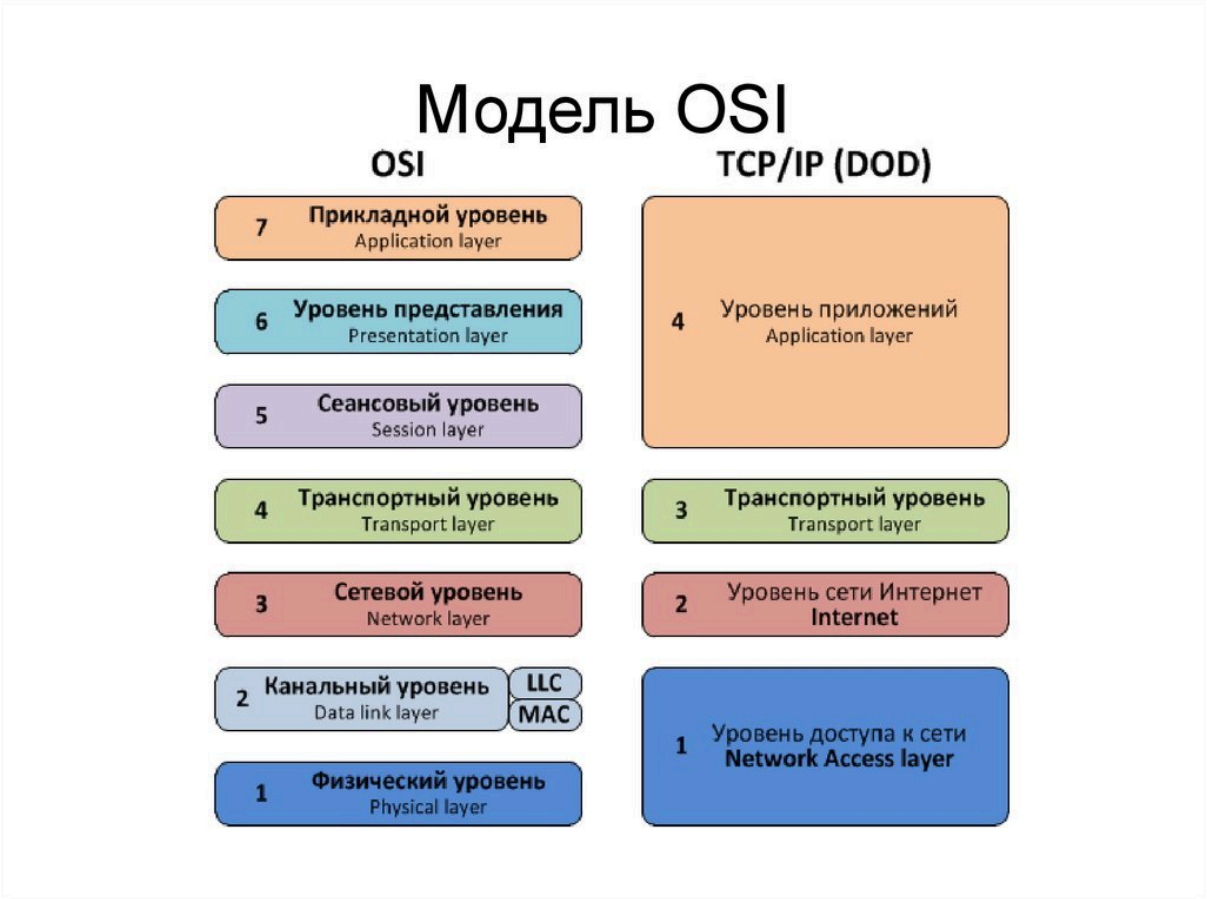
Лабораторна робота № 2

Виконали студенти групи ФІ-32мн: **Ємець Єлизавета**
Карловський Володимир
Коваленко Дар'я

1) На якому рівні проходить функціонування протоколів IPSec згідно з мережевою моделлю OSI?



Функціонування протоколів IPSec відбувається на мережевому рівні (3-й рівень) згідно з моделлю OSI. IPSec призначений для забезпечення безпеки IP-пакетів, які передаються по мережі, і він функціонує безпосередньо на рівні IP, забезпечуючи шифрування, автентифікацію, цілісність і захист від повторних атак.

На мережевому рівні IPSec забезпечує два основних режими:

1. Транспортний режим: захищає тільки корисне навантаження пакета, залишаючи заголовок IP відкритим. Це зазвичай використовується для з'єднань кінцевих точок (наприклад, між двома пристроями).

