# Chapter 7

# Network Security

## Table of Contents

## Overview of Network Security

Network security involves implementing measures to protect the integrity, confidentiality, and availability of data and resources in a network environment.

## What is Network Security?

Any action intended to safeguard the integrity and usefulness of your data and network is known as network security. In other words, Network security is defined as the activity created to protect the integrity of your network and data.

Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks. It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.

*Figure: Network Security*

## Objectives of Network Security

- **Confidentiality**: Ensures that only authorized users have access to specific data.
- **Integrity**: Protects data from being altered or tampered with by unauthorized individuals.
- **Availability**: Ensures that network resources and data are accessible to authorized users when needed.

- **Authentication**: Verifies the identity of users, devices, or systems before granting access.
- **Non-repudiation**: Ensures that actions or transactions cannot be denied after they have been performed.

## How Does Network Security Work?

Network security uses several layers of protection, both at the edge of the network and within it. Each layer has rules and controls that determine who can access network resources.

**These levels are:**

**Physical Network Security**:

- **Purpose**: Protects the physical infrastructure and hardware of the network.

- **Measures**:
  - Secure access to data centers and server rooms with locks, security badges, and surveillance cameras.
  - Ensure proper environmental controls like cooling and fire suppression systems.
  - Use physical barriers to prevent unauthorized access to networking equipment.

**Technical Network Security**:

- **Purpose**: Safeguards data and network systems through technological means.
- **Measures**:
  - **Firewalls**: Control incoming and outgoing network traffic based on predefined security rules.
  - **Encryption**: Protect data in transit and at rest using encryption protocols.

    - **Antivirus Software**: Detects and removes malicious software.
    - **Secure Configurations**: Properly configure network devices and services to minimize vulnerabilities.

**Administrative Network Security**:

- **Purpose**: Establishes policies, procedures, and guidelines for network security management.
- **Measures**:
    - **Access Control Policies**: Define who has access to what resources and under what conditions.
    - **Security Training**: Educate employees about security best practices and awareness.
    - **Incident Response Plan**: Develop procedures for responding to security breaches or incidents.
    - **Regular Audits**: Conduct security assessments

and audits to identify and address vulnerabilities.

## Email Security: S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a technology used to keep email communications secure. Here’s a straightforward explanation:

### What is S/MIME?

S/MIME is like a security system for your emails. It helps protect your messages so that only the people you intend to receive them can read them, and it ensures that the messages haven’t been tampered with.

### How Does It Work?

1. **Encryption**: Think of this as locking your email in a secure box. When you send an email using S/MIME, it gets encrypted, which means it’s turned into a code that only the intended recipient can decode. This way,

even if someone intercepts the email, they can’t read it without the right key.

2. **Digital Signatures**: This is like putting a special seal on your email. When you send an email, S/MIME adds a digital signature, which is a unique code that verifies you’re the one sending the email and confirms that the email hasn’t been altered in transit. The recipient can use this signature to check that the email is genuinely from you and hasn’t been changed.

### Why Use S/MIME?

- **Privacy**: It keeps your email content private, ensuring only the intended recipient can read it.
- **Authenticity**: It confirms that the email truly comes from you and hasn’t been tampered with.
- **Trust**: It helps build trust in email communications by providing a way to verify both the sender and the content.

# Pretty Good Privacy (PGP)

It is an encryption program that provides cryptographic privacy and authentication for data communication.

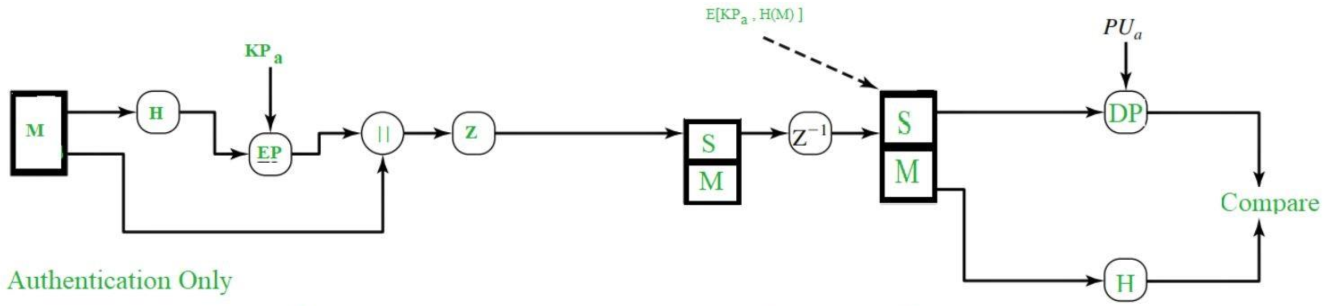
Increases security of email communication via providing the cryptographic privacy and authentication.

