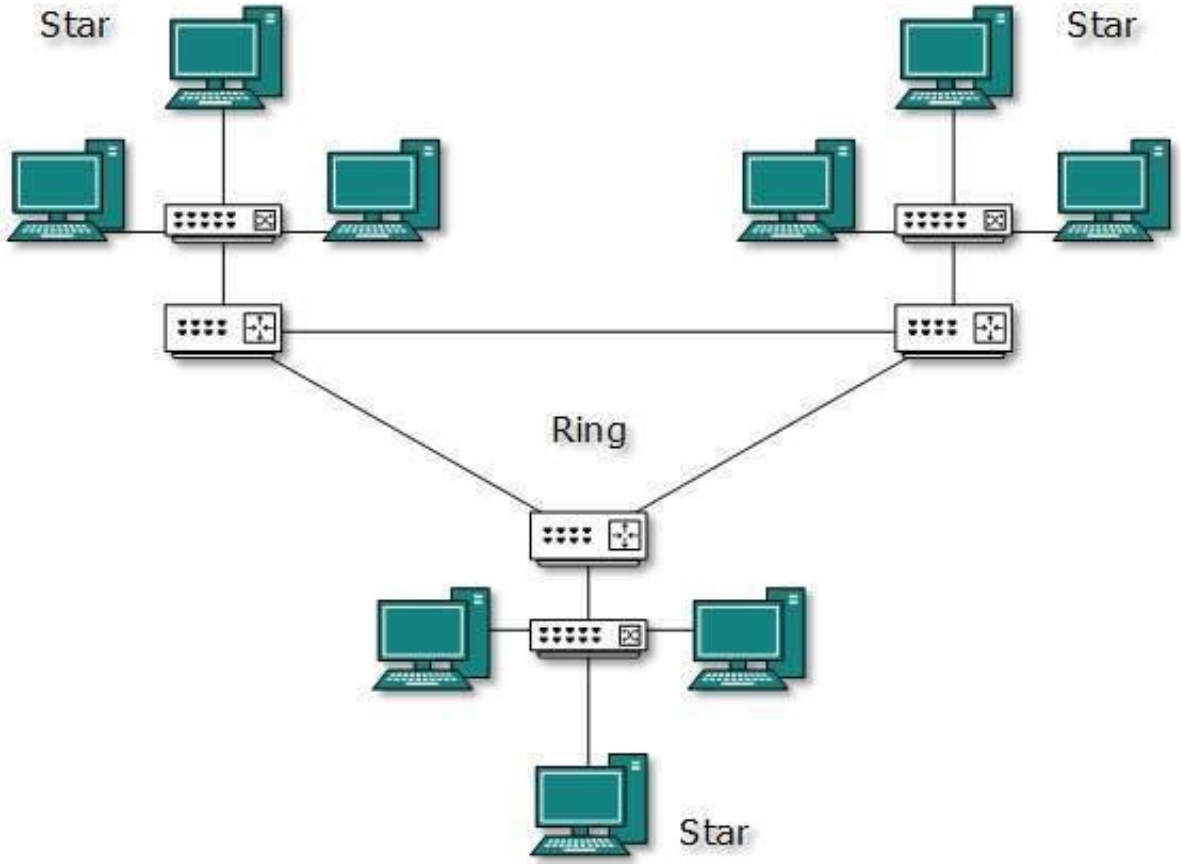

Рис.1.8. Гібридна топологія

1.6 Побудова корпоративної мережі

Інфраструктура комп'ютерної мережі є основою бізнесу. Усі пристрої, програми, програмне забезпечення та більша частина роботи підтримуються комп'ютерною мережею або побудовані на її основі. Тому планування, проектування, закупівля апаратного забезпечення та безпека бізнес-комп'ютерної мережі мають бути пріоритетними для бізнесу.

Щоб побудувати комп'ютерну мережу для компанії, потрібно врахувати чимало речей. Ефективна робота комп'ютерної мережі в бізнес-середовищі дуже відрізняється від налаштування домашньої чи домашньої мережі. Розробка бізнес-мережі має високий ступінь складності та викликів безпеки. Хоча тип мережі для бізнесу залежатиме від потреб конкретних компаній, компоненти комп'ютерної мережі залишаться незмінними [12].

Ось список пристроїв, необхідних для налаштування комп'ютерної мережі для підприємства:

- Модем
- Маршрутизатор
- Брандмауер
- Перемикач
- Кабель локальної мережі / патч-кабель
- Точка доступу
- Повторювач
- Комутаційна панель

А ось опис простого налаштування офісної мережі: підключення до Інтернету здійснюється через кабель від корпоративного провайдера (провайдера послуг Інтернету). Цей кабель підключається до маршрутизатора. Брандмауер фільтрує трафік, що передається через кабель, який потім підключається до комутатора. Тоді всі мережеві пристрої отримають доступ до Інтернету, підключившись до цього комутатора.

Модем, скорочення від «модулятор-демодулятор», — це апаратний компонент корпоративної мережі, який допомагає комп’ютеру та іншим пристроям підключатися до Інтернету. Цей пристрій перетворює цифрові дані, які розуміє комп’ютер, на аналогові дані, які передаються по кабелю.

Модеми, швидше за все, це кабельні модеми, які підтримують DOCSIS (специфікація інтерфейсу служби передачі даних через кабель), яка використовується для передачі Інтернету через гібридні волоконно-коаксіальні кабелі. Таким чином можна отримати телебачення, кабельний Інтернет, цифрову телефонну лінію через той самий кабель.

Із зростанням використання оптоволоконних з’єднань модеми застарівають. Волоконно-оптичні кабелі здатні передавати більшу смугу пропускання на великі відстані. Оскільки потрібна висока швидкість передачі даних у офісі, більш імовірно, що потрібно використовувати оптоволоконне підключення. У цьому випадку не потрібно, щоб модем був частиною мережі.

Маршрутизатор — це компонент мережевого обладнання, який передає пакети даних між мережами. Простіше кажучи, він передає дані з інтернет-кабелю на пристрій. У простому мережевому підключенні інтернет-кабель з’єднується з маршрутизатором, дозволяючи йому передавати й отримувати інформацію з Інтернету. Інші пристрої у офісній мережі підключаються до маршрутизатора за допомогою комутатора Ethernet між ними та отримують доступ до Інтернету.

Брандмауер — це система безпеки корпоративної комп’ютерної мережі. Він відстежує та контролює вхідний і вихідний мережевий трафік на основі встановлених організацією правил безпеки. Іншими словами, брандмауер — це фільтр між внутрішньою мережею та зовнішньою мережею, як-от Інтернет, який захищає бізнес-мережу від неавторизованого зовнішнього доступу.

Незважаючи на те, що комп’ютери оснащені вбудованим програмним брандмауером, корпоративна мережа не в безпеці з цією єдиною слабкою сіткою безпеки. Пристрої мережевої інфраструктури є типовими цілями для кібер-зловмисників, і без спеціального брандмауера мережа та всі підключені пристрої вразливі для хакерів.

Спеціальний апаратний брандмауер надає корпоративній мережі вкрай необхідний додатковий рівень захисту. Апаратний брандмауер оснащений такими розширеними функціями, як VPN, віддалений доступ і розширена веб-фільтрація. Він схожий на маршрутизатор тим, що може працювати з обмеженою кількістю користувачів. Тому подбайте про брандмауер із достатньою потужністю для майбутнього зростання.

Маршрутизатор комерційного рівня зазвичай має вбудовані можливості брандмауера, тому може не знадобитися купувати окреме обладнання брандмауера.

Комутатор є важливим базовим елементом офісної мережі. Це мережевий пристрій, який дозволяє іншим пристроям у мережі спілкуватися та обмінюватися інформацією. У мережі будуть комп'ютери, принтери, пристрої NAS (мережеве сховище), сервери, VoIP (протокол передачі голосу через Інтернет) тощо, а комутатор об'єднує ці пристрої у мережу.

Висновки до першого розділу

Проаналізовано основні компоненти та властивості комп'ютерних мереж. Перераховано елементи мережі, компоненти, протоколи та пристрої для побудови цільної картинки комп'ютерної мережі.

Розглянуто вимоги до розробки великомасштабних мереж для задоволення сучасного динамічного бізнесу та IT-потреб і тенденцій.

Наведено основні принципи проєктування мережі та окремо виділено важливість уніфікованого керування мережею. Досліджено різні топології мереж для побудови корпоративної мережі.

Підкреслено, що організації з розподіленим середовищем тепер більше покладаються на мережу для надання позитивного досвіду та гнучкості бізнесу. Мережеві команди повинні вміти встановлювати нові мережеві підключення та гарантувати їхню безпеку та продуктивність.

2 ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

2.1. Заходи безпеки для корпоративної мережі

Сьогодні все більше корпоративних пристроїв і систем підключаються через Інтернет для обміну інформацією. «Інтернет речей» стає все більш значущим і майже відчутним питанням, включаючи бізнес-додатки, хмарну інфраструктуру та зберігання даних.

Оскільки все більше пристроїв спілкуються один з одним через мережі, користувачі стали залежними від доступності корпоративних мереж. Якщо компонент або система раптово вийде з мережі, це може зашкодити щоденним бізнес-операціям.

В епоху оцифрування більшість бізнес-дій відбувається в корпоративній мережі, тому хакери та зловмисні треті сторони стають все активнішими в планах атак на мережі та сервери. Організації здійснюють фінансові операції та зберігають усі конфіденційні дані в мережі компанії, включно з особистими даними, як-от дані кредитної картки.

Слабка або незахищена мережа може створити ризик. За даними компанії з кібербезпеки Malwarebytes, за останні роки різко зросла кількість кібератак на корпоративні мережі. За перші 3 місяці 2019 року це число зросло на 235% порівняно з тим же періодом 2018 року. Malwarebytes виявив загалом 9 552 414 атак. З іншого боку, кількість атак на споживачів зменшилася, оскільки хакери менше виграють від незначних особистих атак [13].

Кібератаки бувають різних форм і розмірів і можуть бути спрямовані на корпоративні мережі, апаратне або програмне забезпечення. Наприклад, вони можуть обмежити доступність і продуктивність мережі або зосередитися на шпигунстві, крадіжці інформації і навіть знищенні інформації. Ці атаки можуть мати значні наслідки для компаній, негативно вплинувши на їх повсякденну

діяльність і завдавши фінансових збитків через крадіжку фінансових ресурсів, збої у виробництві, шкоду репутації та втрату клієнтів і прибутку.

Компанії все більше усвідомлюють, що належна безпека корпоративних мереж є вирішальним фактором гарантування безпечної та безперервної роботи.

Центри обробки даних забезпечують, серед іншого, стабільне та кондиціоноване середовище для обладнання завдяки численним заходам захисту, таким як клімат-контроль, постійне електроживлення та протипожежний захист. Центри обробки даних також повинні забезпечити політику, запобіжні заходи та заходи фізичної безпеки для запобігання несанкціонованому доступу до обладнання (і запущених на ньому програм). Докладніше про безпеку спільного розташування.

Однак за допомогою спільного розташування організації самі керують усіма різними аспектами апаратного забезпечення та корпоративної мережі. Як клієнт спільного розміщення, вкрай важливо вжити належних заходів для захисту всіх даних, що працюють на апаратному забезпеченні та корпоративній мережі, щоб гарантувати доступність, цілісність, конфіденційність і пропускну здатність мережі.

Безпека мережі включає всі заходи, призначені для захисту доступності, цілісності та конфіденційності мережі, щоб контролювати ризики, пов’язані з усім зв’язком. Це включає рішення, пов’язані як з апаратним, так і з програмним забезпеченням. Кожен рівень заходів реалізує різні політики та елементи керування, щоб дозволити лише авторизованим користувачам доступ до мережі, з кількома компонентами, які працюють разом, щоб забезпечити найбільш безпечне мережеве середовище.

Існують різні заходи, які можна вжити для захисту даних компанії:

1. Створення політики. Захист мережі починається з формулювання політики. Правила повинні описувати, що дозволено, а що заборонено, зазначаючи можливі джерела загроз. Важливо постійно контролювати відповідність політиці та виявляти проблеми, які все ще потребують покращення.

2. Встановлення програмного забезпечення для захисту від шкідливих програм і вірусів. Зловмисне програмне забезпечення – це скорочення від шкідливого програмного забезпечення, яке включає віруси, хробаки, трояни, програми-вимагачі та шпигунські програми. Зловмисне програмне забезпечення вторгається в мережу через експлойт або помилку, яка загрожує програмному або апаратному забезпеченню одержувача. Експлойт поширюється через веб-сайти, спливаючі вікна з рекламою, вкладення в електронному листі або завантаження програм. Ризик не обмежується настільними комп'ютерами та ноутбуками – зловмисне програмне забезпечення може потрапити в корпоративну мережу також через мобільні пристрої.

Зловмисне програмне забезпечення заражає мережу, щоб збирати конфіденційну інформацію, ділитися даними з третіми сторонами, виводити з ладу системи, брати сервери в заручники або переміщувати фінансові ресурси. Гарне антивірусне програмне забезпечення не тільки сканує на наявність шкідливих програм після надходження, але й постійно відстежує файли, щоб знайти відхилення, видалити шкідливе програмне забезпечення та відновити пошкоджені файли. Ніколи не забувайте постійно оновлювати корпоративне програмне забезпечення та сервери, щоб забезпечити постійний захист систем.

3. Використання брандмауерів. Брандмауер створює бар'єр між довіреною внутрішньою мережею та зовнішніми ненадійними мережами. Брандмауери є ефективною першою лінією захисту доступу до мережі. Він фокусується на різних загрозах і запобігає їх проникненню або поширенню в мережі. Брандмауер захищає все, що знаходиться «за» мережею, від усього, що знаходиться «попереду». Зазвичай «передня» частина брандмауера — це сторона, спрямована до Інтернету, а «задня» — внутрішня мережа. Брандмауер діє як воротар і визначає, які пакети можна продовжувати, а які ні.

4. Рішення проти DDoS. DDoS означає розподілену відмову в обслуговуванні. Мета DDoS-атаки полягає в тому, щоб зробити сервер, службу або інфраструктуру недоступними шляхом надсилання величезної пропускної здатності, викликаючи перевантаження та сповільнюючи або блокуючи законний

трафік. Рішення проти DDoS може виявляти та блокувати DDoS-атаки, щоб сервер залишався доступним.

