



Quantum
UNIVERSITY
ROORKEE, INDIA

Growth
Unbound!

The Future is
exciting..



IP SECURITY

PRESENTED BY:

SURAJ KUMAR VISHWAKARMA

QID: 24510031



OUTLINE:

- WHAT IS IP SECURITY?
- OSI MODEL
- WHY IP SECURITY IMPORTANT?
- FEATURES OF IP SECURITY
- ADVANTAGES OF IP SECURITY
- HOW DOES IP SECURITY WORK?
- IP SECURITY CONNECTION ESTABLISHMENT PROCESS
- PROTOCOLS USED IN IP SECURITY





What is IP Security(IPsec)?

IPsec (Internet Protocol Security) is a set of protocols used to secure communication over the Internet Protocol (IP)

- **Example:** IP Security (or IPsec) is like a shield for data traveling over the internet. It protects your information from being stolen or altered by hackers as it moves between devices, like from your phone to a website.
- It ensures that data sent across a network is:
 1. **Confidential:** No one can eavesdrop on it.
 2. **Authentic:** The sender and receiver are verified.
 3. **Untampered:** Data is delivered without any alterations.

IPsec operates at the network layer (Layer 3) of the OSI model, protecting data packets as they travel over the internet or private networks.





OSI Model:

What is the OSI Model?

The OSI (Open Systems Interconnection) model is like a blueprint for how data travels across a network. It divides the process of sending and receiving data into 7 layers, where each layer has a specific job.

.Think of it as a postal service for data:

1. You write a letter (data).
2. It's packed, addressed, and delivered by different people at different steps.
3. Each person (layer) has a specific role to ensure your letter reaches the correct destination.

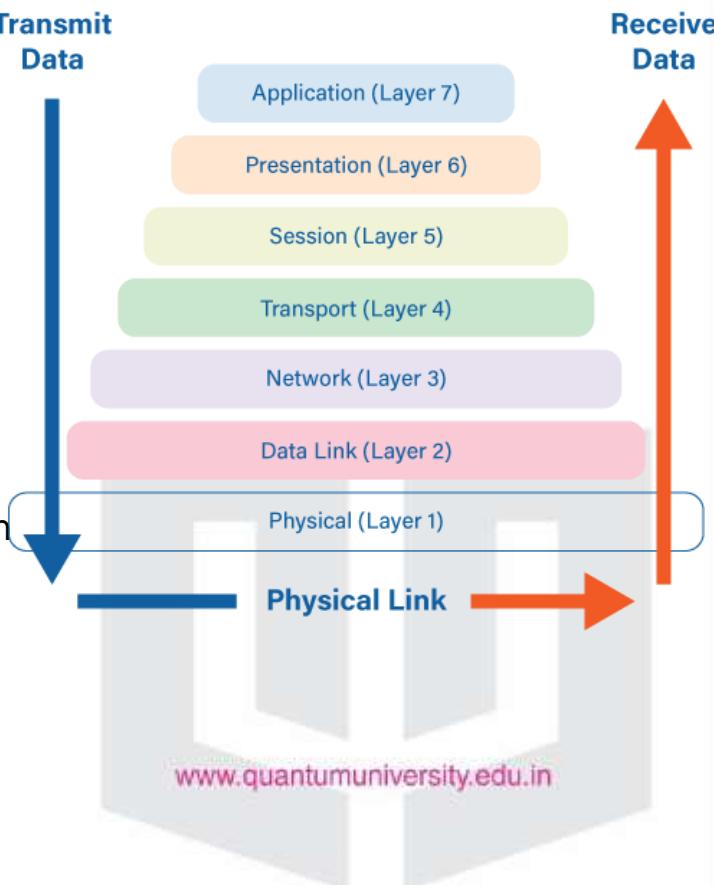
Network Layer (Layer 3):

Job: Finds the best route for the data to travel between devices, even if they are on different networks.