PGP is used for encrypting, and decrypting texts, emails, files, directories, and to increase security of email communications.

It helps on authentication (using digital signature) and confidentiality.

## Working of PGP:

### 1.Authentication Only:



## At Sender Side

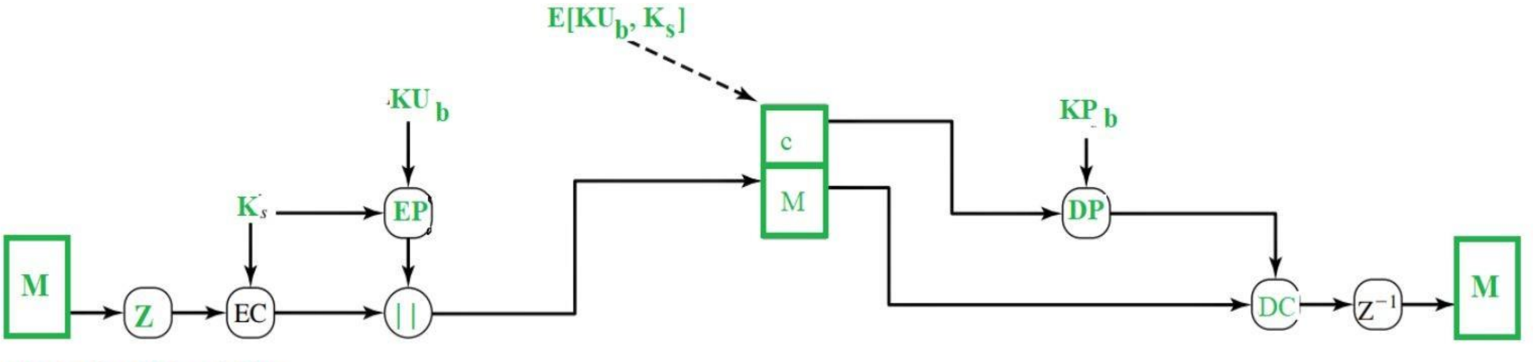
- Hash function (H) calculates the hash value of message (M)
- Then using sender private key (KPa), it is encrypted called as digital signature
- The message is then appended to a signature
- The message is then compressed to reduce transmission overhead and is sent it to receiver

## At Receiver Side

- The data is decompressed and the message and signature are obtained
- The signature is decrypted using sender public’s key (PUa) and hash value is obtained
- The message is again passed to has function and its hash value is calculated and obtained

- Both value one from signature and other from output of hash function are compared and if both are same, email is sent from legit else it means the email has been compromised

2.Confidentiality only



Only Confidentiality

## At Sender

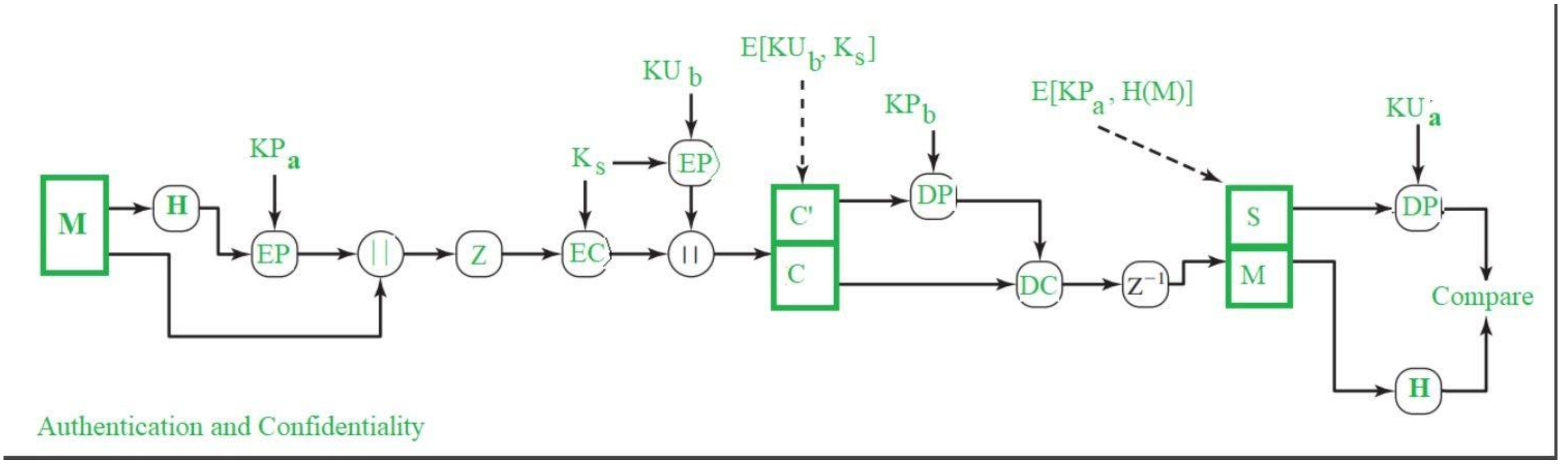
- The message is first compressed
- 128 bit session key (Ks) is used to encrypt the message through symmetric encryption