DDoS-атаки стають все більш поширеними. За даними NBIP, спільного підприємства інтернет-провайдерів, за останні роки кількість DDoS-атак різко зросла. У 2018 році ця цифра зросла на 15% порівняно з роком раніше. Наприклад, ING і ABN AMRO неодноразово ставали жертвами DDoS-атак. Сервери перевантажилися, що вплинуло на споживачів, інтернет-магазини та послуги [14].

Різні сторони на ринку пропонують рішення проти DDoS. Дізнайтеся більше про унікальне рішення i3D.net для захисту від DDoS.

5. Використання системи виявлення та запобігання вторгненням. Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) можуть автоматично виявляти несанкціонований доступ до мережевого обладнання (наприклад, модемів, маршрутизаторів і комутаторів). IDS та IPS іноді плутають з міжмережевими екранами. Найсуттєвіша відмінність полягає в тому, що брандмауер фільтрує та блокує трафік, тоді як IDS та IPS можуть перевіряти вміст пакетів даних. IDS пасивно переглядає пакети даних, що проходять через мережу, і може викликати тривогу при виявленні підозрілої активності. IPS, з іншого боку, активні, негайно блокуючи зовнішні атаки.

6. VPN. VPN означає віртуальну приватну мережу. Завдяки безпечному зашифрованому з’єднанню VPN зовнішні пристрої можуть підключатися до локальної мережі, наприклад корпоративної. Трафік даних надсилається через цю мережу на зовнішній сервер і назад через зашифроване безпечне з’єднання.

2.2. Три рівні безпеки корпоративних мереж

Оскільки кіберзагрози постійно розвиваються у складності та масштабах, боротьба з ними передбачає «поширення» захисту на всі системи корпоративної мережі – сервери, бази даних, служби, встановлене програмне забезпечення тощо. Більше того, слід звернути увагу на забезпечення того, щоб співробітники компанії

розуміють і дотримуються принципів кібербезпеки та не будуть (не)навмисно скомпрометувати безпеку корпоративної мережі своїми діями [15].

Однак заходи кібербезпеки, що застосовуються всередині організації, можуть відрізнятися залежно від розміру компанії, її фінансових можливостей, галузі, у якій вона працює (регульованої чи нерегульованої), інформації, з якою їй доводиться мати справу під час ділової діяльності тощо.

Враховуючи ці та інші фактори, можна визначити три основні рівні захисту кібербезпеки. Залежно від їх складності, ці рівні можуть бути встановлені за допомогою IT-відділу компанії або постачальника послуг кібербезпеки.

Рівень 1 – мінімальний захист. Ключовим моментом кібербезпеки рівня 1 є забезпечення захисту корпоративної мережі від найпоширеніших кіберзагроз, наприклад, фішингових атак (посилання на шкідливі веб-сайти або завантажені файли, заражені вірусами, вкладаються в електронні листи або миттєві повідомлення та надсилаються співробітникам компанії) і зловмисне програмне забезпечення (шкідливе програмне забезпечення, яке потрапляє в мережу компанії через Інтернет або електронну пошту та існує у формі шпигунського програмного забезпечення, програм-вимагачів, програм-викрадачів браузера тощо).

Мінімальний захист поширюється на малий бізнес, який працює в нерегульованих галузях і має суворо обмежені фінансові ресурси. Невеликі та маловідомі (принаймні поки що) компанії, які не працюють з інформацією, важливою для хакерів (наприклад, особисті дані клієнтів, як-от номери кредитних карток, паролі тощо), навряд чи можуть стати об’єктами складних кібератак, таких як DDoS (розподілені Відмова в обслуговуванні) або фішинг.

Мінімум заходів кібербезпеки, необхідних для впровадження, — це належним чином налаштований захист брандмауера, який працює разом із регулярним оновленням антивірусного програмного забезпечення. Брандмауери сканують мережевий трафік, щоб виявити аномальні пакети або фрагменти пакетів. Антивіруси забезпечують захист від таких кіберзагроз, як програми-вимагачі, хробаки, шпигунські програми тощо, перевіряючи кожен файл, який співробітники відкривають або завантажують з Інтернету чи інших джерел.

Для застосування цих заходів безпеки немає необхідності організовувати окремий відділ кібербезпеки. IT-відділ компанії може взяти на себе відповідальність за це, оскільки впровадження захисту брандмауером, встановлення антивірусного програмного забезпечення та постійна підтримка їх продуктивності не вимагає навичок, пов'язаних із кібербезпекою.

Тим не менш, рівень захисту корпоративної мережі необхідно регулярно перевіряти. Для невеликої організації, яка веде свій бізнес у нерегульованій галузі, достатньо щорічного проведення оцінки вразливості та тестування на проникнення. Ці послуги з кібербезпеки, які надаються щорічно, не призведуть до великих витрат для компанії з обмеженим бюджетом. У той же час ці дії можуть допомогти системним адміністраторам бути в курсі слабких місць безпеки в мережі компанії.

Рівень 2 – розширений захист. Кібербезпека рівня 2 забезпечує захист корпоративної мережі від нецільових атак, наприклад, шкідливих програм, надісланих на різні адреси електронної пошти, атак спуфінгу, спаму тощо. У цьому випадку метою зловмисників є викрадення будь-якої цінної інформації з будь-якої IP-адреси. Адреса чутлива до відомих слабких місць безпеки, які, можливо, існують у корпоративній мережі.

Імовірність того, що компанії середнього розміру стануть жертвами нецільових атак, велика. Оскільки таким організаціям не потрібно дотримуватися нормативних стандартів, вони можуть нехтувати суворими заходами кібербезпеки у своїх мережах. Таким чином, вони можуть легко піти на компроміс.

Для забезпечення розширеного захисту корпоративної мережі, окрім елементів мінімального захисту – міжмережевих екранів та антивірусів, необхідно застосовувати наступні компоненти:

Безпека електронної пошти передбачає різноманітні методи (сканування електронних листів на наявність зловмисного програмного забезпечення, фільтрування спаму тощо), щоб захистити корпоративну інформацію як у «внутрішньому», так і «зовнішньому» спілкуванні електронною поштою від будь-

яких кібератак, які використовують електронну пошту як точку входу (шпигунське програмне забезпечення, рекламне ПЗ, тощо).

Сегментація мережі, наприклад, сегментація мережі за відділами з сегментами, з'єднаними через брандмауери, які не дозволяють зловмисному коду чи іншим загрозам переміщатися з одного сегмента мережі в інший. Більше того, сегментація мережі передбачає відокремлення мережевих активів, у яких зберігаються дані компанії, від зовнішніх сегментів (веб-серверів, проксі-серверів), таким чином зменшуючи ризик втрати даних.

Виявлення вторгнень (IDS) і система запобігання вторгненням (IPS), які використовуються для ідентифікації та реєстрації інформації про можливі інциденти безпеки, їх блокування до того, як вони поширяться мережевими середовищами тощо.

Для підтримки такого рівня безпеки мережі компанії потрібні фахівці з інформаційної безпеки, відповідальні за виявлення та управління ризиками кібербезпеки, розробку процедур і політик безпеки тощо. Для цих цілей компанія може організувати власний відділ інформаційної безпеки або звернутися до служби керованої безпеки. постачальник (MSSP).

Організація окремого відділу інформаційної безпеки передбачає значні витрати як на наймання досвідченої служби безпеки, так і на покупку необхідного обладнання та програмного забезпечення. Робота з MSSP є більш економічно ефективним рішенням, яке дозволяє компанії зберегти фокус на основних бізнес-операціях. Тим не менш, компанії все одно знадобиться штатний офіцер безпеки, який координуватиме роботу з MSSP.

Щоб контролювати ефективність захисту кібербезпеки, ретельно розроблена стратегія безпеки повинна передбачати щоквартальну оцінку вразливості та щорічне тестування на проникнення для виявлення, пом'якшення та управління ризиками кібербезпеки. Компанії потрібна стратегія кібербезпеки, оскільки вона зосереджена на захисті корпоративної мережі, враховуючи використання персоналом своїх персональних мобільних пристроїв і ноутбуків у бізнес-цілях (BYOD), широке використання хмарних обчислень тощо, і надає прямі вказівки для

співробітників компанії щодо прийнятних поведінка всередині корпоративної мережі.

3 рівень – максимальний захист. Ключове завдання кібербезпеки третього рівня – захист корпоративної мережі від цілеспрямованих атак. Цей тип кібератак (фішинг, розповсюдження прогресивного шкідливого програмного забезпечення тощо) передбачає спеціально розроблені кампанії, що проводяться проти певної організації.

Жертвами цілеспрямованих атак зазвичай стають компанії середнього розміру та великі підприємства, які працюють у регульованих галузях, наприклад, банківська справа чи охорона здоров'я, або державні установи. Це відбувається тому, що чим більша організація та чим більше даних вона має захищати (регульовані особисті дані, медичні записи пацієнтів, інформація про банківські рахунки тощо), тим відчутніші результати успішних цілеспрямованих атак.

Компанії, які працюють у регульованих сферах, повинні приділяти максимальну увагу підтримці захисту від кіберзагроз, дотримуючись правил і стандартів (HIPAA, PCI DSS тощо). Наступні компоненти кібербезпеки можуть допомогти закрити всі можливі вектори атак:

Безпека кінцевої точки. Цей метод безпеки передбачає захист доступу кожного пристрою (смартфона, ноутбука тощо), який потрапляє в корпоративну мережу і таким чином стає потенційною точкою входу для загроз безпеки. Зазвичай безпека кінцевої точки включає встановлення спеціального програмного забезпечення безпеки на сервері керування в корпоративній мережі разом із встановленням клієнтського програмного забезпечення на кожному пристрої. Сукупність цих заходів дозволяє контролювати дії користувачів під час віддаленого доступу до корпоративної мережі зі своїх смартфонів, планшетів та інших пристроїв. Таким чином, компанія отримує кращу видимість у реальному часі щодо всього спектру потенційних загроз безпеці, з якими їй доведеться мати справу.

Запобігання втраті даних (DLP). Застосування цього заходу є надзвичайно важливим для підприємства, яке працює у фінансовому секторі чи секторі охорони

здоров’я. Програмне забезпечення DLP забезпечує захист і запобігає витоку конфіденційних, особистих і конфіденційних даних, наприклад, номерів кредитних карток клієнтів, номерів соціального страхування тощо, надаючи адміністраторам DLP повний контроль над типами даних, які можна передати за межі корпоративної мережі. DLP може відхиляти спроби пересилати будь-яку ділову електронну пошту за межі корпоративного домену, завантажувати корпоративні файли в хмарні сховища з відкритим кодом тощо.

Інформація про безпеку та керування подіями (SIEM). Рішення SIEM відстежують, збирають, аналізують і звітують про дані журналів і подій про кожну активність, що відбувається в IT-середовищі, що дозволяє уникнути ситуацій типу «я не знаю, що сталося» у разі злому мережі компанії. Серед переваг SIEM – централізація зібраних даних журналу, забезпечення підтримки для виконання вимог PCI DSS, HIPAA та інших нормативних актів, забезпечення реагування на інциденти в реальному часі.

Для належної роботи із зазначеними рішеннями безпеки найкраще послужить поєднання зусиль окремого відділу інформаційної безпеки та допомоги MSSP. Для багатьох компаній надання MSSP повного доступу та контролю над конфіденційними даними, особистою інформацією клієнтів тощо здається досить ризикованим, особливо з точки зору відповідності вимогам безпеки. Однак підписання детальної угоди SLA з компанією, що надає послуги з кібербезпеки, і делегування частини обов’язків із кіберзахисту зовнішньому MSSP має сенс. Це дозволяє підприємствам отримувати цілодобовий моніторинг стану безпеки та звітність і одночасно зменшувати свої витрати на захист кібербезпеки.

Серед необхідних заходів кібербезпеки — розробка та підтримка стратегії безпеки, проведення оцінки вразливості з наступним щоквартальним тестуванням на проникнення (краще проводити перед кожною аудиторською перевіркою, щоб відповідати стандартам і нормам), забезпечення постійного моніторингу загроз та організація структурованого відповідь на інцидент (IR).

Моніторинг загроз передбачає постійний моніторинг корпоративної мережі та кінцевих точок (серверів, бездротових пристроїв, мобільних пристроїв тощо) на

наявність ознак загроз кібербезпеці, наприклад, спроб вторгнення або викрадання даних. Сьогодні моніторинг загроз стає ще більш важливим, оскільки на підприємствах спостерігається тенденція наймати співробітників віддалено та застосовувати політику BYOD, що створює додатковий ризик для захисту корпоративних даних і конфіденційної інформації.

Реагування на інциденти (IR) стосується ситуацій, коли порушення безпеки вже сталися. Таким чином, компанії потрібна спеціальна власна або стороння команда, підготовлена до інцидентів, готова виявляти реальні події, знаходити причини та реагувати на загрози кібербезпеці з найменшими можливими збитками та мінімальним часом, необхідним для відновлення після атаки. Діяльність IR запобігає перетворенню дрібних проблем у більші, такі як порушення даних або збій системи.

Захист хмарних активів. Компанії повинні приділяти особливу увагу захисту своїх хмарних активів. Сьогодні зберігання важливих для бізнесу даних у хмарі стає звичайною практикою. Рішення про хмарні обчислення має сенс, оскільки це дозволяє підприємствам заощадити кошти та підвищити ефективність бізнес-операцій, які вони здійснюють.

Однак хмарні середовища представляють відносно нові сфери для команд безпеки, яким необхідно організовувати та підтримувати заходи кібербезпеки всередині корпоративної мережі. Це також призводить до нових викликів безпеці, оскільки «хмарна природа» передбачає відсутність контролю для системних адміністраторів над ресурсами, які використовує компанія, і даними, які вони зберігають у хмарі.

Фахівці з кібербезпеки застосовують різні стратегії для захисту хмарних активів залежно від моделі хмари.

Інфраструктура як послуга (IaaS) і платформа як послуга (PaaS)

В обох випадках стратегія кібербезпеки схожа на підхід до захисту локальної корпоративної мережі. Різниця полягає в «факторі віддаленості». Основним завданням компанії є вибір надійного постачальника IaaS/PaaS, розміщення серверів у хмарі, які вони пропонують, і встановлення належного рівня контролю

над наданими віртуальними машинами. Існують найкращі практики, які можна застосувати для забезпечення безпеки IaaS/PaaS, наприклад, забезпечення належного шифрування даних, що зберігаються та надсилаються до сторонньої хмари, моніторинг мережевого трафіку на наявність шкідливих дій, регулярне резервне копіювання даних тощо.