Example: The post office decides the best path to deliver the letter across cities or countries.

What Happens Here: IP addresses (like house addresses) are used to identify the sender and receiver.

The 7 Layers of OSI





Why IP Security Important?

IP Security(IPSec) is important because it helps keep your data safe and secure when you send it over the Internet or any network.

Imagine sending a letter through a mailman. Without security:

1. **Anyone** could open the envelope, read your message, or change it.
2. **Fake mailmen** could deliver a forged letter pretending it's from you.

With IPsec:

1. Your letter is sealed in a special box (**encryption**) so no one can read it.
2. Only the person who has the key can open the box (**authentication**).
3. IPsec makes sure the mailman is real and that your letter wasn't tampered with (**integrity**).



Features of IP Security:

1. Data Confidentiality

- **What it means:** Data is encrypted, so no one can read it without permission.
- **Example:** Imagine sending a letter in a locked box. Only the person with the key (the receiver) can open and read it.
- **How IPsec helps:** It keeps your private data, like passwords or messages, safe from hackers.

2. Data Integrity

- **What it means:** Ensures the data is not changed or tampered with during transmission.
- **Example:** If you send a recipe to a friend, IPsec makes sure the recipe stays the same and no one adds or removes ingredients.
- **How IPsec helps:** It confirms the data received is exactly what was sent.



3. Authentication

- **What it means:** Verifies who is sending and receiving the data to ensure they are trusted.
- **Example:** Like checking an ID card before letting someone into a secure building, IPsec ensures only the right devices are communicating.
- **How IPsec helps:** It prevents unauthorized devices or users from accessing your network.

4. Encryption

- **What it means:** Scrambles the data into a secret code that can only be decoded by the intended recipient.
- **Example:** If you send a secret message in a puzzle, only the person with the solution can read it.
- **How IPsec helps:** Even if someone intercepts the data, they can't understand it without the encryption key.



Advantages of IP Security:

1. Strong Security

- **What it means:** IPsec provides robust protection for your data with encryption, authentication, and integrity checks.
- **Example:** Like locking a diary with a code and verifying the person opening it is trusted, IPsec ensures your data stays safe.

2. Wide Compatibility

- **What it means:** IPsec works with all types of applications, protocols, and networks without needing changes.
- **Example:** It's like a universal charger—it works for all devices and applications without any extra effort.



3. Transparency

- **What it means:** IPsec operates in the background, so users don't need to do anything extra for security.
- **Example:** It's like a seatbelt in a car—once it's in place, it protects you without needing constant attention.

4. Improved network performance

IPSec can help improve network performance by reducing network congestion and improving network efficiency.



How Does IP Security Works?

IPSec (Internet Protocol Security) is used to secure data when it travels over the Internet. IPSec works by creating secure connections between devices, making sure that the information exchanged is kept safe from unauthorized access. IPSec majorly operates in two ways:

Transport Mode and **Tunnel Mode**.

To provide security, IPSec uses two main protocols: **AH (Authentication Header)** and **ESP (Encapsulating Security Payload)**. Both protocols are very useful:

Authentication Header (AH): Verifies the data to ensure it comes from a trusted source and hasn't been changed.

Encapsulating Security Payload (ESP): Performs authentication and encrypts the data, making it difficult to read.



For encryption, IPSec uses cryptographic keys. These keys are created and shared using a process called **IKE (Internet Key Exchange)**, which ensures that both devices have the correct keys to establish a secure connection.

When two devices communicate using IPSec:

1. The devices first initiate the connection by sending a request to each other.
 2. They mutually decide on protecting the data using passwords or digital certificates.
 3. They establish a secure tunnel for communication.
 4. Once the tunnel is set up, data can be transmitted safely as IPSec encrypts the data and checks its integrity to ensure it hasn't been altered.
 5. After the communication is finished, the devices close the secure connection.
- In this way, IPSec ensures secure and reliable data communication over the internet.



