ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ МЕРЕЖЕВОГО РІВНЯ КОМП'ЮТЕРНОЇ СИСТЕМИ НА ОСНОВІ ПРОТОКОЛУ IPSEC»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Волковецький І. С.
(прізвище та ініціали)
Керівник Собчук А.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС – Інформаційна Система

IP – Internet Protocol

OSI – The Open Systems Interconnection Model

Ddos – Distributed Denial-Of-Service Attack

LAN – Local Area Network

IDS – Intrusion Detection System

ICMP – Internet Control Message Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

SSL – Secure Sockets Layer

VPN –Virtual Private Network

HTTPS – Hypertext Transfer Protocol Secure

DLP – Data Leak Prevention

URL – Uniform Resource Locator

ВСТУП

Актуальність дослідження. Радикальне усунення вразливостей комп'ютерних мереж можливе при створенні системи захисту не для окремих класів додатків, а для мережі в цілому. Стосовно IP-мереж це означає, що системи захисту повинні діяти на мережевому рівні моделі OSI. Перевага такого вибору полягає у тому очевидному факті, що в IP-мережах саме мережевий рівень відрізняється найбільшою гомогенністю: незалежно від вищележачих протоколів, фізичного середовища передачі та технології канального рівня транспортування даних через мережу не може бути здійснене в обхід протоколу IP. Тому реалізація захисту мережі на третьому рівні автоматично гарантує щонайменше такий самий ступінь захисту всіх мережних додатків, причому без будь-якої модифікації останніх.

Під час формування захищених віртуальних каналів на мережному рівні моделі OSI досягається оптимальне співвідношення між прозорістю та якістю захисту. Розміщення засобів захисту на мережному рівні робить їх прозорими для додатків, оскільки між мережним рівнем та додатком функціонує реалізація протоколу транспортного рівня. Для користувачів процедури захисту виявляються настільки ж прозорими, як і протокол IP. На мережному рівні існує можливість досить повної реалізації функцій захисту трафіку та управління ключами, оскільки саме на мережному рівні виконується маршрутизація пакетів повідомлень.

Об’єкт дослідження – забезпечення безпеки мережевого рівня комп’ютерної системи.

Предмет дослідження – методи та засоби забезпечення безпеки мережевого рівня комп’ютерної системи.

Мета роботи – розробити рекомендації щодо застосування методів та засобів забезпечення безпеки мережевого рівня комп’ютерної системи.

Завдання бакалаврської роботи:

дослідити основні проблеми захисту комп’ютерних мереж;

дослідити основні загрози та вектори атак на мережевому рівні комп’ютерної системи;

проаналізувати існуючі методи та засоби забезпечення безпеки мережевого рівня комп’ютерної системи;

дослідити можливості та функції протоколу IPsec.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

Практичне значення одержаних результатів: рекомендації щодо захисту комп’ютерних мереж можуть бути використані у сфері забезпечення кібербезпеки в інформаційних системах.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Основні поняття комп'ютерних систем

В інформаційних технологіях мережа визначається як з'єднання як мінімум двох комп'ютерних систем за допомогою кабелю або бездротового з'єднання. Найпростіша мережа є комбінацією двох комп'ютерів, з'єднаних кабелем. Такий тип мережі називається одноранговій мережею. У цій мережі немає ієрархії; обидва учасники мають рівні права. Кожен комп'ютер має доступ до даних іншого пристрою та може спільно використовувати такі ресурси, як дисковий простір, програми або периферійні пристрої (принтери тощо).

Сучасні мережі, як правило, трохи складніші і складаються не лише з двох комп'ютерів. Системи з більш як десятьма учасниками зазвичай використовують мережі клієнт-сервер. У цих мережах центральний комп'ютер (сервер) надає ресурси іншим учасникам (клієнтам).

Основне завдання мережі – надати учасникам єдину платформу для обміну даними та спільного використання ресурсів. Це завдання настільки важливе, що багато аспектів повсякденного життя та сучасного світу були б немислимі без мереж.

Наприклад: у типовому офісі на кожній робочій станції є свій комп'ютер. Без мережі комп'ютерів команді було б дуже складно працювати над проектом, оскільки не було б спільного місця для обміну або зберігання цифрових документів та інформації, а члени команди не могли б спільно використовувати певні програми.

Крім того, у багатьох офісах є лише один принтер або кілька принтерів, якими користуються всі. Без мережі IT-відділу довелося б підключати кожен комп'ютер до принтера, що складно реалізувати з технічного погляду. Мережа елегантно вирішує цю проблему, оскільки всі комп'ютери підключені до принтера через центральний вузол.

Основними перевагами мереж є:

— Спільне використання даних

— Спільне використання ресурсів

— Централізоване управління програмами та даними

— Центральне сховище та резервне копіювання даних

— Загальна обчислювальна потужність та ємність сховища

— Просте управління повноваженнями та обов'язками.

У типовій клієнт-серверній мережі є центральний вузол, який називається сервером. Сервер підключено до інших пристроїв, які називають клієнтами. Це з'єднання може бути бездротовим (бездротова локальна мережа), або проводовим (локальна мережа).

У типовій домашній мережі маршрутизатор перебирає роль сервера. Він підключений до Інтернету та надає ресурс «Інтернет» для інших пристроїв (комп'ютерів, смартфонів тощо).

Клієнт-серверна архітектура

У великих мережах, таких як корпоративні мережі, сервером зазвичай є центральний комп'ютер. Цей комп'ютер використовується виключно для запуску спеціального серверного програмного забезпечення та служб, а не звичайних програм та програм. Сервер повинен працювати безперервно, а решта комп'ютерів (клієнтів) може бути відключена.

Сервер та клієнт взаємодіють у цій мережі на основі сервера наступним чином: клієнт спочатку надсилає запит на сервер. Сервер оцінює запит і потім передає відповідь. У цій моделі клієнт завжди підключається до сервера, а чи не навпаки.

Мережеві протоколи

Мережеві протоколи забезпечують безперебійний зв'язок між різними компонентами мережі. Вони контролюють обмін даними та визначають, як встановлюється та припиняється зв'язок, а також які дані передаються. Зазвичай існує кілька мережевих протоколів, кожен з яких виконує певне підзавдання та ієрархічно організований на рівні.

Мережеві адреси

Крім того, необхідно забезпечити правильну ідентифікацію передавача та приймача. Для цього використовуються мережеві адреси. У комп'ютерних мережах кожен комп'ютер зазвичай має IP-адресу, аналогічну номеру телефону, який однозначно ідентифікує комп'ютер. Ця внутрішня IP-адреса використовується лише для зв'язку між учасниками локальної мережі. Для зв'язку в Інтернеті використовують зовнішні IP-адреси, які автоматично призначаються інтернет-провайдером.

Також проводиться різниця між адресами IPv4 та IPv6. Адреси IPv4 раніше були стандартними, але до того, як їх було вичерпано, можна було призначити всього близько 4,3 мільярда таких адрес. У зв'язку з масовим поширенням Інтернету терміново знадобилися додаткові IP-адреси. Тому було розроблено новий стандарт IPv6, що дозволяє використовувати до 3,4 x 1038 (340 секстильйонів) адрес. Цього має вистачити на майбутнє.

Діапазон мережі

Мережі зазвичай класифікуються по діапазону так:

Персональна мережа (PAN): PAN використовується для підключення пристроїв на невеликій відстані приблизно 10 метрів. Приклади включають технологію Bluetooth або спеціальний Wi-Fi Apple Airdrop.

Локальна обчислювальна мережа (LAN): Локальні обчислювальні мережі є одними з найпоширеніших мереж і використовуються в домашніх господарствах або малих та середніх компаніях.

Міська мережа (MAN): Ці типи мереж охоплюють міста чи окремі географічні регіони.

Глобальна мережа (WAN): загальнонаціональна широкосмугова чи стільникова мережа США є прикладом глобальної мережі.

GAN (Глобальна мережа): Найвідомішим прикладом глобальної мережі є Інтернет [1].

1.2 Основні проблеми захисту комп’ютерних мереж

Мережа безпека охоплює всі кроки, зроблені для захисту цілісності комп'ютерної мережі та даних у ній. Безпека мережі важлива, тому що вона захищає конфіденційні дані від кібератак і забезпечує зручність використання та надійність мережі. Успішні стратегії мережної безпеки використовують кілька рішень безпеки для захисту користувачів та організацій від шкідливих програм та кібератак, таких як розподілена відмова в обслуговуванні.

Мережа складається з взаємозалежних пристроїв, таких як комп'ютери, сервери та бездротові мережі. Багато з цих пристроїв уразливі для потенційних зловмисників. Мережева безпека включає використання різних програмних і апаратних інструментів в мережі або у вигляді програмного забезпечення як послуги. Безпека стає все більш важливою в міру того, як мережі стають все більш складними, а підприємства все більше покладаються на свої мережі та дані для ведення бізнесу. Методи безпеки повинні розвиватися у міру суб'єкти загрози створювати нові методи атаки на ці складніші мережі.

Незалежно від конкретного методу чи стратегії безпеки підприємства, безпека зазвичай оформлено як відповідальність кожного, тому що кожен користувач у мережі являє собою можливу вразливість у цій мережі.

Безпека мережі має вирішальне значення, оскільки вона не дозволяє кіберзлочинцям отримати доступ до цінних даних та конфіденційної інформації. Коли хакери отримують такі дані, вони можуть викликати безліч проблем, включаючи крадіжку особистих даних, крадіжку активів та шкоду репутації.

Нижче наведено чотири найважливіші причини, з яких важливий захист мереж і даних, що зберігаються в них:

1. Операційні ризики. Організація без належної мережевої безпеки ризикує порушити свою діяльність. Корпоративні та особисті мережі залежать від пристроїв та програмного забезпечення, які не можуть ефективно працювати через віруси, шкідливі програми та кібератаки. Бізнес також покладається на мережі для більшості внутрішніх та зовнішніх комунікацій.

2. Фінансові ризики, пов'язані зі компрометацією інформації, що дозволяє встановити особу. Витік даних може дорого коштувати як приватним особам, і компаніям. Організації, що займаються персональними даними, такі як номери соціального страхування та паролі, необхідні для забезпечення безпеки. Викриття може коштувати жертвам грошей у вигляді штрафів, реституції та ремонту скомпрометованих пристроїв. Витоки та розкриття даних також можуть підірвати репутацію компанії та призвести до судових позовів. Звіт IBM «Вартість витоку даних за 2022 рік», підготовлений Інститут Понемона, повідомив, що середня вартість витоку даних зросла до 4,35 млн доларів у 2022 році з 4,24 млн доларів у 2021 році.

3. Фінансовий ризик компрометації інтелектуальної власності. Організації також можуть мати власну інтелектуальну власність, яку може бути вкрадено. Втрата ідей, винаходів та продуктів компанії може призвести до втрати бізнесу та конкурентних переваг.

4. Регуляторні питання. Багато урядів вимагають від компаній дотримання правил безпеки даних, які охоплюють аспекти безпеки мережі. Наприклад, медичні організації у Сполучених Штатах зобов'язані дотримуватися положень Закону про переносимість та підзвітність медичного страхування (HIPAA), а організації в Європейському союзі, які мають справу з даними громадян, повинні дотримуватися Загального регламенту захисту даних (GDPR). Порушення цих правил може призвести до штрафів, заборон та можливого тюремного ув'язнення.

