IP SECURITY

By:
Alisha (D111), Dhruvi (D099),
Janavi (D094), Justin (D093).

OVERVIEW

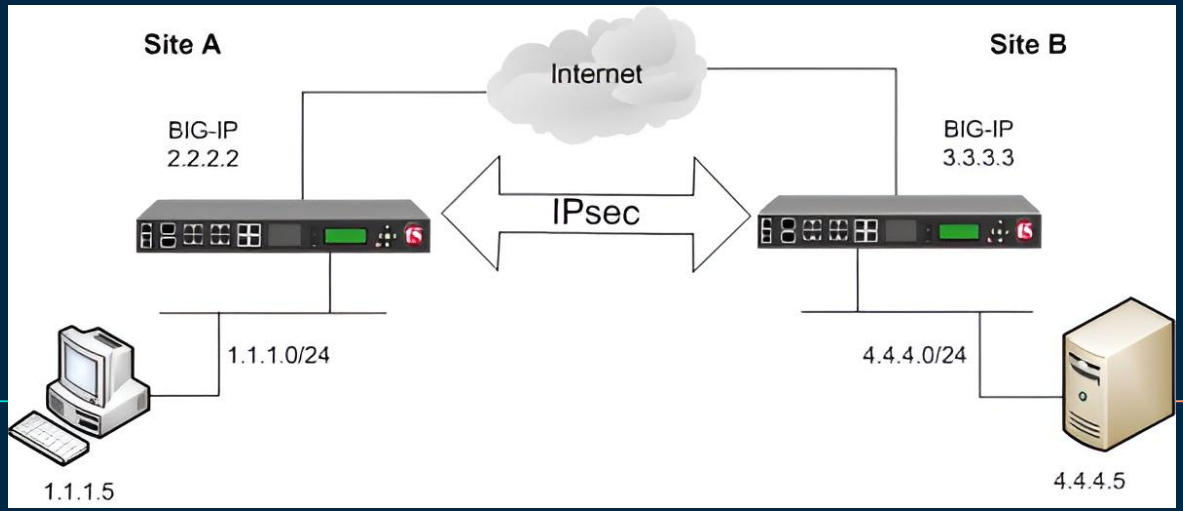
01

What is IP Security?

- **Internet Protocol (IP)** is the common standard that controls how data is transmitted across the internet.
- Refers to a collection of communication rules or protocols used to establish secure network connections.

IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality

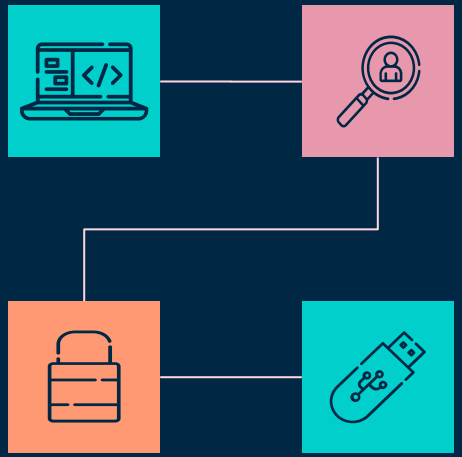
For example, it encrypts data at the source and then decrypts it at the destination. It also verifies the source of the data.



Uses of IP Security

Encryption

To encrypt application layer data.



Authentication

To provide authentication without encryption

Security

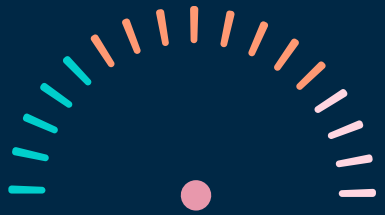
To provide security for routers sending routing data across the public internet.

Protection

To protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted

Components of IP Security

Encapsulation Security Payload(ESP)

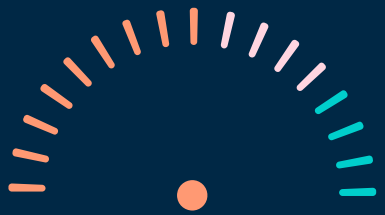


It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

Authentication Header(AH)

The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

Internet Key Exchange(IKE)



It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices

Features of IPSec

- **Authentication**: IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
- **Confidentiality**: IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.
- **Integrity**: IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.