- Then symmetric key (Ks) itself gets encrypted through public key (EP) using the receiver public key (KUb)
- Both encrypted entities are now concatenated and sent to receiver

At receiver

- The encrypted session key is decrypted using receiver private key (KPb)
- The message is decrypted using obtained session key
- Then the message is decompressed to get the original message

## 3.Authentication and confidentiality



Authentication and Confidentiality

**Note:**

M – Message

H – Hash Function

Ks – A random Session Key created for Symmetric Encryption purpose

DP – Public-Key Decryption Algorithm

EP – Public-Key Encryption Algorithm

DC – Asymmetric Decryption Algorithm

EC – Symmetric Encryption Algorithm

KPb – A private key of user B used in Public-key encryption process

KPa – A private key of user A used in Public-key encryption process

PUa – A public key of user A used in Public-key encryption process

PUb – A public key of user B used in Public-key encryption process

|| – Concatenation

Z – Compression Function

Z-1 – Decompression Function

# Secure Socket Layer (SSL) and Transport Layer Security (TLS)

Secure Socket Layer (SSL):

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

## What is a Secure Socket Layer?

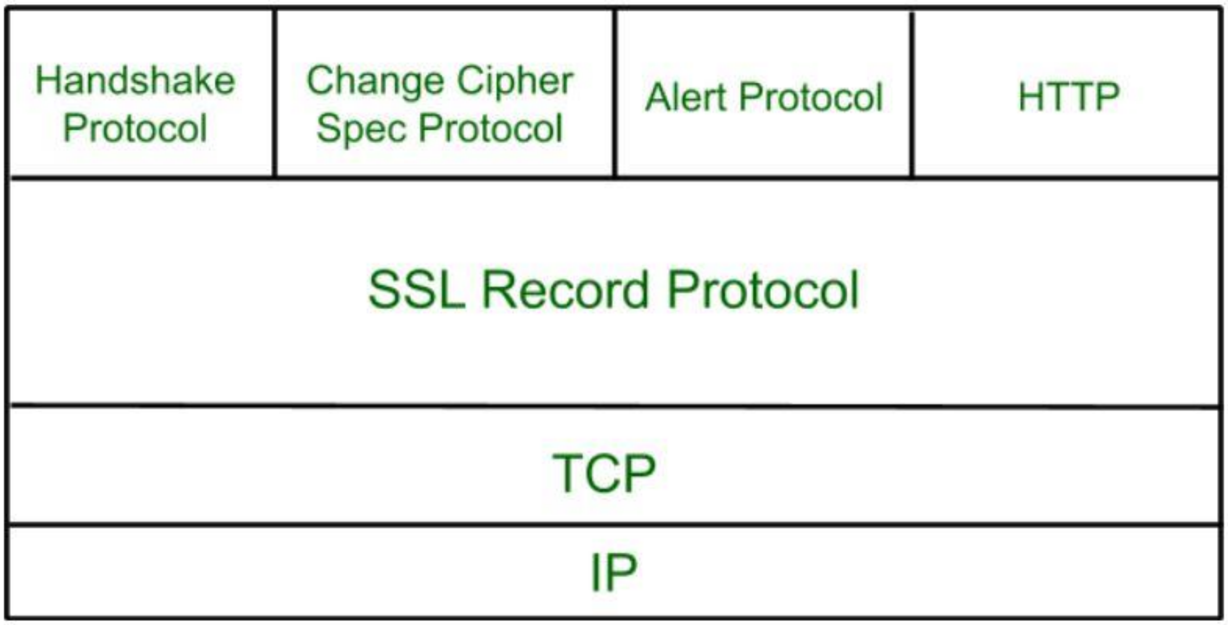
SSL, or Secure Sockets Layer, is an Internet security protocol that encrypts data to keep it safe. It was created by Netscape in 1995 to ensure privacy, authentication, and data integrity in online communications. SSL is the older version of what we now call TLS (Transport Layer Security).

Websites using SSL/TLS have “HTTPS” in their URL instead of “HTTP.”