5. Безпека мережі настільки важлива, що деякі організації зосереджуються на розробці та спільному використанні стратегій адаптації до сучасних загроз. Mitre ATT&CK, Національний інститут стандартів та технологій і Центр інтернет-безпеки надають безкоштовні непатентовані платформи безпеки та бази знань для обміну інформацією про кіберзагрози та допомагають підприємствам та іншим організаціям оцінювати свої методи мережевої безпеки [7].

1.3 Основні загрози комп’ютерних мереж

Вразливі місця в безпеці мережі – це слабкі місця в процесах та інфраструктурі організації. Коли ці недоліки скомпрометовані, вони можуть призвести до порушення безпеки.

На найширшому рівні загрози безпеці мережі можна розділити на три категорії:

Фізичні вразливості: будь-які слабкі місця в системі даних або середовищі її розміщення, які можуть вплинути на апаратне забезпечення та на комп’ютерні мережі, є фізичними вразливими місцями.

Нефізичні вразливості: це вразливості даних, програмного забезпечення та операційної системи, якими можуть скористатися зловмисники. Проводячи планове обслуговування, оновлення та виправлення, можна краще уникнути нефізичних вразливостей.

Людські вразливості: найслабшою ланкою в більшості архітектур кібербезпеки є людські вразливості, такі як помилки користувача, які можуть розкрити конфіденційну інформацію, порушити роботу ваших систем і створити точки доступу, які можна використовувати. Одним зі способів боротьби організацій із цими загрозами є навчання з питань кібербезпеки.

Розглянемо найпоширеніші загрози, з якими стикаються підприємства, і способи їх вирішення.

1. Безпека фізичного пристрою

Кіберзловмисники часто отримують доступ до внутрішньої мережі через неконтрольований фізичний доступ до таких пристроїв, як ноутбуки, смартфони та планшети.

У деяких випадках кіберзлочинці навіть надсилали поштою USB-накопичувачі зі шкідливим кодом і зловмисним програмним забезпеченням, які дозволяли їм проникати в мережу організації для викрадення конфіденційних даних.

2. Неправильно налаштовані брандмауери

Брандмауер служить важливою лінією захисту від загрозливої кібератаки. Без правильно налаштованого брандмауера ризик безпеки значно зростає, оскільки брандмауер не зможе запобігти несанкціонованому доступу до мережі або IP-адресам із чорного списку, які впливають на мережу.

3. Пристрої IoT

Відбувся значний сплеск впровадження пристроїв Інтернету речей (IoT).

Працюючи як «розумні» пристрої, пристрої IoT мають можливість передавати дані в мережі, але часто не мають належного захисту від кіберзагроз. Крім того, локальні пристрої IoT, такі як інтелектуальні термостати та камери спостереження, часто ігноруються як потенційні вразливі місця в мережі. Щоб зменшити вразливість Інтернету речей, безпека Інтернету речей і контроль доступу є важливими.

4. Погано налаштований Wi-Fi

Офіс організації та віддалені співробітники значною мірою залежать від використання та підключення бездротового підключення до Інтернету. Без добре налаштованого маршрутизатора та мережі кіберзловмисники можуть проникнути у мережу, викрасти дані та створити більш придатні для використання точки доступу, щоб відкрити злам.

Двома типовими способами, якими організації захищають своє з'єднання Wi-Fi, є:

— Використання шифрування WPA2

— Зміна стандартних паролів на надійні

5. Однофакторна автентифікація

Однофакторна автентифікація (SFA) — це метод автентифікації, який покладається на один фактор для перевірки особи користувача. Найпоширенішим SFA є комбінація імені користувача та пароля, яка використовується для автентифікації в онлайн-банкінгу та на платформах соціальних мереж.

Проблема з SFA полягає в тому, що його можуть легко обійти зловмисники, які скомпрометували облікові дані бізнес-електронної пошт. Кілька способів, за допомогою яких компанія може посилити свою позицію автентифікації, це

використання двофакторної автентифікації (2FA) або багатофакторної автентифікації (MFA) замість однофакторної автентифікації.

6. Застаріле програмне забезпечення

У перші роки оновлень програмного забезпечення було небагато, і вони часто випускалися для впровадження нових функцій і покращення взаємодії з користувачем.

Однак, враховуючи постійну еволюцію та складність загроз мережевій безпеці, оновлення програмного забезпечення стали більш рутинними та частими, оскільки нові версії програмного забезпечення спрямовані на усунення помилок та інших вразливостей мережевої безпеки.

Без звичайного програмного забезпечення та забезпечення актуальності операційних систем збільшуються ризики безпеки та відповідальність організації.

7. Захист паролем

Багато співробітників не використовують достатньо надійні паролі, оскільки вони не помічають ризиків безпеки або не знають про них.

На жаль, це викликає серйозні проблеми з безпекою організації, оскільки дає хакерам доступ до робочих облікових записів, викрадає інформацію компанії та створює додаткові шлюзи до мережі компанії. Щоб уникнути цих ризиків, слід використовувати лише надійні паролі.

Додаткова підтримка покращеного захисту паролем надається у вигляді генераторів паролів, менеджерів паролів або багатофакторної автентифікації.

8. Незахищені рішення електронної пошти

Незважаючи на те, що на компрометацію бізнес-електронної пошти припадає лише 4% порушень даних, це в середньому призвело до найвищих витрат у 5,01 мільйона доларів США за порушення.

Причина цього полягає в тому, що хакери знають, що людські вразливості є одним із найкращих способів полювання на конфіденційні дані, перехоплення приватних повідомлень, створення несанкціонованих мережевих шлюзів і поширення шкідливого програмного забезпечення.

Для боротьби з уразливістю електронної пошти організації повинні:

Використовувати надійні паролі для облікових даних електронної пошти

Слідкувати за звичками електронної пошти своїх співробітників

Використовувати двофакторну аутентифікацію

Уникати взаємодії з фішинговими електронними листами

Не відкривати вкладення без їх попереднього сканування

Не використовувати електронну пошту в публічній мережі WiFi

Використовувати рішення для захисту електронної пошти та захисту від спаму

9. Уразливості мобільних пристроїв

Співробітники часто використовують свої телефони на місці або як частину політики BYOD компанії.

Незважаючи на те, що мобільні пристрої є корисним активом, існує багато способів перетворити мобільні пристрої на вразливі місця мережі. Наприклад, фізична крадіжка телефону, підключеного до корпоративної мережі, може надати кіберзлочинцям доступ до конфіденційної інформації.

Додаткові вразливості мобільних пристроїв включають:

Фішингові атаки

Мобільні програми-вимагачі

Експлойти пристрою та ОС

Атаки людини посередині (MitM).

Передові методи джейлбрейка та рутування

Щоб зменшити мережеві загрози для мобільних пристроїв, компаніям слід запровадити заходи безпеки мобільних пристроїв за допомогою:

Створення чіткої політики використання мобільних пристроїв

Сегментація даних і додатків на корпоративних пристроях

Шифрування та мінімізація видимості пристроїв, які мають доступ до мережі компанії

Встановлення програмного забезпечення безпеки мобільного пристрою

Моніторинг поведінки користувачів

Використання керованого постачальника послуг, який пропонує послуги захисту кінцевих точок

10. Атаки соціальної інженерії

Кіберзловмисники використовують атаки соціальної інженерії, щоб обійти протоколи автентифікації та авторизації для доступу до мережі компанії.

Оскільки на фішингові атаки припадає 17% витоків даних, очевидно, що зловмисники використовують співробітників, оскільки вони, як правило, є найслабшою ланкою безпеки мережі в організації.

Додаткові типи атак соціальної інженерії включають вішинг, смішінг, tailgating, spear phishing, плечовий серфінг і dump diving.

Деякі способи організації запобігання атакам соціальної інженерії:

Проведення тестування на проникнення

Включення фільтра спаму та електронної пошти

Використання багатофакторної аутентифікації

Використання керованого постачальника послуг

Перевірка особи відправника електронної пошти

Постійний моніторинг продуктивності їх критичних систем

Використання хмарних брандмауерів веб-додатків нового покоління [7].

1.4 Атаки на рівні моделі OSI

Мережі містять шари, представлені Моделлю взаємодії відкритих систем (OSI). Дані проходять через ці рівні в міру їхнього переміщення між пристроями, і різні кіберзагрози націлені на різні рівні. Отже, кожен рівень у стеку має бути захищений, щоб мережа вважалася захищеною.

Ця таблиця порівнює рівні OSI з відповідним типом мережної безпеки.

Таблиця 1.1.

Рівні моделі OSI

Рівні (ICO 7498-1)	Модель безпеки ISO 7498-2
Прикладний	Аутентифікація
Представлень	Контроль доступу
Сеансовий	Невідмовність
Транспортний	Цілісність даних
Мережевий	Конфіденційність
Канальний	Гарантія та доступність
Фізичний	Нотаріальне завірення та підпис

Зверніть увагу, що третій рівень знизу називається мережею, але безпека мережі поширюється не тільки на цей рівень. Кожен пристрій у комп'ютерній мережі функціонує на кількох рівнях обробки інформації. З огляду на це кожен рівень повинен бути безпечним, щоб мережа вважалася безпечною. Іншими словами, слово «мережа» у цьому визначенні мережевої безпеки в широкому розумінні відноситься до корпоративної інфраструктури загалом, а не лише до мережного рівня.

Наприклад, деякі люди можуть зробити відмінність між хмарною безпекою та мережевою безпекою. Хмарна безпека включає безпеку додатків та безпеку контейнерів, які існують за межами мережевого рівня моделі OSI. Проте ці хмарні функції, як і раніше, можна вважати частиною загальної корпоративної мережі, і їх захист є частиною мережевої безпеки.

1 – Фізичний рівень

Цей рівень відповідає за передачу та прийом необроблених бітових потоків (двійкові 1 та 0) по фізичних носіях, таких як кабелі, дроти та бездротові сигнали. Він може встановлювати, підтримувати та деактивувати фізичну сполуку. Він синхронізує біти даних і визначає швидкість передачі даних та режими передачі даних, такі як повнодуплексний та напівдуплексний режими. Пристрої, що

використовуються фізично, являють собою кабелі, такі як Ethernet, коаксіальні, оптоволоконні та інші роз'єми.

Атаки відмови в обслуговуванні (DoS) орієнтовані на фізичний рівень, оскільки це апаратне забезпечення, матеріальний рівень системи. DoS-атаки зупиняють усі мережеві функції. DoS-атаку можна здійснити, фізично перерізавши або відключивши мережевий кабель. Вразливість фізичного рівня можна зменшити за допомогою заходів фізичної безпеки, таких як контроль доступу, відеоспостереження, захищені від несанкціонованого доступу екрани від електромагнітних перешкод та використання резервних каналів.

2 – Канальний рівень

Цей рівень працює з інформаційними потоками, інкапсульованими у «фрейми». Цей рівень виявляє і виправляє помилки даних, забезпечуючи надійну передачу між мережевими пристроями по фізичному каналу. Він відповідає за послідовний та узгоджений обмін даними, контроль помилок та управління потоком. Cyclic Redundancy Check (CRC) відстежує втрачені кадри, які потім можуть бути повторно передані. Такі пристрої, як мости, комутатори та контролери мережевих інтерфейсів (NIC), а також такі протоколи, як протокол дозволу адрес (ARP), протокол двоточкового з'єднання (PPP), протокол сполучного дерева (STP), протокол управління агрегацією каналів (LACP), відносяться до цього шару.