Деякі постачальники рішень IaaS або PaaS також надають своїм клієнтам «вбудовані» послуги кібербезпеки, але це не поширена практика. Наприклад, Microsoft Azure пропонує клієнтам різноманітні способи захисту робочих навантажень у хмарі, захисту програм від поширених уразливостей тощо. Amazon Web Services (AWS) представляє ще одного постачальника хмарних служб, що надає своїм клієнтам застосовані засоби безпеки у хмарі (вбудовані у брандмауерах, можливостях шифрування тощо), послугах оцінки безпеки для виявлення слабких місць кібербезпеки, ідентифікації та керування доступом для визначення доступу користувачів до ресурсів AWS тощо.

Програмне забезпечення як послуга (SaaS). У цьому випадку постачальник SaaS бере на себе відповідальність за створення, розміщення та захист програмного забезпечення, яке він пропонує. Однак компанії ще потрібно зробити певну роботу, щоб забезпечити безпеку рішення. Їм необхідно зосередитися на управлінні доступом до додатків для своїх співробітників з урахуванням відділів, у яких вони працюють, їхніх посад тощо. Таким чином, першочерговим завданням співробітників служби безпеки компанії є встановлення контролю доступу користувачів, тобто налаштування параметрів правильно.

Office 365 є прикладом хмарного рішення з багаторівневою безпекою. Вбудовані функції кібербезпеки дозволяють безперервно контролювати центри обробки даних, виявляти та запобігати зловмисним спробам отримати доступ до особистої чи конфіденційної інформації, шифрувати збережені та передані дані, використовувати антивірусний і антиспамовий захист для захисту від загроз кібербезпеці, що надходять до корпоративної мережі ззовні, тощо.

2.3. Поширені загрози мережевій безпеці

Кіберзлочинці можуть використовувати багато методів, щоб завдати шкоди. Ці зловмисники можуть використовувати загрози безпеці мережі, щоб використовувати вектори атак або вразливості корпоративної мережі. Мережеві загрози мають різні форми, але всі вони спрямовані на схожу кінцеву мету: доступ до системи для викрадення корпоративних даних.

Протягом останніх двох десятиліть кібератаки стають все більш частими, витонченими і складними для захисту. Експерти з кібербезпеки також вважають, що ризики мережевої безпеки продовжуватимуть ставати все більш складними та агресивними. Наведемо 8 найпоширеніших загроз мережевій безпеці [16].

1. Атаки шкідливих програм — це всеосяжний термін для шкідливих програм, які кіберзлочинці використовують для пошкодження цільової мережі. Під час атак зловмисного програмного забезпечення кіберзлочинець використовує зловмисне програмне забезпечення, щоб використовувати вразливі місця системи безпеки та викликати витік даних. Приклади атак шкідливих програм включають:

Комп'ютерний вірус — це зловмисний код, який вбудовано в справжню програму, яка називається хост-файлом. Вірус також використовує переваги програми для саморозмноження. Віруси можуть залишатися бездіяльними в системі, доки користувач не запустить головну програму. Потім запущений вірус може пошкодити, видалити або викрасти корпоративні дані, поставити під загрозу безпеку системи та зруйнувати структуру копоративної мережі. Віруси також можуть використовувати корпоративну мережу для зараження інших систем.

Троянські атаки можуть надати кіберзлочинцям несанкціонований доступ до корпоративної мережі, викрасти конфіденційні дані або вплинути на загальну продуктивність системи. Під час атак троянів кіберзлочинці ховають зловмисне програмне забезпечення за легітимною електронною поштою чи файлом, щоб змусити запустити програму. Щойно відкривається електронний лист або завантажується файл, у системі негайно встановлюється зловмисне програмне забезпечення.

- Рекламне програмне забезпечення — це програма, яка відстежує активність у веб-переглядачі та використовує дані для постійного показу небажаної реклами. Розробники можуть навіть включити рекламне ПЗ у свої безкоштовні програми, щоб допомогти відшкодувати витрати на розробку.
- Шпигунське програмне забезпечення — це шкідлива програма, яка вторгається в конфіденційність мережі, щоб стежити за корпоративними даними та відправляти їх назад зловмиснику.
- *Комп'ютерні хробаки.* Комп’ютерний черв’як — це зловмисне програмне забезпечення, яке самовідтворюється і використовує переваги хост-мережі для зараження багатьох систем. Як тільки хробак заражає систему, він швидко досліджує мережу в пошуках підключених систем. Потім він створює свої копії, щоб заразити підключені системи.

Програмне забезпечення Rogue Security. Атаки зловмисного програмного забезпечення починаються зі спливаючих вікон під час перегляду веб-сайту. Спливаючі вікна містять повідомлення про те, що у корпоративній системі є віруси або застаріле оновлення безпеки. Спливаюче вікно запропонує натиснути посилання, щоб завантажити платне програмне забезпечення, щоб стерти вірус або оновити систему безпеки. Однак завантаження програмного забезпечення встановлює шкідливе програмне забезпечення у систему.

2. Фішингова атака — це соціальна інженерія, яка використовується для маніпулювання, щоб розкрити паролі чи іншу конфіденційну інформацію. Фішингові атаки зазвичай використовують фальшиві електронні листи. Вміст електронних листів різниться, але зазвичай вони пропонують відкрити шкідливий сайт. Там зловмисник викрадає корпоративні дані.

Коли кіберзлочинець отримує несанкціонований доступ до системи, він може вбудувати руткіт у мережу. Руткіт — це набір зловмисних програм, які ховаються глибоко в операційній системі комп’ютера. Руткіти надають кіберзлочинцям бекдор-доступ, уникаючи стандартних заходів безпеки мережі. Потім кіберзлочинці можуть контролювати копоративну мережу, вимикати захист від зловмисного програмного забезпечення або викрадати корпоративні дані.

3. Атаки «людина посередині». Під час атак «людина посередині» (MITM) кіберзлочинці проникають у корпоративне спілкування. Таким чином вони можуть перехоплювати дані та зв'язок між пристроями. Потім вони можуть викрасти корпоративні дані під час їх передачі в мережі. Ці кіберзлочинці можуть змінити інформацію, що передається між обома пристроями, або викрасти конфіденційні особисті дані.

Спуфінг також є поширеною атакою MITM, коли кіберзлочинець маскує відображуване ім'я, веб-сайт, текстове повідомлення, електронну адресу, номер телефону чи URL-адресу веб-сайту, щоб переконати цільову особу, що вона взаємодіє з відомим, надійним джерелом.

4. DoS і DDoS атаки. Відмова в обслуговуванні (DoS) і розподілена відмова в обслуговуванні (DDoS) — поширені мережеві атаки, націлені на сервери веб-сайту. Ці атаки працюють, заповнюючи сервер пакетами даних, що спричиняє перевантаження та збій сервера. Коли це відбувається, законні користувачі веб-сайту не можуть отримати доступ до його послуг.

Різниця між DoS-атаками та DDoS-атаками полягає в тому, що DoS-атака виконується одним комп'ютером, тоді як DDoS-атаки здійснюються кількома комп'ютерами по всьому світу. Зазвичай комп'ютери, задіяні в DDoS-атаці, є частиною ботнету, який кіберзлочинець створює, встановлюючи зловмисне програмне забезпечення під час попередньої атаки.

5. Атака SQL Injection. Багато веб-сайтів і веб-додатків використовують сервери SQL для зберігання даних користувачів. Кіберзлочинці використовують уразливості сервера веб-сайту, щоб викрасти інформацію користувача та інші відповідні дані за допомогою атак із впровадженням SQL. Під час цих атак зловмисник вводить шкідливий SQL-запит у поле введення веб-додатку. База даних SQL отримує зловмисний запит, а потім виконує команди, вбудовані в запит. У результаті це дає кіберзлочинцям контроль над веб-програмою.

6. Підвищення привілеїв. Ескалація привілеїв – це група мережевих атак, які дозволяють користувачам збільшити обсяг своїх дозволів у системі. Кіберзлочинці

зазвичай здійснюють ескалацію привілеїв, щоб збільшити свій доступ до даних після отримання несанкціонованого доступу до мережі.

7. Внутрішні загрози. Деякі ризики безпеці походять від людей, які мають авторизований доступ до системи безпеки організації, відомих як інсайдерські погрози, і зазвичай здійснюються незадоволеними співробітниками. Їх також важко виявити або запобігти, і вони дуже дорогі для організацій.

8. Атаки на ланцюги поставок. Під час атак на ланцюг постачання кіберзлочинці отримують доступ до систем безпеки, використовуючи авторизовану третю сторону або зовнішнього постачальника, який має доступ до даних і систем безпеки. Ці атаки важко виявити, оскільки кіберзлочинці не використовують об’єкт безпосередньо. Навпаки, вони використовують переваги систем постачальника об’єкта, щоб отримати доступ до мережі.

2.4. Надійність мережі та відмовостійкість

Розробка будь-якої системи для стійкості до несправностей спочатку вимагає вибору моделі несправності, набору можливих сценаріїв відмови разом із розумінням частоти, тривалості та впливу кожного сценарію. Проста модель несправностей просто перераховує набір несправностей, які слід розглянути; рішення про включення в набір визначається на основі поєднання очікуваної частоти, впливу на систему та можливості або вартості забезпечення захисту. Більшість надійних мережевих конструкцій усуває відмову будь-якого окремого компонента, а деякі конструкції допускають численні відмови. Навпаки, мало хто намагається впоратися з ворогуючими умовами, які можуть виникнути під час терористичної атаки, і катастрофічні події майже ніколи не розглядаються в будь-якому масштабі, більшому за місто [17].

Тимчасові характеристики несправностей дуже різноманітні, але їх можна приблизно класифікувати як постійні, періодичні або тимчасові. Несправності, які перешкоджають функціонуванню компонента до ремонту або заміни, наприклад, руйнування волокна мережі екскаватором, вважаються постійними. Збої, які

дозволяють компоненту деякий час нормально функціонувати, називаються періодичними. Пошкоджені з’єднувачі та електричні компоненти іноді призводять до періодичних збоїв, які працюють належним чином, доки механічні вібрації чи температурні коливання не спричинять збій, і відновлюються, коли умови знову змінюються. Останню категорію, тимчасові несправності, як правило, найлегше впоратися. Перехідні несправності варіюються від змін у вмісті комп’ютерної пам’яті через космічні промені до бітових помилок через тепловий шум у демодуляторі, і зазвичай вони нечасті та непередбачувані. Різниця між періодичною несправністю та тимчасовою несправністю іноді полягає виключно в частоті; для тимчасових несправностей комбінація кодів виправлення помилок і повторної передачі даних зазвичай забезпечує адекватний захист.

Надмірність має дві форми, просторову та часову. Просторова надмірність відтворює компоненти або дані в системі. Прикладами просторової надлишковості є передача кількома шляхами через мережу та використання кодів виправлення помилок. Тимчасова надмірність лежить в основі алгоритмів автоматичного повторного запиту (ARQ), таких як абстракція ковзного вікна, яка використовується для підтримки надійної передачі в Інтернет-протоколі керування передачею (TCP). Надійна мережа, як правило, забезпечує як просторову, так і часову надлишковість, щоб терпіти несправності з різною часовою стійкістю. Просторова надлишковість необхідна для подолання постійних збоїв у фізичних компонентах, тоді як часова надлишковість вимагає менше ресурсів і, отже, є кращою при роботі з тимчасовими помилками [18].

Крім вибору моделі несправності, при розробці відмовостійкої системи необхідно враховувати кілька додаткових проблем. Система повинна бути здатна виявляти кожну помилку в моделі та мати можливість ізолювати кожну помилку від функціонуючої частини системи таким чином, щоб запобігти поширенню помилкової поведінки. Оскільки механізм виявлення несправностей може виявляти більше ніж одну можливу несправність, система також повинна звертатися до процесу діагностики (або локалізації) несправностей, що звужує набір можливих несправностей і дозволяє застосовувати більш ефективні методи ізоляції

несправностей. Помилка, виявлена системою, не обов’язково звужується до однієї можливої несправності, але менший набір можливостей зазвичай дозволяє більш ефективну стратегію відновлення [19].

Межі ізоляції несправності зазвичай розроблені для забезпечення поведінки безвідмовної зупинки для бажаної моделі несправності. Термін «відмовна зупинка» означає, що неправильна поведінка не поширюється через межу ізоляції несправності; натомість несправні компоненти перестають видавати будь-які сигнали. Fail-stop не передбачає самодіагностики; Компоненти, розташовані поруч із несправним компонентом, можуть діагностувати несправність і навмисно ігнорувати будь-які сигнали від несправного компонента, але фізична конструкція системи повинна дозволяти таке рішення. У маршрутизаторі, наприклад, з’єднання між платами, що керують окремими з’єднаннями, має забезпечувати електричну ізоляцію, щоб підтримувати роботу несправних плат у режимі зупинки. З’єднання комп’ютера на основі шини не допускає зупинки при збої, оскільки ніщо не може перешкодити несправній карті неналежним чином управляти лініями шини. У сучасних серверах високого класу такі шини були замінені комутованими мережами з можливістю широкомовлення, щоб забезпечити таку ізоляцію. Викорінення подібних явищ під час переходу від спільних до комутованих Ethernet у середині 1990-х років було однією з головних адміністративних переваг змін, оскільки невдалі хости мають набагато меншу ймовірність зробити комутаційну мережу непридатною, переповнивши її безперервним трафіком.

Дві моделі мережевих послуг домінували в дослідженнях і комерційних мережах. Перший – це телефонна мережа, або, загалом, мережа, в якій квазіпостійні маршрути, звані ланцюгами, передають фіксовану ємність даних з однієї точки в іншу. У цифровій телефонії голосова лінія потребує 64 Кбіт/с; один світловий шлях в оптичній мережі з мультиплексуванням за довжиною хвилі (WDM) може забезпечити до 40 Гбіт/с, але концептуально подібний до схеми, яка використовується для здійснення телефонного дзвінка.

Другою моделлю мережевих послуг є мережа передачі даних з комутацією пакетів, яка еволюціонувала від ранніх проектів ARPANET і NSFNET до сучасного

Інтернету. Мережі з комутацією пакетів зазвичай не забезпечують сильних гарантій щодо швидкості передачі даних або максимальної затримки, але, як правило, ефективніші, ніж схеми, орієнтовані на канали, які мають базувати гарантовані угоди на найгірших сценаріях навантаження трафіку.