## How does SSL work?

- **Encryption**: SSL encrypts data transmitted over the web, ensuring privacy. If someone intercepts the data, they will see only a jumble of characters that is nearly impossible to decode.
- **Authentication**: SSL starts an authentication process called a handshake between two devices to confirm their identities, making sure both parties are who they claim to be.
- **Data Integrity**: SSL digitally signs data to ensure it hasn’t been tampered with, verifying that the data received is exactly what was sent by the sender.

SSL protocol stack:



## Secure Socket Layer Protocols

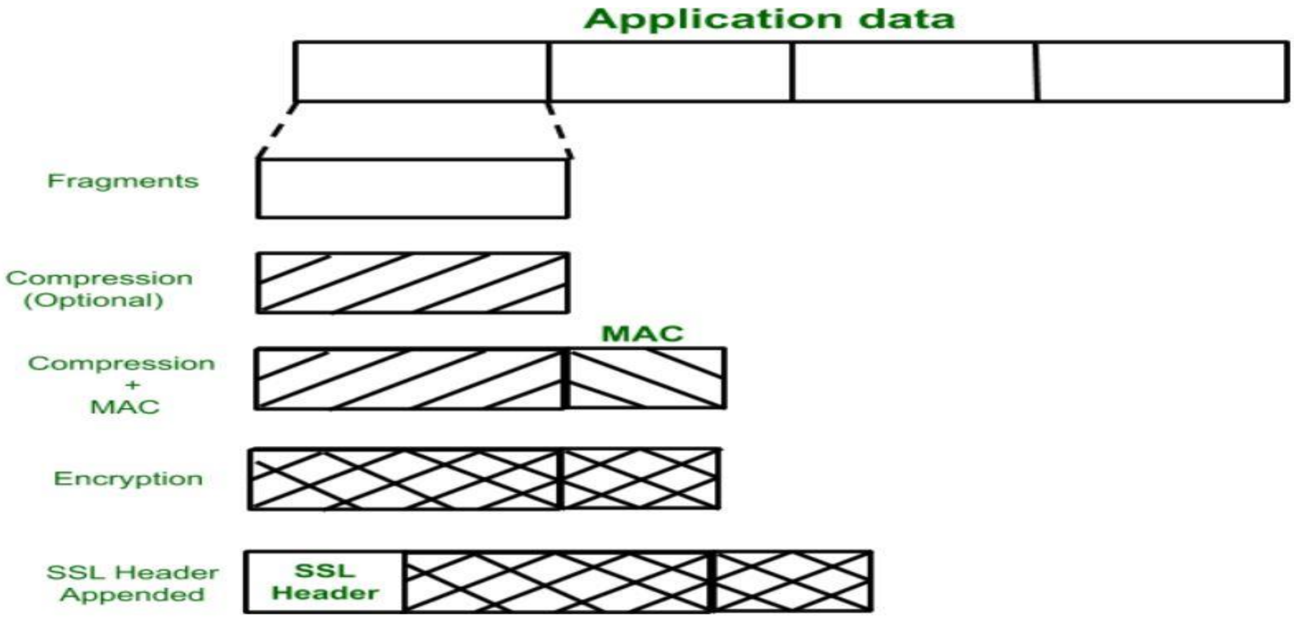
- SSL Record Protocol
- Handshake Protocol
- Change-Cipher Spec Protocol
- Alert Protocol

