НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання кваліфікаційного дослідження

ДОСЛІДЖЕННЯ РЕАЛІЗАЦІЙ ПРОТОКОЛІВ IPSEC

Виконали студенти
групи ФІ-32мн
Баєвський Констянтин,
Шифрін Денис,
Кріпака Ілля

Київ — 2024

ЗМІСТ

ВСТУП

0.1 Мета практикуму

Дослідження особливостей реалізації криптографічних механізмів протоколів IPSec.

0.1.1 Постановка задачі

Треба виконати	**Зроблено**
Провести дослідницьку роботу з метою аналізу особливостей реалізації криптографічних механізмів протоколів IPSec.	✓
Описати основне призначення протоколів IPSec, їх місце в мережевій моделі OSI та взаємодію зі стеком протоколів TCP/IP та ін.	✓
Дослідити архітектуру стеку протоколів IPSec.	✓
Описати призначення, особливості та відмінності криптографічних механізмів протоколів AH, ESP, ISAKMP, IKE, IKEv2, KINK та ін.	✓
Проаналізувати концепцію безпечних асоціацій (SA), її особливості та бази даних SPD і SAD (їх призначення та способи заповнення і використання).	✓
Дослідити детально особливості структури заголовків протоколів AH і ESP в тунельному та транспортному режимах з повним описанням їх полів та можливих значень.	✓
Визначити особливості обробки вхідних та вихідних IPSec-пакетів для кожного з протоколів та режимів.	✓
Дослідити нижній рівень архітектури стеку протоколів IPSec – домен інтерпретації DOI.	✓
Визначити зареєстровані алгоритми автентифікації, шифрування, геш-функцій та ін. криптографічних алгоритмів для стеку протоколів IPSec.	✓
Визначити та описати особливості основних схем застосування протоколів IPSec: хост-хост, шлюз-шлюз та хост-шлюз. А також використання протоколів IPSec для побудови VPN-тунелів.	✓

1 ПРОТОКОЛИ IPSEC

1.1 Особливості реалізації криптографічних механізмів протоколів IPSec

IPSec (Internet Protocol Security) є набором протоколів для забезпечення захисту передачі даних в IP-мережах. Його криптографічні механізми ґрунтуються на шифруванні, автентифікації, цілісності даних та управлінні ключами. Основні протоколи, що складають IPSec, включають Authentication Header (AH) та Encapsulating Security Payload (ESP), а також механізм Internet Key Exchange (IKE) для обміну ключами.

1.1.1 Authentication Header (AH)

AH забезпечує автентифікацію джерела даних та гарантує цілісність IP-пакетів, захищаючи їх від модифікацій під час передачі. Цей протокол додає до пакета спеціальний заголовок, який містить криптографічний хеш (наприклад, HMAC-SHA1 або HMAC-SHA256), розрахований з урахуванням певного секретного ключа. Формула для хешування виглядає так:

$$HMAC = H\left(K \oplus opad || H\left(K \oplus ipad || Message\right)\right),$$

де K – це секретний ключ, а $ipad$ та $opad$ – константи для внутрішнього та зовнішнього заповнення.

AH застосовується до IP-заголовка і, зазвичай, не шифрує дані, але забезпечує їхню цілісність і аутентифікацію. Його головний недолік — відсутність конфіденційності, що означає, що дані залишаються видимими для третіх сторін.

1.1.2 Encapsulating Security Payload (ESP)

ESP реалізує шифрування, а також автентифікацію даних, що забезпечує конфіденційність, цілісність і автентичність повідомлень. У транспортному режимі ESP шифрує лише корисні дані (payload), а в тунельному режимі — весь IP-пакет, включаючи заголовок. Основні алгоритми шифрування для ESP — AES і 3DES. Формула для шифрування пакету:

$$C = Encrypt_{AES}(K, Payload),$$

де C — зашифроване повідомлення, K — секретний ключ, а $Payload$ — дані пакету.

У тунельному режимі ESP створює додатковий IP-заголовок, щоб захистити оригінальну IP-адресу від перехоплення, що є важливим для захисту внутрішньої мережі організації від атак.

1.1.3 Internet Key Exchange (IKE)

IKE відповідає за обмін ключами і встановлення Security Association (SA) — набору параметрів безпеки, що визначають тип захисту для з'єднання. Основним механізмом IKE є протокол Diffie-Hellman для встановлення загальних ключів, що використовуються для шифрування та автентифікації. Формула обміну:

$$K_{AB} = g^{a \cdot b} \mod p,$$

де a та b — секретні ключі сторін, а g та p — спільні параметри.

IKE використовує два порти (500 та 4500) для підтримки NAT-Traversal, що забезпечує сумісність з мережами, де змінюються IP-адреси під час пересилання пакетів через маршрутизатори, що використовують NAT.

1.2 Основне призначення протоколів IPSec та взаємодія зі стеком протоколів TCP/IP

Протоколи IPSec (Internet Protocol Security) використовуються для захисту передачі даних на мережевому рівні (Layer 3) моделі OSI. Вони забезпечують цілісність, автентифікацію та конфіденційність даних шляхом шифрування та контролю автентичності IP-пакетів. Основною перевагою IPSec є його незалежність від додатків, оскільки він працює на рівні IP. Це дозволяє захищати всі протоколи вищих рівнів (таких як TCP і UDP) та мережеві додатки, незалежно від їхнього типу.

