МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО”

Фізико-технічний інститут

«Проектування, розробка і реалізація криптографічних систем»

Лабораторна робота №2

Тема: «Дослідження реалізацій протоколів IPSec».

Мета роботи: «Дослідження особливостей реалізації криптографічних механізмів протоколів IPSec».

Виконав: студент групи ФІ-42мн

Сергеєв Станіслав

Хід роботи:

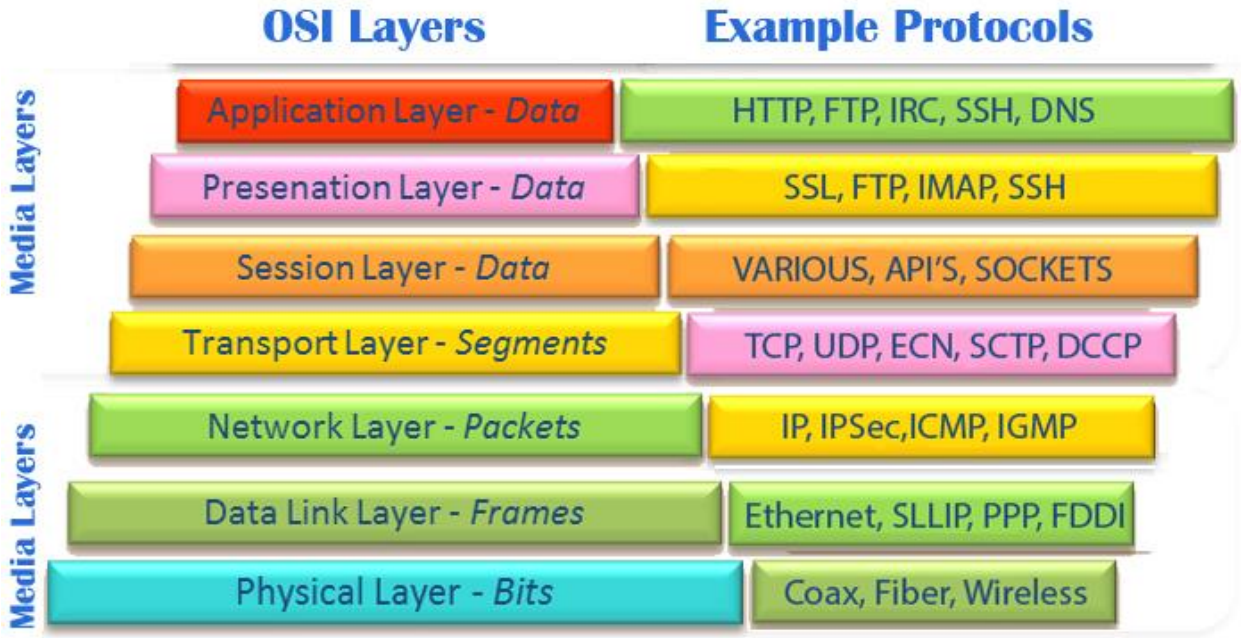
Провести дослідницьку роботу з метою аналізу особливостей реалізації криптографічних механізмів протоколів IPSec. Описати основне призначення протоколів IPSec, їх місце в мережевій моделі OSI та взаємодію зі стеком протоколів TCP/IP та ін. Дослідити архітектуру стеку протоколів IPSec. Описати призначення, 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.

Аналіз:

Протоколи IPSec (Internet Protocol Security) розроблено для забезпечення сумісної високоякісної криптографічної безпеки зв'язку через IP-мережі, гарантуючи конфіденційність, цілісність та автентичність даних. IPSec часто використовується для створення віртуальних приватних мереж (VPN) та захисту зв'язку між мережевими пристроями. IPsec шифрує й автентифікує IP-пакети, що передаються між двома вузлами (наприклад, між двома комп'ютерами або між комп'ютером і маршрутизатором).