## 1. SSL Record Protocol

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

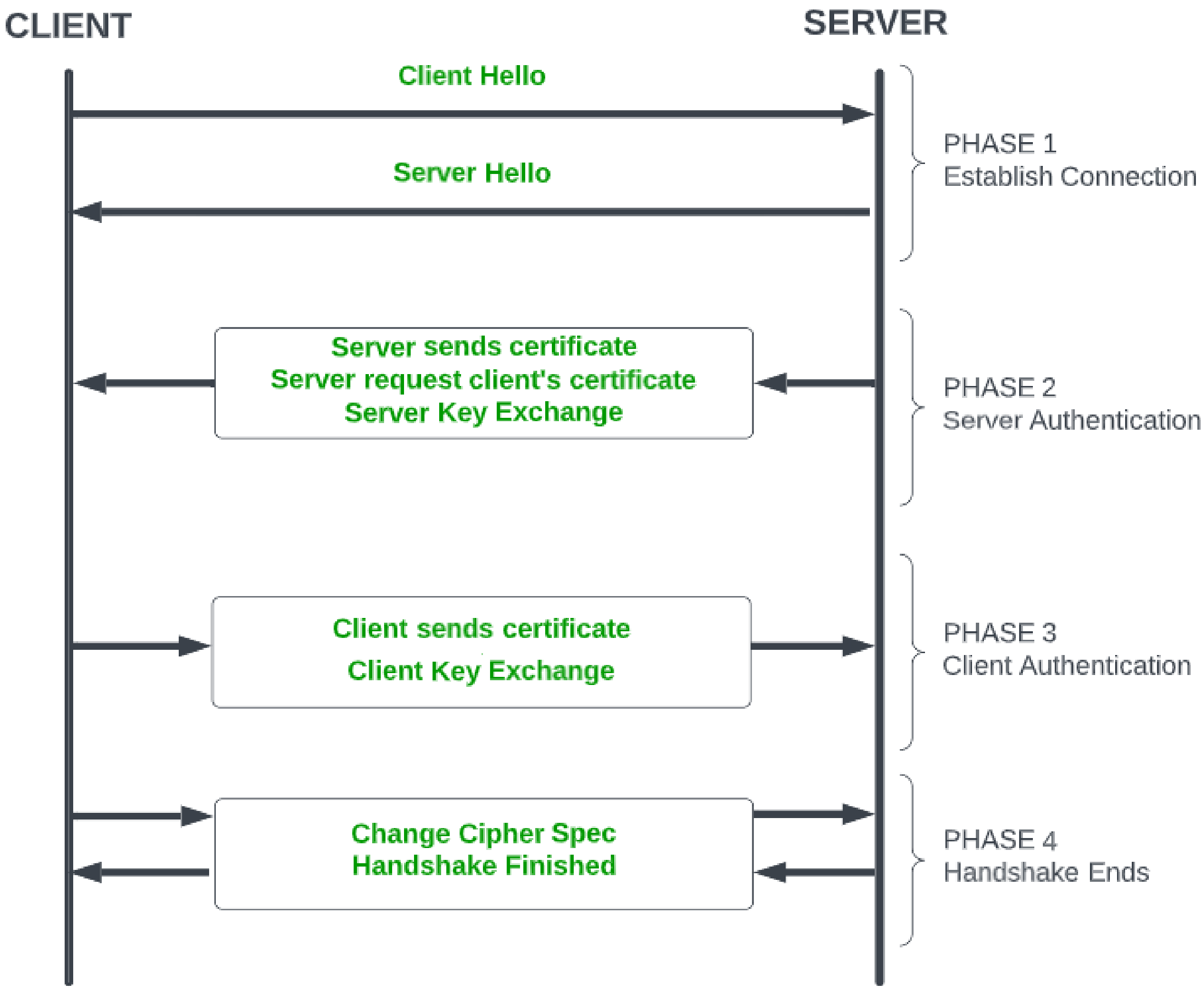
In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA and MD5 is appended. After that encryption of the data is done and in last SSL header is appended to the data.



## 2. Handshake Protocol

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

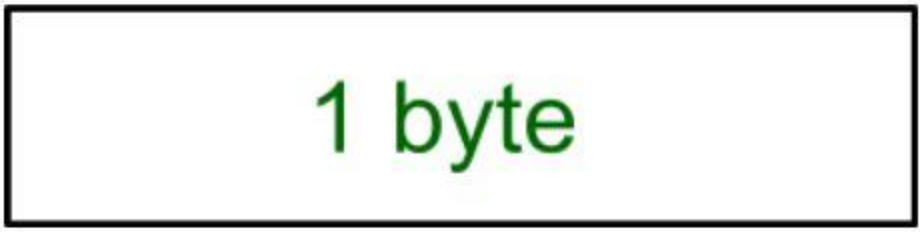
- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurs and after this the Handshake Protocol ends.



SSL HANDSHAKE PROTOCOL

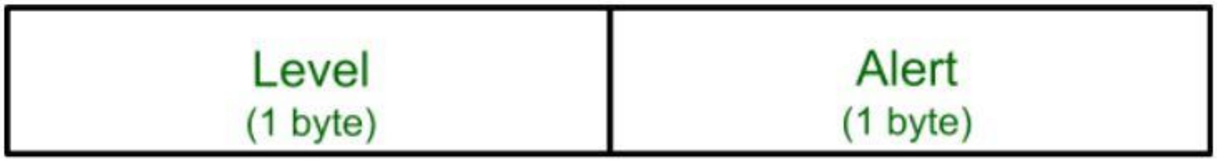
## 3. Change-Cipher Protocol

This protocol uses the SSL record protocol. Unless handshake Protocol is completed, the SSL record Output will be in a pending state. After the handshake protocol, the Pending state is converted into the current state. Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.



### 4. Alert Protocol

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.