На відміну від інших протоколів безпеки, таких як TLS (Transport Layer Security), що працює на транспортному рівні (Layer 4), або SSH (Secure Shell), який функціонує на прикладному рівні (Layer 7), IPSec забезпечує безпеку безпосередньо на рівні IP-пакетів. Завдяки цьому він може захищати будь-який тип даних, що передається через IP, забезпечуючи універсальну конфіденційність і цілісність трафіку на основі IP.

Взаємодія IPSec із протоколами стеку TCP/IP реалізується через його ключові компоненти — Authentication Header (AH) та Encapsulating Security Payload (ESP).

У контексті стеку TCP/IP IPSec автоматично забезпечує захист мережевого рівня (Internet Layer), дозволяючи захищати всі транспортні протоколи (TCP, UDP) та додатки, які їх використовують. Це робить IPSec універсальним рішенням для забезпечення безпеки корпоративних мереж, зокрема для реалізації VPN-з'єднань. Таким чином, IPSec гарантує безпечну передачу даних між віддаленими мережами та пристроями, забезпечуючи захист як у межах локальних мереж, так і при використанні глобального Інтернету.

1.3 Архітектура стеку протоколів IPSec

Архітектура стеку протоколів IPSec представлена у вигляді багаторівневої структури, яка забезпечує комплексний підхід до безпеки IP-мереж. IPSec складається з ряду протоколів, механізмів та алгоритмів, які взаємодіють між собою для забезпечення конфіденційності, цілісності та автентифікації даних на мережевому рівні.

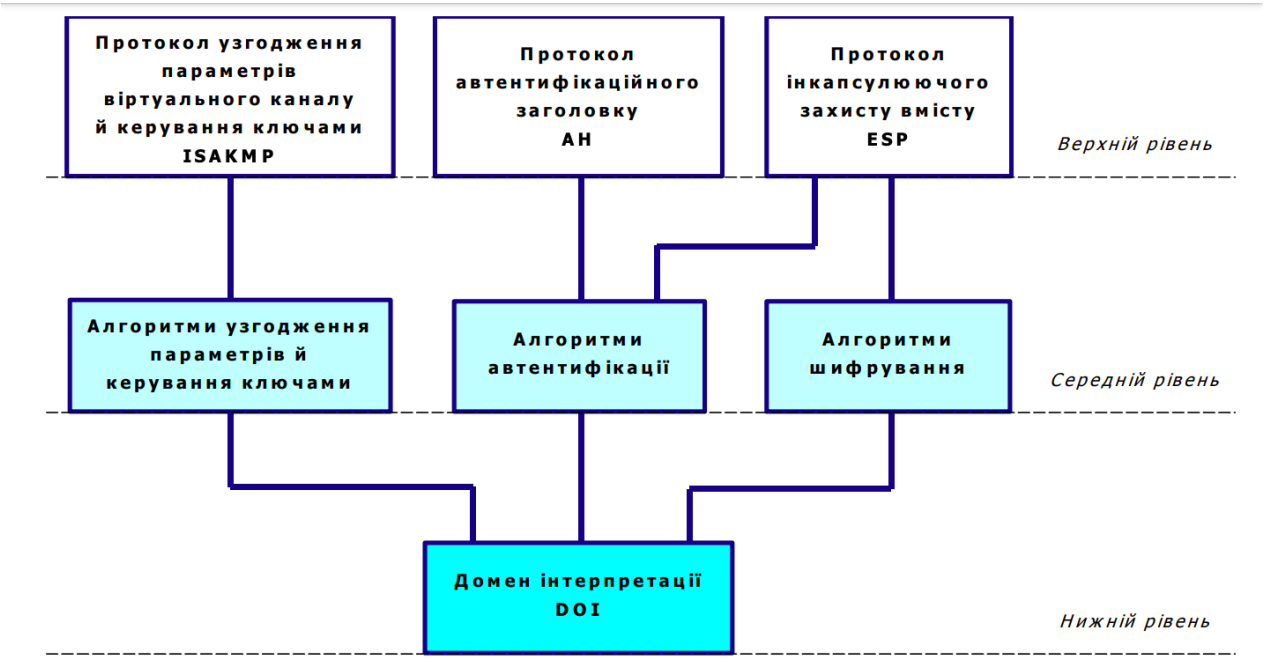


Рисунок 1.1 – Архітектура стеку протоколів IPSec.

На верхньому рівні архітектури IPSec зосереджені ключові протоколи та механізми, які забезпечують основні функції безпеки:

– **Authentication Header (AH)** — забезпечує автентифікацію джерела даних і контроль цілісності IP-пакетів, проте не забезпечує конфіденційності.

– **Encapsulating Security Payload (ESP)** — відповідає за шифрування, автентифікацію та цілісність даних, забезпечуючи конфіденційність переданої інформації.

– **Internet Security Association and Key Management Protocol**

(ISAKMP) — регламентує встановлення та управління безпечними асоціаціями (SA), а також координує узгодження параметрів безпеки.

Середній рівень архітектури включає механізми та алгоритми для:

– узгодження параметрів шифрування та автентифікації;

– вибору криптографічних алгоритмів відповідно до вимог безпеки (наприклад, AES, HMAC-SHA-256 тощо);

– реалізації протоколів обміну ключами, таких як IKE (Internet Key Exchange) і його вдосконалена версія IKEv2.