IPSec працює на мережевому рівні (Layer 3) моделі OSI, він є прозорим для протоколів та програм вищого рівня. Візуально діаграма з прикладами протоколів, місцезнаходження IPSec в моделі OSI виглядає так, де видно, що IPSec займає 3 рівень (мережевий):

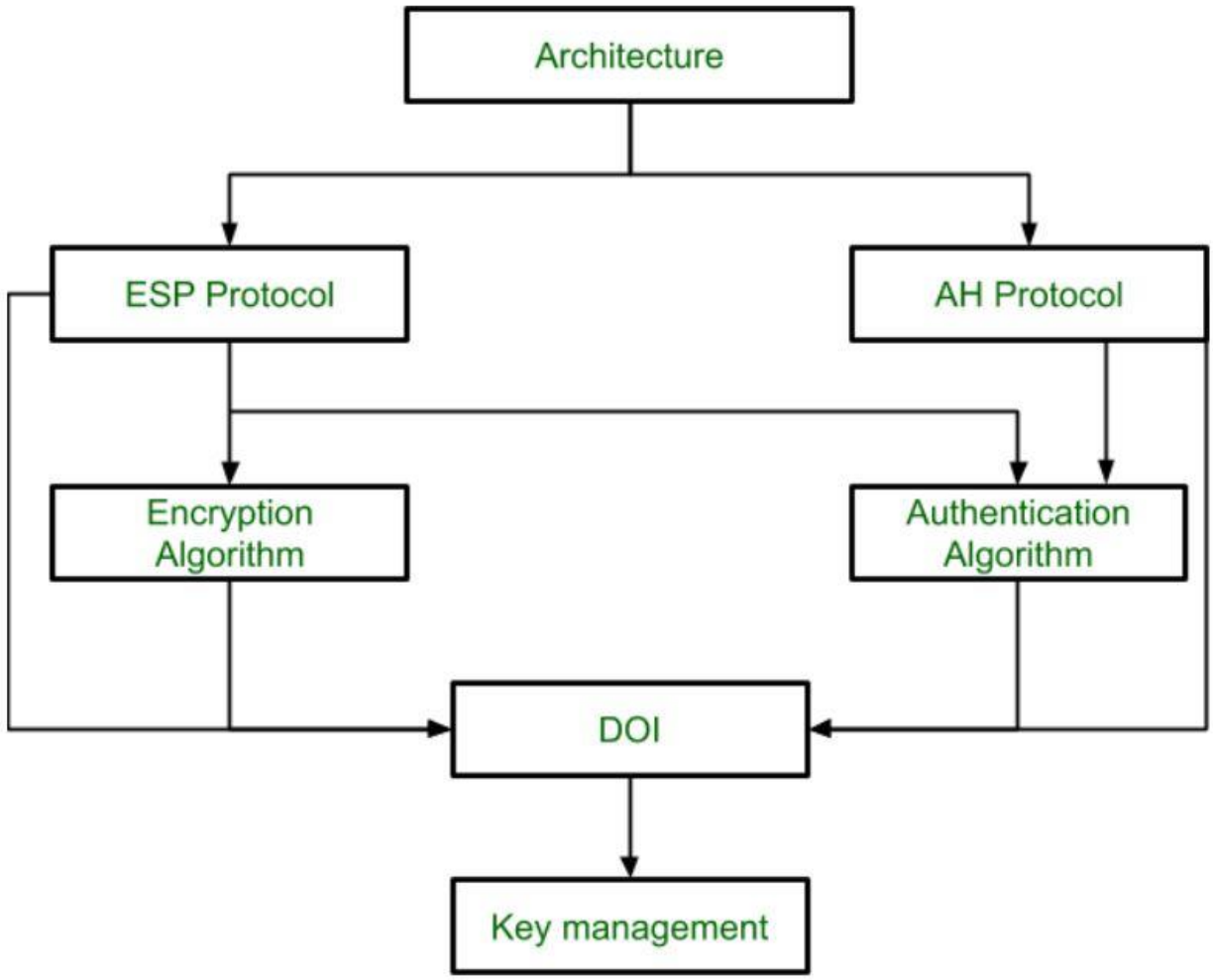


IPSec являє собою розширення протоколів TCP/IP, IPsec пакети виглядають як звичайні IP-пакети, тільки поле "Protocol" у заголовку IP вказує, що це ESP (Encapsulating Security Payload)