The level is further classified into two parts:

**Warning (level = 1)**

This Alert has no impact on the connection between sender and receiver. Some of them are:

- **Bad Certificate:** When the received certificate is corrupt.
- **No Certificate:** When an appropriate certificate is not available.
- **Certificate Expired:** When a certificate has expired.
- **Certificate Unknown:** When some other unspecified issue arose in processing the certificate, rendering it unacceptable.
- **Close Notify**: It notifies that the sender will no longer send any messages in the connection.
- **Unsupported Certificate:** The type of certificate received is not supported.

### Fatal Error (level = 2):

This Alert breaks the connection between sender and receiver. The connection will be stopped, cannot be resumed but can be restarted. Some of them are :

- **Handshake Failure:** When the sender is unable to negotiate an acceptable set of security parameters given the options available.
- **Decompression Failure**: When the decompression function receives improper input.
- **Illegal Parameters:** When a field is out of range or inconsistent with other fields.
- **Bad Record MAC:** When an incorrect MAC was received.
- **Unexpected Message:** When an inappropriate message is received.

The second byte in the Alert protocol describes the error.

## Transport Layer Security (TLS):

Transport Layer Security (TLS) is a protocol designed to keep communications secure over the internet. It evolved from an earlier protocol called Secure Socket Layer (SSL). TLS ensures that no one can intercept or alter the messages being sent between a client (like your web browser) and a server (like a website).

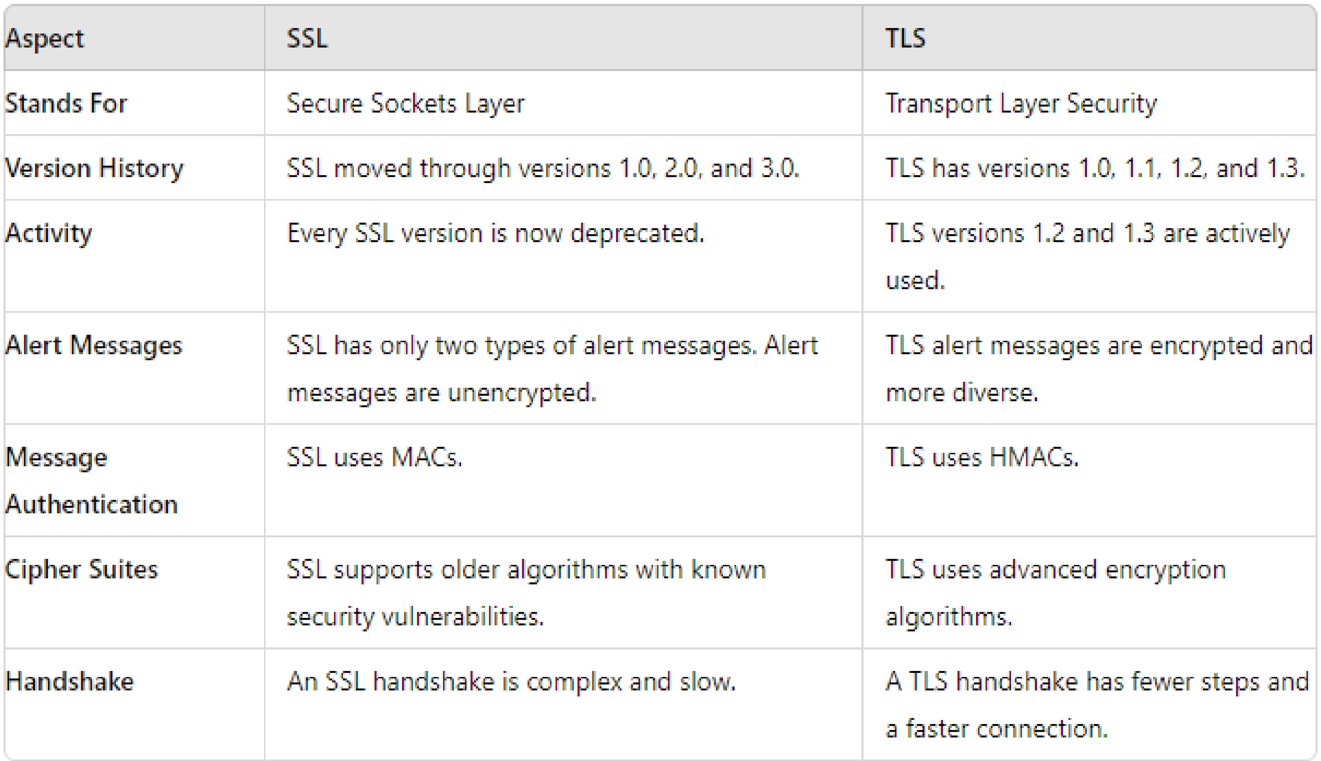
## The benefits of TLS:

1. **Encryption**: TLS uses encryption to protect the data being sent over the internet. This means that even if someone tries to intercept the data, they won't be able to read or understand it without the right decryption key.