Для цілей нашого обговорення ключова відмінність між цими двома моделями полягає в тому, що додатки, які використовують мережі з комутацією пакетів, загалом можуть терпіти більш серйозні збої в роботі, ніж програми, засновані на мережах з комутацією каналів. Останній клас програм може припускати, що гарантії швидкості передачі даних, затримки та тремтіння, надані мережею, будуть дотримані навіть у разі виникнення збоїв, тоді як незначні збої можуть виникати навіть за звичайних обставин у мережах з комутацією пакетів через коливання моделей трафіку та навантажень. . Таким чином, питання відмовостійкості вирішуються помітно різними способами в обох типах мереж. У мережах з комутацією пакетів, таких як Інтернет, користувачі наразі допускають час відновлення в хвилинах , тоді як відмовостійкість для мереж з комутацією каналів можна вважати компонентом якості обслуговування (QoS), і зазвичай досягається за мілісекунди або, в гіршому випадку, за секунди [20].

2.5. Сучасні тенденції розвитку шкідливого програмного забезпечення

Стрімкий розвиток комунікаційних та інформаційних технологій визначає основні тенденції розвитку шкідливого програмного забезпечення. Шкідливе програмне забезпечення — це збірний термін для шкідливого програмного забезпечення або коду, який може завдати шкоди комп’ютерній системі.

Шкідливе програмне забезпечення навмисно розроблено таким чином, щоб бути ворожим, нав’язливим і агресивним. Він намагається проникнути в систему, завдати шкоди, частково взяти під контроль деякі процеси або повністю вивести з ладу комп’ютери, комп’ютерні системи, мережі, планшети та мобільні пристрої. Як і вірус людського грипу, він заважає нормальному функціонуванню [15].

Метою шкідливого програмного забезпечення є отримання незаконної вигоди за рахунок користувача. Незважаючи на те, що зловмисне програмне забезпечення не може пошкодити апаратне або мережеве обладнання системи, воно може викрасти, зашифрувати або видалити дані, змінити функції комп'ютера або отримати контроль над ним. Крім того, він може контролювати діяльність комп'ютера без відома користувача.

Віруси вже дуже рідкісні. Їх повністю замінюють усілякі мережеві хробаки та шпигунські програми. Сьогодні можна нарахувати з десяток файлових вірусів, які залишаються активними і навіть іноді демонструють спалахи активності. Ці сплески пов'язані з побічним ефектом цих недавніх вірусів, що відображається в зараженні виконуваних файлів поштовими хробаками. Ці файли надсилаються разом із електронними листами, зараженими хробаками. Дуже часто зустрічаються поштові хробаки Mydoom, NetSky або Bagle, заражені файловими вірусами, такими як Funlove, Xorala, Parite або Spaces.

Основними і домінуючими представниками сучасних вірусів є мережеві хробаки, які активно використовують усі види технологій класичних вірусів. Все дуже просто, з появою Інтернету мережеві та комунікаційні технології отримали сильний поштовх у своєму розвитку. Обсяг інформації, що передається по всіх видах каналів зв'язку, значно зріс за останні кілька років і продовжить зростати в майбутньому. Все це створює сприятливе середовище для швидкого розвитку шкідливих програм, особливо на тлі низької безпеки більшості мереж. Автори вірусів активно шукають усілякі вразливості програмного та системного програмного забезпечення, які потім використовується для мережевих атак і впровадження вірусів.

Основні характерні ознаки, які найбільш яскраво проявилися в останні роки в сучасних вірусах: [21]

• активне використання всіляких уразливостей в різних операційних системах і програмному забезпеченні;

• використання спам-технологій дозволяє швидко поширювати віруси в Інтернеті;

• використання в одному вірусі: stealth, polymorphic, trojan, backdoor технологій;

• створення гігантської мережі «зомбі-машин», що дозволяє проводити масові DDoS-атаки та розсилка копій вірусу;

• розсилка повідомлень електронною поштою з метою залучення користувачів на заражені сайти;

• фактичне виділення троянських проксі-серверів в окремий клас, тісно пов'язаний з розсилкою спаму;

• використання для розповсюдження бекдорів і вразливостей, залишених іншими хробаками (хробак Mydoom.a);

• саморозсилка у вигляді архівів (Bagle, NetSky);

• розсилка себе у вигляді захищених паролем архівів з паролем у тексті листа або у вигляді малюнка (Bagle);

• відмова від надсилання тексту електронною поштою, а замість нього надсилання в листі посилання на сайт або на раніше заражений комп’ютер (NetSky);

• активне використання соціальної інженерії.

Категорія мережевих хробаків включає програми, які поширюють свої копії локально та/або глобальних мереж, щоб:

• проникнення на віддалені комп'ютери;

• запуск його копії на віддаленому комп'ютері;

• подальше поширення на інші комп'ютери мережі.

Для поширення хробаки використовують різноманітні комп’ютерні та мобільні мережі: електронну пошту, системи обміну файлами та системи обміну миттєвими повідомленнями.

Більшість відомих хробаків поширюються у вигляді файлів: вкладення до електронного листа, посилання на заражений файл на якомусь веб-ресурсі чи FTP, файл у каталозі обміну тощо.

Деякі хробаки (так звані безтілесні або пакетні хробаки) поширюються у вигляді мережевих пакетів, проникають безпосередньо в пам'ять комп'ютера і активують свій код.

Для проникнення на віддалені комп’ютери та запуску їх копій черв’яки використовують різні методи: соціальну інженерію (наприклад, текст електронного листа із закликом відкрити вкладений файл), прогалини в конфігурації мережі (наприклад, копіювання на диск з повний доступ), помилки в службах безпеки операційних систем і додатків.

До категорії класичних комп'ютерних вірусів відносяться програми, які розповсюджують свої копії по ресурсах локального комп'ютера для наступних цілей:

• для подальшого запуску його коду при будь-яких діях користувача;

• для його подальшого впровадження в інші комп'ютерні ресурси.

На відміну від хробаків, віруси не використовують мережеві служби для проникнення на інші комп’ютери. Копія вірусу потрапляє на віддалені комп'ютери тільки в тому випадку, якщо заражений об'єкт активується на іншому комп'ютері з якоїсь причини, що не залежить від функціональності вірусу, наприклад:

• під час зараження доступних дисків вірус проникав у файли, розташовані на мережевому ресурсі;

• вірус скопіював себе на знімний носій або заразив на ньому файли;

• користувач надіслав електронний лист із зараженим вкладенням.

Троянське програмне забезпечення включає програмне забезпечення, яке виконує різноманітні дії, несанкціоновані користувачем:

збирання інформації та передача її зловмиснику, її знищення або зловмисна зміна, порушення продуктивності комп’ютера або використання ресурсів комп’ютера в непристойних цілях.

До категорії хакерських утиліт відносяться:

• утиліти для автоматизації створення вірусів, хробаків і троянських програм (конструктори);

• програмні бібліотеки, призначені для створення шкідливого програмного забезпечення;

• хакерські утиліти для приховування коду заражених файлів від антивірусної перевірки (шифрувальники файлів);

• Утиліти, які грають «нечисті шутки» з комп'ютером. Такого роду утиліти ускладнюють роботу з комп'ютером;

• програмне забезпечення, яке повідомляє користувачеві завідомо неправдиву інформацію про його дії в системі;

• інші програми, які навмисно завдають прямого чи непрямого збитку комп'ютерам (як локальним, так і віддаленим).

Аналіз класифікації шкідливого програмного забезпечення виявив наявність величезної кількості різноманітних програм такого роду з класифікаційними ознаками. Кожне шкідливе програмне забезпечення, у свою чергу, має різні функції, завдання та властивості. Реалізація загроз інформаційній безпеці, пов’язаних із використанням шкідливого програмного забезпечення, може призвести до порушення всіх властивостей інформаційної безпеки (конфіденційності, доступності та цілісності). У той же час, кількість шкідливого програмного забезпечення зростає в міру розвитку та ускладнення програмного забезпечення, а взаємодії, що призводять до реалізації таких загроз, є досить складними.

Незважаючи на інтенсивний розвиток комп'ютерної техніки та інформаційних технологій, вразливість сучасних інформаційних систем і комп'ютерних мереж, на жаль, не зменшується. Тому проблеми забезпечення інформаційної безпеки привертають пильну увагу як фахівців у галузі комп'ютерних систем і мереж, так і численних користувачів, у тому числі компаній, що працюють у сфері електронного бізнесу.

Висновки до другого розділу

Перераховано заходи безпеки для корпоративних мереж та окремо наведено три рівні безпеки з мінімальним, розширеним та максимальним рівнями відповідно.

Проаналізовано найпоширеніші загрози мережевій безпеці з урахуванням сучасних тенденцій.

Доведено, що надійність та відмовостійкість є важливими компонентами безпечної та комфортної роботи корпоративної мережі. Більшість комунікаційних програм, від мобільних телефонних розмов до транзакцій кредитними картками, передбачає наявність надійної мережі. На цьому рівні очікується, що дані пройдуть мережею та прибудуть неушкодженими до місця призначення. Фізичні системи, що утворюють мережу, з іншого боку, піддаються широкому спектру проблем, починаючи від спотворення сигналу до збоїв компонентів.

3 ТЕХНОЛОГІЇ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯ CISCO AVVID

3.1. Огляд мережевої інфраструктури Cisco AVVID

Мережна інфраструктура Cisco AVVID забезпечує технологічну основу для Cisco AVVID. Це аналог фундаменту із залитого бетону та сталевої арматури, над яким стоїть конструкція промислової міцності. Без цієї основи не існує єдиної системи, що об'єднує програми. З його допомогою можна побудувати масштабовану, стійку структуру мережі, яка підтримує весь набір комунікаційних вимог підприємства. Мережева інфраструктура Cisco AVVID забезпечує корпоративну основу, яка поєднує IP-з'єднання з високою продуктивністю, безпекою та доступністю. Хоча багаторівневі прикладні рішення, такі як голосові або відеомережі, можуть вимагати змін в інфраструктурі, цей архітектурний підхід забезпечує основу для оптимізації принципів і методів проектування [22].

Оскільки вимоги до мережі відрізняються, конкретні варіанти топології (сітка або концентратор і спиця), медіа (Frame Relay або асинхронний режим передачі [ATM]) і загальна мережа (LAN, WAN або MAN) повинні бути враховані в кожній реалізації.

Мережна інфраструктура Cisco AVVID забезпечує гнучкість проектування для задоволення цих різноманітних вимог.

Створення фундаменту для стійких мереж. Передумова стійкості є центральною темою Cisco AVVID та мережевої інфраструктури Cisco AVVID. Цю тему можна розділити на чотири основні рівні: стійкість мережі, стійкість комунікацій, стійкість додатків і стійкість бізнесу.

Відмовостійкість мережі — інтелект мережі забезпечує адаптивність, гнучкість і розподілену реакцію на окремі точки збою. Виміри стійкості мережі включають фізичну надмірність (лінії та вузли) і конструкцію мережі на основі сітки. Однак Cisco суттєво вдосконалює принципи здорового глузду дизайну за

допомогою ключових можливостей Cisco IOS, включаючи стійку маршрутизацію, комутацію, IP-сервіси та багатопротокольну комутацію міток (MPLS).

Відмовостійкість комунікацій — комунікації на основі IP безпосередньо виграють від стійкості мережі. Створюючи конвергентну мережеву інфраструктуру, організації можуть економічно ефективно розгортати різноманітні комунікації, такі як IP-телефонія, дистанційна робота, відеоконференції та уніфікований обмін повідомленнями, що збільшує та покращує контакт із клієнтами, партнерами та постачальниками навіть у разі збоїв.

Відмовостійкість додатків. Мережеві додатки безпосередньо виграють від відмовостійкості мережі та комунікацій. Наприклад, стійкість додатків забезпечується такими елементами дизайну мережевої інфраструктури Cisco AVVID, як дизайн розподілених центрів обробки даних, відновлення центрів обробки даних і віддалена реплікація даних.

Стійкість бізнесу. Стійкість робочого місця досягається шляхом розподілу працівників між кількома розрізненими середовищами. Технології, які забезпечують дистанційну роботу, спільне використання робочого столу, офісні готелі та мобільність співробітників, є важливими для забезпечення оптимальної продуктивності під час збоїв.

Стійкість бізнесу є наступним етапом еволюції від традиційних структур підприємства, орієнтованих на місце, до високовіртуалізованих організацій, орієнтованих на людей, які дозволяють людям працювати будь-коли та будь-де. Стійкість бізнесу, збудована від інфраструктури, дозволяє організаціям швидко, рішуче та ефективно реагувати на непередбачені сили.

Навіщо впроваджувати мережеву інфраструктуру Cisco AVVID. Змінний бізнес-клімат глобальної економіки вимагає від великих і малих організацій впровадження систем управління інформацією, які сприяють адаптації та стійкості, одночасно забезпечуючи стабільність усієї комунікаційної інфраструктури. Як компаніям продовжувати процвітати та виживати в цьому новому бізнес-середовищі? Компанії повинні використовувати потужність Інтернету та

ефективну мережеву інфраструктуру, щоб підвищити продуктивність і прибутковість.

Саме тут Cisco Systems може допомогти. Мережна інфраструктура Cisco AVVID забезпечує принципи проектування, щоб увімкнути основні трансформаційні технології. Ці технології життєво важливі для оптимізації інтеграції критично важливих програм у конвергентне мережеве середовище.

Значне підвищення продуктивності можна підвищити, розробивши конвергентне мережеве середовище, здатне обробляти весь набір комунікаційних програм організації, одночасно розширюючи послуги для віддалених сайтів, дистанційних працівників і мобільних співробітників.

Це твердження було нещодавно підтверджено результатами опитування спеціалістів із голосових і даних, проведеного компанією META Group:

• Майже 70 відсотків респондентів вважають, що конвергенція їхніх мереж дозволить заощадити істотну або помірну інфраструктуру

• 50 відсотків респондентів очікують значної або помірної економії адміністративних витрат

• 60 відсотків респондентів очікують від суттєвої до помірної економії на платній об’їзній дорозі

Мережева інфраструктура Cisco AVVID надає набір інструментів для плавної та безпечної інтеграції різноманітних організаційних елементів, що змінюються, для створення більш ефективного комунікаційного середовища. Сьогоднішня бізнес-реальність — це повернення до основ прибутку, грошового потоку та продуктивності. Cisco AVVID може допомогти використати потужність мережі, щоб увімкнути продуктивні програми, які керують цими бізнес-константами.