2. Тунельний режим: захищає як заголовок IP, так і корисне навантаження, що дозволяє створювати захищені тунелі (наприклад, між двома мережами через інтернет).

Таким чином, IPSec працює на мережевому рівні, надаючи додатковий рівень захисту для пакетів, що передаються через IP, і часто використовується в VPN-з'єднаннях для створення безпечного тунелю між мережами або пристроями.

2) Чи можуть протоколи IPSec використовуватися не в IP-мережах?

Протоколи IPSec створені виключно для роботи в IP-мережах, оскільки вони розроблені для захисту саме IP-пакетів і функціонують на мережевому рівні, працюючи безпосередньо з протоколом IP. IPSec забезпечує шифрування, автентифікацію та контроль цілісності для IP-пакетів, і всі механізми IPSec орієнтовані на обробку IP-адрес і структури IP-заголовків.

Через цю орієнтованість на IP, IPSec не може бути використаний у мережах, що використовують інші протоколи (наприклад, Ethernet, Frame Relay або ATM) на рівні мережевих адрес. Для захисту даних у таких мережах застосовують інші протоколи, такі як MACsec для Ethernet або специфічні рішення, розроблені для конкретних типів мереж.

3) Чи сумісні протоколи IPSec з протоколами IPv4 та пртоколами IPv6?

IPv4 та IPv6 – це дві версії системи адресації за протоколом IP. Протокол IP визначає набір правил зв'язку обміну даними через Інтернет. По суті Інтернет є сукупністю мільярдів пристроїв, які використовують мережеві технології для обміну даними один з одним. IP використовує систему нумерації, в якій кожному підключеному пристрою надається унікальний ідентифікаційний номер (адреса).

Протоколи IPSec сумісні як з протоколом IPv4, так і з IPv6, хоча їх реалізація та інтеграція в цих протоколах мають деякі відмінності:

1. IPv4:
   - IPSec для IPv4 є опціональним, і не всі мережі та пристрої підтримують його за замовчуванням.
   - У мережах IPv4 IPSec часто використовується як додатковий протокол для створення VPN-з'єднань, оскільки він не був частиною початкового стандарту IPv4.
   - Підтримує тунельний і транспортний режими для шифрування та захисту IP-пакетів.

2. IPv6:
   - IPSec вбудований у специфікацію IPv6, де він є обов'язковою частиною протоколу. Хоча фактично він теж може бути опціонально реалізований у деяких випадках, IPv6 розроблений з урахуванням можливостей IPSec.
   - У специфікації IPv6 IPSec забезпечує нативну підтримку автентифікації, цілісності та шифрування на мережевому рівні.
   - Це дозволяє підвищити безпеку комунікацій в мережах, які використовують IPv6, з меншою потребою в сторонніх засобах захисту.

4) Яке призначення стеку протоколів IPSec з криптографічної точки зору?

З криптографічної точки зору, призначення стеку протоколів IPSec полягає в забезпеченні конфіденційності, цілісності, автентифікації та захисту від повторних атак для IP-трафіку. IPSec реалізує ці функції за допомогою різних криптографічних механізмів та протоколів:

1. Конфіденційність (Encryption):
   - Використовує симетричне шифрування (наприклад, AES, 3DES) для захисту переданих даних від несанкціонованого доступу.
   - Шифрування застосовується в транспортному та тунельному режимах, залежно від потреб.

2. Цілісність даних (Integrity):

- IPSec забезпечує перевірку цілісності кожного пакета, щоб упевнитися, що дані не були змінені в процесі передачі.
- Для цього використовуються алгоритми хешування, такі як HMAC з SHA-1 або SHA-256, які генерують контрольні суми (MAC). Це дозволяє одержувачу перевірити, чи пакет був змінений.

3. Автентифікація (Authentication):
   - IPSec підтримує автентифікацію відправника для гарантії того, що пакет надійшов від надійного джерела.
   - Для цього використовується протокол AH (Authentication Header), який додає автентифікаційний заголовок до пакета.

4. Захист від повторних атак (Anti-Replay Protection):
   - IPSec забезпечує захист від повторних атак за допомогою механізмів відстеження послідовності пакетів.
   - Кожен пакет має унікальний номер, який приймаюча сторона перевіряє, щоб переконатися, що пакет не є повтором (такі пакети відкидаються).

Основні протоколи в IPSec:
- AH (Authentication Header): забезпечує автентифікацію та цілісність пакету, але не шифрує його, що робить його менш придатним для конфіденційної інформації.
- ESP (Encapsulating Security Payload): забезпечує конфіденційність (шифрування), автентифікацію та цілісність пакету. Це основний протокол для забезпечення шифрування в IPSec.