Нижній рівень архітектури забезпечує підтримку інтероперабельності через використання **Domain of Interpretation (DOI)**. DOI виконує роль стандарту, який визначає набір параметрів і правил для взаємодії між різними реалізаціями IPSec, включаючи ідентифікатори криптографічних алгоритмів, параметри політик безпеки та формати даних.

1.3.1 Режими передачі в IPSec

IPSec підтримує два основних режими передачі:

1) **Транспортний режим**: захищає лише корисне навантаження пакета, залишаючи IP-заголовок без змін. Використовується для прямого з'єднання між пристроями (host-to-host).

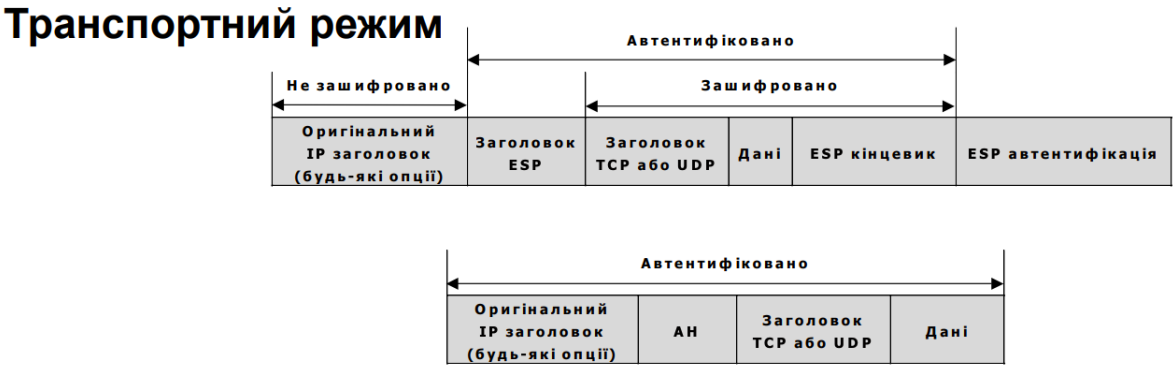


Рисунок 1.2 – Транспортний режим у IPSec.

2) **Тунельний режим**: захищає весь пакет, включаючи заголовок IP.

Використовується для з'єднання між мережевими шлюзами (gateway-to-gateway).

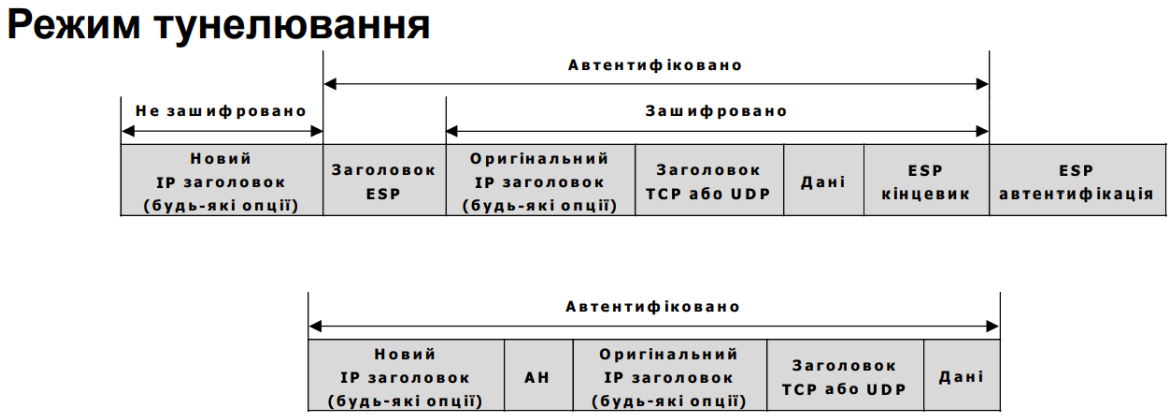


Рисунок 1.3 – Тунельний режим у IPSec.

1.3.2 Основні принципи побудови архітектури

Архітектура IPSec спроєктована таким чином, щоб забезпечити:

– **Гнучкість:** підтримка різних сценаріїв використання (хост-хост, шлюз-шлюз, хост-шлюз).

– **Модульність:** можливість додавання нових криптографічних алгоритмів і протоколів без кардинальних змін у базовій структурі.

– **Інтеграція:** сумісність із стеком TCP/IP, що дозволяє захищати всі рівні транспортного протоколу (TCP, UDP) і додатки, які їх використовують.

1.4 Призначення, особливості та відмінності криптографічних механізмів протоколів AH, ESP, ISAKMP, IKE, IKEv2, KINK та ін.

Протоколи IPSec, такі як AH (Authentication Header), ESP (Encapsulating Security Payload), ISAKMP (Internet Security Association and

Key Management Protocol), IKE (Internet Key Exchange), IKEv2, та KINK (Kerberized Internet Negotiation of Keys), використовуються для забезпечення безпеки, аутентифікації та конфіденційності в IP-мережах. Кожен із цих протоколів має своє особливе призначення та механізми роботи.

1.4.1 AH (Authentication Header)

Основна мета: Забезпечення аутентифікації джерела та цілісності даних IP-пакетів.

Особливості: AH використовує HMAC для автентифікації даних та не забезпечує шифрування (тобто, не гарантує конфіденційності).

Призначення: Відкрито захищає цілісність даних, зокрема, шляхом перевірки на справжність всього пакету, окрім змінних полів (наприклад, IP TTL).

