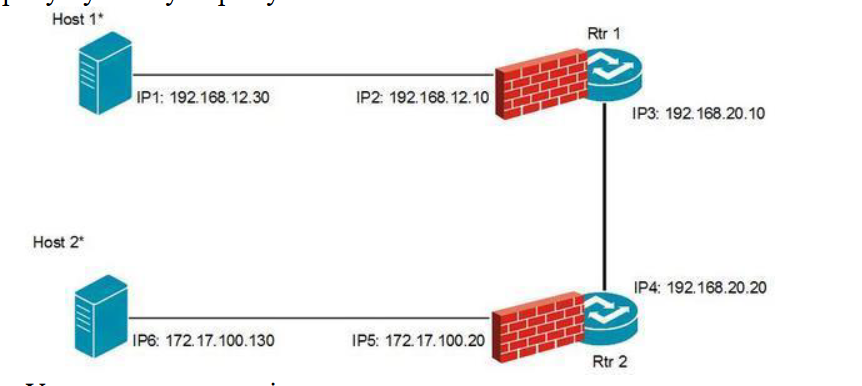
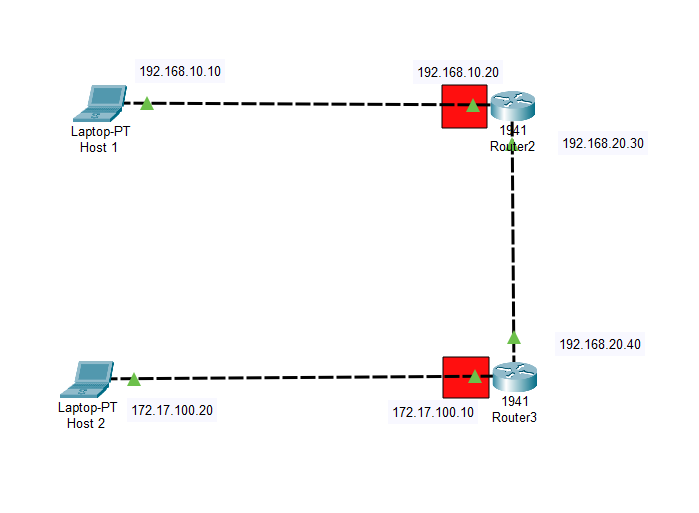
**Звіт**: Реалізація VPN на основі протоколу IPSec

**Виконав**: 05 09

Варіант завдання:



Вигляд в Packet tracer:



В рамках цього проекту було розроблено та реалізовано безпечне з'єднання між двома хостами за допомогою відкритої мережі. Для досягнення цієї мети був використаний протокол IPSec, який забезпечує шифрування, аутентифікацію та інтегрітет даних у віртуальній приватній мережі (VPN).

**IPSec (Internet Protocol Security)** - це протокол, призначений для захисту даних, переданих через IP-мережі. Він працює на рівні мережевого протоколу ІР і забезпечує шифрування, цілісність та аутентифікацію даних. IPSec може бути реалізований у різних режимах, але в даному проекті використовувався режим тунелювання.

Основні завдання протоколів IPSec:

– Забезпечення криптографічного захисту на рівні IP для протоколів IPv4 і IPv6, а саме забезпечення конфіденційності й цілісності даних і цілісності деякої послідовності дейтаграм.

– Забезпечення прозорості для IP-трафіку, для якого не потрібне

використання протоколів IPSec.

– Забезпечення розширюваності, тобто можливості додавати нові набори

алгоритмів без зміни самого протоколу.

IPSec призначений для безпечної взаємодії з використанням криптографії для протоколів IPv4 і IPv6. Сервіси безпеки включають керування доступом, цілісність і конфіденційність даних і захист від replay-атак, що забезпечується гарантуванням цілісності деякої послідовності дейтаграм. Ці сервіси надаються на рівні IP, забезпечуючи захист для IP-протоколу й протоколів більше високого рівня.

IPSec підтримує дві форми цілісності:

– цілісність даних;

– цілісність визначеної послідовності дейтаграм.

Цілісність даних виявляє модифікацію конкретної IP-дейтаграми, безвідносно послідовності дейтаграм у потоці трафіку. Цілісність послідовності дейтаграм є анти-replay сервісом, за допомогою якого визначається одержання дублікатів IP-дейтаграм. Це відрізняється від забезпечення цілісності з'єднання, для якого існують більше строгі вимоги до цілісності трафіку, а саме, можливість визначення загублених або з повідомлень.

Розглянемо виконання протоколів IPSec, основні компоненти системи і їхня взаємодія для забезпечення сервісів безпеки.

IPSec виконується на хості (Host – H) або шлюзі безпеки (Security Gateway – SG), забезпечуючи захист IP-трафіку. Термін "шлюз безпеки" використовується для позначення маршрутизатора, що реалізує IPsec-протоколи.

Захист заснований на вимогах, визначених у базі даних політики безпеки (Security Policy Database – SPD), установлюваної й підтримуваної адміністратором. У загальному випадку пакети обробляються одним із трьох способів, заснованих на інформації IP-заголовка й транспортного рівня відповідно до записів в SPD. Кожний пакет або відкидається, або пропускається без обробки, або обробляється відповідно до запису SPD для даного пакета.

Опис архітектури VPN на основі IPSec: Для реалізації VPN на основі IPSec було використано такі компоненти:

1. Як відкрита мережа(192.168.20.0/24), через яку відбувається зв'язок між хостами.
2. Хост 1 (192.168.10.10/24);
3. Хост 2 (172.17.100.20/24);
4. Протокол IPSec (використовується для шифрування, аутентифікації та забезпечення цілісності даних в тунелюванні);
5. Ключі безпеки.

Кроки реалізації:

1. Налаштування хостів A та B: На обох хостах було встановлено та налаштовано програмне забезпечення IPSec. Були створені ключі безпеки для обох хостів.
2. Встановлення VPN-тунелю: Хост A ініціює встановлення VPN-тунелю до хоста B. За допомогою протоколу IPSec, тунель встановлюється і забезпечується безпека комунікації між хостами.
3. Шифрування даних: Після успішного встановлення VPN-тунелю, дані, що передаються між хостами A та B, шифруються за допомогою ключів безпеки, що були попередньо обмінені.
4. Аутентифікація та перевірка цілісності: Протокол IPSec забезпечує аутентифікацію та перевірку цілісності даних, що передаються між хостами. Це дозволяє перевірити, що дані не були модифіковані під час передачі і походять від автентичного джерела.

**Висновки**: Реалізація VPN на основі протоколу IPSec дозволяє створювати безпечні з'єднання між хостами через відкриту мережу. Використання IPSec забезпечує шифрування, аутентифікацію та цілісність даних, що передаються між хостами, що робить цю комунікацію надійною та захищеною. Реалізація VPN на основі IPSec може бути використана для захисту конфіденційної інформації, особливо у випадках, коли дані передаються через ненадійну мережу, таку як Інтернет.