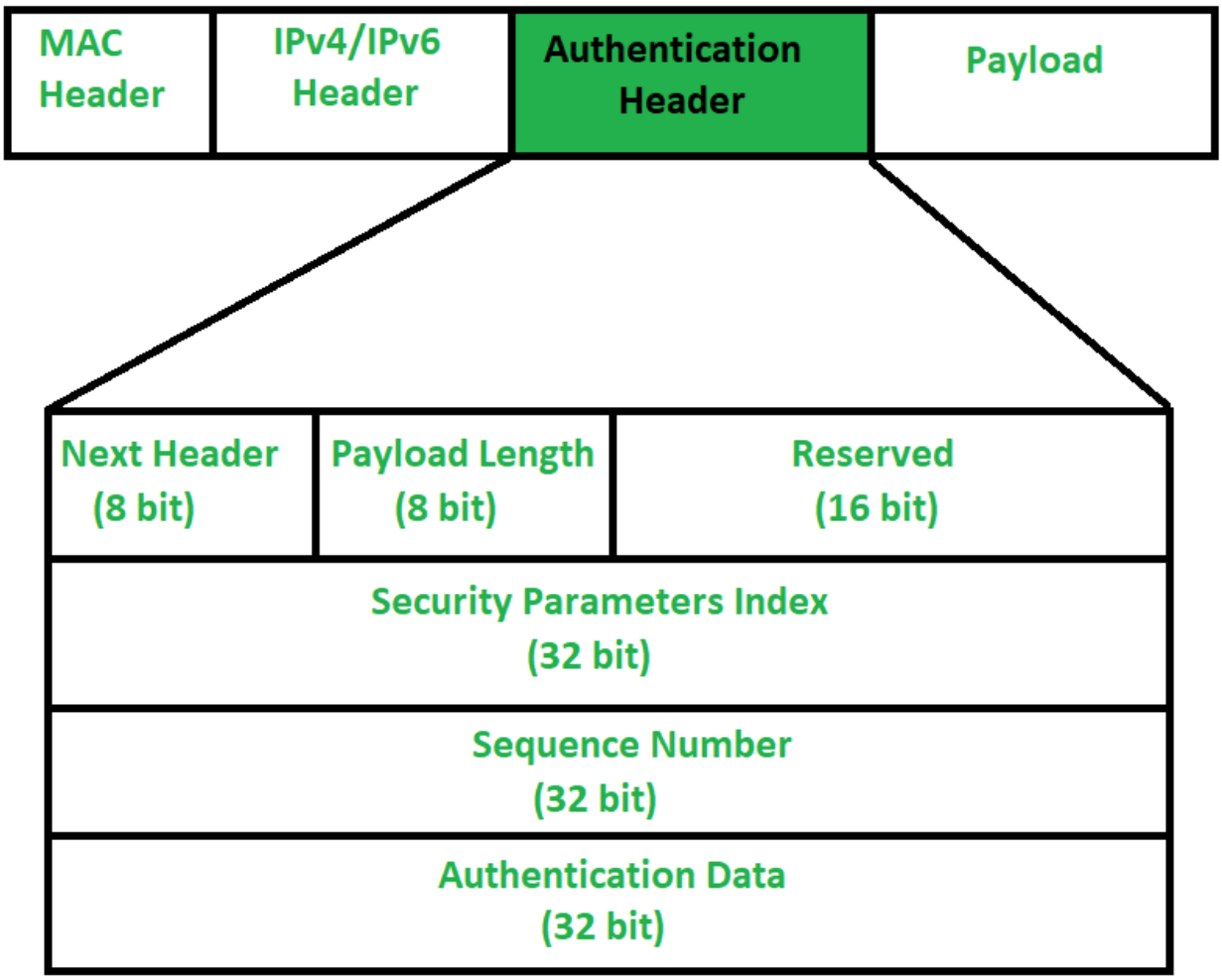
або AH (Authentication Header). Говорячи про інші стеки протоколів, варто зазначити, що IPSec захищає пакети будь-яких транспортних протоколів (TCP, UDP, ICMP).

Архітектура IPSec використовує два основні протоколи для захисту трафіку або потоку даних, які вже згадувались вище. Це ESP (Encapsulating Security Payload) та AH (Authentication Header). Архітектура IPSec включає протоколи, алгоритми, DOI (Domain of Interpretation) та менеджмент ключів. Ці компоненти дуже важливі для забезпечення трьох основних цілей: конфіденційність, аветонтифікація та цілісність.