1.4.2 ESP (Encapsulating Security Payload)

Основна мета: Забезпечення конфіденційності, аутентифікації та цілісності.

Особливості: ESP надає шифрування та цілісність даних за допомогою криптографічних методів (AES, 3DES). У деяких реалізаціях також додається підтримка аутентифікації.

Відмінність від AH: ESP захищає тільки корисне навантаження пакету (тобто, він забезпечує конфіденційність), але не аутентифікує IP заголовок.

1.4.3 ISAKMP (Internet Security Association and Key Management Protocol)

Основна мета: Створення, обробка та видалення Security Associations (SA), що відповідають за організацію захищених каналів зв'язку.

Особливості: ISAKMP забезпечує незалежну від протоколів IPsec роботу та може використовуватися для аутентифікації різними методами (наприклад, з використанням сертифікатів).

Переваги: ISAKMP не обмежується жодним конкретним криптоалгоритмом, а отже може бути оновлений для підтримки нових алгоритмів та протоколів (наприклад, IKE та IKEv2).

1.4.4 IKE (Internet Key Exchange)

Основна мета: Автентифікація та управління ключами.

Особливості: IKE об'єднує в собі ISAKMP, OAKLEY та SKEME, що дозволяє автоматизувати створення та захист каналів передачі. IKE працює в двох фазах — для встановлення SAs (Security Associations) та для забезпечення стійкого зв'язку.

1.4.5 IKEv2

Особливості: Відрізняється від IKE більш оптимізованими функціями управління ключами та покращеною стійкістю до збоїв.

Оновлення: IKEv2 використовує надійніші методи шифрування та автентифікації, зокрема алгоритми групового обміну ключами (Diffie-Hellman) та перевірки ідентичностей.

1.4.6 KINK (Kerberized Internet Negotiation of Keys)

Основна мета: Полегшення обміну ключами для IPsec, використовуючи автентифікацію за допомогою протоколу Kerberos.

Особливості: Цей протокол використовує наявну систему Kerberos для генерації ключів без необхідності вручну налаштовувати IPSec. Це полегшує конфігурацію в мережах, де використовується Kerberos для автентифікації користувачів.

1.5 Концепція безпечних асоціацій (SA) та бази даних SPD і SAD

1.5.1 Концепція безпечних асоціацій (SA)

У протоколах IPSec поняття безпечної асоціації (Security Associations, SA) є ключовим, оскільки воно визначає налаштування, за допомогою яких забезпечується безпека обміну даними між двома вузлами. SA встановлює, які методи автентифікації та шифрування застосовувати для певного каналу зв'язку. В IPSec кожна SA є унікальною для напрямку передачі: для кожної з двох сторін зв'язку встановлюється своя SA (тобто одна для передавання та одна для приймання даних). Кожна SA містить такі компоненти:

1) Security Parameters Index (SPI) – унікальний ідентифікатор, який використовується для відстеження окремих SA в IPSec.

2) Тип протоколу – AH (Authentication Header) або ESP (Encapsulating Security Payload).

3) IP-адреса призначення – адреса кінцевої точки SA.

SA зберігаються у базі даних безпечних асоціацій (Security Associations Database, SAD), яка надає контекст для обробки вхідних і вихідних пакетів згідно з параметрами захисту. Наприклад, коли пристрій IPSec отримує пакет, він шукає SPI в SAD, щоб визначити відповідну SA

для автентифікації або шифрування даних пакета.

1.5.2 База даних політик безпеки (SPD)

База даних політик безпеки (Security Policy Database, SPD) містить правила, які визначають, як слід обробляти трафік відповідно до політики безпеки. SPD містить три основних дії для трафіку:

– PROTECT: трафік захищається за допомогою шифрування або автентифікації відповідно до визначених у SA параметрів.

– BYPASS: трафік передається без захисту.

– DISCARD: трафік відхиляється.

SPD, таким чином, є "фільтром"для пакету даних, визначаючи, який трафік підлягає захисту, а який – ні. Якщо правило в SPD визначає, що трафік потребує захисту, він посилається на SAD для визначення конкретної SA, яка буде використана для цього трафіку.

1.5.3 Взаємодія SPD і SAD

1) Коли пакет надходить у систему, IPSec перевіряє його відповідність до правил у SPD.

2) Якщо трафік відповідає правилу "PROTECT IPSec звертається до SAD, щоб знайти відповідну SA на основі SPI.