5) Назвіть криптографічні примітиви, які використовуються стеком протоколів IPSec.

Симетричні алгоритми шифрування

HMAC-SHA1/SHA2 - для захисту цілісності та автентичності.
TripleDES-CBC, AES-CBC і AES-CTR - як блокові загального призначення шифри.
AES-GCM і ChaCha20-Poly1305 як швидкі блокові шифри.

CBC - Cipher block chaining (Типу віженера)
CTR - Counter
GCM - Galois/counter

Алгоритми обміну ключами

Diffie–Hellman
ECDH

Алгоритми автентифікації

RSA
ECDSA - Elliptic Curve Digital Signature Algorithm
PSK - Secure Pre-Shared Key
EdDSA - Edwards-curve Digital Signature Algorithm

6) Назвіть основні компоненти реалізацій протоколів IPSec.
SAD - Security Association Database
SDP - Security Policy Database
SA - Security Association
AH - Authentication Header
ESP - Encapsulating Security Payload

SA — це зв'язок між двома або більше об'єктами, який описує, як ці об'єкти використовуватимуть безпеку для безпечного обміну даними. Кожне з'єднання IPSec може забезпечити шифрування, цілісність і автентичність. Асоціації безпеки — це метод, який IPSec використовує для відстеження своїх одночасних сеансів, без цього IPSec не працюватиме.

SAD – це таблиця, яка містить усі активні зв'язки безпеки для вхідного та вихідного трафіку, кожен запис зберігатиме параметри для окремого SA. У SAD зазвичай зберігаються такі записи.

- Індекс параметрів безпеки
- Адреса призначення
- Порядковий номер
- Вікно захисту від повторів
- Протокол безпеки IP
- Алгоритм
- ключ
- SA Тривалість життя

SDP - містить правила, які визначають, чи підлягає пакет обробці IPSec. Увесь трафік, включаючи вхідний і вихідний, має оброблятися через цю базу даних; для обробки трафіку використовуватиметься перша відповідна політика.

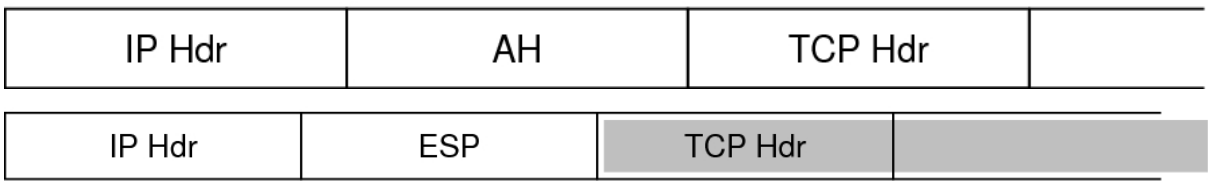
7) Назвіть основні характеристики та відмінності протоколів AH і ESP.

Authentication Header (AH)

Encapsulating Security Payload (ESP)

AH забезпечує цілісність даних за допомогою алгоритму автентифікації. Він не шифрує пакет.

ESP зазвичай захищає пакет за допомогою алгоритму шифрування та забезпечує цілісність даних за допомогою алгоритму автентифікації. Деякі алгоритми шифрування забезпечують як шифрування, так і автентифікацію, наприклад AES GCM.



[IP(a -> b) *параметри* + TCP + дані]
[IP(a -> b) + ESP [IP(a -> b) *параметри* + TCP + дані]]