- **Key management**: IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
- **Tunneling**: IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
- **Flexibility**: IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
- **Interoperability**: IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

Advantages & Disadvantages Of IPSEC:

Advantages:

- **Security**: Provides robust cryptographic security for data protection and network integrity.
- **Wide Compatibility**: Open standard supported by many vendors, suitable for diverse environments.
- **Flexibility**: Configurable for various network topologies like point-to-point, site-to-site, and remote access.
- **Scalability**: Effective for securing large-scale networks, adaptable to changing needs.
- **Improved Performance**: Reduces network congestion and enhances efficiency.

Disadvantages:

- **Configuration Complexity**: Requires specialized knowledge and skills for setup.
- **Key Management**: Needs effective key management for secure encryption and authentication.
- **Limited Protection**: Only protects IP traffic, leaving other protocols like ICMP, DNS, and routing protocols vulnerable.

ARCHITECTURE

02

IP SECURITY ARCHITECTURE

Uses two protocols to secure the Traffic or Data Flow

Includes Protocols, Algorithms , DOI, and Key Management

Provides services like Confidentiality, Authentication, Integrity

TYPES OF PROTOCOLS

ESP (Encapsulation Security Payload) Protocol

- ★ Provides a confidentiality service.
- ★ Implemented in either two ways:
  - ○ ESP with optional Authentication.
  - ○ ESP with Authentication.

AH (Authentication Header) Protocol

- ★ Provides both Authentication and Integrity service.
- ★ implemented in one way only:
  - ○ Authentication along with Integrity

ALGORITHM

Encryption algorithm

The encryption algorithm is the document that describes various encryption algorithms used for Encapsulation Security Payload

Authentication Algorithm

Contains the set of documents that describe the authentication algorithm used for AH and for the authentication option of ESP

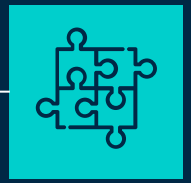
DOI (Domain of Interpretation)

- DOI is the identifier that supports both AH and ESP protocols. It contains values needed for documentation related to each other

Key Management

- Key Management contains the document that describes how the keys are exchanged between sender and receiver.