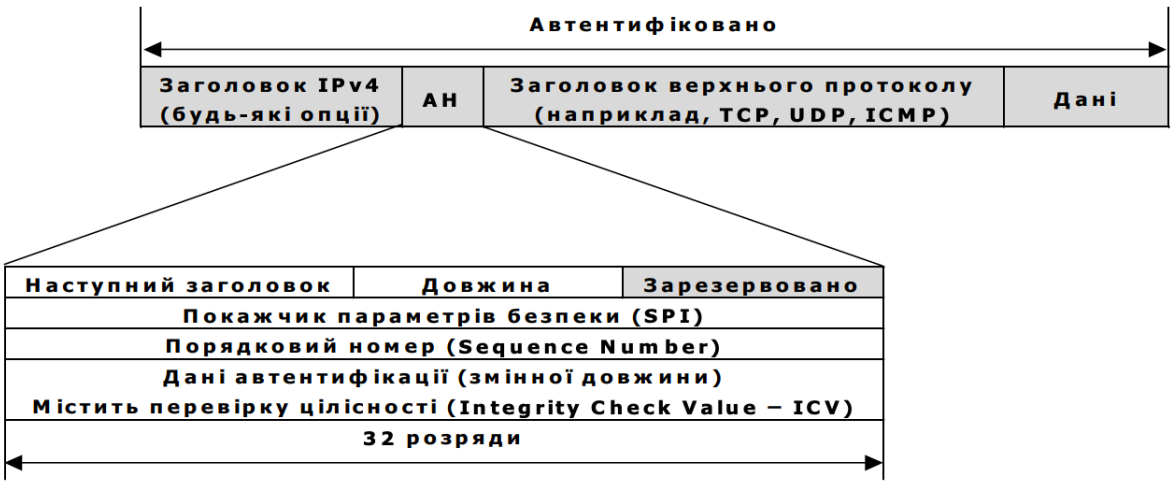
3) Якщо SA у SAD не знайдено, система ініціює новий процес для встановлення безпечної асоціації, як правило, за допомогою протоколу IKE або IKEv2.

Таким чином, SPD визначає, який трафік потребує захисту, а SAD надає параметри для цього захисту.

1.6 Особливості структури заголовків протоколів AH і ESP в тунельному та транспортному режимах з повним описанням їх полів та можливих значень

IPSec використовує два основні протоколи, Authentication Header (AH) та Encapsulating Security Payload (ESP), кожен з яких має специфічну структуру заголовків та режими роботи — тунельний та транспортний.

1.6.1 Заголовок AH



AH забезпечує автентифікацію джерела та цілісність даних IP-пакету без шифрування. Основні поля заголовка AH включають:

– Next Header (8 біт): ідентифікує наступний протокол в пакеті.

– Payload Length (8 біт): вказує довжину заголовка AH.

– Reserved (16 біт): зарезервовано для майбутнього використання.

– Security Parameters Index (SPI) (32 біт): визначає асоціацію безпеки для пакету.

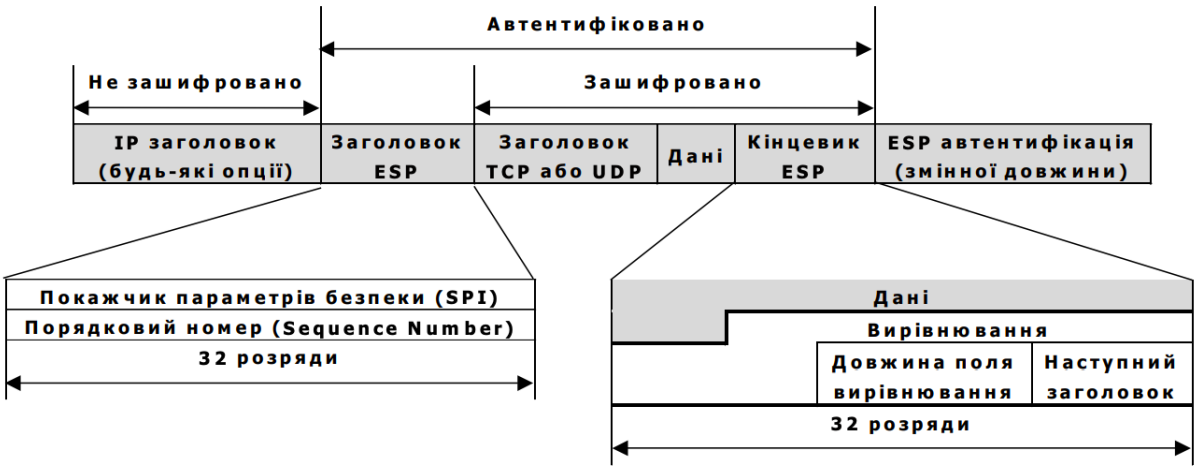
– Sequence Number (32 біт): захист від атак повтору (replay attacks).

– Integrity Check Value (ICV) (перемінна довжина): містить хеш для

перевірки цілісності пакету.

У транспортному режимі AH додає свій заголовок між IP-заголовком та корисним навантаженням, а в тунельному режимі — на початку новоствореного зовнішнього IP-заголовка, забезпечуючи цілісність і автентифікацію всього внутрішнього IP-пакету. Це робить AH більш вразливим до змін у заголовках (наприклад, через NAT), що обмежує його використання в порівнянні з ESP.

1.6.2 Заголовок ESP



ESP надає як автентифікацію, так і шифрування. Його структура складається з:

– SPI (32 біт): визначає асоціацію безпеки для ESP.

– Sequence Number (32 біт): захист від атак повтору.

– Encrypted Payload: зашифрований корисний вантаж.

– ESP Trailer: містить інформацію про кінцевий маркер даних.

– ESP Authentication (опціонально): забезпечує автентифікацію даних.

У транспортному режимі ESP шифрує лише корисне навантаження IP-пакету, залишаючи оригінальний IP-заголовок відкритим. У тунельному режимі, натомість, шифрується весь внутрішній пакет разом із

оригінальним IP-заголовком, а зовні додається новий IP-заголовок, що робить цей режим оптимальним для захищеного з'єднання між мережами через небезпечні середовища, наприклад, Інтернет.