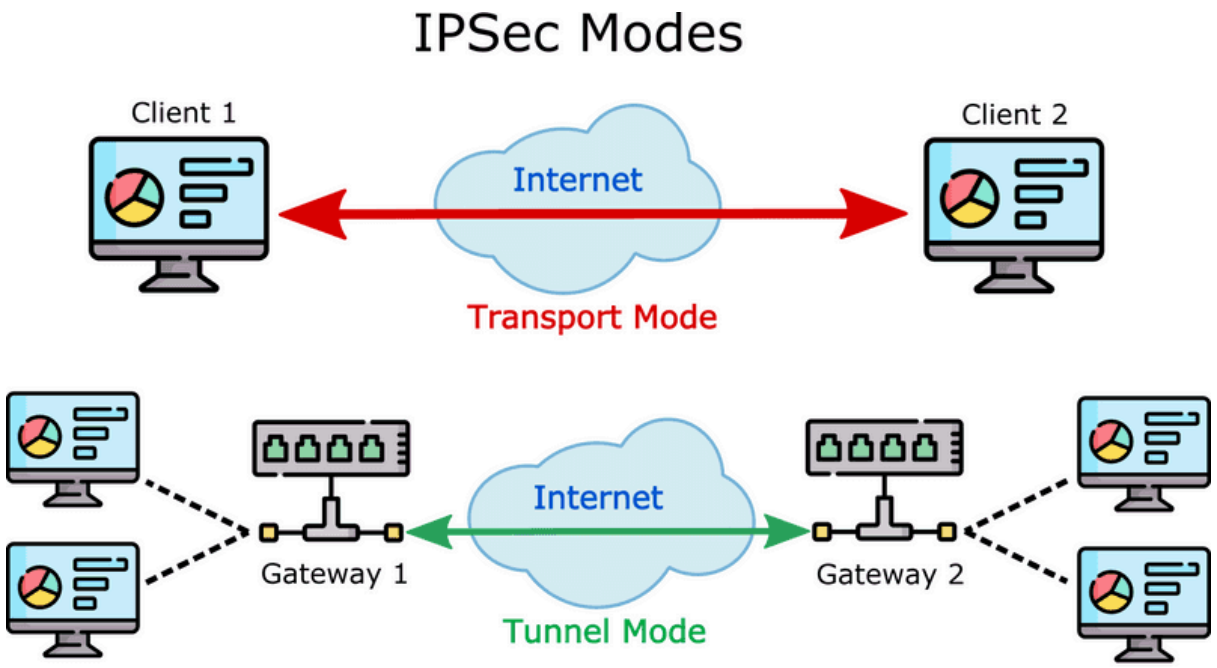
8) В чому полягають відмінності транспортного та тунельного режимів?

Режим тунелю

У режимі тунелю весь оригінальний IP-пакет інкапсулюється, щоб стати корисним навантаженням нового IP-пакета. Крім того, новий IP-заголовок додається поверх оригінального IP-пакета. Оскільки новий пакет створюється з використанням вихідної інформації, тунельний режим корисний для захисту трафіку між різними мережами. Додатковою перевагою цього режиму є те, що він дозволяє дуже легко встановити «тунель» між двома безпечними шлюзами IPsec.

Транспортний режим

Основна відмінність транспортного режиму полягає в тому, що він зберігає оригінальний IP-заголовок. Іншими словами, дані корисного навантаження, що передаються в оригінальному IP-пакеті, захищені, але не IP-заголовок. У транспортному режимі зашифрований трафік надсилається безпосередньо між двома хостами, які попередньо встановили безпечний тунель IPsec.



Типові застосування:
Транспортний: віддалений доступ, з'єднання клієнт-сервер
Тунельний: VPN, з'єднання між шлюзами безпеки

9) Назвіть основні зареєстровані криптографічні алгоритми протоколів IPSec.

1. **Алгоритми автентифікації (AH)**:

- HMAC-MD5-96
    - Довжина хеш-значення: 128 біт
    - Забезпечує помірний рівень захисту
    - Швидкий, але зараз вважається застарілим через вразливості MD5
- HMAC-SHA1-96
    - Довжина хеш-значення: 160 біт
    - Надійніший за MD5, але теж поступово виходить з використання
    - Все ще широко підтримується обладнанням
- HMAC-SHA256-128
    - Сучасний стандарт
    - Висока криптографічна стійкість
    - Рекомендований для нових впроваджень

2. Алгоритми шифрування (ESP):

- DES-CBC
    - Застарілий, 56-бітний ключ
    - Небезпечний для використання
    - Підтримується лише для сумісності зі старим обладнанням
- 3DES-CBC
    - Потрійний DES, ефективна довжина ключа 112 біт
    - Надійніший за DES, але повільний
    - Поступово виводиться з експлуатації
- AES-CBC
    - Розміри ключів: 128, 192, 256 біт
    - Сучасний стандарт шифрування
    - Оптимальне співвідношення безпеки та продуктивності

- AES-GCM
    - Автентифіковане шифрування
    - Висока продуктивність
    - Рекомендований для нових впроваджень

3. Алгоритми узгодження ключів (IKE):

- Diffie-Hellman Groups
    - Group 1 (768 біт) - застарілий
    - Group 2 (1024 біт) - мінімально прийнятний
    - Group 5 (1536 біт) - рекомендований мінімум
    - Groups 14-21 (2048-8192 біт) - сучасні рекомендовані
    - Groups 19-21 (ECC) - найбільш ефективні

10) В чому полягають особливості концепції безпечних асоціацій (SA)?