Лише ті організації, які стратегічно використовують мережі для поєднання бізнесу та інноваційних технологічних рішень, досягнуть успіху в новій Інтернет-економіці. Завдяки такому інтуїтивному підходу організації можуть підвищувати прибутковість і підвищувати лояльність клієнтів за рахунок підвищення продуктивності.

3.2. Компоненти мережевої інфраструктури Cisco AVVID

Адміністратори мереж, які проектують і будують мережі для підтримки таких рішень, як голос і відео, повинні спочатку розглянути компоненти, які дозволяють мережам працювати належним чином. Окремі пристрої або вузли часто стають центром проектних рішень організацій. Однак окремий елемент — будь то комутатор, маршрутизатор чи будь-який інший мережевий пристрій — є лише одним із компонентів усієї мережі. Дедалі важливішим стає зосередження на тому, як підключаються пристрої, які функції та протоколи використовуються, а також на тому, як вони використовуються для створення основи для того, що можна розмістити на вершині мережі. Якщо фундамент нестабільний, розкладання технологічних рішень у мережі створює додаткові проблеми.

Створюючи міцну основу базового підключення та впровадження протоколу, мережева інфраструктура Cisco AVVID вирішує п’ять основних проблем розгортання мережі: висока доступність, якість обслуговування (QoS), безпека, мобільність і масштабованість.

***Висока доступність*.** Визначення того, наскільки мережа стійка до змін або збоїв, є основною проблемою для менеджерів мережі. Ця оцінка доступності мережі є критичною. Важливо, щоб кожне розгортання мережі наголошувало на доступності як на першому етапі базового проектування мережі.

Доступність потрібно розглядати з точки зору користувача. Для користувача мережа не працює незалежно від того, чи виходить з ладу програма, вимикається маршрутизатор чи розривається шматок оптоволокна. Основні проблеми доступності, які необхідно вирішити, включають:

• Апаратне резервування — часто це перший рівень резервування в мережі. Cisco пропонує, наприклад, у своїх модульних продуктах варіанти резервних механізмів диспетчера та подвійних джерел живлення. Це часто є першим захистом від збою мережі.

• Відмовостійкість протоколу. Належна практика проектування визначає, як і коли використовувати резервування протоколу, включаючи розподіл

навантаження, швидкість конвергенції та керування резервуванням шляхів. Всупереч поширеній думці, якщо деяка надлишковість є хорошою, то більша надлишковість не обов'язково є кращою.

• Проектування пропускної здатності мережі. Хороша практика проектування включає планування пропускної здатності. Скільки трафіку може обслуговувати з'єднання в гіршому випадку? Необхідно переконатися, що зв'язок може обробляти подвійний трафік, якщо надлишкове з'єднання виходить з ладу. Планування потужності має бути включено на етапі проектування мережі, щоб забезпечити плавну інтеграцію нових технологій (таких як відеоконференції). За допомогою рішень мережевої інфраструктури Cisco AVVID для апаратного резервування та стійкості протоколів у поєднанні з ефективним плануванням можна оптимізувати високу доступність мережевих ресурсів.

Якість обслуговування (QoS). Програми для передачі голосу, відео та критично важливих даних є важливими базовими інструментами продуктивності, які роблять бізнес успішним. Забезпечення ефективної доставки цих програм вимагає вмілого керування трафіком, особливо в контексті інтегрованого мережевого рішення. Якість обслуговування (QoS) є ключовою мережевою інфраструктурою Cisco AVVID, що забезпечує можливість такого середовища.

Безпека. Безпеку слід розглядати як невід'ємний елемент будь-якої мережі Cisco AVVID. Комунікаційна мережа організації — це базове середовище, що з'єднує всіх користувачів, сервери, програми та постачальників послуг. Впровадження надійного пакету безпеки забезпечує найкращий захист від можливої втрати інформації, втручання або порушення продуктивності. Пакет безпеки Cisco наголошує на трьох ключових областях: безпека внутрішньої мережі, безпека зовнішньої мережі та ідентифікація користувачів і програм для забезпечення належного призначення політики.

• Внутрішня безпека мережі. Забезпечення безпеки внутрішньої мережі включає відстеження фізичних проблем, проблем кінцевої точки, додатків і рівня безпеки 2.

• Безпека зовнішньої мережі — безпека зовнішньої мережі зосереджена на захисті інтерфейсу між внутрішньою мережею організації та зовнішнім світом (краєм Інтернету).

• Ідентифікація мережі. Розглядаючи загальну схему безпеки мережі, важливо створити структуру, яка дозволить мережевому адміністратору впроваджувати контроль доступу до мережі на основі ідентичності та застосування політики аж до рівня користувача та індивідуального порту доступу.

Можливості мережевої інфраструктури Cisco AVVID представляють величезний набір додатків і функцій безпеки як на основі пристроїв, так і на сервері. Списки контролю доступу (ACL), брандмауери, аутентифікація на основі сервера, системи виявлення вторгнень і можливості віртуальної приватної мережі можуть бути інтегровані в безперебійне середовище безпеки. Разом ці можливості забезпечують адаптовану, стійку зону безпеки для забезпечення безпечної передачі даних, голосового зв’язку та спільного доступу до програм.

3.3. Налаштування безпеки в Cisco AVVID для корпоративної мережі

За допомогою багатоадресної IP-адреси важливо захистити трафік від атак типу «Відмова в обслуговуванні» (DoS) або викрадення потоку з боку шахрайських джерел або шахрайських RP для корпоративної мережі.

DoS-атаки впливають на доступність і ефективність мережі. Якщо шахрайська програма або пристрій може генерувати достатньо трафіку та націлювати цей трафік на джерело, це може серйозно вплинути на ресурси процесора та пам’яті.

• Викрадення потоку дозволяє будь-якому хосту в мережі стати активним джерелом для будь-якої легітимної багатоадресної групи. Легко завантажити з Інтернету безкоштовну програму чату з підтримкою багатоадресної передачі та змінити групову адресу IP Multicast на таку саму, як у законно налаштованих додатках багатоадресної передачі. Якщо мережеві пристрої не захищені від «прийняття» неавторизованих джерел, шахрайське джерело може вплинути на

потоки IP Multicast. Здебільшого одержувачі не знають деталей, пов’язаних із тим, яке джерело дійсно відповідає за яку групу.

Потрібно використати наступні команди на IP-маршрутизаторах із підтримкою Multicast для захисту від шахрайських джерел і шахрайських RP:

• *ip pim accept-register*

• *rp-announce-filter*

• *ip pim rp-address*

• *ip igmp access-group*

Джерело — це будь-який хост, який може надсилати багатоадресний IP-трафік. Несанкціоновані джерела — це неавторизовані джерела, які надсилають багатоадресний IP-трафік.

Джерела надсилають груповий трафік на маршрутизатор першого стрибка. Маршрутизатор першого переходу надсилає повідомлення Register до RP з інформацією про активне джерело. Щоб захистити маршрутизатор від несанкціонованих повідомлень Register, використовуйте команду ip pim accept-register. Ця команда, яка може бути використана лише для RP-кандидатів, налаштовує RP на прийом повідомлень Register лише з певного джерела. Якщо повідомлення реєстру відхилено, повідомлення про зупинку реєстру надсилається назад ініціатору реєстру.

• Якщо використовується атрибут list acl, можна налаштувати розширені списки доступу, щоб визначити, які пари (джерело та група) дозволені або заборонені, коли вони відображаються в повідомленні реєстрації.

• Якщо використовується атрибут карти маршруту, на маршрутизаторі можна застосувати типові операції карти маршруту для адреси джерела, яка відображається в повідомленні реєстрації.

У наступному прикладі показано конфігурацію, яка дозволяє реєстрацію з перелічених джерел (сервер 10.5.10.20 MoH і сервер 10.5.11.20 IP/TV):

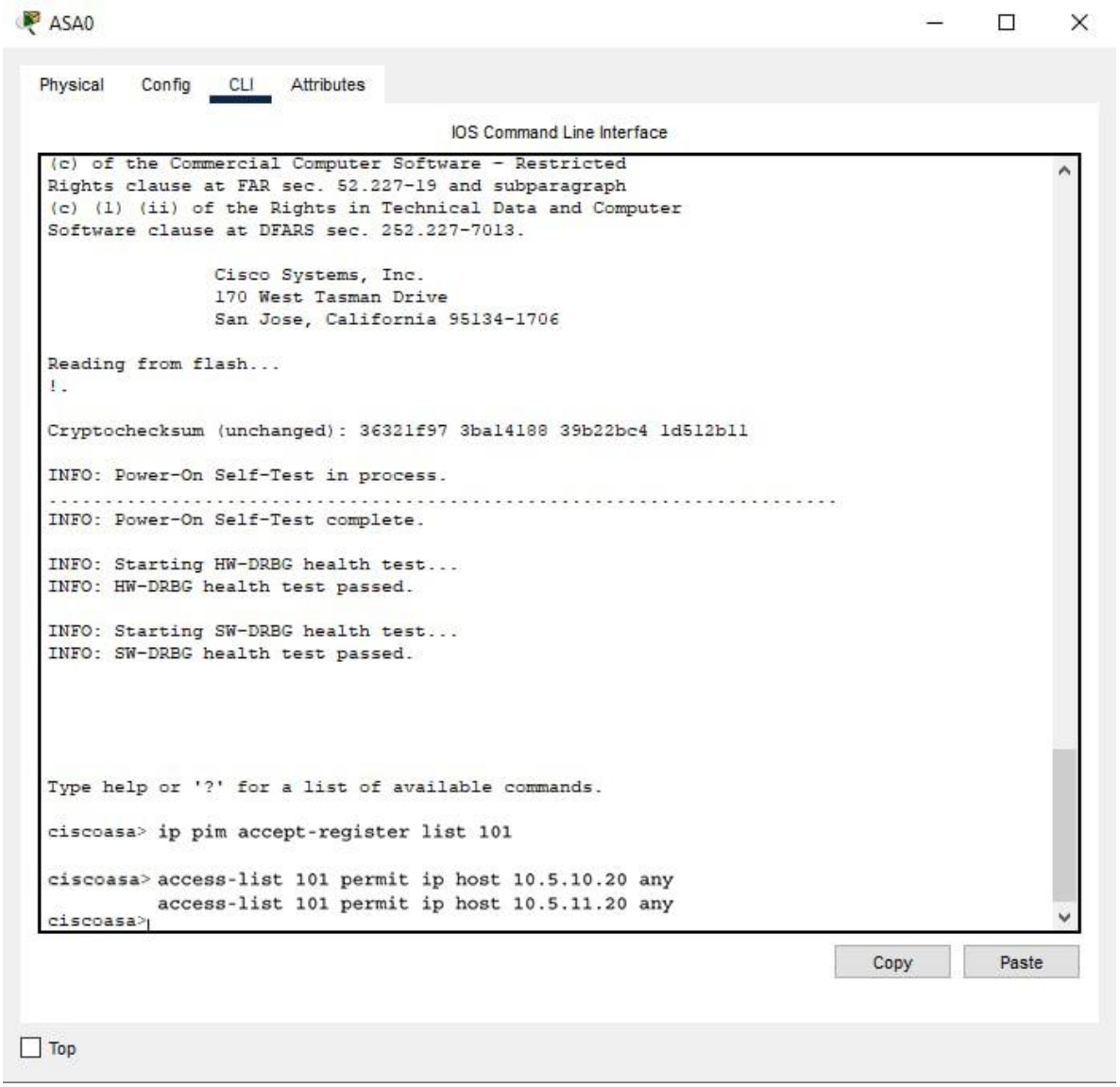

Рис.3.1. Налаштування конфігурації

Крім того, можна налаштувати список, який вказує, які групи дозволені з джерел на момент реєстрації. Наступний приклад ілюструє конфігурацію, яка дозволяє групову адресу MoH із сервера MoH і три групи IP/TV із сервера IP/TV.

access-list 101 permit ip host 10.5.10.20 239.192.240.0 0.0.3.255

access-list 101 permit ip host 10.5.11.20 239.192.244.0 0.0.3.255

access-list 101 permit ip host 10.5.11.20 239.192.248.0 0.0.3.255

access-list 101 permit ip host 10.5.11.20 239.255.0.0 0.0.255.255

Якщо несанкціоноване джерело підключається до Інтернету та маршрутизатор першого переходу намагається зареєструвати це нове джерело в RP, реєстрацію буде відхилено. У наступному прикладі показано вихідні дані

налагодження для невдалої спроби реєстрації маршрутизатором 10.0.0.37 для джерела 10.5.12.1 і групи 239.194.1.1 [23].

1d03h: PIM: Received v2 Register on Vlan59 from 10.0.0.37

1d03h: (Data-header) for 10.5.12.1, group 239.194.1.1

1d03h: PIM Register for 10.5.12.1, group 239.194.1.1 rejected

1d03h: PIM: Send v2 Register-Stop to 10.0.0.37 for 10.5.12.1, group 239.194.1.1

Інженерія трафіку. Розробка трафіку додає великий контроль над розгортанням і роботою багатоадресної IP-адреси. Це також додає складності. Одним із варіантів керування багатоадресною IP-адресою є використання обмежених меж.

Команда ip multicast boundary налаштовує адміністративну межу інтерфейсу та дозволяє або забороняє групові адреси багатоадресної передачі, знайдені в списку доступу. Жодним багатоадресним пакетам не буде дозволено проходити через кордон з обох напрямків. Це дозволяє повторно використовувати ту саму групову адресу багатоадресної розсилки в різних адміністративних доменах.