IPsec Tunnel Mode





IP Security Establishment Process:

IPSec secures communication by ensuring every packet in a session is authenticated and encrypted. The process of establishing an IPSec connection involves **two main phases**:

Phase 1: Establishing the IKE (Internet Key Exchange) Tunnel

- The first step is to create a secure channel called the **IKE tunnel**, which is used for further communication and negotiations.
- This phase can work in two modes:

•1. Main Mode:

- A six-message exchange that is highly secure.
- Takes longer because identity details (like who is communicating) are protected during the exchange.
- **Example:** Like having a detailed background check before allowing two people to start a secret meeting.



2. Aggressive Mode:

- A three-message exchange that is faster but less secure.
- Discloses more information, such as identities, during negotiations.
- **Example:** Like skipping the background check to start the meeting quickly, even if it means some details might get exposed.

Phase 2: Establishing the IPSec Tunnel

•What happens in Phase 2:

- After the IKE tunnel is set up, the **IPSec tunnel** is created for secure data exchange.
- This phase is called **Quick Mode** and involves negotiating the rules for protecting data (called Security Associations).
- Phase 2 operates in two modes:



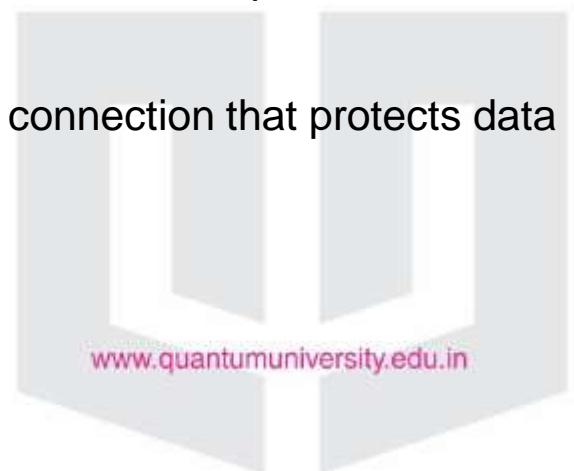
1. Tunnel Mode:

- Encrypts the entire IP packet, including both the header and the data.
- Used mostly in **site-to-site VPNs** where networks (not just devices) are connected securely.
- **Example:** Like wrapping an entire parcel, including the shipping label, in a sealed envelope for secure delivery.

2. Transport Mode:

- Encrypts only the actual data (payload), leaving the IP header unchanged.
- Used in **end-to-end communication** between two devices, like your computer and a server.
- **Example:** Like sending a letter where only the content is hidden, but the envelope shows the sender and receiver's addresses.

By following these two phases, IPSec ensures a secure, encrypted connection that protects data from unauthorized access during transmission.





Protocols Used in IPSec:

It has the following components:

1. Encapsulating Security Payload (ESP):

It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

2. Authentication Header (AH):

It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

3. Internet Key Exchange (IKE):

- What it does:**

- IKE is a network security protocol designed to dynamically exchange encryption keys and set up a **Security Association (SA)** between two devices.



- **IKE** is a network security protocol designed to dynamically exchange encryption keys and set up a **Security Association (SA)** between two devices.
- The **Security Association (SA)** establishes shared security attributes between two network entities to support secure communication.
- **ISAKMP (Internet Security Association and Key Management Protocol)** provides a framework for authentication and key exchange.
- **ISAKMP** specifies how the **Security Associations (SAs)** are set up and how direct connections between two hosts using IPSec are created.
- **IKE** also ensures message content protection and provides a framework for implementing standard algorithms like **SHA** (Secure Hash Algorithm) and **MD5**.
- IPSec users produce a **unique identifier** for each packet, which allows a device to verify whether a packet is correct.
- **Unauthorized packets** are discarded and not passed on to the receiver.



THANK YOU!

INNOVATE EMPOWER PERSEVERE SUCCEED

www.quantumuniversity.edu.in