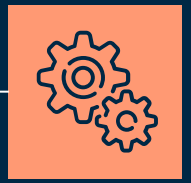
SERVICES



01

CONFIDENTIALITY

Encrypts Ip packets to prevent unauthorized access to the data



02

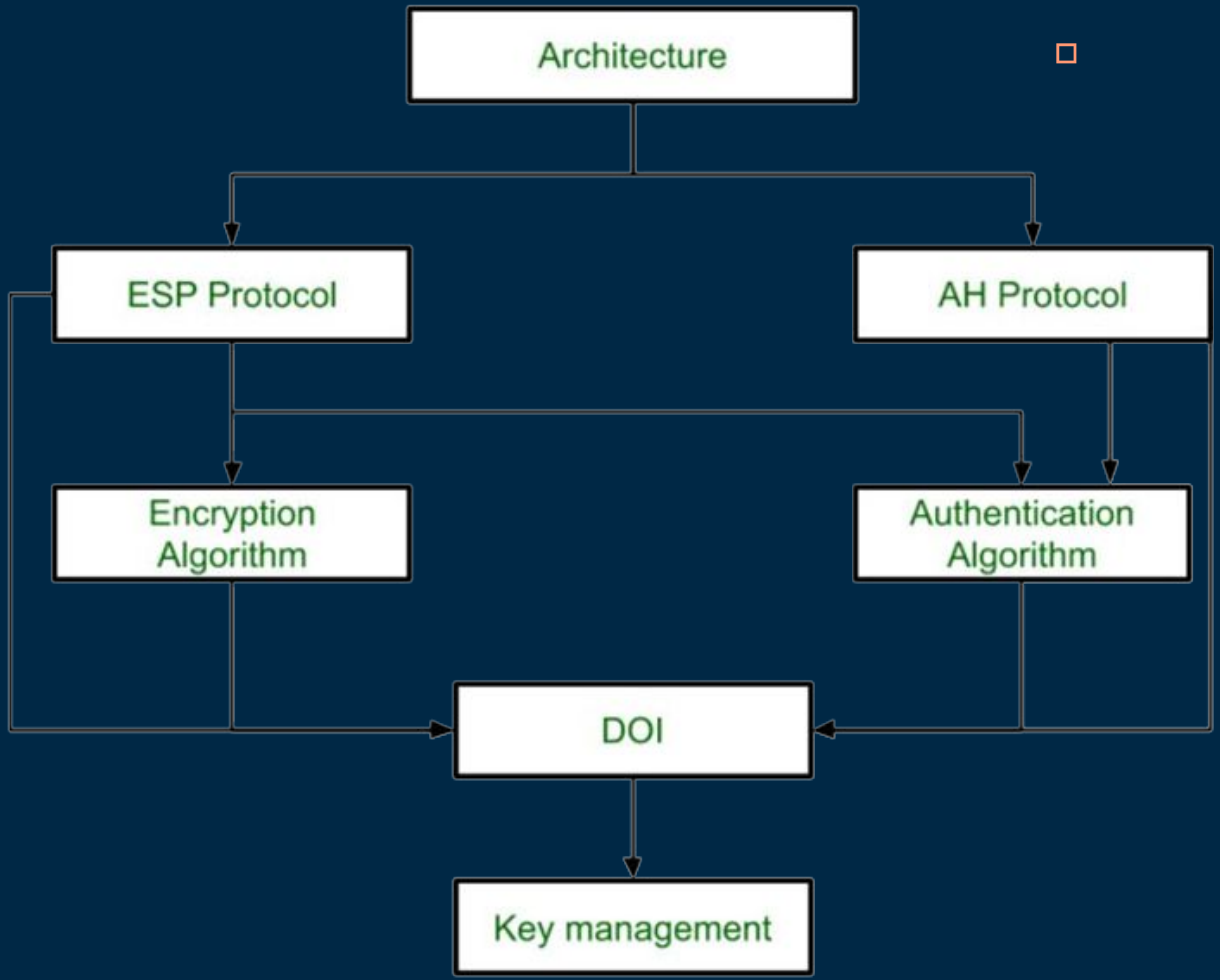
INTEGRITY

Ensures the Integrity of data by providing authentication

03

AUTHENTICATION

Authenticates the source of data by verifying the identity of parties


Architecture
ESP Protocol
AH Protocol
Encryption Algorithm
Authentication Algorithm
DOI
Key management

AUTHENTICATION HEADER

03

WHAT IS AUTHENTICATION HEADER ?

Authentication header is a security protocol that provide data origin authentication, data integrity and replay protection for IP datagrams

Message Integrity

It ensures the message has not been modified during transmission

Source Authentication

Source is exactly the source from whom we were expecting the data

Replay Protection

It uses a sequence number to prevent replay attacks where an attacker sends a previously transmitted packet

NOTE	Replay attack is a attack where the hacker just retransmits the data over again to perform malicious action.

TYPES OF OPERATIONS MODES

Transport Mode

Auth header is inserted between the original IP header and upper layer protocol

Tunnel Mode

The original IP packet is authenticated and a new IP header is added

Next Header

8-bit field that identifies the type of header present after Auth header

Payload Length

Length of Auth header

Reserved

Reserved bit for future use

Security Parameter Index (SPI)