Схематично архітектура виглядає так:



Структура заголовку AH виглядає наступним чином:

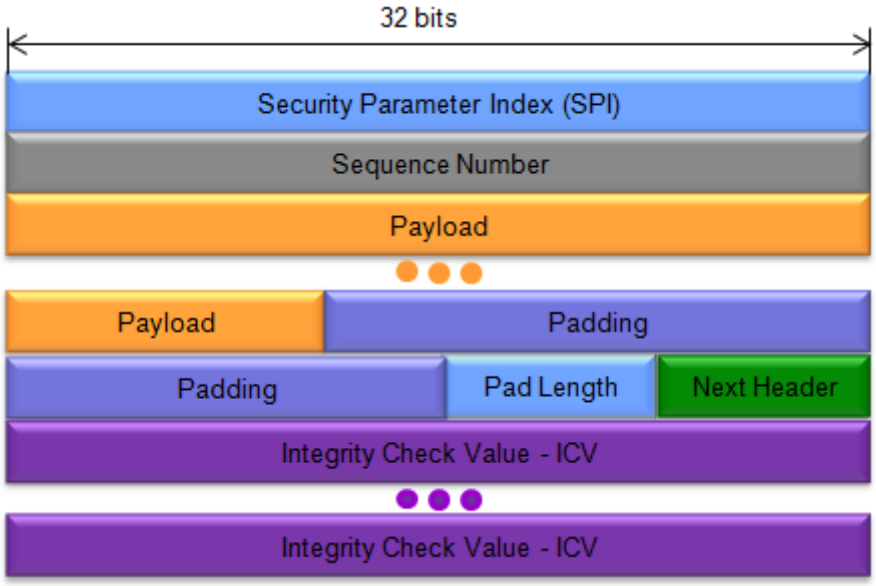


У транспортному режимі AH вставляється після IP-заголовка й перед транспортним протоколом (TCP/UDP/ICMP). У тунельному режимі створюється новий “зовнішній” IP-заголовок. AH вставляється після зовнішнього IP-заголовка. Захищено весь “внутрішній” IP-пакет (заголовок + дані).

Поля AH заголовка:

- Next Header (розміром 8 біт) – ідентифікатор протоколу, що йде після AH (значення з веб-сайту IANA (Internet Assigned Numbers Authority), наприклад, TCP=6, IPv4=4, IPv6=41).
- Payload Len (розміром 8 біт) – довжина AH-заголовка в 32-бітних словах, мінус 2.
- Reserved (розміром 16 біт) – зарезервоване поле, має бути 0 при відправленні, але отримувач ігнорує це поле.
- SPI (Security Parameters Index) розміром 32 біти – ідентифікатор SA, призначений отримувачем.
- Sequence Number (розміром 32 біти) – значення збільшується на 1 для кожного відправленого пакету.
- Integrity Check Value (ICV) зі змінною довжиною, кратною 32 бітам – MAC або інша аутентифікаційна перевірка над пакетом залежно від алгоритму.

А структура ESP виглядає таким чином:



У транспортному режимі заголовок ESP вставляється після IP-заголовка (і опцій) і перед транспортним протоколом або іншими IPsec-заголовками. У тунельному режимі створюється новий "зовнішній" IP-заголовок. ESP вставляється після цього зовнішнього IP-заголовка і перед зашифрованим "внутрішнім" IP-пакетом.

Поля заголовка ESP:

- SPI (Security Parameters Index) розміром 32 біти – використовується отримувачем для ідентифікації SA, до якої прив'язаний вхідний пакет.
- Sequence Number – аналогічно до AH, значення збільшується на 1 для кожного відправленого пакету.
- Payload Data – зашифровані (або незашифровані, залежно від налаштування) дані від оригінального IP пакету, описаного полем Next Header.
- Padding – додаткові байти, щоб забезпечити вирівнювання блоків шифрування (або TFC – Traffic Flow Confidentiality padding)
- Pad Length: 8 біти – довжина padding.
- Next Header розміром 8 бітів – тип протоколу, що йде після Payload Data (наприклад TCP/UDP/ICMP або "no next header").
- Integrity Check Value (ICV) (опціонально) – MAC або тег автентифікації/цілісності, якщо SA налаштоване з аутентифікацією.