Атаки на канальному рівні походять із внутрішньої LAN (локальної мережі), деякі з цих атак:

- ARP-спуфінг - ARP-спуфінг - це атака "Людина посередині" (MiTM), при якій суб'єкт загрози прикидається обома сторонами мережевого каналу зв'язку; перехоплення пакетів для крадіжки даних та зміни зв'язку, перехоплення сеансу та атаки розподіленої відмови в обслуговуванні (DDoS). Щоб запобігти цій атаці, увімкніть приватні VLANS, статичний ARP та встановіть системи виявлення вторгнень (IDS).
- Атака з переповненням MAC-адрес. Ця атака здійснюється на мережевому комутаторі. Зловмисник переповнює таблицю адрес управління доступом до середовища (MAC) комутатора підробленими MAC-адресами, які

замінюють дійсні адреси. Це змушує комутатор вести себе як мережевий концентратор, тобто, коли дійсний користувач намагається отримати доступ до мережі, він створює широкомовний флуд по всій мережі. Дані, призначені для справжнього користувача, будуть отримані зловмисником. Цю атаку можна пом'якшити, увімкнувши захист портів та аутентифікацію за допомогою сервера аутентифікації, авторизації та обліку (AAA).

- Атака сполучного дерева. Протокол сполучного дерева (STP) усуває потенційні петлі між резервними комутаторами, щоб вони не викликали нескінченний шторм широкомовного трафіку. Зловмисник змінює операцію, додаючи новий STP-пристрій, який стає кореневим мостом, після чого трафік передаватиметься через комутатор зловмисника. Увімкнення захисту блоку даних протоколу мосту (BPDU) на комутаторах запобігатиме цій атаці.

3 – Мережевий рівень

Мережевий рівень працює з «пакетами», маршрутизуючи їх між пристроями та мережами. Він керує логічною ідентифікацією та адресацією пристроїв, а також виконує маршрутизацію, вибираючи найкоротший та найбільш логічно ефективний шлях для пересилання пакетів. Маршрутизатори та комутатори є найбільш поширеними пристроями, пов'язаними з цим рівнем. Протоколи, які функціонують на цьому рівні, включають Інтернет-протокол (IP), Інтернет-протокол керуючих повідомлень (ICMP), Протокол інформації про маршрутизацію (RIP) та Протокол відкриття найкоротшого шляху (OSPF).

Атаки на мережному рівні здійснюються через Інтернет, наприклад DDoS-атаки, коли маршрутизатор стає метою та перевантажений нелегітимними запитами, що згодом робить його нездатним приймати справжні запити. Елементи керування фільтрацією пакетів та механізми безпеки, такі як віртуальні приватні мережі (VPN), IPsec та брандмауери, є поширеними методами обмеження ймовірності атак на мережному рівні.

4 – Транспортний рівень

Цей рівень встановлює двоточкове з'єднання між джерелом та одержувачем, гарантуючи, що дані передаються у правильному порядку. Він також виконує

керування потоком, контроль помилок, повторне складання даних та сегментацію. Протокол управління передачею (TCP) та протокол користувальницьких дейтаграм (UDP) є прикладами протоколів транспортного рівня.

Атаки на цьому рівні часто проводять через вразливі відкриті порти, виявлені при скануванні портів.

- SYN-флуд-атака - тип DDoS-атаки, що використовує тристороннє рукостискання TCP. Зловмисник відправляє кілька пакетів синхронізації (SYN) на порт сервера. Сервер підтверджує надсилання повідомлення Synchronize-Acknowledge (SYN-ACK) для кожного пакета SYN. Якщо шкідливий клієнт не надсилає остаточний пакет ACK, як очікувалося, він створює на сервері напіввідкриті сеанси. У міру того, як спроможність сервера обробляти запити виснажується, нові запити та послуги законним клієнтам будуть відхилені. Якщо SYN-флуд продовжиться, сервер вийде з ладу або вийде з ладу. Атаки SYN Flood можна пом'якшити шляхом виділення мікроблоків, всього 16 байтів для запиту SYN, та збереження файлів cookie SYN та RST.
- Атаку Smurf названо на честь популярної іграшкової фігурки 1980-х років, яка, здавалося, була всюди. Атака Smurf також є різновидом DDoS-атаки. Ця атака здійснюється шляхом створення підроблених пакетів exo-запиту ICMP (PING) у широкомовну IP-мережу з використанням IP-адреси цільового сервера як вихідну IP-адресу. З такою кількістю відповідей ICMP, які, здається, приходять звідусіль, цільовий сервер перевантажується та падає. Перевірка вхідного трафіку та блокування незаконних відповідей ICMP знизить ймовірність атаки Smurf.

5 – Сеансовий рівень

Цей рівень відповідає за встановлення, підтримання та завершення сеансів між локальним та віддаленим пристроєм. Відповідає за синхронізацію та відновлення, додає контрольні точки під час передачі даних. У разі виникнення помилок передачі під час будь-якого примірника передача відновиться з останньої справної контрольної точки.

Загальні атаки на цьому рівні включають:

- Перехоплення сеансу. Зловмисник захоплює веб-сеанс, скомпрометувавши токен сеансу, щоб отримати доступ до особистої інформації та паролів. Надійні паролі з багатофакторною автентифікацією, віртуальні приватні мережі та постійне оновлення програмного забезпечення – це лише деякі засоби захисту від атак з перехопленням сеансу.
- Атака MiTM. Під час цієї атаки суб'єкт загрози перебуває між сеансами передачі даних двох сторін, щоб підслуховувати та ретранслювати повідомлення. Відкриті незахищені з'єднання Wi-Fi є найбільш популярним вектором для цього типу атак. Інші комунікаційні технології, такі як Secure Shell (SSH), обмежуватимуть атаки такого типу.

6 - Рівень уявлення

Цей рівень відповідає за перетворення даних із формату, що залежить від відправника, у загальний формат, зрозумілий прикладному рівню. Наприклад, переклад різних наборів символів, таких як ASCII до EBCDIC. Що найважливіше з погляду кібербезпеки, цей рівень обробляє шифрування та дешифрування даних. Стиснення даних передачі по мережі також управляється лише на рівні представлення. Перехоплення захищених сокетів (SSL), також відомий як перехоплення сеансу, відбувається на рівні вистави. Технології шифрування забезпечують конфіденційність та цілісність даних при передачі.

7 – Прикладний рівень

Цей рівень надає послуги кінцевого користувача, такі як поштові служби, служби каталогів, передача файлів, доступ і управління (FTAM). Протокол передачі файлів (FTP), простий протокол керування мережею (SNMP), система доменних імен (DNS), протокол передачі гіпертексту (HTTP) та протоколи електронної пошти (SMTP, POP3, IMAP) є деякими прикладами протоколів прикладного рівня.

Від атак прикладного рівня найскладніше захиститися, тому що тут зустрічається багато вразливостей, оскільки цей рівень найбільш схильний до зовнішнього світу. Використання технологій моніторингу додатків для виявлення

атак 7-го рівня та атак нульового дня, а також регулярне оновлення додатків – найкращі методи захисту прикладного рівня.

На цьому рівні відбуваються найпоширеніші кібератаки, включаючи віруси, черв'яки, троянські коні, фішингові атаки, DDoS-атаки, HTTP-флуди, SQL-ін'єкції, міжсайтові сценарії та багато іншого [9].

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Аналіз методів та засобів захисту комп'ютерних мереж

Мережева безпека забезпечується за допомогою комбінації апаратних та програмних засобів. Основною метою мережевої безпеки є запобігання несанкціонованому доступу до частин мережі або між її частинами.

Співробітник служби безпеки чи група визначає стратегії та політики, що забезпечують безпеку мережі організації та допомогти йому відповідати стандартам та правилам безпеки. Всі в мережі повинні дотримуватися цих безпекових політик. Кожна точка в мережі, де авторизований користувач може отримати доступ до даних, також є точкою, де дані можуть бути скомпрометовані або зловмисником, або через неуважність чи помилки користувача.

Типи програмного забезпечення та інструментів мережевої безпеки

Вибір політик та інструментів безпеки залежить від мережі та змінюється з часом. Надійна безпека часто включає використання кількох підходів, відомих як багаторівнева безпека або багаторівневий захист, щоб надати організаціям якомога більше засобів управління безпекою. Нижче наведено деякі типи інструментів і програмного забезпечення, що часто використовуються, для мережної безпеки:

- Контроль доступу. Цей метод обмежує доступ до мережних додатків та систем певною групою користувачів та пристроїв. Ці системи забороняють доступ користувачам та пристроям, які ще не були санкціоновані.
- Антивірус та антишкідливе ПЗ. Антивірус та антишкідливе ПЗ— це програмне забезпечення, призначене для виявлення, видалення або запобігання зараженню комп'ютера і, отже, мережі вірусами та шкідливими програмами, такими як троянські коні, програми-вимагачі та програми-шпигуни.
- Безпека додатків. Дуже важливо відстежувати та захищати програми, які організації використовують для ведення свого бізнесу. Це вірно незалежно від

того, чи створює організація це додаток чи купує його, оскільки сучасні шкідливі програми часто націлені на Відкритий вихідний код та контейнери, які організації використовують для створення програмного забезпечення та додатків.

- Поведінкова аналітика. Цей метод аналізує поведінку мережі та автоматично виявляє та попереджає організації про ненормальну активність.
- Хмарна безпека. Хмарні провайдери часто продають доповнення хмарна безпека_інструменти, які забезпечують можливості безпеки у їхній хмарі. Постачальник хмарних послуг керує безпекою своєї спільної інфраструктури та пропонує користувачам інструменти для захисту своїх екземплярів у рамках загальної хмарної інфраструктури. Наприклад, Веб-сервіси Амазон надає групи безпеки, які контролюють вхідний та вихідний трафік, пов'язаний із додатком або ресурсом.
- Захист від втрат даних (DLP). Ці інструменти відстежують дані в процесі використання, у русі та в стані спокою, щоб виявляти та запобігати витоку даних. DLP часто класифікує найбільш важливі та схильні до ризику дані та навчає співробітників передовим методам захисту цих даних. Наприклад, не надсилати важливі файли у вигляді вкладень у повідомленнях електронної пошти – одна з таких рекомендацій [7].
- Безпека електронної пошти. Електронна пошта є одним із найуразливіших місць у мережі. Співробітники стають жертвами фішинг_та атаки шкідливих програм, коли вони натискають на посилання електронної пошти, які таємно завантажують зловмисне програмне забезпечення. Електронна пошта також є небезпечним методом надсилання файлів та конфіденційних даних, які працівники мимоволі використовують.
- Брандмауер. Програмне забезпечення перевіряє вхідний та вихідний трафік для запобігання несанкціонованому доступу до мережі. Брандмауери є одними з засобів безпеки, що найбільш широко використовуються. Вони розташовані у кількох областях мережі. Міжмережеві екрани нового покоління забезпечують підвищений захист проти атак на рівні додатків та розширеного захисту від шкідливого ПЗ із вбудованою глибокою перевіркою пакетів.