Arbitrary 32-bit field

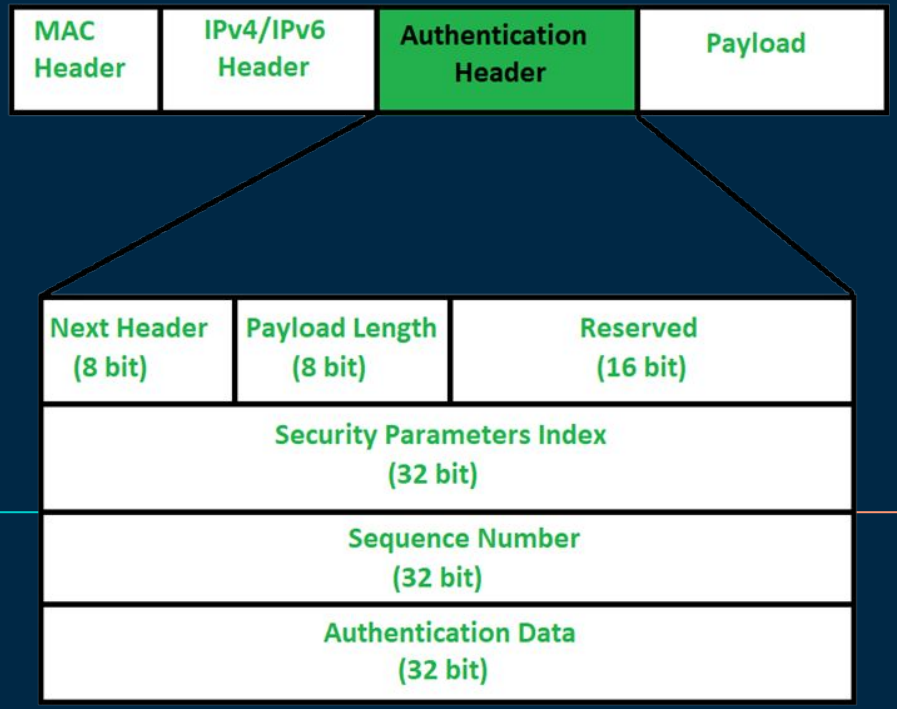
Sequence Number

Unsigned 32-bit field that contains counter value

Auth Data

Integrity check value

Authentication Header format



Advantages & Disadvantages Of AH:

Advantages:

- **Message Integrity -** AH ensures that the message has not been modified in transit.
- **Source Authentication -** AH provides a way to verify the identity of the sender.
- **Replay Protection -** AH uses sequence numbers to protect against replay attacks.

Disadvantages:

- AH only provides authentication and integrity, but not confidentiality. The data is not encrypted.
- AH has higher overhead compared to using just encryption (ESP protocol), as it requires additional processing for the authentication calculations
- AH has compatibility issues, as it may not work well with certain network address translation (NAT) devices

ESP

Encapsulating Security Payload

04

What is ESP?

ESP (Encapsulating Security Payload) is a protocol within the IPsec suite (Internet Protocol Security). It's designed to provide confidentiality, integrity, and authentication for data transmitted between devices in a network (for the payload and not for the IP header).

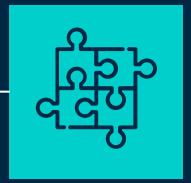
In simpler terms, it ensures that information sent over the network remains secure and protected.

- The difference between ESP and the Authentication Header (AH) protocol is that while both protocols provide authentication, integrity checking, and replay protection, ESP provides encryption.

- With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.

- If you decide to use both encryption and authentication, then the responding system first authenticates the packet and then, if the first step succeeds, the system proceeds with decryption. This type of configuration reduces processing overhead, as well as reduces your vulnerability to denial-of-service attacks.

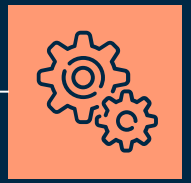
WORKING OF ESP



01

ENCRYPTION

Encrypts the payload (the actual data) of IP packets.



02

AUTHENTICATION

Verifies the origin of the payload.

03

CONFIDENTIALITY

By encrypting the payload, it keeps it confidential, preventing unauthorized access.

Modes in ESP

You can apply ESP in two ways: transport mode or tunnel mode.

- In **transport mode**, the original IP header remains intact.
- Only the payload (the actual data portion of the IP packet) is encrypted and protected by the Encapsulating Security Payload (ESP).
- The ESP header is inserted between the original IP header and the payload.
- If the datagram already has an IPSec header (e.g., if it's part of an existing IPSec-protected communication), the ESP header goes before that existing header.
- The ESP trailer (if used) and optional authentication data follow the payload.
- Transport mode is typically used for end-to-end communication between hosts or devices.

- In **tunnel mode** (the default mode), the entire original IP packet is protected by IPSec.
- IPSec wraps the original packet, encrypts it, adds a new IP header, and sends it to the other side of the VPN tunnel (IPSec peer).
- Tunnel mode is commonly used between gateways (e.g., routers or firewalls) or from an end-station to a gateway.
- An IPSec header (either AH or ESP) is inserted between the IP header and the upper layer protocol.
- Between AH and ESP, ESP is more commonly used in IPSec VPN tunnel configurations.