Порівняння AH і ESP

Поле	AH	ESP
Шифрування	Ні	Так
Автентифікація	Так	Опціонально
Захист від повторів	Так	Так
Режими	Транспортний і тунельний	Транспортний і тунельний
Сумісність з NAT	Погано сумісний	Краще сумісний

Таблиця 1.1 – Порівняння AH і ESP

Таким чином, ESP є більш універсальним через підтримку шифрування, тоді як AH обмежений забезпеченням тільки цілісності та автентифікації без шифрування, що робить його менш захищеним у відкритих мережах.

1.7 Особливості обробки вхідних та вихідних IPSec-пакетів для кожного з протоколів та режимів

Процес обробки вхідних і вихідних пакетів у протоколах IPSec, таких як AH і ESP, залежить від режиму використання (транспортного чи тунельного) і типу пакета (вхідний або вихідний).

Обробка вхідних пакетів:

1) AH у транспортному режимі: AH використовується для автентифікації даних. Після отримання пакета пристрій перевіряє автентичність заголовка та його цілісність, використовуючи алгоритми, визначені в заголовку AH. Поле заголовка AH включає значення хеш-функції (наприклад, HMAC), яке приймаюча сторона повинна перевірити, щоб переконатися, що дані не були змінені під час передачі.

2) AH у тунельному режимі: Весь оригінальний IP-пакет вкладається у

новий IP-заголовок і захищається AH. Усі внутрішні IP-дані перевіряються, що забезпечує цілісність і автентичність не тільки верхніх рівнів даних, але й оригінального IP-заголовка.

3) ESP у транспортному режимі: У транспортному режимі ESP захищає лише дані транспортного рівня, залишаючи оригінальний IP-заголовок незахищеним. Після отримання пакета пристрій декриптує і перевіряє цілісність корисного навантаження. Поля для автентифікації можуть бути відсутні, якщо ESP використовується лише для шифрування.

4) ESP у тунельному режимі: Усі дані оригінального пакета, включно з IP-заголовком, шифруються й автентифікуються. Після отримання пристрій видаляє зовнішній IP-заголовок, розшифровує та перевіряє дані, включаючи внутрішній заголовок.

Обробка вихідних пакетів:

1) AH у транспортному режимі: Після формування вихідного IP-пакета пристрій додає заголовок AH між IP-заголовком і корисним навантаженням. Виконується обчислення автентифікаційного значення, яке додається в заголовок AH для подальшої перевірки отримувачем.

2) AH у тунельному режимі: Пристрій створює новий IP-заголовок, що інкапсулює весь оригінальний пакет, і додає AH між новим і оригінальним заголовками. Далі обчислюється значення автентифікації, яке підтверджує цілісність усього пакета.

3) ESP у транспортному режимі: Перед відправкою дані пакетів шифруються, після чого додаються заголовок ESP і значення автентифікації (якщо застосовується). Таким чином, захищаються тільки дані транспортного рівня, а IP-заголовок залишається без змін.

4) ESP у тунельному режимі: Весь оригінальний IP-пакет шифрується, включно з заголовком, і інкапсулюється у новий IP-заголовок. Цей режим забезпечує повний захист внутрішнього пакета і часто використовується для VPN-з'єднань.

Такий підхід до обробки пакетів дозволяє адаптувати IPSec до різних сценаріїв захисту мережевого трафіку, від забезпечення цілісності даних до

їхнього повного шифрування і захисту IP-інформації.

1.8 Нижній рівень архітектури стеку протоколів IPSec – домен інтерпретації DOI

Домен інтерпретації (Domain of Interpretation, DOI) є ключовим компонентом архітектури IPSec, який визначає параметри та політики, необхідні для встановлення та управління безпечними з'єднаннями. DOI забезпечує узгодженість між різними реалізаціями протоколів, встановлюючи стандарти для обміну інформацією та управління безпекою.

1.8.1 Роль DOI в архітектурі IPSec

DOI визначає набір параметрів, політик та процедур, які використовуються під час встановлення та управління безпечними з'єднаннями в IPSec. Він забезпечує узгодженість між різними реалізаціями протоколів, встановлюючи стандарти для обміну інформацією та управління безпекою.

Основні функції DOI:

1) Визначення параметрів безпеки: DOI встановлює, які алгоритми шифрування та хешування можуть використовуватися, а також їхні параметри.

2) Узгодження політик: DOI забезпечує, щоб обидві сторони з'єднання мали спільне розуміння політик безпеки, що застосовуються.

3) Ідентифікація протоколів: DOI визначає, які протоколи та механізми використовуються для встановлення та управління безпечними з'єднаннями.

Структура DOI:

– Ідентифікатор DOI: унікальний номер, який визначає конкретний домен інтерпретації.

– Атрибути безпеки: набір параметрів, що визначають політики та

алгоритми безпеки.

– Протоколи управління: механізми, що використовуються для обміну інформацією та управління безпекою.

1.8.2 Взаємодія DOI з іншими компонентами IPSec

DOI тісно інтегрований з іншими компонентами IPSec, такими як ISAKMP (Internet Security Association and Key Management Protocol). ISAKMP забезпечує загальну структуру для встановлення та управління асоціаціями безпеки, тоді як DOI визначає специфічні параметри та політики для цих асоціацій.

Домен інтерпретації (DOI) є невід'ємною частиною архітектури IPSec, яка забезпечує узгодженість та стандартизацію параметрів безпеки між різними реалізаціями протоколів. Він визначає, які алгоритми та політики можуть використовуватися, забезпечуючи надійне та безпечне з'єднання між сторонами.