- Система виявлення вторгнень (IDS). IDS виявляє спроби несанкціонованого доступу та позначає їх як потенційно небезпечні, але не видаляє їх. IDS та система запобігання вторгненням (IPS) часто використовуються у поєднанні з брандмауером.
- Система запобігання вторгненням. IPS призначені для запобігання вторгненням шляхом виявлення та блокування несанкціонованих спроб доступу до мережі.
- Безпека мобільних пристроїв. Бізнес-програми для смартфонів та інших мобільних пристроїв зробили ці пристрої важливою частиною мережевої безпеки. Моніторинг та контроль того, які мобільні пристрої отримують доступ до мережі та що вони роблять після підключення до мережі, має вирішальне значення для безпеки сучасної мережі.
- Багатофакторна автентифікація (MFA). MFA – це просте у використанні та все більш популярне рішення для мережної безпеки, яке потребує двох або більше факторів для перевірки особистості користувача. Прикладом цього є Google Authenticator, додаток, який генерує унікальні коди безпеки, які користувач вводить разом із паролем для підтвердження своєї особистості.
- Сегментація мережі. Організації з великими мережами та мережевим трафіком часто використовують сегментація мережі розбити мережу на дрібніші, простіші в управлінні сегменти. Такий підхід дає організаціям більший контроль над потоком трафіку та підвищує його прозорість. Безпека промислових мереж - це частина сегментації мережі, що забезпечує підвищену прозорість промислових систем управління (ICS). АСУ більше піддаються кіберзагрозам через тіснішу інтеграцію з хмарою.
- Пісочниця. Цей підхід дозволяє організаціям сканувати шкідливі програми, відкриваючи файл у ізольованому середовищі, як надати йому доступом до мережі. Після відкриття в пісочниця, організація може спостерігати, чи файл зловмисно чи показує якісь ознаки шкідливого ПЗ.
- Інформація про безпеку та управління подіями (SIEM). Цей метод управління безпекою реєструє дані з додатків та мережного обладнання та

відстежує підозрілу поведінку. При виявленні аномалії SIEM система повідомляє організацію і робить інші відповідні дії.

- Програмно-визначуваний периметр (SDP). SDP це метод безпеки, який знаходиться поверх мережі, що захищається, приховуючи її від зловмисників і неавторизованих користувачів. Він використовує критерії ідентифікації для обмеження доступу до ресурсів та формує віртуальний кордон навколо мережевих ресурсів.
- Віртуальна приватна мережа (VPN). VPN_захищає з'єднання кінцевої точки з мережею організації. Він використовує протоколи тунелювання для шифрування інформації, що надсилається менш захищеною мережею. VPN із віддаленим доступом дозволяють співробітникам отримувати віддалений доступ до мережі своєї компанії.
- Веб-безпека. Ця практика контролює використання співробітниками веб-сайтів у мережі та на пристроях організації, включаючи блокування певних загроз та веб-сайтів, а також захист цілісності самих веб-сайтів організації.
- Бездротова безпека. Бездротові мережі є однією з найбільш ризикованих частин мережі і потребують суворого захисту та моніторингу. Важливо слідувати кращі практики безпеки бездротової мережі, такі як сегментація користувачів Wi-Fi за ідентифікаторами наборів послуг або SSID, а також використання 802.1X автентифікація. Для забезпечення безпеки бездротової мережі також потрібні хороші інструменти моніторингу та аудиту.
- Безпека робочого навантаження. Коли організації розподіляють робочі навантаження між кількома пристроями в хмарних та гібридних середовищах, вони збільшують потенційні поверхні атак. Заходи безпеки робочого навантаження та безпека балансувальники навантаження мають вирішальне значення захисту даних, які у цих робочих навантаженнях.
- Доступ до мережі з нульовою довірою. Подібно до контролю доступу до мережі, нульовий рівень довіри_мережний доступ надає користувачеві лише той доступ, який він повинен мати для виконання своєї роботи. Він блокує всі інші дозволи [9].

2.2 Аналіз методів та засобів захисту мережевого рівня комп’ютерної системи

Мережевий рівень пропонує управління роботою підмережі. Мережевий рівень допомагає передавати всі пакети від джерела до місця призначення через кілька хостів по мережі. Мережевий рівень не потрібний для з'єднання двох комп'ютерних систем з однаковим каналом. Він перенаправляє всі сигнали різними каналами в іншу точку і відіграє роль мережного контролера. Мережевий рівень розбиває всі вихідні повідомлення на невеликі блоки (пакети) і збирає вхідні пакети у форму повідомлень для пересилання більш високі рівні.

Протоколи мережевого рівня

Існують різні типи протоколів, що використовуються на мережному рівні.

Список протоколів мережного рівня

- CLNS (мережева служба в режимі без встановлення з'єднання)
- DP (протокол доставки дейтаграм)
- EGP (протокол зовнішнього шлюзу)
- EIGRP (Розширений протокол маршрутизації внутрішнього шлюзу)
- ICMP (протокол керування повідомленнями в Інтернеті)
- IGMP (протокол управління інтернет-групами)
- IPsec (безпека інтернет-протоколу)
- IPv4/IPv6 (Інтернет-протокол)
- IPX (обмін міжмережевими пакетами)
- OSPF (спочатку відкрийте найкоротший шлях)
- PIM (багатоадресне розсилання, незалежно від протоколу)
- RIP (протокол інформації про маршрутизацію)

Приклади протоколів мережного рівня

CLNS (мережева служба в режимі без встановлення з'єднання): Він також відомий як "Мережева служба без встановлення з'єднання", яка використовується як служба дейтаграм на мережному рівні OSI і не вимагає створення будь-якого ланцюга перед передачею даних. CLNS — це послуга, яку пропонує CLNP

(мережевий протокол без встановлення з'єднання), тому вона в основному реалізована в декількох телекомунікації мережі по всьому світу.

DDP (протокол доставки дейтаграм): це сегментна одиниця набору мережевих протоколів Apple Talk, яка допомагає передавати всі дейтаграми з використанням сокету в сокет через мережу AppleTalk. Цей протокол більш зручний для тих додатків, які не потребують надійної доставки даних.

EGP (протокол зовнішнього шлюзу): EGP - це протокол, який використовується для обміну всією маршрутною інформацією між двома сусідніми вузлами шлюзу по мережі. У таблиці маршрутизації є список відомих маршрутизаторів, а також адрес, і ця інформація таблиці маршрутизації допомагає вибрати найкращий маршрут з усіх доступних маршрутів.

EIGRP (Розширений протокол маршрутизації внутрішнього шлюзу): EIGRP - це протокол динамічної маршрутизації, і його основним завданням є визначення кращого шляху між кількома шляхами, а також доставка пакетів по них. Він використовує протоколи 88 номерів і працює за протоколом мережного рівня Модель OSI.

ICMP (протокол керування повідомленнями в Інтернеті): протокол ICMP використовується мережними пристроями для визначення всіх проблем та помилок мережного обміну даними, а також для контролю того, чи всі дані прибувають у відповідну цільову точку із зазначенням тривалості чи ні. Цей протокол також використовується в розподілених атаках типу "відмова в обслуговуванні" (DDoS).

IGMP (протокол управління інтернет-групами): протокол IGMP використовується для керування членством у групах багатоадресної мережі. У багатоадресній мережі використовується кілька маршрутизаторів, які допомагають спрямовувати пакети маршрутів для всіх комп'ютерів, пов'язаних із певною групою. Маршрутизатори багатоадресної розсилки збирають всю інформацію з IGMP, щоб ідентифікувати всі хости, які набувають членства в групі.

IPSec (безпека інтернет-протоколу): IPSec — це набір протоколів, які використовуються для встановлення зашифрованих з'єднань між кількома пристроями. Він пропонує функцію безпеки для надсилання даних через

загальнодоступну мережну систему. IPSec в основному використовується для налаштування VPN та допомагає працювати за рахунок шифрування IP-пакетів.

IPv4/IPv6 (Інтернет-протокол): IPv4 - це четверта версія інтернет-протоколу, а IP означає інтернет-протокол. Він містить 32-бітові цілі числа разом із чотирма адресами, вираженими у шістнадцятковому форматі, наприклад 192.1.4.126.

IPv6- це шосте покоління інтернет-протоколу, розроблене Інженерною групою Інтернету (IETF) у грудні 1998 року. Він використовує 128-бітові інтернет-адреси з вісьмома групами з чотирьох шістнадцяткових цифр, наприклад 2001:0da8:75a3:0000:0000:8a2e. :0370:8543

IPX (обмін міжмережевими пакетами): IPX був випущений у 1980-х, але набирав популярності у 1990-х Це мережевий протокол, який використовується Novell NetWare і через деякий час він був прийнятий Windows.

OSPF (спочатку відкрийте найкоротший шлях): OSPF розроблений Інженерною групою Інтернету (IETF) та працює як протокол внутрішнього шлюзу (IGP). Це протокол маршрутизації стану каналу, який допомагає знайти найкращий шлях між вихідним та цільовим маршрутизаторами.

PIM (багатоадресне розсилання, незалежно від протоколу): PIM допомагає розподіляти багатоадресні дані з використанням маршрутів, що збираються іншими протоколами. Він використовує таблицю одноадресної маршрутизації для створення та підтримки дерев багатоадресної маршрутизації з використанням переадресації по зворотному шляху. PIM має два варіанти PIM-Dense Mode та PIM-Sparse Mode.

RIP (протокол інформації про маршрутизацію): RIP — це протокол динамічної маршрутизації, який використовує кількість переходів (кількість маршрутизаторів між вихідною та цільовою мережею), наприклад, як метрика маршрутизації для пошуку найкращого маршруту між вихідною та кінцевою точками.

Функції мережного рівня

Функції мережного рівня поділені на чотири різні області; такий як:

Система маршрутизації: це основна частина мережевого рівня, оскільки вона допомагає краще визначити оптимальний шлях від джерела кількох шляхів до цільової точки. Коли маршрутизатор захоплює всі пакети через вхідний канал, він передає ці пакети на вихідний канал маршрутизатора. Наприклад; якщо пакет намагається перемістити M1 на N1, він повинен бути переданий наступному маршрутизатору на шляху до M2.

Система адресації: мережевий рівень використовує логічну адресацію, оскільки ця адреса допомагає ідентифікувати точку джерела та точку призначення. Мережевий рівень додає логічні адреси до заголовка кадру.

Міжмережева система: Основна мета мережевого рівня - забезпечити логічний зв'язок між різними видами мереж і мережеві пристрої.

Сегментація: У цьому процесі всі пакети, отримані від верхнього рівня, розбиваються на маленькі сегменти. Цей процес також відомий як пакетування і виконується за допомогою інтернет-протоколу (IP) [8].

2.3 Аналіз основних функцій протоколу IPsec

Оскільки формат інтернет-пакетів чітко визначений та широко відомий, пакет, що проходить через Інтернет, може бути перехоплений будь-яким маршрутизатором, який знаходиться на його шляху. IP-пакети не мають функції безпеки. Його вміст доступний для перегляду та редагування. Навіть контрольні суми, включені до формату інтернет-пакету, не можуть захистити пакет від несанкціонованої зміни. Вони відкриті для широкого спектру атак, таких як підроблені адреси, заміна вмісту, повторна передача застарілих пакетів та повна модифікація під час передачі.