2. **Interoperability**: TLS works with most web browsers (like Chrome, Firefox, and Internet Explorer) and is compatible with many operating systems and web servers. This widespread compatibility ensures that

users can securely access websites regardless of the software they use.

3. **Algorithm Flexibility**: TLS supports a variety of algorithms for authentication (verifying identities), encryption (securing data), and hashing (ensuring data integrity). This flexibility allows TLS to adapt to different security needs and technologies.
4. **Ease of Use**: TLS operates beneath the application layer, meaning that most of its functions are handled automatically. For users, this means that the security features of TLS are generally invisible and don't require any special action on their part.



| Aspect | SSL | TLS |
|---|---|---|
| Stands For | Secure Sockets Layer | Transport Layer Security |
| Version History | SSL moved through versions 1.0, 2.0, and 3.0. | TLS has versions 1.0, 1.1, 1.2, and 1.3. |
| Activity | Every SSL version is now deprecated. | TLS versions 1.2 and 1.3 are actively used. |
| Alert Messages | SSL has only two types of alert messages. Alert messages are unencrypted. | TLS alert messages are encrypted and more diverse. |
| Message Authentication | SSL uses MACs. | TLS uses HMACs. |
| Cipher Suites | SSL supports older algorithms with known security vulnerabilities. | TLS uses advanced encryption algorithms. |
| Handshake | An SSL handshake is complex and slow. | A TLS handshake has fewer steps and a faster connection. |

# IP Security (IPSec)

## What is IP Security?

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

IPSec enhances the protocol's security by introducing encryption and authentication. 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

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.

# Components of IP Security (IPsec):

1. **Encapsulating Security Payload (ESP)**:
    - **What It Does**: ESP makes sure that the data you send over the internet is protected in several ways:
        - **Encryption**: It scrambles the data so that only the intended recipient can read it.
        - **Data Integrity**: It ensures the data hasn't been changed during transmission.
        - **Authentication**: It verifies the sender’s identity.
        - **Anti-Replay**: It prevents attackers from capturing and replaying old messages to trick the system.
    - **How It Works**: ESP wraps the data in a secure envelope, protecting it from prying eyes and tampering.

2. **Authentication Header (AH)**:
    - **What It Does**: AH focuses on protecting the data but not encrypting it:
        - **Data Integrity**: Ensures that the data hasn't been altered.
        - **Authentication**: Verifies the sender's identity.
        - **Anti-Replay**: Prevents old messages from being reused maliciously.
    - **How It Works**: AH adds a header to the data to check that it hasn't been tampered with, but it doesn't hide the data itself.
3. **Internet Key Exchange (IKE)**:
    - **What It Does**: IKE helps set up a secure connection between two devices by exchanging encryption keys. It manages how these devices agree on security rules for communication.

## IP Security Architecture

It uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authenticity
- Integrity

The architecture is organized as follows:

1. **Architecture:** Represents the overall framework of IPsec.
2. **ESP Protocol:** Handles data confidentiality and integrity through encryption.
3. **AH Protocol:** Ensures authentication and data integrity.

4. **Encryption Algorithm:** Used by ESP to encrypt the data packet's payload.
5. **Authentication Algorithm:** Used by AH to generate a MAC for authentication and integrity verification.
6. **DOI (Data Originator Identifier):** Used to identify the source of the data packet.
7. **Key Management:** Responsible for managing the keys used for encryption and authentication.