1.9 Зареєстровані алгоритми автентифікації, шифрування, геш-функцій та ін. для IPSec

IPSec (Internet Protocol Security) використовує різноманітні криптографічні алгоритми для забезпечення конфіденційності, цілісності та автентифікації даних під час їх передачі через мережу.

1.9.1 Алгоритми шифрування

– Алгоритми шифрування забезпечують конфіденційність даних, перетворюючи їх у форму, недоступну для несанкціонованого доступу.

– DES (Data Encryption Standard): Симетричний блоковий шифр з довжиною ключа 56 біт. Через низьку стійкість до сучасних атак

вважається застарілим.

– 3DES (Triple DES): Розширена версія DES, яка застосовує алгоритм тричі з різними ключами, забезпечуючи підвищену безпеку.

– AES (Advanced Encryption Standard): Симетричний блоковий шифр з довжиною ключа 128, 192 або 256 біт. Є стандартом для сучасних систем шифрування завдяки високій безпеці та ефективності.

– Blowfish: Симетричний блоковий шифр з довжиною ключа від 32 до 448 біт. Відомий своєю швидкістю та гнучкістю.

1.9.2 Алгоритми автентифікації

Алгоритми автентифікації гарантують, що дані надходять від достовірного джерела та не були змінені під час передачі.

– HMAC-MD5 (Hashed Message Authentication Code with MD5): Використовує хеш-функцію MD5 для створення коду автентифікації повідомлення. Через виявлені вразливості MD5 рекомендується використовувати більш надійні альтернативи.

– HMAC-SHA-1: Застосовує хеш-функцію SHA-1 для генерації коду автентифікації. Хоча SHA-1 вважається більш безпечним, ніж MD5, існують рекомендації переходити на більш стійкі алгоритми.

– HMAC-SHA-256/384/512: Використовують хеш-функції сімейства SHA-2 з різною довжиною вихідного хешу, забезпечуючи вищий рівень безпеки.

1.9.3 Хеш-функції

Хеш-функції перетворюють вхідні дані довільної довжини у фіксований розмір, що використовується для перевірки цілісності даних.

– MD5 (Message Digest Algorithm 5): Генерує 128-бітний хеш. Через виявлені криптографічні вразливості не рекомендується для використання в

сучасних системах безпеки.

– SHA-1 (Secure Hash Algorithm 1): Генерує 160-бітний хеш. Хоча більш безпечний, ніж MD5, також має відомі вразливості.

– SHA-2 (SHA-256, SHA-384, SHA-512): Сімейство хеш-функцій, що генерують хеші довжиною 256, 384 та 512 біт відповідно. Рекомендуються для використання завдяки високій стійкості до атак.

1.9.4 Алгоритми обміну ключами

Для безпечного обміну ключами в IPSec використовуються наступні алгоритми:

DH (Diffie-Hellman): Протокол, що дозволяє двом сторонам безпечно обмінюватися криптографічними ключами через незахищений канал. Існують різні групи DH з різним рівнем безпеки (групи 1, 2, 5 тощо).

1.9.5 Протоколи управління ключами

IPSec використовує протоколи для узгодження параметрів безпеки та управління ключами:

IKE (Internet Key Exchange): Протокол для встановлення асоціацій безпеки та обміну ключами між двома сторонами. Існують версії IKEv1 та IKEv2, де IKEv2 пропонує покращену безпеку та ефективність.

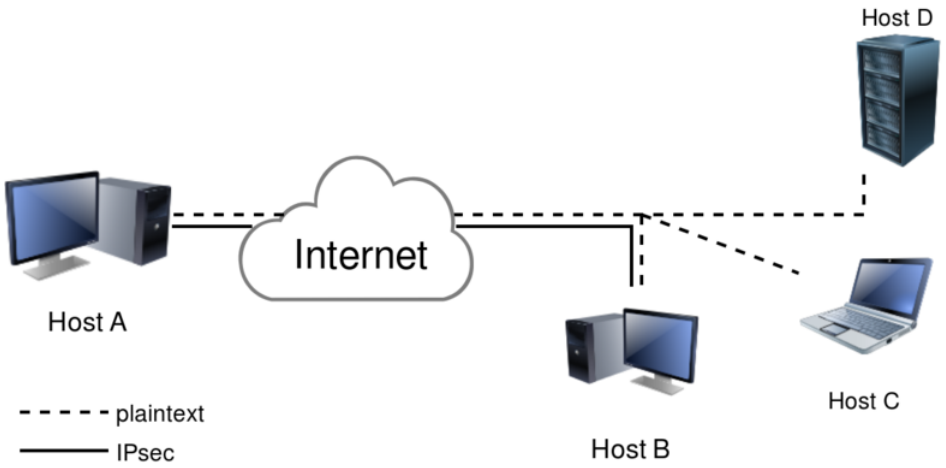
Вибір конкретних алгоритмів залежить від вимог до безпеки та сумісності між сторонами з'єднання. Рекомендується використовувати сучасні та стійкі до відомих атак алгоритми, такі як AES для шифрування та HMAC-SHA-256 для автентифікації.