Для інтернет-пакетів немає гарантії, що відправник та вміст пакету відповідають тому, що було призначено для передачі. Немає впевненості, що інформація залишилася секретною та не просочилася. IPSec був розроблений для усунення цих вразливостей шляхом додавання безлічі рівнів безпеки до зв'язку, включаючи аутентифікацію повідомлення, аутентифікацію відправника,

шифрування та аутентифікацію самого повідомлення. Протоколи IPsec – це вдосконалення інтернет-пакетів, які дозволяють надсилати та отримувати інтернет-пакети, захищені криптографічно. Спеціальні заголовки IPsec надають кілька форм криптографічного захисту, які були застосовані до пакету, а також додаткові відомості, необхідні для успішного розшифрування.

Перша версія IPsec була створена Джоном Іоаннідісом, Філом Карном та Вільямом Алленом Сімпсоном у 1992 році. У жовтні 1993 року Джон Іоаннідіс з Колумбійського університету та Метт Блейз із Bell Laboratories представили аргументи на користь безпеки рівня IP. Він називався «Архітектура та реалізація безпеки мережевого рівня в UNIX». Ця робота ознаменувала собою прорив у застосуванні засобів безпеки та зв'язку та набагато випередила свій час. У статті описані способи впровадження функцій безпеки без зміни структури IP, а потім розглянуті реалізації інкапсуляції дейтаграм IP в нову дейтаграму IP. Також було розглянуто переваги інкапсуляції протоколів та процедур аутентифікації, а також прозорість, яка може бути забезпечена діям, що відбуваються на верхньому рівні.

У зв'язку зі швидким розповсюдженням Інтернету та властивими протоколу TCP/IP уразливістю системи безпеки виникла гостра необхідність у вирішенні, яке гарантувало б безпеку даних, що передаються через Інтернет. Рада з архітектури Інтернету (IAB) опублікувала звіт під назвою «Безпека в архітектурі Інтернету» у 1994 році. У документі були позначені важливі області для покращення безпеки та підкреслено спільну думку про те, що Інтернет потребує більшої та кращої безпеки.

Безпека інтернет-протоколу (IPsec) перетворилася на елемент управління безпекою мережевого рівня, що найбільш широко використовується, для захисту зв'язку. IPsec – це відкрита стандартна структура для забезпечення приватного зв'язку через IP-мережі. IPsec може забезпечити будь-яку комбінацію наступних типів захисту, залежно від того, як вона реалізована та налаштована:

- Конфіденційність: IPsec може гарантувати, що дані не проглядається сторонніми особами. Це робиться шляхом шифрування даних за допомогою криптографічного методу та секретного ключа (значення, відоме лише двом людям,

які обмінюються даними). Дані можуть бути розшифровані лише тим, хто має секретний ключ.

- Аутентифікація однорангових вузлів: кожна кінцева точка IPsec перевіряє ідентифікацію іншої кінцевої точки IPsec, з якою вона має намір взаємодіяти, щоб переконатися, що мережевий трафік та дані надходять із правильного хоста.
- Цілісність: IPsec пропонує можливість ідентифікувати навмисні або ненавмисні модифікації даних під час передачі. Створення значення коду автентифікації повідомлення (MAC) криптографічної контрольної суми даних допомагає забезпечити цілісність даних. Коли MAC-адреса перераховується після зміни даних, старі та нові MAC-адреси будуть відрізнятися.
- Контроль доступу: IPsec може виконувати фільтрацію, щоб гарантувати, що користувачі можуть отримати доступ лише до певних мережних ресурсів та використовувати певні типи мережного трафіку. Реалізація IPsec найчастіше використовується для надання послуг віртуальної приватної мережі (VPN). Віртуальна приватна мережа (VPN) - це мережа, створена поверх існуючих мереж для забезпечення безпечного методу передачі даних та IP-інформації, якими обмінюються мережі. IPsec – це стандартна технологія VPN, розроблена Цільовою групою інженерів Інтернету (IETF) для пакету TCP/IP [5].

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОГО РІВНЯ НА БАЗІ ПРОТОКОЛУ IPSEC

3.1 Можливості протоколу IPsec

IPsec (Internet Protocol Security) – це великий набір протоколів та алгоритмів. IPsec в основному використовується для захисту даних, що передаються по всьому Інтернету. Інженерна робоча група Інтернету, або IETF, розробила виключно протоколи IPsec з метою забезпечення безпеки на рівні IP за допомогою аутентифікації та шифрування мережних пакетів IP.

Спочатку безпека інтернет-протоколу визначала лише два протоколи для захисту IP-пакетів: заголовок аутентифікації (AH) та інкапсуляція корисного навантаження безпеки (ESP). Перший протокол, тобто AH, забезпечує цілісність даних та послуги без повторення, а другий протокол, тобто ESP, шифрує та автентифікує дані.

Пакет Internet Protocol Security також включає Internet Key Exchange (IKE), який широко використовується для створення спільних ключів безпеки з метою встановлення асоціації безпеки (SA). Асоціації безпеки переважно необхідні для цілей процесу шифрування, а також для процесу дешифрування для узгодження рівня безпеки між двома об'єктами. Потрібний спеціальний маршрутизатор або брандмауер, який працює між двома мережами, що допомагає обробляти процес узгодження зіставлення безпеки.

Протоколи, що лежать в основі IPsec:

В основі IPsec лежать чотири основні протоколи, а саме:

1. Заголовок аутентифікації інтернет-протоколу (IP AH): заголовок аутентифікації інтернет-протоколу в основному включає такі функції, як цілісність даних і служби захисту транспорту. Заголовок аутентифікації був розроблений для додавання аутентифікації даних. Він також забезпечує цілісність даних, аутентифікацію та захист від відтворення, а одним з його недоліків є те, що він не

забезпечує шифрування. Захист від повторного використання захищає від несанкціонованої передачі пакетів. Ще одним недоліком є те, що він взагалі не захищає конфіденційність даних.

2. Інкапсуляція корисних даних безпеки Інтернет-протоколу (IP ESP). Інкапсуляція корисних даних безпеки інтернет-протоколу була в основному описана в RFC 4303. ESP надає приголомшливі функції, такі як автентифікація, цілісність та конфіденційність за допомогою шифрування IP-пакетів. Це також допомагає забезпечити цілісність даних, шифрування та автентифікацію. Аутентифікація корисного навантаження є одним із його важливих функцій.

3. Обмін ключами Інтернету (IKE). Обмін ключами в Інтернеті – це спеціальний протокол, який дозволяє двом системам або пристроям встановити безпечний та надійний канал зв'язку у ненадійній мережі. Цей протокол досягає цього, використовуючи серію обмінів ключами для створення безпечного та надійного тунелю між клієнтом та сервером, за допомогою якого вони можуть легко та безпечно відправляти зашифрований трафік. Безпека тунелю заснована на методі обміну ключами Діффі-Хеллмана, який є одним із методів забезпечення безпеки, які широко використовуються.

4. Асоціація безпеки Інтернету та протокол управління ключами (ISAKMP): Асоціація безпеки Інтернету та протокол управління ключами просто вказані як одна з частин протоколу IKE. Це структура, яка в основному використовується для встановлення ключа, аутентифікації та узгодження асоціації безпеки для безпечного обміну пакетами на рівні інтернет-протоколу. Інакше кажучи, можна сказати, що це протокол визначає параметри безпеки того, як дві системи можуть взаємодіяти друг з одним. Кожна асоціація безпеки визначає з'єднання в одному напрямку від одного хоста до іншого. Асоціація безпеки включає всі атрибути, необхідні для з'єднання, включаючи криптографічний алгоритм, режим IPsec, ключ шифрування і будь-які інші параметри, пов'язані з передачею даних, необхідні для встановлення безпечного з'єднання [10].

Використання IPsec

IPsec – це протокол безпеки, який в основному використовується для захисту конфіденційних даних, забезпечення безпечної передачі інформації, такої як фінансові транзакції, медичні записи, корпоративні повідомлення тощо. Він також використовується для захисту віртуальних приватних мереж (VPN), де тунелювання безпеки Інтернет-протоколу в основному допомагає в шифруванні всіх даних, що передаються між двома кінцевими точками або хостами. IPsec також може допомогти надійно зашифрувати дані прикладного рівня та забезпечити високий рівень безпеки для маршрутизаторів, які легко надсилають дані маршрутизації через загальнодоступний Інтернет. Надання аутентифікації без шифрування – одна з найкращих функцій безпеки інтернет-протоколу.

Без використання протоколу IPsec високорівневе шифрування у додатку або на транспортних рівнях моделі взаємодії відкритих систем (OSI) може забезпечити безпечну передачу даних. На прикладному рівні основну роль виконанні шифрування грає захищений протокол передачі гіпертексту (HTTPS). На транспортному рівні протокол безпеки транспортного рівня (TLS) відіграє важливу роль у забезпеченні шифрування. Однак шифрування та автентифікація на цих вищих рівнях збільшує ймовірність розкриття даних [2].

3.2 Архітектура протоколу IPsec

IPSec — це набір із трьох протоколів транспортного рівня, які використовуються для автентифікації походження та вмісту IP-пакетів і, за бажанням, для шифрування їх корисного навантаження. Два з протоколів, AH (Authentication Header) і ESP (Encapsulating Security Payload), забезпечують автентифікацію, що включає підтвердження джерела даних, цілісності даних і захисту від повторного відтворення. Крім того, ESP (але не AH) забезпечує шифрування даних. Третій протокол IPSec, IKE (Internet Key Exchange), є складним гібридним протоколом, який використовується для однорангової автентифікації та процесів обміну ключами, які обов’язково передують послугам, що надаються AH та ESP.