Основною метою SA є створення захищеного каналу комунікації між двома або більше учасниками інформаційного обміну, що особливо важливо в сучасному цифровому середовищі, де кількість кіберзагроз постійно зростає. Наприклад, при проведенні банківських операцій онлайн, SA забезпечує конфіденційність та цілісність всіх транзакцій.

Ключовою особливістю безпечних асоціацій є їх **багаторівнева система захисту**, яка включає криптографічні методи (AES, RSA), механізми автентифікації та системи контролю доступу. Це дозволяє створити комплексний захист від різноманітних типів атак, включаючи man-in-the-middle атаки та спроби несанкціонованого доступу. Важливим аспектом є **використання сучасних криптографічних алгоритмів**, таких як AES для шифрування та RSA для обміну ключами, що забезпечує максимальний рівень захисту при передачі даних.

Процес встановлення безпечної асоціації включає кілька критичних етапів, починаючи від ініціалізації з'єднання до завершення сесії. На кожному етапі **здійснюється верифікація параметрів безпеки та перевірка повноважень сторін**, що гарантує надійність всього процесу обміну даними. Наприклад, при встановленні VPN-з'єднання, система спочатку перевіряє сертифікати обох сторін, узгоджує параметри шифрування, і лише потім дозволяє передачу даних.

Особливу увагу в концепції SA приділено питанням **масштабованості та гнучкості системи**. Це дозволяє легко інтегрувати нові компоненти та адаптувати систему до зміни вимог безпеки. Наприклад, в корпоративних мережах можна легко додавати нові вузли або змінювати політики безпеки без необхідності повної реконфігурації системи.

Важливим елементом SA є **система моніторингу та аудиту**, яка дозволяє відслідковувати всі спроби встановлення з'єднань та виявляти потенційні загрози. Це забезпечує можливість швидкого реагування на інциденти безпеки та запобігання можливим атакам. **Механізми протоколювання та аналізу подій** дозволяють створювати детальні звіти про стан системи безпеки та проводити розслідування інцидентів.

Концепція SA передбачає **регулярне оновлення та вдосконалення механізмів захисту**, що є критичним для підтримки належного рівня безпеки в умовах появи нових загроз. Це включає оновлення криптографічних алгоритмів, зміну ключів шифрування та модифікацію політик безпеки. Наприклад, при виявленні нових вразливостей у протоколах шифрування, система може бути швидко адаптована для використання більш безпечних алгоритмів.

11) Як використовуються протоколи IPSec для побудови VPN-тунелів хост-хост, шлюз-шлюз та хост-шлюз?

1. **VPN-тунель типу хост-хост (Host-to-Host)**
   При такому з'єднанні IPSec встановлює захищений канал безпосередньо між двома кінцевими пристроями.
   Наприклад, між двома комп'ютерами в різних мережах. Особливості реалізації включають:
   - Використання транспортного режиму IPSec
   - Безпосередню автентифікацію кінцевих хостів
   - Шифрування даних на рівні IP-пакетів
   - Можливість використання цифрових сертифікатів для автентифікації

2. **VPN-тунель типу шлюз-шлюз (Gateway-to-Gateway)**
   Цей тип з'єднання забезпечує захищений канал між двома мережами

через шлюзи безпеки.
Характерні особливості:

- Використання тунельного режиму IPSec
- Повне шифрування вихідних IP-пакетів
- Автоматичне шифрування всього трафіку між мережами
- Централізоване управління політиками безпеки
- Масштабованість для великої кількості користувачів

3. **VPN-тунель типу хост-шлюз (Host-to-Gateway)**
   Цей варіант забезпечує віддалений доступ користувачів до корпоративної мережі.
   Ключові особливості включають:
   - Гнучке налаштування політик доступу
   - Можливість використання як транспортного, так і тунельного режиму
   - Підтримка мобільних користувачів
   - Інтеграція з системами автентифікації

Процес встановлення IPSec-тунелю включає кілька важливих етапів:

1. Ініціалізація з'єднання через протокол IKE (Internet Key Exchange)
2. Узгодження параметрів безпеки та створення SA (Security Association)
3. Обмін ключами та встановлення захищеного каналу
4. Періодичне оновлення ключів для підтримки безпеки

Переваги використання IPSec для VPN включають:

- Високий рівень безпеки завдяки сильній криптографії
- Гнучкість налаштування та масштабованість
- Сумісність з різними платформами та пристроями
- Можливість інтеграції з існуючими системами безпеки

IPSec забезпечує надійну основу для побудови захищених VPN-з'єднань різних типів, дозволяючи організаціям створювати безпечну інфраструктуру для передачі даних через публічні мережі.