Криптографічні механізми в IPSec

В AH та ESP криптографічні механізми використовуються для перевірки цілісності пакетів, щоб переконатись, що дані не були змінені і що вони походять від автентичного джерела. Сучасні алгоритми, які використовуються для цього: HMAC-SHA-2 (SHA-256, SHA-384, SHA-512), MD5 та HMAC-SHA1. Вважається, що MD5 та HMAC-SHA1 це найбільш застарілі механізми та найменш захищені. Рекомендується використовувати алгоритми HMAC-SHA-2.

ESP також може забезпечувати конфіденційність даних з допомогою алгоритмів шифрування, наприклад, AES, DES, 3DES.

У протоколі IKE (Internet Key Exchange) використовуються відповідно алгоритми обміну ключами. Ці протоколи існують у версіях IKEv1 та IKEv2. IKE використовується для встановлення безпечного каналу обміну ключами, автентифікації сторін, узгодження алгоритмів шифрування, хешування, автентифікації, створення SA (Security Association). IKE використовує

ISAKMP Internet Security Association and Key Management Protocol). IKEv2 є сучасною версією, яка підтримує сучасні криптографічні алгоритми (AES-GCM, ECDH, SHA-2, EdDSA), на відміну від IKEv1, який вважається застарілим. Протокол KINK (Kerberized Internet Negotiation of Keys) використовується для цих самих цілей, як альтернативний протокол для обміну ключами в IPSec, але набагато рідше.

SA (Security Association), про що згадувалось вище, - це визначення набору параметрів для інкапсуляції IP протоколу, зазвичай ESP, та надсилання пакетів між двома сторонами. SA також описує автентифікацію та шифрування. SA створюється в результаті узгодження, наприклад, з допомогою IKE протоколу чи задається вручну.

Нижче наведено приклад, як виглядає SA разом зі значеннями полів:

```
IPsec::SecurityAssociations
172.16.1.1 -> 172.16.2.1
------------------------------------------------------------------------------------------------------
  tmm: 6
  Direction: out;  SPI: 0xbec2922(200026402);  Policy ID: 0xe991(59793)
  Protocol: esp;  Mode: tunnel;  State: mature
  Authenticated Encryption : aes-gcm128
  Current Usage: 3634816 bytes
  Hard lifetime: 24158 seconds; unlimited bytes
  Soft lifetime: 7646 seconds; unlimited bytes
  Replay window size: 32
  Last use: 06/13/2024:04:40                                          Create:  06/12/2024:11:23
```

SDP (Security Policy Database) та SAD (Security Association Database)

SDP – це база даних, яка описує політики, що визначають проходження всього IP трафіку. Є три операції, які, згідно SPD, можуть бути застосовані до IP пакету: DISCARD, BYPASS, PROTECT.

Перший варіант стосується трафіку, якому не дозволено перетинати межу IPsec (у вказаному напрямку). Другий варіант стосується трафіку, якому дозволено перетинати межу IPsec без захисту IPsec. Третій варіант стосується трафіку, якому надається захист IPsec, і для такого трафіку SPD повинен вказати протоколи безпеки, що будуть використовуватися, їх режим, параметри служби безпеки та криптографічні алгоритми, що будуть використовуватися.

Адміністратор або система керування задає правила у SPD: селектори (джерело IP, призначення IP, протокол, порти, тощо) та дію (BYPASS, DISCARD, PROTECT).

SAD – це база даних, в якії кожен запис визначає параметри, пов'язані з одним SA. Кожна SA має запис у SAD. Для пакета, який захищений IPsec, пристрій звертається до SAD, щоб знайти, яку саме SA потрібно застосувати. SAD містить також динамічні параметри: лічильники пакетів (Sequence Number Counters), anti-replay window, життєві обмеження та інші.

Розглянемо нижній рівень архітектури стеку протоколів IPSec

Нижній рівень – це домен інтерпретації DOI. Це база даних, яка містить інформацію про усі протоколи і алгоритми, що застосовуються в IPSec, а також про їхні параметри, ідентифікатори тощо. Усім цим користуються механізми такі як IKEv2 (або IKEv1) щоб узгодити SA.