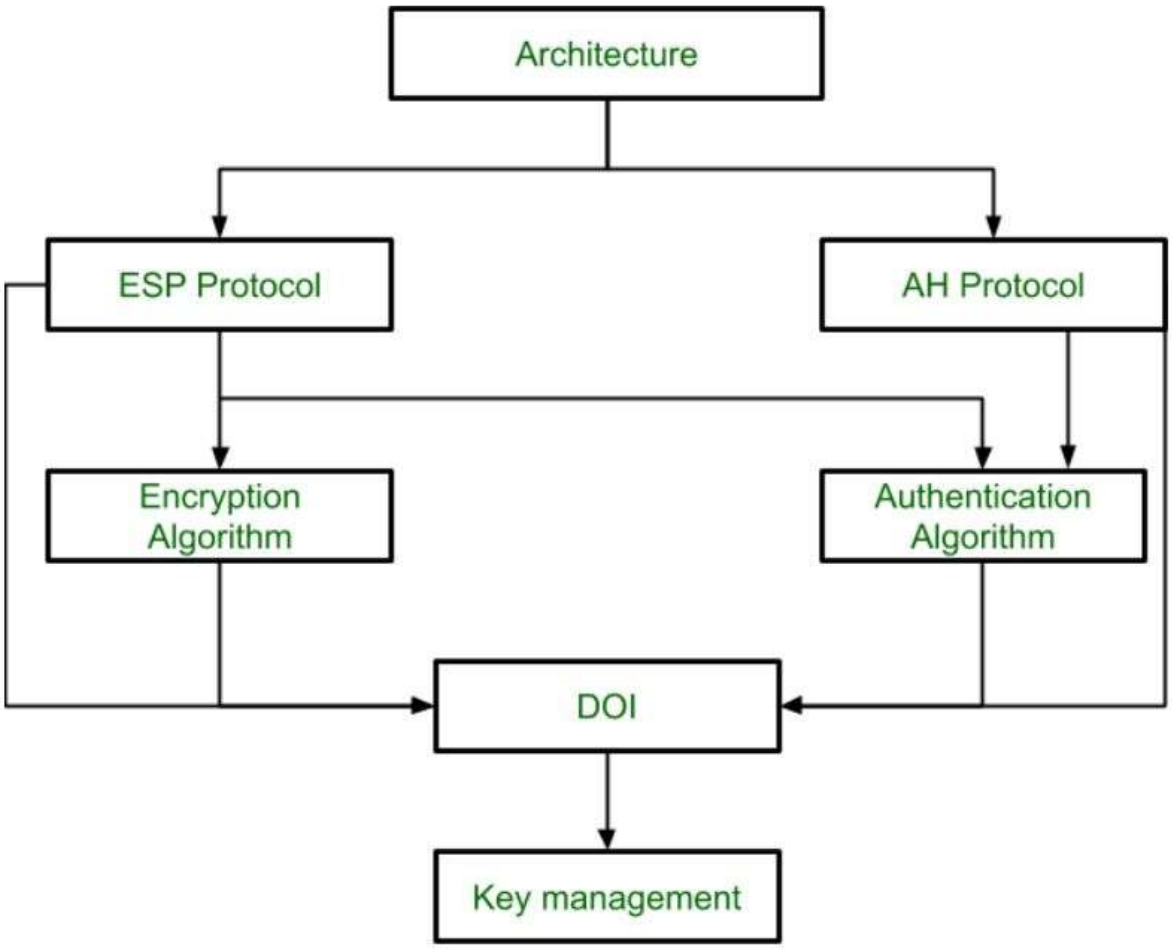

Рис.3.1. Архітектура IPSec

Протоколи IPSec не визначають, які алгоритми слід використовувати для обчислень, пов’язаних із шифруванням або створенням цифрових підписів. Це робить визначення протоколів повністю загальними, тобто вони можуть враховувати такі розробки, як нові криптографічні методи, коли вони стають доступними. Алгоритми, які будуть використовуватися, визначаються окремо як частина загальної політики безпеки, налаштованої на кожній з однорангових станцій. Початкові переговори IKE дозволяють партнерам узгодити конкретну комбінацію протоколів і алгоритмів, які будуть використовуватися для всієї наступної обробки IPSec.

Асоціації безпеки IPSec (SA)

SA є фундаментальними для роботи IPSec. Перед передачею захищених дейтаграм дві однорангові станції повинні досягти згоди щодо того, як IPSec має

обробляти розмови між ними. Вони узгоджують протокол, перетворення, ключі та час життя ключа. Цей «контракт» між парою партнерів IPSec є Асоціацією безпеки (SA).

SA є симплексними (тобто односпрямованими) за своєю природою. Якщо дві станції, X і Y, безпечно спілкуються, кожна з них підтримуватиме дві SA, одну для вихідного та одну для вхідного трафіку. Таким чином, має бути очевидно, що (SAout) X матиме спільні криптографічні параметри з (SAin) Y.

Визначальні характеристики активної SA є результатом узгодження між двома партнерами IPSec. Кожен одноранговий вузол має бути налаштований заздалегідь із вибором протоколів і перетворень, які він бажає прийняти або може запропонувати одноранговому вузлу. Припустимо, що станція X налаштована на пропонування ESP із шифруванням DES і алгоритмами цілісності MD5, а також на пропонування AH з алгоритмом MD5, тоді як станція Y налаштована лише на використання AH з алгоритмом MD5; узгодження SA між цими двома одноранговими вузлами призведе до згоди кожного з них захистити свої розмови за допомогою протоколу AH та алгоритму MD5. Оскільки станція Y не налаштована на використання ESP, вона не створюватиме SA, використовуючи цей протокол. Ці попередньо визначені політики відомі як база даних політики безпеки (SPD). Грубі збої в обробці IPSec часто викликані відсутністю будь-якого спільного протоколу чи алгоритму в SPD двох однорангових пристроїв. Таким чином, початкові переговори в основному режимі IKE не досягають згоди, і SA не може бути встановлено.

Індекс параметрів безпеки (SPI)

При отриманні дейтаграми, захищеної IPSec, дуже важливо, щоб станція, на яку було надіслано пакет, могла визначити, який із своїх SA їй слід використовувати під час обробки захищеного пакету. SPI — це довільне 32-розрядне значення, яке разом із IP-адресою призначення зовнішнього IP-заголовка та протоколом (AH або ESP) однозначно ідентифікує SA для приймаючої станції. Станція-відправник включає SPI з кожним пакетом, який вона відправляє, ідентифікуючи вхідний SA приймаючого вузла. Якщо SA не може бути розпізнано,

станція-одержувач відкидає пакет без будь-якої подальшої обробки. У термінології бази даних кортеж SPI, IP-адреса призначення, протокол може розглядатися як первинний ключ бази даних SA станції-одержувача. (Кортеж — це впорядкований набір значень (часто розділених комами) і аналогічний запису в нереляційній базі даних).

Порядкові номери

Відправник надсилає це унікальне та монотонно зростаюче 32-розрядне ціле число без знаку з кожним захищеним пакетом для захисту від атак повтору. Станція-одержувач перевіряє це поле, щоб визначити, чи є пакет дублікатом уже отриманого. Порядковий номер збільшується на одиницю для кожного пакета, обробленого через даний SA. SAs зазвичай переглядаються до того, як ця кількість переповниться.

Порядкові номери потрібні для захисту від атаки відтворення, під час якої зловмисник перехоплює та зберігає пакети, що надходять від станції-відправника. Потім зловмисник заповнює приймальну станцію, повторно надсилаючи ці перехоплені пакети. Це форма атаки на відмову в обслуговуванні.

Управління SA

Керування SA стосується їх створення та видалення. Створення асоціацій безпеки — це двоетапний процес, у якому параметри спочатку узгоджуються з одноранговим IPSec, а потім база даних SA оновлюється новим SA. Для всіх реалізацій IPSec обов’язковою є підтримка ручного введення, при якому всі необхідні параметри узгоджуються офлайн (наприклад, за допомогою телефонної розмови). Створені вручну SA ніколи не закінчуються, а процеси, задіяні в їх створенні, є громіздкими та небезпечними. Тому бажано, щоб для створення SA було розгорнуто протокол керування ключами, наприклад IKE. Різні тригери викликають видалення SA. Вони включають:

— закінчення терміну служби ключа
— скомпрометовані ключі
— кількість байтів, оброблених через SA, досягаючи порогового значення
— одноранговий вузол безпеки запитує, щоб SA було розірвано.

Щоб уникнути непотрібних перерв, незадовго до видалення існуючого буде узгоджено нову заміну SA. Після повного встановлення цього нового SA його буде використано негайно, а старий буде видалено незабаром після цього [11].

Режими IPSec

Основна функція IPSec полягає в тому, щоб забезпечити основу на основі стандартів, що визначає, як IP-пакети можуть бути захищені під час їх передачі. Існує також важлива допоміжна функція, завдяки якій IPSec забезпечує тунелювання пакетів, які він захищає. Переважні обставини визначають, чи необхідно тунелювати захищені пакети, тому IPSec може працювати в двох різних режимах, у яких функція тунелювання активна або пригнічена. Різниця між двома режимами стосується розташування заголовка IPSec у вихідному IP-пакеті. Це, у свою чергу, впливає на ступінь захисту, який надає IPSec.

Режим тунелю

Якщо адресат оригінального незахищеного пакета не збігається з віддаленою кінцевою точкою безпеки, IPSec має працювати в режимі тунелю. Заголовок IPSec і новий заголовок IP додаються до вихідного пакета, як показано.

Висновок полягає в тому, що в режимі тунелю захист надається всьому IP-пакету, а не лише його корисному навантаженню між кінцевими точками тунелю. На рисунку 8 зображено типовий сценарій, коли IPSec потрібен для роботи в тунельному режимі.

Дві станції, що спілкуються, підключені до мереж із приватними номерами і тому не можуть спілкуватися напряму. Підключені до Інтернету маршрутизатори діють як кінцеві точки безпеки. Пакети приймаються від станції-відправника та інкапсулюються вихідним маршрутизатором. Новий зовнішній IP-заголовок містить дійсні в Інтернеті адреси маршрутизатора як джерела та призначення. Коли тунельовані пакети надходять на маршрутизатор призначення, зовнішній IP-заголовок видаляється, а вихідний IP-пакет генерується заново в результаті обробки IPSec. Потім цей пакет перетворюється на кадр Ethernet і доставляється до локального пункту призначення звичайним способом.

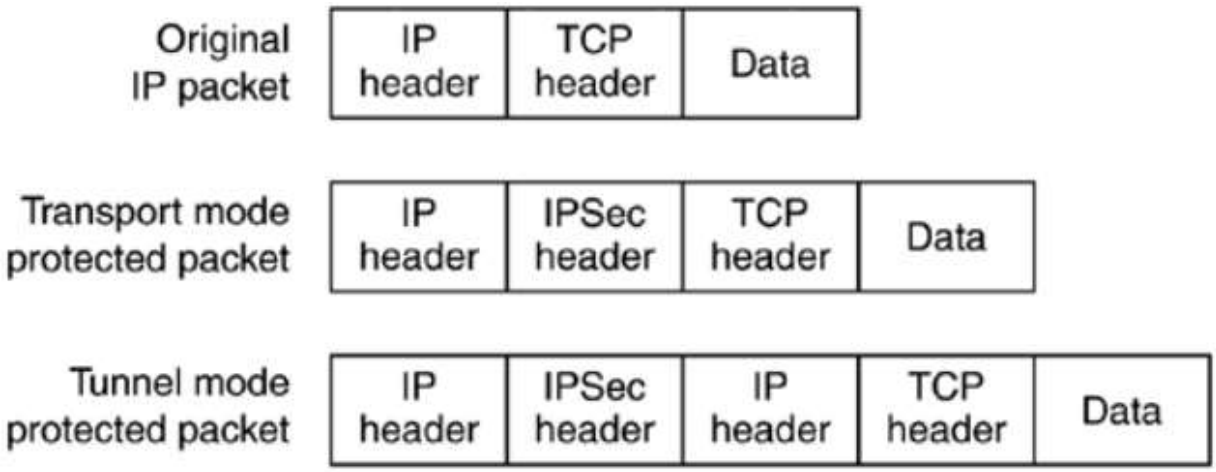

Рис.3.2. Пакет протоколу IPsec

Транспортний режим

Тут заголовок IPSec (AH або ESP) вставляється між мережевим і транспортним заголовками вихідного пакета, як показано нижче.

Отже, корисне навантаження IP захищене в транспортному режимі, а заголовок – ні. Спосіб транспортування підходить за двох обставин.

По-перше, якщо дві станції, що беруть участь у базовому зв'язку, також є одноранговими IPSec, тоді явно немає потреби тунелювати захищені пакети. Зазвичай це відбувається, якщо дві станції можуть спілкуватися безпосередньо, оскільки вони працюють на дійсних Інтернет-адресах.