Якщо інтерфейс RPF для багатоадресного маршруту має межу багатоадресної передачі, налаштовану для цієї групи, її вихідні інтерфейси не будуть заповнені станом багатоадресної переадресації. Повідомлення про приєднання, отримані на інших інтерфейсах, ігноруватимуться, поки межа залишається на інтерфейсі RPF. Якщо інтерфейс RPF змінюється, і межі більше не застосовуються до нового інтерфейсу RPF, буде запроваджено затримку приєднання через затримку заповнення вихідних інтерфейсів. Межа контролює трафік на основі дозволу/заборони конфігурації ACL, пов’язаної з командою boundary. [23]

У наступному прикладі показано межу VLAN2, підключеної до рівня доступу. Показана межа дозволяє груповий діапазон 239.255.0.0 і забороняє всі інші потоки на інтерфейсі VLAN2.

```
interface VLAN2
 description To Access VLAN 2
 ip multicast boundary moh
!
ip access-list standard moh
 remark Permit 239.255, Deny all others
 permit 239.255.0.0 0.0.255.255
 deny any
```

Рис.3.2. Дозвіл групового діапазону 239.255.0.0

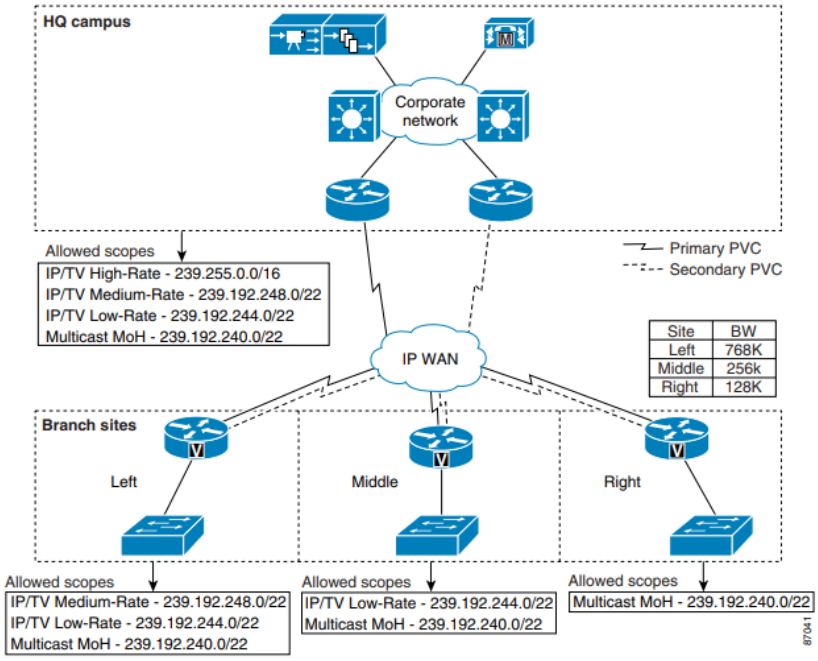

Рис.3.3. Графічне подання адміністративного масштабу, що використовується з межами

Нижче наведено приклад конфігурації маршрутизатора агрегації WAN (Frame-relay). Межа розміщена на послідовних підінтерфейсах, які підключаються до кожного відділення. Граничні команди також можна налаштувати на VLAN/інтерфейсі від комутаторів рівня ядра до маршрутизаторів агрегації WAN.

```
interface Serial4/0.1 point-to-point
 description To leftrtr - 768k
 ip multicast boundary medium-low-moh          Enable a multicast boundary for the 768kbps link

ip access-list standard medium-low-moh
 remark Deny High-rate (.255)
 deny   239.255.0.0 0.0.255.255
 permit any

interface Serial4/0.2 point-to-point
 description To middlertr - 256k
 ip multicast boundary low-moh                 Enable a multicast boundary for the 256kbps link

ip access-list standard low-moh
 remark Deny High-rate (.255), Medium (.248)
 deny   239.255.0.0 0.0.255.255
 deny   239.192.248.0 0.0.3.255
 permit any

interface Serial4/0.3 point-to-point
 description To rightrtr - 128k
 ip multicast boundary moh                     Enable a multicast boundary for the 128kbps link

ip access-list standard moh
 remark Deny High-rate (.255), Medium (.248), Low (.244)
 deny   239.255.0.0 0.0.255.255
 deny   239.192.248.0 0.0.3.255
 deny   239.192.244.0 0.0.3.255
 permit any
```

Рис. 3.4. Приклад конфігурації маршрутизатора агрегації WAN

3.4. Дослідження стратегії Cisco AVVID та SAFE для захисту корпоративних мереж

Організації, які керують великими мережами, все частіше прагнуть створити інфраструктуру на рівні підприємства, яка б служила міцною основою для нових технологій, таких як IP-телефонія та зберігання.

Технологічна структура для Cisco AVVID Архітектура Cisco для голосу, відео та інтегрованих даних (AVVID) є ключовою мережевою архітектурою підприємства від Cisco Systems.

Основна мета безпечного проекту Cisco для корпоративних мереж (safe) полягає в тому, щоб надати зацікавленим сторонам інформацію про найкращі практики щодо проектування та впровадження безпечних мереж. Safe служить посібником для розробників мереж, які розглядають вимоги безпеки їхньої мережі. Safe використовує глибокий підхід до розробки безпеки мережі. Цей тип дизайну зосереджується на очікуваних загрозах і методах їх пом’якшення, а не на

«розмістіть брандмауер тут, розмістіть систему виявлення вторгнень там». Ця стратегія призводить до багаторівневого підходу до безпеки, де збій однієї системи безпеки навряд чи призведе до компрометації мережевих ресурсів. Safe базується на продуктах Cisco та продуктів її партнерів.

Хост є найвірогіднішою ціллю під час атаки та представляє одні з найскладніших викликів з точки зору безпеки. Існують численні апаратні платформи, операційні системи та програми, усі з яких мають оновлення, виправлення та виправлення, доступні в різний час. Оскільки хости надають послуги додатків іншим хостам, які їх запитують, вони надзвичайно помітні в мережі.

Архітектура Cisco для передачі голосу, відео та інтегрованих даних (AVVID) і SAFE — це комплексні стратегії Cisco, які допомагають організаціям успішно та безпечно розробляти та впроваджувати проекти наскрізних мереж.

Наближення конвергенції телефонних послуг, відеоконференцій, IP-мереж передачі даних, послуг на основі програмного забезпечення та нескінченної пропозиції нових технологій створює багато можливостей як для катастрофи, так і для успіху. AVVID надає засновану на стандартах мережеву архітектуру та повний набір найкращих практик, що дозволяє компаніям розробляти бізнес-стратегії та технологічні стратегії, які масштабуються відповідно до мінливих вимог електронного бізнесу. AVVID надає наскрізні мережеві рішення, які допомагають організаціям планувати швидке розгортання нових технологій і нових Інтернет-рішень.

Наскрізне мережеве рішення AVVID включає мережеві клієнтські пристрої, мережеву інфраструктуру від мережевих платформ до інтелектуальних мережевих служб, інструменти проміжного програмного забезпечення Інтернету, обов’язки системного інтегратора та рішення для Інтернет-бізнесу. Стратегія AVVID вирішує три основні проблеми розгортання мережі: продуктивність, масштабованість і доступність.

Стратегія Cisco щодо захищених мереж (SAFE) розпочалася з оригінального «SAFE: план безпеки для корпоративних мереж», 66-сторінкового плану, який

надає найкращу інформацію тим, хто бере участь у розробці та впровадженні захищених мереж. SAFE представляє глибокий захист підходу до проектування безпеки мережі, зосереджуючись на очікуваних загрозах і найкращих способах пом'якшення цих загроз, а не на єдиному наборі правил, яких слід дотримуватися. Результатом є «багаторівневий підхід» до проектування та реалізації безпеки, спрямований на те, щоб запобігти відмові однієї системи безпеки від компрометації мережевих ресурсів організації.

SAFE максимально точно імітує функціональні вимоги сучасних корпоративних мереж. Рішення про впровадження змінювалися залежно від необхідної функціональності мережі. Однак наступні цілі проектування, перелічені в порядку пріоритетності, керувалися процесом прийняття рішень.

Перш за все, SAFE — це архітектура безпеки. Він повинен запобігти більшості атак від успішного впливу на цінні ресурси мережі. Атаки, яким вдається проникнути на першу лінію захисту або походять зсередини мережі, повинні бути точно виявлені та швидко стримані, щоб мінімізувати їхній вплив на решту мережі. Однак для забезпечення безпеки мережа повинна продовжувати надавати критично важливі послуги, які очікують користувачі. Одночасно можна забезпечити належну безпеку мережі та хорошу мережеву функціональність. Архітектура SAFE — це не революційний спосіб проектування мереж, а лише схема захисту мереж.

SAFE також стійкий і масштабований. Стійкість у мережах включає фізичне резервування для захисту від збою пристрою через неправильне налаштування, фізичний збій або мережеву атаку. Хоча можливі простіші конструкції, особливо якщо потреби в продуктивності мережі невисокі, у цьому документі використовується складна конструкція як приклад, оскільки розробка безпеки в складному середовищі є більш складною, ніж у простіших середовищах. Варіанти обмеження складності дизайну обговорюються в цьому документі.

На багатьох етапах процесу проектування мережі потрібно вибирати між використанням інтегрованої функціональності в мережевому пристрої чи використанням спеціалізованого функціонального пристрою. Інтегрована функціональність часто приваблива, оскільки ви можете реалізувати її на наявному

обладнанні або тому, що функції можуть взаємодіяти з рештою пристрою, щоб забезпечити краще функціональне рішення. Прилади часто використовуються, коли необхідна глибина функціональності дуже просунута або коли потреби продуктивності вимагають використання спеціалізованого обладнання. Прийміть рішення, виходячи з потужності та функціональності пристрою в порівнянні з перевагою інтеграції пристрою. Наприклад, іноді можна вибрати інтегрований маршрутизатор Cisco IOS більшої ємності з програмним забезпеченням брандмауера IOS на відміну від меншого маршрутизатора IOS з окремим брандмауером. У цій архітектурі використовуються обидва типи систем. Більшість критично важливих функцій безпеки переходять на спеціальні пристрої через вимоги до продуктивності великих корпоративних мереж.

Незважаючи на те, що більшість корпоративних мереж розвиваються разом зі зростаючими вимогами IT підприємства, архітектура SAFE використовує модульний підхід із нуля. Модульний підхід має дві основні переваги. По-перше, це дозволяє архітектурі вирішувати відносини безпеки між різними функціональними блоками мережі. По-друге, це дозволяє розробникам оцінювати та впроваджувати безпеку на основі модуля за модулем, замість того, щоб намагатися створити повну архітектуру за один етап.

Рисунок 3.5. ілюструє перший рівень модульності в SAFE. Кожен блок представляє функціональну область. Модуль постачальника послуг Інтернету (ISP) не впроваджено підприємством, але включено в тій мірі, в якій у провайдера потрібно запитувати певні функції безпеки, щоб пом’якшити певні атаки.

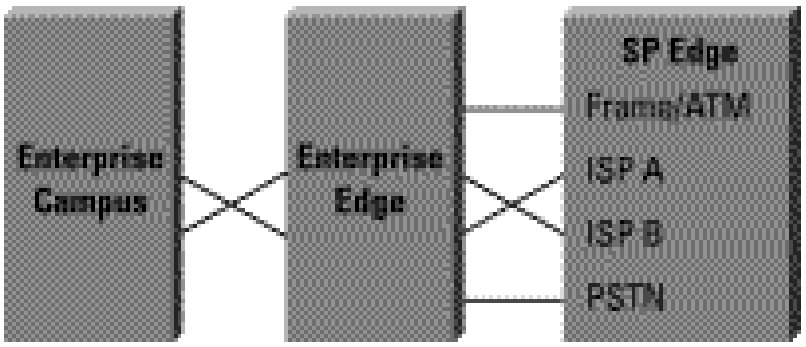

Рис.3.5. Корпоративний композитний модуль

Другий рівень модульності, який показано на рисунку 3.4, представляє вигляд модулів у кожній функціональній області. Ці модулі виконують певні ролі в мережі та мають певні вимоги до безпеки, але їхні розміри не відповідають їхньому масштабу в реальній мережі. Наприклад, будівельний модуль, який представляє пристрої кінцевого користувача, може включати 80 відсотків мережевих пристроїв. Дизайн безпеки кожного модуля описується окремо, але перевіряється як частина повного корпоративного дизайну.

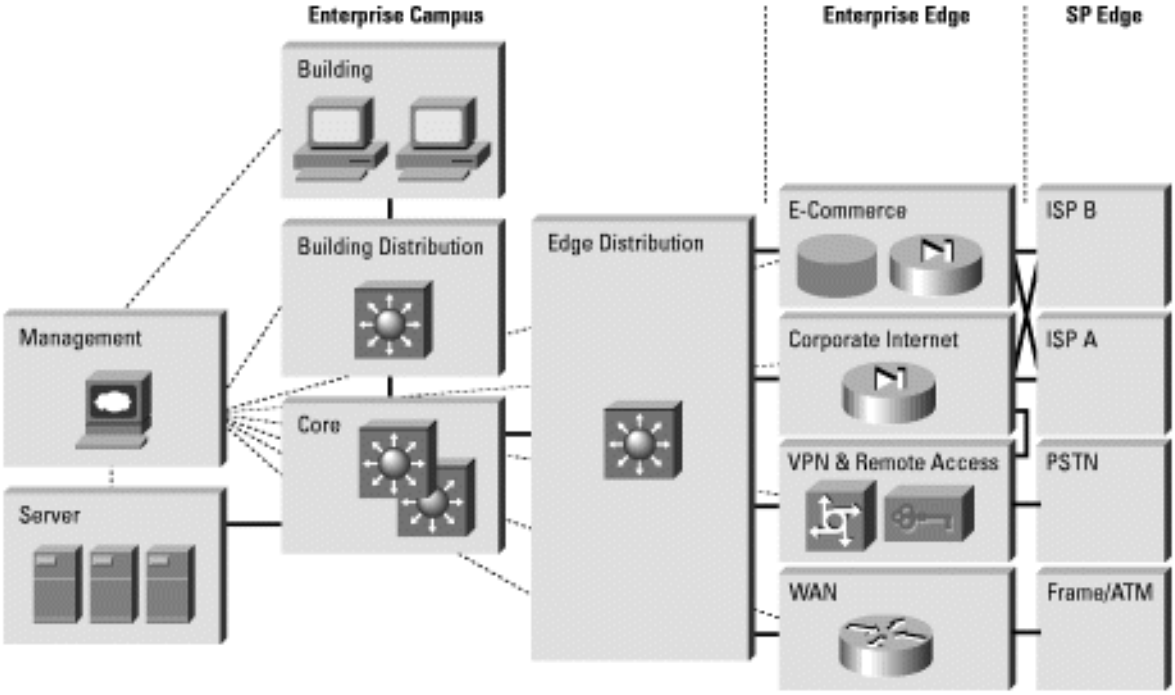

Рис.3.6. Блок-схема Enterprise SAFE

Хоча це правда, що більшість існуючих корпоративних мереж не можна легко розділити на чіткі модулі, цей підхід дає керівництво для впровадження різних функцій безпеки в усій мережі. Автори не очікують, що мережеві інженери розроблятимуть свої мережі, ідентичні реалізації SAFE, а радше використовують комбінацію описаних модулів та інтегрують їх у існуючу мережу.