Advantages:

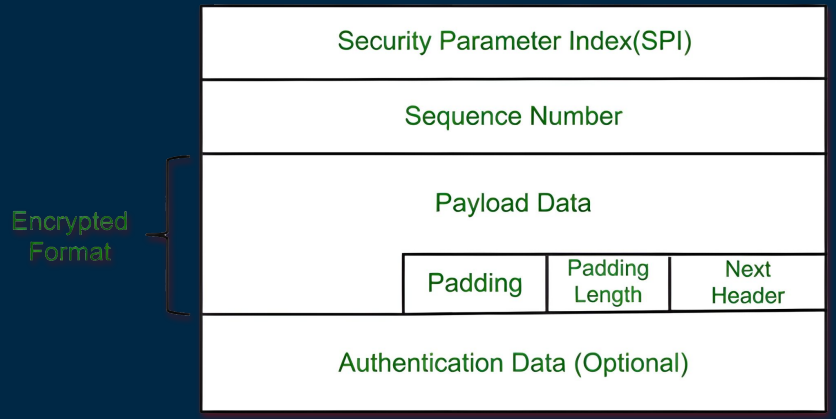
1. **Data Encryption:** It protects sensitive information from unauthorized access.
2. **Secure Gateway:** It establishes a secure gateway for data or message exchange between network entities.
3. **Authentication:** This prevents spoofing and ensures that data comes from a legitimate source.
4. **Data Integrity:** Detects any unauthorized modifications or tampering.
5. **Confidentiality:** By encrypting the payload, ESP maintains data confidentiality.
6. **Anti-Replay Service:** Includes an optional authentication header that helps prevent replay attacks (where an attacker retransmits intercepted packets).

Disadvantages:

1. **Encryption Restrictions:** There are limitations on the encryption methods allowed by ESP. Some algorithms may not be supported.
2. **Global Implementation:** For global use, weaker encryption algorithms (due to export restrictions) may be mandatory. This compromises security to some extent.

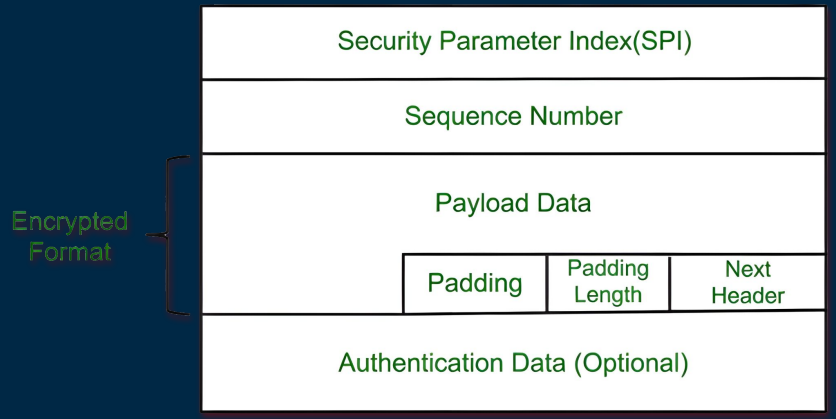
Components

- **Security Parameters Index (32 bits):** Identifies a security association (SA). This is mandatory for managing secure connections. The value of zero is reserved and not transmitted.
- **Sequence Number (32 bits):** A counter that increments with each packet, starting at 1. It helps prevent replay attacks by ensuring packets are received in order.
- **Payload Data (variable size):** The actual data being protected, which could be a transport-level segment or an entire IP packet. It's encrypted for security.



Components

- **Padding (0-255 bytes):** Extra bytes added to align the payload data to the encryption block size, ensuring it fits correctly.
- **Pad Length (8 bits):** Indicates how many padding bytes are present.
- **Next Header (8 bits):** Specifies the type of data in the payload, identifying the first header of the payload content.
- **Authentication Data (variable size):** Optional field that contains integrity information, used if the security association requires it.



Q&A Document:

THANKS