По-друге, обставини можуть диктувати, що хоча IPSec використовується для надання послуг безпеки, слід розгорнути альтернативну технологію тунелювання. Наприклад, IPSec може використовуватися для захисту пакетів, які пройшли через тунельний інтерфейс на маршрутизаторі Cisco. Тунель рівня III тут виконується за допомогою іншої (зазвичай GRE) інкапсуляції, тому IPSec доцільно працювати в транспортному режимі, оскільки зовнішній IP-заголовок уже надано. Це може здатися надуманим методом досягнення тієї ж мети, що й IPSec у тунельному режимі, але є випадки, коли такі методи потрібні.

Протоколи IPSec

Два протоколи IPSec, AH і ESP, працюють на тому самому транспортному рівні моделі OSI, що й більш звичні протоколи, такі як TCP і UDP. Щоб захистити

пакет за допомогою IPSec, цей пакет має бути інкапсульований за допомогою одного з цих двох протоколів.

Заголовок автентифікації

Оскільки AH забезпечує лише автентифікацію, а не конфіденційність, це досить простий протокол, який створює лише заголовок без трейлера. Заголовок містить SPI, порядковий номер і дані автентифікації (Рис.3.2.).

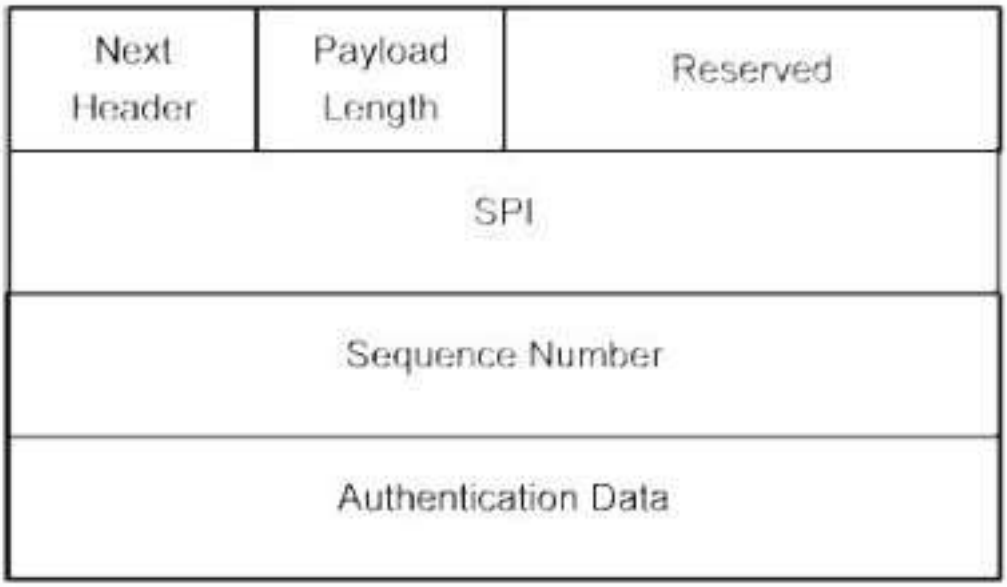

Рис.3.3. Заголовок автентифікації.

Це останнє поле містить значення перевірки цілісності, яке гарантує, що пакет не було змінено під час передачі. SA вказує алгоритм, який використовується для розрахунку цього значення. Сімейством відповідних алгоритмів є MAC, наприклад MD5 або SHA-1. Наступний заголовок — це 8-бітове поле, яке вказує, який протокол слідує за заголовком AH. Коли IPSec працює в режимі тунелю, значення цього поля буде 4 (IP-in-IP). У транспортному режимі захищатиметься протокол верхнього рівня (зазвичай UDP або TCP).

Інкапсуляція корисного навантаження безпеки (ESP)

Цей протокол необхідно використовувати, коли потрібне шифрування даних. Оскільки це заголовок IPSec, ESP надає SPI та порядкові номери, призначення яких обговорювалося в попередньому розділі. Заповнення (до максимум 255 байт) використовується ESP для збереження меж байтів. Якщо використовується

алгоритм шифрування, який вимагає, щоб відкритий текст був кратним певній кількості байтів (наприклад, розмір блоку блокового шифру), поле заповнення використовується для заповнення відкритого тексту до необхідного розміру. Також може знадобитися доповнення незалежно від вимог алгоритму шифрування, щоб гарантувати, що кінцевий зашифрований текст закінчується на 4-байтовій межі, таким чином вирівнюючи трейлер по правому краю (Рис.3.3.).

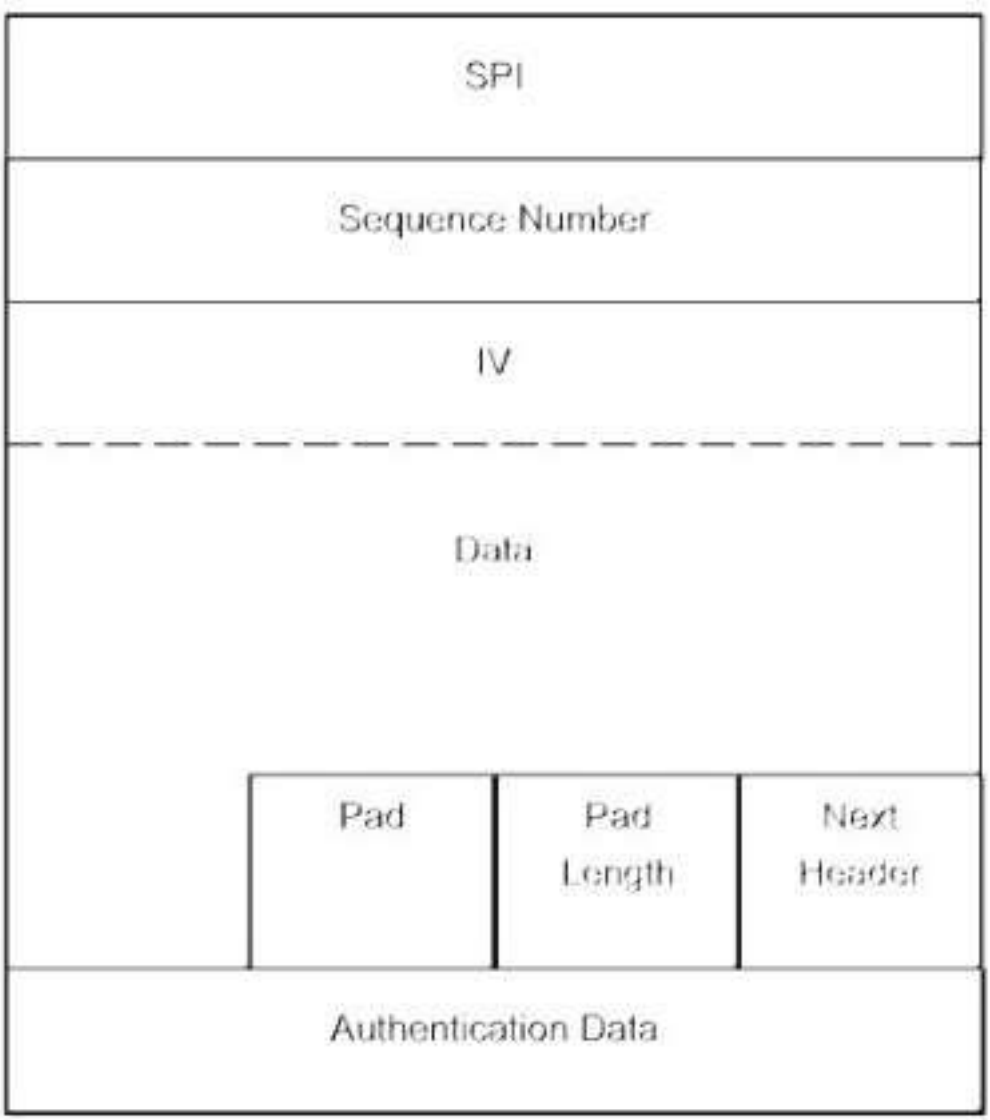

Рис.3.4. ESP

Інтернет-обмін ключами (IKE)

Перш ніж пакети можна буде захистити за допомогою AH або ESP, має існувати відповідний SA. Третім членом сімейства протоколів IPSec є IKE, який використовується для однорангової автентифікації, узгодження ключів і

динамічної побудови SA. Незважаючи на те, що тонкі деталі IKE є складними та виходять за межі цього посібника, розуміння методів, які використовуються під час створення IPSec SA, є неоціненним під час усунення несправностей.

Гібридний протокол IKE поєднує частини протоколу визначення ключа Oakley і SKEME (механізм обміну ключами безпеки), обидва протоколи обміну ключами, з ISAKMP (протокол керування ключами асоціації безпеки Інтернету). Останній визначає структуру для однорангової автентифікації, обміну ключами та керування SA через IP-мережу та працює на UDP-порту 500.

Узгодження IKE складається з двох етапів, на яких спочатку встановлюється IKE SA (фаза 1), щоб забезпечити безпечний канал зв'язку, через який можуть бути створені SA для інших протоколів (наприклад, IPSec) (фаза 2). Існує два взаємовиключні методи, за допомогою яких можна продовжити переговори IKE фази 1; основний режим або агресивний режим. Переговори фази 2 проводяться за допомогою швидкого режиму обміну.

Основний режим

Обмін в основному режимі використовує шість повідомлень у трьох поворотах. Під час першого обміну однорангові вузли обговорюють параметри IKE SA та те, як будуть здійснюватися інші обміни. Наступні два обміни використовуються для обміну матеріалом ключа Діффі-Хеллмана. Остання пара повідомлень основного режиму використовується для автентифікації однорангових користувачів. Цей останній обмін шифрується за допомогою попередньо узгодженого ключа, таким чином захищаючи ідентифікаційні дані однорангових користувачів від перехоплювачів.

Агресивний режим

Обмін в агресивному режимі виконує те саме, що й в основному режимі, але використовує лише половину кількості повідомлень шляхом вбудовування деяких повідомлень в інші. Отже, переговорні здібності агресивного режиму обмежені, а ідентичності однолітків не приховані.

Швидкий режим

Після встановлення IKE SA за допомогою обміну фази 1 (у основному або агресивному режимі) його можна використовувати для створення SA IPSec за допомогою обміну фази 2 у швидкому режимі. За винятком заголовка ISAKMP, усі швидкі обміни в режимі шифруються та автентифікуються.

Компанії безпеки обмінюються ключами IPSec (по одному для кожного SA) у рамках швидкого обміну. Це робиться шляхом попереднього обміну псевдовипадковими одноразовими номерами (нонце — це параметр, який змінюється з часом), які хешуються зі спільним секретом IKE. Отримані унікальні ключі IPSec не мають властивості ідеальної прямої безпеки (PFS), оскільки всі вони походять від того самого спільного секрету IKE. За допомогою PFS, якщо один ключ скомпрометовано, попередні та наступні ключі залишаються безпечними, оскільки наступні ключі не є похідними від попередніх ключів. Додатковий обмін Діффі-Хеллмана виконується з кожним обміном швидким режимом, якщо PFS указано в політиці IPSec. Оскільки кожен обмін Діффі-Хеллмана потребує великого піднесення до степеня, PFS точно встановлюватиме вартість продуктивності. Спільний секрет, отриманий у швидкому режимі обміну Diffie-Hellman, використовується для генерації ключів IPSec, які не мають «пам’яті» своїх попередників.