Маршрутизатори контролюють доступ від кожної мережі до кожної мережі. Вони рекламують мережі та фільтрують, хто може ними користуватися, і потенційно є найкращими друзями хакерів. Безпека маршрутизатора є критично важливим елементом будь-якого розгортання безпеки. За своєю природою

маршрутизатори забезпечують доступ, тому треба захистити їх, щоб зменшити ймовірність прямого зламу.

Як і маршрутизатори, комутатори (як рівня 2, так і рівня 3) мають власний набір міркувань безпеки. На відміну від маршрутизаторів, доступно не так багато загальнодоступної інформації про ризики безпеці комутаторів і те, що можна зробити, щоб зменшити ці ризики. Більшість методів безпеки, описаних у попередньому розділі «Маршрутизатори — цілі», застосовуються до комутаторів. Крім того, слід вжити наступних запобіжних заходів:

Для портів, які не потребують транка, будь-які параметри транка повинні бути вимкнені, а не автоматично. Це запобігає тому, що хост стане магістральним портом і отримує весь трафік, який зазвичай перебуває на магістральному порту.

Переконайтеся, що магістральні порти використовують номер віртуальної локальної мережі (VLAN), який більше ніде не використовується на комутаторі. Це запобігає досягненню пакетами, позначеними тією ж VLAN, що й магістральний порт, іншої VLAN без перетину пристрою рівня 3 [24].

Налаштуйте всі невикористовувані порти на комутаторі на VLAN, яка не має підключення рівня 3. А ще краще вимкнути будь-який непотрібний порт. Це запобігає підключенню хакерів до невикористаних портів і спілкуванню з рештою мережі.

Потрібно уникати використання VLAN як єдиного методу захисту доступу між двома підмережами. Можливість людської помилки в поєднанні з розумінням того, що VLAN і протоколи тегування VLAN не були розроблені з урахуванням безпеки, робить їх використання в чутливих середовищах недоцільним. Якщо для розгортання безпеки потрібні VLAN, обов’язково зверніть увагу на конфігурації та вказівки, згадані вище.

У межах існуючої VLAN приватні VLAN забезпечують додаткову безпеку для певних мережевих програм. Приватні VLAN обмежують, які порти в межах VLAN можуть спілкуватися з іншими портами в тій же VLAN. Ізольовані порти в межах VLAN можуть обмінюватися даними лише з безладними портами. Порти співтовариства можуть спілкуватися лише з іншими членами того ж співтовариства

та безладних портів. Безладні порти можуть спілкуватися з будь-яким портом. Це ефективний спосіб пом’якшити вплив одного скомпрометованого хоста. Розглянемо стандартний сегмент загальнодоступних послуг із сервером Web, FTP і системою доменних імен (DNS). Якщо DNS-сервер зламано, хакер може переслідувати два інших хости, не проходячи назад через брандмауер. Якщо розгорнуто приватні VLAN, коли одна система скомпрометована, вона не може спілкуватися з іншими системами. Єдина ціль, яку може переслідувати хакер, це хости по інший бік брандмауера.

Хост є найвірогіднішою ціллю під час атаки та представляє одні з найскладніших викликів з точки зору безпеки. Існують численні апаратні платформи, операційні системи та програми, усі з яких мають оновлення, виправлення та виправлення, доступні в різний час. Оскільки хости надають послуги додатків іншим хостам, які їх запитують, вони надзвичайно помітні в мережі. Наприклад, багато людей відвідували www.whitehouse.gov, який є хостом, але мало хто намагався отримати доступ до s2-0.whitehouseisp.net, який є маршрутизатором. Через таку видимість хости є пристроями, які найчастіше атакуються під час будь-якої спроби вторгнення в мережу.

Частково через проблеми безпеки, згадані вище, хости також є найбільш успішно скомпрометованими пристроями. Наприклад, даний веб-сервер в Інтернеті може запускати апаратну платформу від одного постачальника, мережеву карту від іншого, операційну систему від ще одного постачальника та веб-сервер з відкритим кодом або від ще одного постачальника. Крім того, той самий веб-сервер може запускати програми, які вільно поширюються через Інтернет, і може спілкуватися з сервером бази даних, який запускає варіації заново. Це не означає, що вразливі місця в безпеці спричинені саме багатоджерельною природою всього цього, а радше те, що зі збільшенням складності системи зростає ймовірність збою [25].

Щоб убезпечити хости, приділяйте особливу увагу кожному компоненту системи. Підтримуйте будь-які системи в актуальному стані за допомогою останніх патчів, виправлень тощо. Зокрема, зверніть увагу на те, як ці патчі впливають на роботу інших компонентів системи. Оцініть усі оновлення на тестових системах,

перш ніж застосовувати їх у робочому середовищі. Невиконання цього може призвести до того, що сам патч спричинить відмову в обслуговуванні (DoS).

Найстрашніша атака - це та, яку не можна зупинити. При правильному виконанні розподілена відмова в обслуговуванні (DDoS) є саме такою атакою. «Початок безпеки мережі», DDoS працює, змушуючи десятки чи сотні машин одночасно надсилати помилкові дані на IP-адресу. Мета такої атаки, як правило, полягає не в тому, щоб вимкнути окремий хост, а в тому, щоб змусити всю мережу припинити реагувати. Наприклад, розглянемо організацію з підключенням до Інтернету DS3 (45 Мбіт/с), яка надає послуги електронної комерції користувачам свого веб-сайту. Такий сайт має особливу увагу до безпеки та має функцію виявлення вторгнень, брандмауери, журналювання та активний моніторинг. На жаль, усі ці пристрої безпеки не допомагають, коли хакер запускає успішну DDoS-атаку.

Розглянемо 100 пристроїв у всьому світі, кожен із яких має підключення до Інтернету DS1 (1,5 Мбіт/с). Якщо цим системам віддалено наказати заповнити послідовний інтерфейс Інтернет-маршрутизатора організації електронної комерції, вони можуть легко заповнити DS3 помилковими даними. Навіть якщо кожен хост здатний генерувати лише 1 Мбіт/с трафіку (лабораторні випробування показують, що стандартна робоча станція Unix може легко генерувати 50 Мбіт/с за допомогою популярного інструменту DDoS), цей обсяг все одно більш ніж удвічі перевищує обсяг трафіку електронної мережі. комерційний сайт може впоратися. Як наслідок, законні веб-запити втрачаються, і сайт, здається, не працює для більшості користувачів. Локальний брандмауер видаляє всі помилкові дані, але до того часу шкода вже зроблена. Трафік перетнув підключення WAN і заповнив посилання.

Лише завдяки співпраці зі своїм провайдером ця фіктивна компанія електронної комерції може сподіватися запобігти такій атаці. Інтернет-провайдер може налаштувати обмеження швидкості на вихідному інтерфейсі до сайту компанії. Це обмеження швидкості може зменшити більшість небажаного трафіку, якщо він перевищує заздалегідь визначену кількість доступної пропускної здатності. Головне – правильно позначити трафік як небажаний.

Поширеними формами DDoS-атак є ICMP-флуд, TCP SYN-флуд або UDP-флуд. У середовищі електронної комерції цей тип трафіку досить легко класифікувати. Лише в разі обмеження атаки TCP SYN на порт 80 (http) адміністратор ризикує заблокувати законних користувачів під час атаки. Навіть тоді краще тимчасово заблокувати нових законних користувачів і зберегти з'єднання для маршрутизації та керування, ніж мати маршрутизатор переповнений і втратити всі з'єднання [25].

Більш складні атаки використовують трафік порту 80 із встановленим бітом ACK, щоб трафік виглядав як законні веб-транзакції. Малоймовірно, що адміністратор зможе належним чином класифікувати таку атаку, оскільки підтверджені зв'язки TCP – це саме той тип, який ви хочете дозволити у своїй мережі.

Один із підходів до обмеження такого роду атак полягає в дотриманні вказівок, викладених у RFC 1918 і RFC 2827 [26]. RFC 1918 визначає мережі, які зарезервовано для приватного використання та ніколи не повинні бути доступні в загальнодоступному Інтернеті. Для вхідного трафіку на маршрутизаторі, підключеному до Інтернету, можна застосувати фільтрацію RFC 1918 і 2827, щоб запобігти несанкціонованому трафіку від досягнення корпоративної мережі. Якщо цей фільтр реалізований у провайдера Інтернет-послуг, він запобігає проходженню пакетів DDoS-атаки, які використовують ці адреси як джерела, через канал WAN, потенційно зберігаючи пропускну здатність під час атаки. Загалом, якби інтернет-провайдери в усьому світі запроваджували вказівки в RFC 2827, підробка адреси джерела була б значно зменшена. Хоча ця стратегія безпосередньо не запобігає DDoS-атакам, вона запобігає маскуванню джерела таких атак, що значно полегшує відстеження до атакуючих мереж.

Програми кодуються людьми (переважно) і, як такі, піддаються численним помилкам. Ці помилки можуть бути доброякісними (наприклад, помилка, через яку документ друкується неправильно), або злоякісні (наприклад, помилка, через яку номери кредитних карток на сервері корпоративної бази даних стають доступними через анонімний FTP). Системи виявлення вторгнень (IDS) мають на меті виявляти

злоякісні проблеми, а також інші більш загальні вразливості безпеки. Виявлення вторгнень діє як система сигналізації у фізичному світі. Коли IDS виявляє щось, що вона вважає атакою, вона може або сама вжити коригувальних заходів, або повідомити систему керування про дії адміністратора. Деякі системи більш-менш обладнані для реагування та запобігання такій атаці. Виявлення вторгнень на основі хосту може працювати, перехоплюючи виклики ОС і програм на окремому хості. Він також може працювати шляхом постфактум аналізу локальних файлів журналу. Перший підхід дозволяє краще запобігати атакам, тоді як другий підхід диктує більш пасивну роль у відповідь на атаку. Через специфіку своєї ролі системи IDS на основі хоста (HIDS) часто краще запобігають конкретним атакам, ніж Network IDS (NIDS), які зазвичай видають сповіщення лише після виявлення атаки. Однак ця специфіка спричиняє втрату перспективи для загальної мережі. Ось де NIDS перевершує. Cisco рекомендує поєднання двох систем — HIDS на критичних хостах і NIDS, що переглядає всю мережу — для повної системи виявлення вторгнень.

Після розгортання треба налаштувати реалізацію IDS, щоб підвищити її ефективність і видалити «помилкові спрацьовування». Помилкові спрацьовування визначаються як тривоги, спричинені законним трафіком або діяльністю. Хибнонегативні атаки – це атаки, які система IDS не бачить. Після того, як IDS налаштовано, можна налаштувати його точніше щодо його ролі пом’якшення загроз. Як згадувалося вище, потрібно налаштувати HIDS, щоб зупинити більшість дійсних загроз на рівні хоста, оскільки він добре підготовлений для визначення того, що певна діяльність справді є загрозою.

При прийнятті рішення щодо пом’якшувальних ролей для NIDS є два основні варіанти:

Перший варіант, потенційно найшкідливіший у разі неправильного розгортання, полягає в «уникненні» трафіку через додавання фільтрів контролю доступу на маршрутизаторах. Коли NIDS виявляє атаку від певного хоста через певний протокол, він може заблокувати цей хост від входу в мережу на заздалегідь визначений проміжок часу. Хоча на перший погляд це може здатися чудовою

підмогою для адміністратора безпеки, насправді це має бути дуже обережно реалізовано, якщо взагалі. Перша проблема полягає в підроблених адресах. Якщо NIDS бачить трафік, який відповідає атаці, і цей конкретний сигнал тривоги викликає відповідь уникнення, NIDS розгорне список доступу до пристрою. Проте, якщо атака, яка викликала тривогу, використовувала підроблену адресу, NIDS тепер заблокував адресу, яка ніколи не ініціювала атаку. Якщо IP-адреса, яку використав хакер, виявилася IP-адресою вихідного HTTP-проксі-сервера основного провайдера, величезна кількість користувачів може бути заблокована. Це саме по собі може бути цікавою загрозою DoS у руках креативного хакера.

Щоб пом'якшити ризики уникнення, зазвичай слід використовувати його лише для TCP-трафіку, який значно складніше успішно підробити, ніж UDP. Використовуйте його лише у випадках, коли загроза реальна, а ймовірність хибного спрацьовування атаки дуже мала. Однак усередині мережі існує набагато більше варіантів. З ефективним розгортанням фільтрації RFC 2827 підроблений трафік має бути дуже обмеженим. Крім того, оскільки клієнти зазвичай не перебувають у внутрішній мережі, можна прийняти більш обмежувальну позицію проти внутрішніх спроб атак. Ще одна причина цього полягає в тому, що внутрішні мережі часто не мають того самого рівня фільтрації стану, який мають крайові з'єднання. Таким чином, на IDS потрібно покладатися більше, ніж на зовнішнє середовище.

Другий варіант пом'якшення загрози NIDS – це використання скидання TCP. Як випливає з назви, скидання TCP працює лише з трафіком TCP і припиняє активну атаку, надсилаючи повідомлення скидання TCP на атакуючий і атакуваний хост. Оскільки TCP-трафік складніше підробити, потрібно частіше використовувати скидання TCP, ніж уникати.

З точки зору продуктивності, NIDS спостерігає за пакетами в дроті. Якщо пакети надсилаються швидше, ніж NIDS може їх обробити, погіршення роботи мережі не відбувається, оскільки NIDS не знаходиться безпосередньо в потоках даних. Однак NIDS втратить ефективність, і пакети можуть бути пропущені, викликаючи як хибнонегативні, так і хибнопозитивні результати. Обов'язково

уникайте перевищення можливостей IDS, щоб отримати від них переваги. З точки зору маршрутизації, IDS, як і багато механізмів з усвідомленням стану, не працює належним чином у середовищі з асиметричною маршрутизацією. Пакети, надіслані з одного набору маршрутизаторів і комутаторів і повернувшись через інший, призведуть до того, що системи IDS бачитимуть лише половину трафіку, спричиняючи помилкові спрацьовування та негативні результати.

Корпоративний Інтернет-модуль забезпечує підключення внутрішніх користувачів до Інтернет-сервісів, а користувачів Інтернету – доступ до інформації на публічних серверах. Трафік також надходить від цього модуля до VPN і модуля віддаленого доступу, де відбувається завершення VPN. Цей модуль не призначений для обслуговування додатків типу електронної комерції. Зверніться до розділу «Модуль електронної комерції» далі в цьому документі, щоб дізнатися більше про надання послуг Інтернет-комерції.