Нижче наведено зареєстровані алгоритми в DOI.

1) *Алгоритми автентифікації / цілісності для AH*

У DOI-таблиці для AH присутні такі трансформи:

- Transform ID 2 = AH_MD5 – означає використання MD5 (зазвичай HMAC-MD5-96) як алгоритму автентифікації.
- Transform ID 3 = AH_SHA – означає використання SHA-1.
- Transform ID 4 = AH_DES → (DES-MAC) – опціонально.

В IANA “IPSEC AH Transform Identifiers” наведені більш сучасні значення (наприклад AH_SHA2-256, AH_AES-GMAC) в реєстрі.

2) *Алгоритми шифрування / конфіденційності для ESP*

У DOI-таблиці для ESP:

- Encryption Algorithm class (value 1) – значення: 1 = DES-CBC; 2 = IDEA-CBC; 3 = Blowfish-CBC; 4 = RC5-R16-B64-CBC; 5 = 3DES-CBC; 6 = CAST-CBC; 7 = AES-CBC; 8 = CAMELLIA-CBC.
- Для ESP Transform Identifiers: transform ID = ESP_3DES, ESP_IDEA, ESP_CAST, ESP_BLOWFISH тощо.

3) Інші класи атрибутів обміну ключами

У IANA “Internet Key Exchange (IKE) Attributes” містяться значення класів атрибутів:

- Class 1 = Encryption Algorithm
- Class 2 = Hash Algorithm
- Class 3 = Authentication Method
- Class 4 = Group Description
- Class 11 = Life Type

Наприклад:

Hash Algorithm class: 1 = MD5; 2 = SHA; 3 = Tiger.

Authentication Method class: 1 = pre-shared key; 2 = DSS signatures; 3 = RSA signatures; 4 = Encryption with RSA; 5 = Revised encryption with RSA.

Схема застосування протоколів IPSec: хост-хост

IPsec можна налаштувати для підключення одного настільного комп'ютера або робочої станції до іншого за допомогою з'єднання "хост-хост". Цей тип з'єднання використовує мережу, до якої підключений кожен хост, для створення безпечного тунелю один до одного. Вимоги до з'єднання "хост-хост" мінімальні, як і налаштування IPsec на кожному хості. Хостам потрібне лише виділене з'єднання з мережею оператора (наприклад, Інтернетом) та Red Hat Enterprise Linux для створення з'єднання IPsec.

У цій схемі два хости встановлюють SA між собою. Захищено всі IP-пакети між цими хостами та використовується транспортний режим (transport mode) IPsec.

Схема застосування протоколів IPSec: шлюз-шлюз

У конфігурації «шлюз-шлюз» два пристрої створюють VPN-тунель між двома окремими приватними мережами. Шлюзи встановлюють SA між собою, щоб захистити трафік між двома мережами.

Схема застосування протоколів IPSec: хост-шлюз

Один хост (часто мобільний або віддалений) встановлює SA з VPN-шлюзом. Зазвичай використовується тунельний режим, щоб захистити трафік до шлюза. PSK використовується для автентифікації між локальним та віддаленим шлюзами. Тунель IPsec шифрує трафік, захищаючи всі дані, що проходять через тунель. Трафік між хостом і локальним шлюзом шифрується не самим IPsec, а політиками безпеки локального шлюзу.

Використання протоколів IPSec для побудови VPN-тунелів

Найчастіше IPsec використовується для створення site-to-site VPN-тунелів – це приклад “шлюз-шлюз” схеми, де мережі на відстані з’єднуються через зашифрований тунель. Також використовується для віддаленого доступу (remote access VPN) – приклад схеми «хост-шлюз».

В тунельному режимі весь внутрішній IP-пакет інкапсулюється й захищається — це приховує мережеву топологію, підвищує безпеку.

При налаштуванні тунелю важливо узгоджувати IKE SA та IPsec SA параметри: алгоритми шифрування, автентифікації, час життя SA, група Diffie–Hellman, PFS (perfect forward secrecy) тощо.

Висновки.

В ході виконання роботи було досліджено особливості реалізації криптографічних механізмів IPSec, їх призначення, місце в моделі OSI та архітектуру стеку протоколів, а також компоненти цієї архітектури.