1.10 Особливості основних схем застосування протоколів IPSec: хост-хост, шлюз-шлюз та хост-шлюз. А також використання протоколів IPSec для побудови VPN-тунелів

IPSec (Internet Protocol Security) — це набір протоколів, що забезпечують захист даних на мережевому рівні шляхом шифрування та автентифікації IP-пакетів. Існують три основні схеми застосування IPSec: «хост-хост», «шлюз-шлюз» та «хост-шлюз». Крім того, IPSec широко використовується для побудови VPN-тунелів.

1.10.1 Особливості основних схем застосування протоколів IPSec

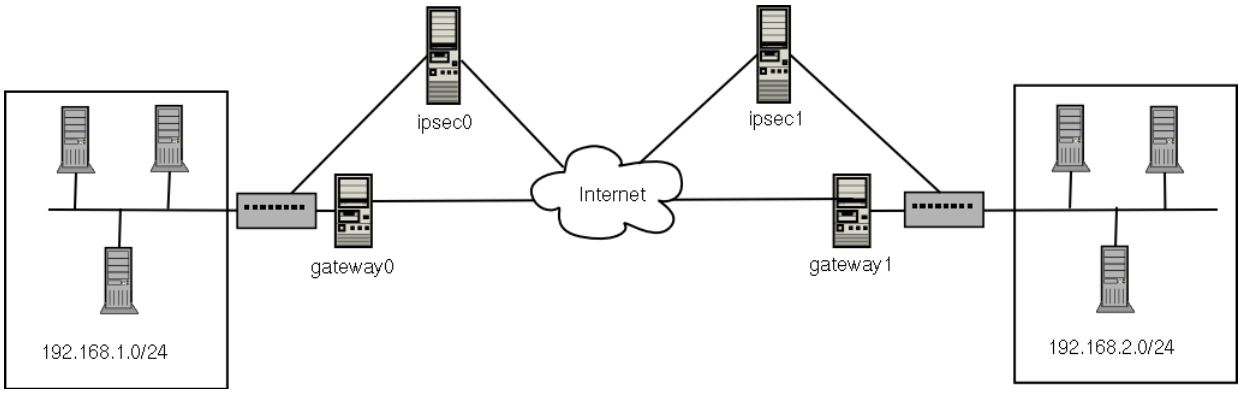
1) Схема «хост-хост»



У цій схемі захищене з'єднання встановлюється безпосередньо між двома кінцевими пристроями (хостами). Зазвичай використовується транспортний режим IPSec, який забезпечує шифрування та автентифікацію лише корисного навантаження IP-пакета, залишаючи заголовок без змін. Це підходить для захисту трафіку між двома конкретними пристроями в

мережі.

2) Схема «шлюз-шлюз»



У цій конфігурації захищене з'єднання встановлюється між двома мережевими шлюзами (наприклад, маршрутизаторами або брандмауерами), які з'єднують різні локальні мережі. Використовується тунельний режим IPSec, при якому весь IP-пакет (включаючи заголовок) інкапсулюється в новий IP-пакет з новим заголовком. Це дозволяє забезпечити захист даних між двома мережами через незахищене середовище, наприклад, Інтернет.

3) Схема «хост-шлюз»

У цій схемі один кінець з'єднання є кінцевим пристроєм (хостом), а інший — мережевим шлюзом. Це корисно для віддалених користувачів, які підключаються до корпоративної мережі через захищене з'єднання. Зазвичай використовується тунельний режим IPSec, що забезпечує безпечний доступ віддаленого хоста до ресурсів мережі через шлюз.

1.10.2 Використання IPSec для побудови VPN-тунелів

IPSec широко застосовується для створення віртуальних приватних мереж (VPN), забезпечуючи захищений канал зв'язку через незахищені мережі, такі як Інтернет. VPN-тунелі на базі IPSec використовують тунельний режим для інкапсуляції та шифрування всього IP-пакета, що гарантує конфіденційність, цілісність та автентифікацію переданих даних.

ВИСНОВКИ

У ході виконання дослідницької роботи було проведено аналіз реалізації протоколів IPSec, їх архітектури, функціональних можливостей та взаємодії з мережею. IPSec зарекомендував себе як надійний механізм захисту даних на мережевому рівні моделі OSI, забезпечуючи автентифікацію, цілісність і конфіденційність. Основною перевагою є його незалежність від протоколів вищих рівнів, що дозволяє захищати будь-який IP-трафік.

Архітектура IPSec представлена багаторівневою структурою, яка включає протоколи AH, ESP та ISAKMP. AH забезпечує автентифікацію і цілісність, ESP додає конфіденційність через шифрування, а ISAKMP керує параметрами безпеки. Домен інтерпретації (DOI) забезпечує стандартизацію і сумісність між різними реалізаціями.

Особливу увагу приділено концепції безпечних асоціацій (SA), які визначають параметри безпеки та управляються через бази SPD і SAD. Протоколи AH і ESP підтримують транспортний і тунельний режими, що дозволяє адаптувати їх до різних мережевих сценаріїв.

Було досліджено структуру заголовків протоколів AH і ESP, процес обробки пакетів, а також підтримувані криптографічні алгоритми. Завдяки модульності архітектури IPSec забезпечує гнучкість і високий рівень захисту IP-трафіку.

IPSec ефективно використовується у схемах хост-хост, шлюз-шлюз, хост-шлюз та для побудови VPN-тунелів, що гарантують безпечну передачу даних між віддаленими мережами або пристроями.

Таким чином, IPSec залишається одним із ключових рішень для захисту даних у сучасних мережах завдяки своїй універсальності, модульності та підтримці сучасних криптографічних механізмів.