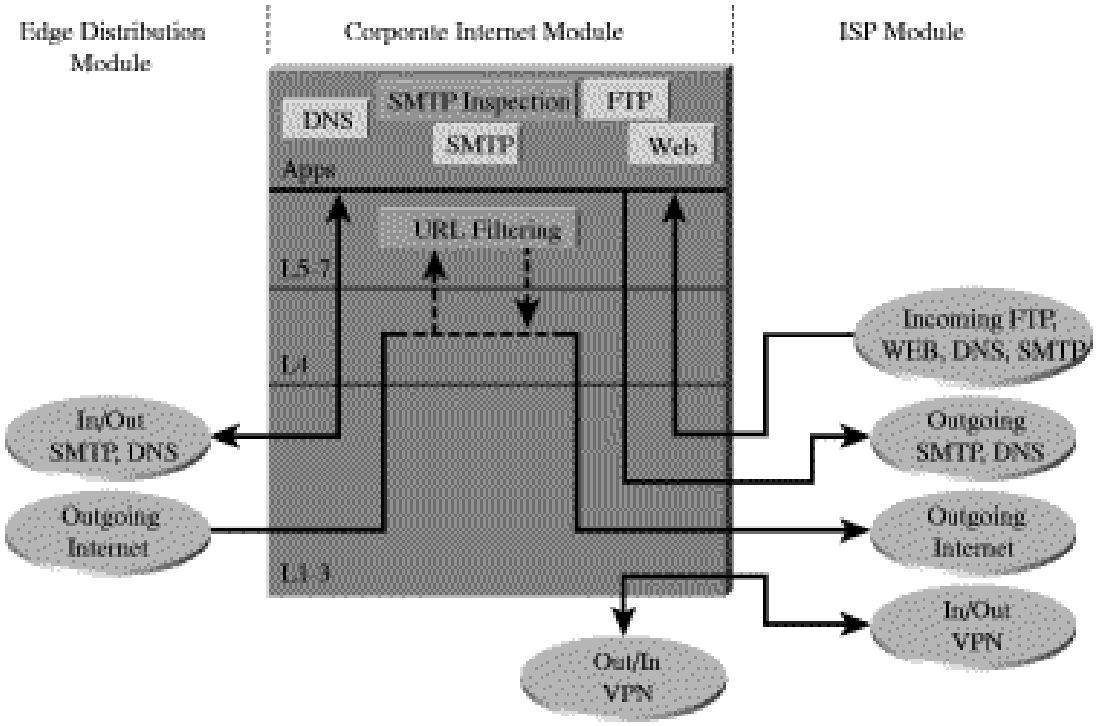

Рис.3.7. Корпоративний Інтернет-трафік

Ключові пристрої:

- Сервер smtp – діє як ретранслятор між інтернетом і поштовими серверами інтернету – перевіряє вміст

- Dns-сервер - служить авторитетним зовнішнім dns-сервером для підприємства, передає внутрішні запити в інтернет
- Ftp/http сервер - надає публічну інформацію про організацію
- Брандмауер - забезпечує захист ресурсів на рівні мережі та фільтрацію трафіку з урахуванням стану
- Пристрій nids - забезпечує моніторинг рівня від 4 до рівня 7 ключових сегментів мережі в модулі
- Сервер фільтрації url-адрес - фільтрує неавторизовані url-запити від підприємства

Загрози:

- Несанкціонований доступ – пом’якшується за допомогою фільтрації в інтернет-провайдера, периферійного маршрутизатора та корпоративного брандмауера
- Атаки рівня додатків – пом’якшуються через ids на рівні хоста та мережі
- Віруси та троянський кінь – пом’якшені за допомогою фільтрації вмісту електронної пошти та ids хосту
- Атаки паролем — обмежені служби, доступні грубою форсою, ос і ids можуть виявити загрозу
- Відмова в обслуговуванні - car на межі провайдера та налаштування tcp на брандмауері
- Ip spoofing - фільтрація rfc 2827 і 1918 на межі провайдера та корпоративному маршрутизаторі
- Packet sniffers – комутована інфраструктура та хост ids обмежують ризики
- Network reconnaissance – ids виявляє розвідку, протоколи фільтруються для обмеження ефективності
- Експлуатація довіри – обмежувальна модель довіри та приватні vlan обмежують атаки на основі довіри

- Перенаправлення портів - обмежувальна фільтрація та атака на обмеження ids хоста

Серцем модуля є пара стійких міжмережевих екранів, які забезпечують захист публічних служб інтернету та внутрішніх користувачів. Перевірка стану перевіряє трафік у всіх напрямках, гарантуючи, що лише законний трафік перетинає брандмауер. Крім стійкості рівня 2 і рівня 3, вбудованої в модуль, і можливості брандмауера з відтворенням після відмови, усі інші міркування щодо дизайну зосереджені навколо безпеки та пом'якшення атак.

Починаючи з маршрутизатора на межі клієнта в інтернет-провайдері, швидкість виходу з інтернет-провайдера обмежує несуттєвий трафік, який перевищує попередньо встановлені порогові значення, щоб пом'якшити (d)dos-атак. Також на виході з маршрутизатора isp фільтрація rfc 1918 і rfc 2827 запобігає підробці адреси джерела локальних мереж і діапазонів приватних адрес.

На вході першого маршрутизатора в корпоративну мережу базова фільтрація обмежує трафік до очікуваного (адреси та ip-сервіси) трафіку, забезпечуючи грубий фільтр для найпростіших атак. Фільтрація rfc 1918 і 2827 також надається тут як перевірка фільтрації isp. Крім того, через величезну загрозу безпеці, яку вони створюють, маршрутизатор налаштований на відкидання більшості фрагментованих пакетів, які зазвичай не слід бачити для стандартних типів трафіку в інтернеті. Будь-який законний трафік, втрачений через цю фільтрацію, вважається прийнятним порівняно з ризиком дозволу такого трафіку. Нарешті, будь-який трафік ipsec, призначений для vpn і модуля віддаленого доступу, маршрутизується належним чином. Фільтрація на інтерфейсі, підключеному до модуля vpn, налаштована таким чином, щоб дозволяти проходити лише трафік ipsec і лише тоді, коли він походить від авторизованих вузлів і надсилається їм. За допомогою vpn віддаленого доступу зазвичай не відома ip-адреса системи, що надходить, тому фільтрація може бути специфічною лише для однорангових вузлів, з якими спілкуються віддалені користувачі.

Пристрій nids на загальнодоступній стороні брандмауера відстежує атаки на основі аналізу від рівня 4 до рівня 7 і порівняння з відомими сигнатурами. Оскільки

інтернет-провайдер і крайовий маршрутизатор підприємства фільтрують певні діапазони адрес і порти, це дозволяє пристрою nids зосередитися на деяких складніших атаках. Тим не менш, цей nids повинен мати сигнали тривоги, встановлені на нижчому рівні, ніж пристрої всередині брандмауера, оскільки сповіщення, які тут видно, не представляють фактичні порушення, а лише спроби.

Брандмауер забезпечує контроль за станом підключення та детальну фільтрацію для сеансів, ініційованих через брандмауер. Сервери з загальною адресацією мають певний захист від затоплення tcp syn через використання обмежень на напіввідкриті з'єднання на брандмауері. З точки зору фільтрації, крім обмеження трафіку в сегменті загальнодоступних послуг відповідними адресами та портами, також має місце фільтрація в протилежному напрямку. Якщо атака скомпрометує один із загальнодоступних серверів (шляхом обходу брандмауера, ids на основі хоста та ids на основі мережі), цей сервер не зможе атакувати мережу далі. Щоб пом'якшити цей тип атак, спеціальна фільтрація запобігає створенню будь-яких неавторизованих запитів публічними серверами до будь-якого іншого місця. Наприклад, веб-сервер має бути відфільтрований таким чином, щоб він не міг створювати власні запити, а лише відповідав на запити клієнтів. Це допомагає запобігти завантаженню хакером додаткових утиліт у скомпрометований блок після початкової атаки. Це також допомагає зупинити небажані сеанси, які хакер запускає під час основної атаки. Прикладом такої атаки є атака, яка генерує xterm з веб-сервера через брандмауер на машину хакера. Крім того, приватні vlan запобігають атаці зламаного загальнодоступного сервера на інші сервери в тому ж сегменті. Цей трафік навіть не виявляється брандмауером, тому приватні vlan є критичними.

Трафік у сегменті перевірки вмісту обмежується запитами фільтрації url-адрес від брандмауера до пристрою фільтрації url-адрес. Крім того, автентифіковані запити дозволені від корпоративного пристрою фільтрації url-адрес на головний сервер для оновлення бази даних. Пристрій фільтрації url-адрес перевіряє вихідний трафік на наявність неавторизованих www-запитів. Він зв'язується безпосередньо з брандмауером і схвалює або відхиляє url-запити,

надіслані брандмауером механізму перевірки url-адрес. Його рішення ґрунтується на політиці, якою керує підприємство, використовуючи інформацію про класифікацію www, надану службою третьої сторони. Перевірці url-адрес віддали перевагу перед стандартною фільтрацією доступу, оскільки ip-адреси часто змінюються для неавторизованих веб-сайтів, і такі фільтри можуть бути дуже великими. Програмне забезпечення ids на базі хосту на цьому сервері захищає від можливих атак, які якимось чином обходять брандмауер.

Сегмент загальнодоступних послуг включає пристрій nids для виявлення атак на порти, на які налаштований брандмауер. Найчастіше це атаки рівня програми на певну службу або атака паролем на захищену службу. Потрібно налаштувати цей nids у більш обмежувальну позицію, ніж nids на зовнішній стороні брандмауера, оскільки сигнатури, які збігаються тут, успішно пройшли через брандмауер. Кожен із серверів має програмне забезпечення для виявлення вторгнень на хост для відстеження будь-якої шахрайської діяльності на рівні ос, а також активності в звичайних серверних програмах (http, ftp, smtp тощо). Хост dns має бути заблокований, щоб відповідати лише на бажані команди та усувати будь-які непотрібні відповіді, які можуть допомогти хакерам у розвідці мережі. Це включає в себе запобігання передачі зон з будь-якого місця, крім внутрішніх серверів dns. Сервер smtp містить служби перевірки вмісту електронної пошти, які запобігають атакам вірусів і троянських програм на внутрішню мережу, які зазвичай поширюються через поштову систему. Брандмауер сам фільтрує smtp-повідомлення на рівні 7, дозволяючи лише необхідні команди на поштовий сервер.

Пристрій nids на внутрішньому інтерфейсі брандмауера забезпечує остаточний аналіз атак. У цьому сегменті має бути виявлено дуже мало атак, оскільки всередину дозволено лише відповіді на ініційовані запити та кілька обраних портів із сегмента загальнодоступних послуг. У цьому сегменті слід розглядати лише складні атаки, оскільки вони зазвичай означають, що систему в сегменті публічних послуг було скомпрометовано, і хакер намагається використати цю опору для атаки на внутрішню мережу. Наприклад, якщо загальнодоступний сервер smtp було зламано, хакер може спробувати атакувати внутрішній поштовий

сервер через tcp-порт 25, якому дозволено передавати пошту між двома хостами. Якщо атаки спостерігаються на цьому сегменті, відповіді на ці атаки мають бути більш серйозними, ніж на інші сегменти, оскільки вони, ймовірно, вказують на те, що компрометація вже сталася. Слід серйозно розглянути використання скидання tcp для запобігання, наприклад, атаці smtp, згаданій вище.

Висновки до третього розділу

Оглянуто мережеву інфраструктуру Cisco AVVID, яка забезпечує корпоративну основу, та поєднує IP-з'єднання з високою продуктивністю, безпекою та доступністю.

Досліджено компоненти мережевої інфраструктури Cisco AVVID та налаштування безпеки для корпоративної мережі та стратегії Cisco AVVID та SAFE для захисту корпоративних мереж, який розроблений на основі принципів відкритих стандартів, щоб забезпечити гнучкість, надійність і важливі мережеві механізми, які дозволяють підприємствам стати гнучкими та адаптованими. Ця мережева архітектура також дозволяє організаціям ефективно планувати оновлення та вдосконалення мережі.

ВИСНОВКИ

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

Проаналізовано основні компоненти та властивості комп'ютерних мереж. Перераховано елементи мережі, компоненти, протоколи та пристрої для побудови цільної картинки комп'ютерної мережі; та вимоги до розробки великомасштабних мереж для задоволення сучасного динамічного бізнесу та IT-потреб і тенденцій.

Наведено основні принципи проєктування мережі та окремо виділено важливість уніфікованого керування мережею.

Досліджено різні топології мереж для побудови корпоративної мережі.

Підкреслено, що організації з розподіленим середовищем тепер більше покладаються на мережу для надання позитивного досвіду та гнучкості бізнесу. Мережеві команди повинні вміти встановлювати нові мережеві підключення та гарантувати їхню безпеку та продуктивність.

Перераховано заходи безпеки для корпоративних мереж та окремо наведено три рівні безпеки з мінімальним, розширеним та максимальним рівнями відповідно.

Проаналізовано найпоширеніші загрози мережевій безпеці з урахуванням сучасних тенденцій.

Доведено, що надійність та відмовостійкість є важливими компонентами безпечної та комфортної роботи корпоративної мережі. Більшість комунікаційних програм, від мобільних телефонних розмов до транзакцій кредитними картками, передбачає наявність надійної мережі. На цьому рівні очікується, що дані пройдуть мережею та прибудуть неушкодженими до місця призначення. Фізичні системи, що утворюють мережу, з іншого боку, піддаються широкому спектру проблем, починаючи від спотворення сигналу до збоїв компонентів.

Оглянуто мережеву інфраструктуру Cisco AVVID, яка забезпечує корпоративну основу, та поєднує IP-з’єднання з високою продуктивністю, безпекою та доступністю.

Досліджено компоненти мережевої інфраструктури Cisco AVVID та налаштування безпеки для корпоративної мережі; та стратегії Cisco AVVID та SAFE для захисту корпоративних мереж, який розроблений на основі принципів відкритих стандартів, щоб забезпечити гнучкість, надійність і важливі мережеві механізми, які дозволяють підприємствам стати гнучкими та адаптованими. Ця мережева архітектура також дозволяє організаціям ефективно планувати оновлення та вдосконалення мережі.