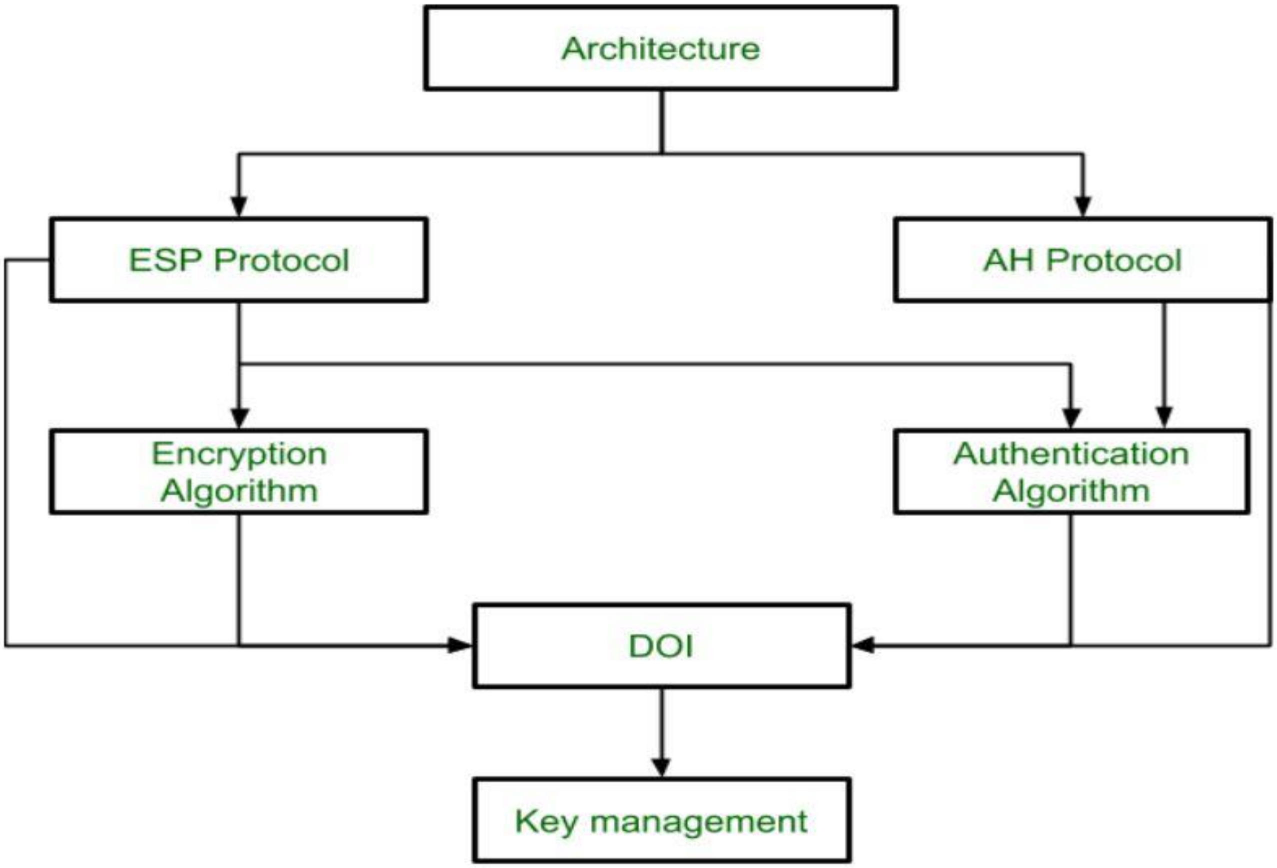


*Figure: IP Security Architecture*

## Firewalls and their types

Firewalls are essential components of network security, designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between a trusted internal network and an untrusted external network, such as the internet. Here's a breakdown of the different types of firewalls and their functions:

### Types of Firewalls

1. **Packet-Filtering Firewalls**:
   - **Function**: Examines packets of data against a set of rules and either allows or blocks them based on attributes like IP addresses, port numbers, and protocols.
   - **Pros**: Simple and efficient; has minimal impact on network performance.
   - **Cons**: Limited in functionality; cannot inspect the contents of packets for more complex threats.

2. **Stateful Inspection Firewalls**:
   - **Function**: Tracks the state of active connections and makes decisions based on the state of the connection (e.g., established, related, new).
   - **Pros**: Provides more security than packet-filtering firewalls by keeping track of connection states.
   - **Cons**: More complex than packet-filtering firewalls; still limited in examining the content of packets.
3. **Proxy Firewalls**:
   - **Function**: Acts as an intermediary between the client and the server, forwarding requests and responses on behalf of the client. It can perform deep packet inspection.
   - **Pros**: Provides strong security by hiding the internal network structure and can filter content based on specific criteria.

- **Cons**: Can introduce latency and may require significant resources.

4. **Next-Generation Firewalls (NGFW)**:
    - **Function**: Combines traditional firewall functionalities with additional features like intrusion prevention systems (IPS), deep packet inspection (DPI), and application awareness.
    - **Pros**: Offers comprehensive security by inspecting traffic at multiple levels and integrating with other security technologies.
    - **Cons**: Can be more complex and expensive to deploy and manage.
5. **Network Address Translation (NAT) Firewalls**:
    - **Function**: Hides internal IP addresses from external networks by mapping them to a single public IP address. This helps prevent external threats from targeting internal network devices directly.

- **Pros**: Provides an additional layer of security and helps manage IP address usage.
- **Cons**: May complicate certain types of network communication, like peer-to-peer applications.

6. **Unified Threat Management (UTM) Firewalls**:
    - **Function**: Integrates multiple security features, including firewall, antivirus, anti-spam, and content filtering, into a single device.
    - **Pros**: Simplifies security management by consolidating multiple functions into one device.
    - **Cons**: May not offer the same level of specialization as dedicated security devices.