Домен інтерпретації IPSec (DOI)

Протокол IKE визначає, як узгоджуються параметри безпеки та встановлюються спільні ключі для інших протоколів. Він не визначає, про що вести переговори. Це функція документа домену інтерпретації (DOI), який визначає, серед іншого, атрибути, які IKE узгоджує в швидкому режимі. Наразі існують документи DOI для IPSec і для протоколів маршрутизації RIP (Routing Information Protocol) і OSPF (Open Shortest Path First) [4].

3.3 Можливості IPsec VPN

IPsec забезпечує безпечну двосторонню передачу через приватні та навіть загальнодоступні мережі, включаючи відкриті точки доступу WiFi і глобальний

Інтернет. IPsec використовує техніку, яка шифрує всі дані під час передавання та ефективно їх кодує, щоб лише авторизовані отримувачі могли їх розшифрувати.

У порівнянні з іншими конкуруючими протоколами, сильна сторона IPsec полягає в його гнучкості та зрілості. Широка різноманітність алгоритмів і підпротоколів, доступних компаніям, дозволяє їм розробляти власну систему зв’язку для віддалених клієнтів. IPsec VPN широко використовуються завдяки стандартизованому підходу IPsec до безпеки, який базується на IPv4 та IPv6. IPsec використовує шифрування AES-256, яке практично неможливо зламати сучасним комп’ютерним обладнанням, що робить його неймовірно безпечним.

Підводячи підсумок, IKE можна розглядати як автентифікований обмін Діффі-Хеллмана з ISAKMP, що забезпечує необхідну мережеву структуру.

VPN або приватна віртуальна мережа – це мережне програмне забезпечення, яке дозволяє користувачам анонімно та безпечно користуватися Інтернетом. IPSec VPN – це програмне забезпечення VPN, яке використовує протокол IPSec для створення зашифрованих тунелів в Інтернеті. Він забезпечує наскрізне шифрування, що означає, що дані шифруються на комп'ютері і розшифровуються на сервері, що приймає [2].

SSL VPN

SSL означає рівень захищених сокетів. Це протокол безпеки, який захищає веб-трафік. SSL VPN – це сервіс мережної безпеки на основі браузера, яка використовує вбудований протокол SSL, щоб шифрувати та захищати мережевий обмін даними.

IPSec VPN та SSL VPN

Обидва протоколи безпеки працюють на різних рівнях моделі взаємодії відкритих систем (OSI). Модель OSI визначає багаторівневу структуру того, як комп'ютери обмінюються даними у мережі.

Протоколи IPSec застосовуються до мережного та транспортного рівня в середині моделі OSI. А SSL шифрує дані на верхньому рівні програми. Ви можете підключитися до SSL VPN з веб-браузера. Для використання IPSec VPN потрібно встановити окреме програмне забезпечення.

SSL VPN працює на іншому мережевому рівні, ніж IPsec VPN. SSL VPN працює на прикладному рівні, тоді як IPsec VPN працює на мережевому рівні (L3).

IKE — це механізм керування ключами та автентифікації, який використовується IPsec VPN. IKE генерує спільний секретний ключ за допомогою алгоритму Діффі-Хеллмана, який потім використовується для шифрування зв'язку між двома хостами. SSL VPN шифрує зв'язок за допомогою Transport Layer Security (TLS). Інфраструктура відкритих ключів (PKI) використовується TLS для керування ключами.

Попередньо спільні ключі необхідні для з'єднань IPSec для шифрування та передачі зв'язку між клієнтом і сервером. SSL VPN не має цієї проблеми, оскільки вони встановлюють з'єднання та безпечно обмінюються ключами шифрування за допомогою криптографії з відкритим ключем.

IPsec VPN захищає будь-який трафік між двома точками, позначеними IP-адресами. SSL VPN ідеально підходить для забезпечення обміну даними через загальнодоступний Інтернет, з'єднання між клієнтом електронної пошти та сервером електронної пошти, веб-браузером і веб-сервером [6].

3.4 Рекомендації шодо захисту мережевого протоколу комп'ютерних систем на основі протоколу IPsec

Система стандартів IPSec увібрала прогресивні методики та досягнення в галузі мережевої безпеки, завоювала визнання фахівців як надійна і легко інтегрована система безпеки для IP-мереж. Система IPSec міцно займає сьогодні лідируючі позиції у наборі стандартів для створення VPN. Цьому сприяє її відкрита побудова, здатна включати нові досягнення в галузі криптографії. IPSec дозволяє захистити мережу від більшості мережевих атак, «скидаючи» чужі пакети ще до того, як вони досягнуть рівня IP на комп'ютері, що приймає. У комп'ютер або мережу, що захищається, можуть увійти тільки пакети від зареєстрованих партнерів по взаємодії.

IPSec забезпечує:

Автенифікацію - доказ відправлення пакетів вашим партнером по взаємодії, тобто володарем секрету, що розділяється;

Цілісність - неможливість зміни даних у пакеті;

Конфіденційність - неможливість розкриття даних, що передаються;

Надійне управління ключами - протокол IKE обчислює секрет, що розділяється, відомий тільки одержувачу і відправнику пакета;

Тунелювання - повне маскування топології локальної мережі підприємства.

Робота в рамках стандартів IPSec забезпечує повний захист інформаційного потоку даних від відправника до одержувача, закриваючи трафік для спостерігачів на проміжних вузлах мережі. VPN-рішення на основі стека протоколів IPSec забезпечують побудову віртуальних захищених мереж, їх безпечну експлуатацію та інтеграцію з відкритими комунікаційними системами.

Привабливість VPN-технології на основі IPSec пояснюється цілою низкою причин:

Захист мережного рівня прозорий для всіх прикладних систем, що працюють у мережі; це означає, що всі програми продовжують працювати в захищеній мережі так само, як працювали у відкритій, не вимагаючи жодних доопрацювань та змін;

Забезпечення масштабованісті системи захисту в тому сенсі, що для захисту об'єктів різної складності та продуктивності можна використовувати адекватний за рівнем складності, продуктивності та вартості програмний або програмно-апаратний засіб захисту;

Всі продукти захисту масштабованого ряду сумісні між собою, тому продукти захисту інформації на об'єктах різного рівня - від віддалених одиничних терміналів до локальних мереж довільного масштабу - можуть бути об'єднані в єдину корпоративну мережу, доступ до ресурсів і трафіку якої буде закритий для всіх сторонніх.

Використання засобів захисту інформації на основі протоколу IPSec у розподілених мережних інформаційних системах має такі переваги:

За допомогою засобів захисту на основі IPSec може бути захищена вся корпоративна мережа: від великих локальних мереж офісів до окремих терміналів (робочих місць);

Організація як окремих комунікаційних ланок мережі можуть використовуватися ресурси відкритих мереж загального користування; всі загрози, що виникають під час використання мереж загального користування, будуть компенсовані засобами захисту IPSec;

Поряд із захистом трафіку забезпечується підконтрольність роботи мережі, достовірна ідентифікація всіх джерел інформації; при необхідності може бути забезпечена автентифікація трафіку лише на рівні окремих користувачів;

Програмні та програмно-апаратні засоби захисту інформації дозволяють сегментувати інформаційну систему та організувати безпечну експлуатацію системи, яка обробляє інформацію різних рівнів конфіденційності;

Система захисту інформації накладає обмеження на додатки та легко інтегрується з існуючими системами захисту інформації прикладного рівня та загальною адміністрацією безпеки підприємства (відомства, організації);

В основі системи захисту лежить логіка відкритих ключів Діффі-Хеллмана; це дозволяє суттєво спростити систему розподілу та оновлення ключів, зробити її більш економічною, ефективною та безпечною;

Для всіх елементів системи захисту можуть бути забезпечені централізоване дистанційне керування та аудит; ця можливість має першорядне значення для суттєво розподіленої структури інформаційної системи;

Засоби захисту мережевого рівня не обмежують загальну структуру та стратегію розвитку прикладної підсистеми ІС.

ВИСНОВКИ

В бакалаврській роботі було проаналізовано основні проблеми захисту мережевого рівня комп’ютерних систем, основні загрози та досліджено методи та засоби захисту комп’ютерних мереж.

Досліджено, що протокол Internet Protocol Security (IPSec) є системою відкритих стандартів, які запропонувала Робоча група інженерів Інтернету (IETF - Internet Engineering Task Force) IPSec, які забезпечують захист мереж, використовуючи при цьому криптографічні протоколи безпеки і динамічне управління ключами. IPSec використовує модель наскрізної безпеки з встановленням довіри та безпеки між вихідними та кінцевими IP-адресами. IPSec дозволяє захищати IP-трафік як від вузла до вузла у разі, коли два вузла IPSec обмінюються даними, і серед мережного шляху у разі, коли IPSec маршрутизатори забезпечують захист трафіку з Інтернету.

Про трафік, що захищається, повинні знати тільки два комп'ютери - відправляючий і приймаючий. Крім цього, протокол IPSec можна використовувати для забезпечення захисту всіх комунікацій між усіма сторонами за допомогою автентифікації та шифрування без необхідності зміни будь-яких додатків або протоколів. Тобто, якщо необхідно переконатися в тому, що на виході повідомлення не змінюється і зловмисник не може прочитати їх, IPSec забезпечує чудове рішення для забезпечення цих цілей. Варто запам'ятати, що IPSec не є компонентом брандмауера операційної системи. Але незважаючи на це, для зниження навантаження на адміністраторів IPSec використовує адміністрування на основі політик.

Таким чином, цей протокол дозволяє централізовано керувати політиками, призначеними для дозволу, блокування або призначення безпеки, для одноадресного IP-трафіку, на основі конкретних адрес, протоколів та портів.

ПЕРЕЛІК ПОСИЛАНЬ

1. What is a network? Definition, explanation, and examples [Електронний ресурс] – Режим доступу: https://www.ionos.com/digitalguide/server/know-how/what-is-a-network/
2. What is IPsec VPN and How does it Work? The Complete Guide for IPsec [Електронний ресурс] – Режим доступу: https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-ipsec-vpn
3. How IPsec works, it's components and purpose [Електронний ресурс] – Режим доступу: https://www.csoonline.com/article/2117067/how-ipsec-works.html
4. IPsec: The Complete Guide to How It Works and How to Use It [Електронний ресурс] – Режим доступу: https://www.twingate.com/blog/ipsec
5. An overview of the OSI model and its security threats [Електронний ресурс] – Режим доступу: https://www.tripwire.com/state-of-security/overview-osi-model-and-its-security-threats
6. NIST Special Publication 800-77 Revision 1. Guide to IPsec VPNs [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf
7. Network security [Електронний ресурс] – Режим доступу: https://www.techtarget.com/searchnetworking/definition/network-security
8. Network Layer in OSI Model: Protocols, Examples, Functions [Електронний ресурс] – Режим доступу: https://digitalthinkerhelp.com/network-layer-in-osi-model-protocols-examples-functions/
9. Common Network Security Threats & Vulnerabilities [Електронний ресурс] – Режим доступу: https://www.caltech.com/network-security-threats-and-vulnerabilities/
10. IPsec Protocols [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/ipsec-protocols/

11. IP security: overview and architecture [Електронний ресурс] – Режим доступу: https://community.jisc.ac.uk/library/advisory-services/ip-security-overview-and-architecture

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (презентація)