

University of Technology
الجامعة التكنولوجية



Computer Sciences Department /
Network Management Branch

قسم علوم الحاسوب / فرع اداره الشبكات

Network Security II

امنيه الشبكات II

Prof. Dr. Soukaena hassan hashem

ا.د. سكينه حسن هاشم



cs.uotechnology.edu.iq

Network Security II

- Application layer security
 - Secure E-Mail
 - PGP scheme
- TCP layer Security
 - Securing TCP Connections
 - Securing Socket Layer (SSL)
- Network Layer Security
 - IPsec and Virtual Private Networks
 - The AH and ESP Protocols
 - IKE: Key Management in IPsec
- Securing Wireless LANs
 - Firewalls
 - Intrusion Detection Systems

References:

1. Computer Networking-A Top Down Approach-Kurose Ross – eighth Edition-2016

Application layer security

Secure E-Mail

PGP scheme

Application layer security

Application layer security refers to ways of protecting web applications at the application layer (layer 7 of the OSI model) from malicious attacks.

Since the application layer is the closest layer to the end user, it provides hackers with the largest threat surface. Poor app layer security can lead to performance and stability issues, data theft, and in some cases the network being taken down. Examples of application layer attacks include **distributed denial-of-service attacks (DDoS) attacks**, HTTP floods, **SQL injections**, **cross-site scripting**, parameter tampering, and Slowloris attacks. To combat these and more, most organizations have an arsenal of application layer security protections, such as **web application firewalls (WAFs)**, secure web gateway services, and others.

Secure E-Mail

Email security helps protect an organization's [attack surface](#) from cyber threats that use email account [attack vectors](#) such as [phishing](#) and spam to gain unauthorized access to the network. By following [email security best practices](#) for [cybersecurity](#) including email accounts, organizations can reduce the spread of [malware](#), such as [ransomware](#) and [viruses](#), to prevent successful [cyber attacks](#).

Email security is important because email contains sensitive information, is used by everyone in the organization, and is therefore one of a company's largest targets for attacks. The shift to cloud-based email like Gmail and others comes

with several benefits, but cloud-based email has become a tempting attack surface for cyber criminals.

How Secure Is Email?

Email is a top threat vector because it is a ubiquitous tool that everyone in an organization uses. It is in an open format that can be read on any device without decryption once it is intercepted.

An email does not go straight to the recipient. Rather, it travels between networks and servers, some vulnerable and unsecured, before landing in an inbox. Even though an individual's computer may be secure from an attacker, the network or server the email has to travel through may have been compromised. Also, cyber criminals can easily impersonate a sender or manipulate email content in the form of body copy, attachments, Uniform Resource Locators (URLs), or a sender's email address. This is fairly straightforward for a hacker attacking an unsecured system because each email has fields that contain metadata detailing information about the email, who it came from, where it is headed, etc. A hacker only needs to access this metadata and change it, and it will look like the email came from someone or someplace it did not.

Types Of Email Attacks

Cyber criminals use many different tactics to hack email, and some methods can cause considerable damage to an organization's data and/or reputation. [Malware](#), which is malicious software used to harm or manipulate a device or its data, can be placed on a computer using each of the following attacks.

A [phishing](#) attack targets users by sending them a text, direct message, or email. The attacker pretends to be a trusted individual or institution and then uses their relationship with the target to steal sensitive data like account numbers, credit card details, or login information. Phishing comes in several forms, such

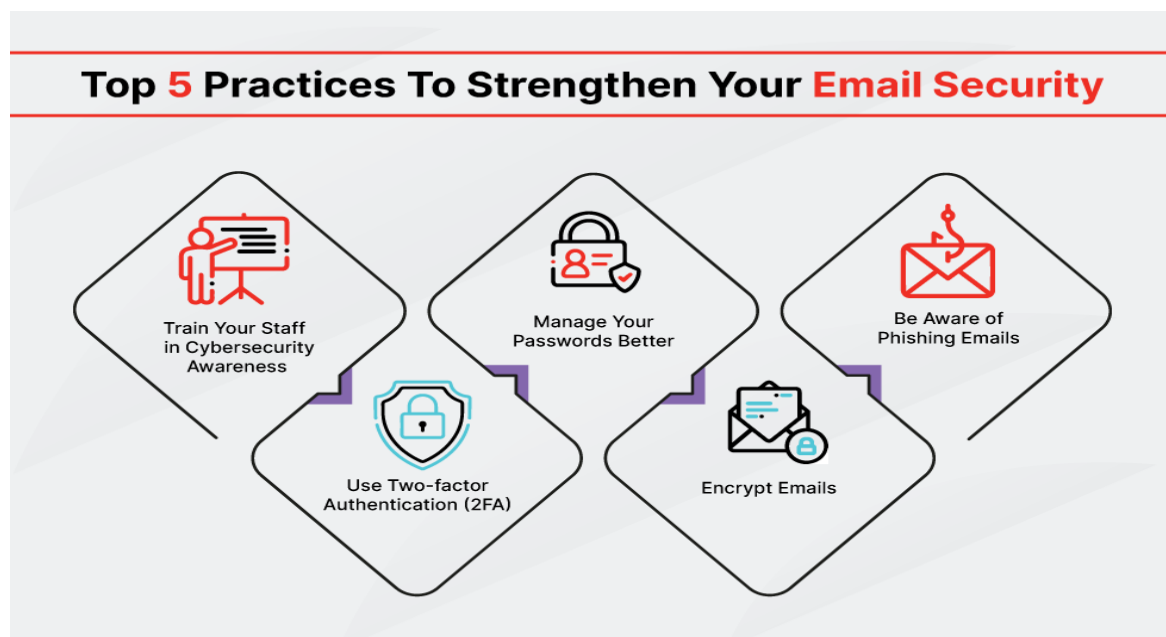
as [spear phishing](#), regular phishing, and [whaling](#). Spear phishing targets a particular person, while a whaler targets someone high up in the organization by pretending to be someone they trust.

A Spoofing is a dangerous email threat because it involves fooling the recipient into thinking the email is coming from someone other than the apparent sender. This makes [spoofing](#) an effective [business email compromise \(BEC\)](#) tool. The email platform cannot tell a faked email from a real one because it merely reads the metadata—the same data the attacker has changed. This makes the impersonation of a person the victim either knows or respects relatively easy for an attacker.

Email Security Tactics

These are the top 5 practices for strengthening email security:

1. Train staff in cybersecurity awareness
2. Use 2-factor authentication
3. Improve password management
4. Encrypt emails
5. Be aware of phishing emails



PGP scheme

Pretty Good Privacy (PGP) is a security program used to decrypt and encrypt email and authenticate email messages through digital signatures and file [encryption](#).

PGP was first designed and developed in 1991 by Paul Zimmerman, a political activist. PGP software was owned and sold by a company called PGP Corporation, which was founded in 2002 then sold to Symantec in 2010.

Email is a prime attack method for cyber criminals who can easily forge messages using a victim's name or identity. PGP aims to solve this and enhance [email security](#) by encrypting the data to make the communication method more private.

PGP was one of the first public-key cryptography software publicly available for free. Originally, it was used to enable individual users to communicate on bulletin board system computer servers. Later, it was standardized and supported by other applications such as email. It has now become a core standard in email security and has been widely used to protect individuals and organizations.

The data encryption program provides cryptographic authentication and privacy for data used in online communication. This allows PGP to be used for encrypting and decrypting text messages, emails, and files.

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to

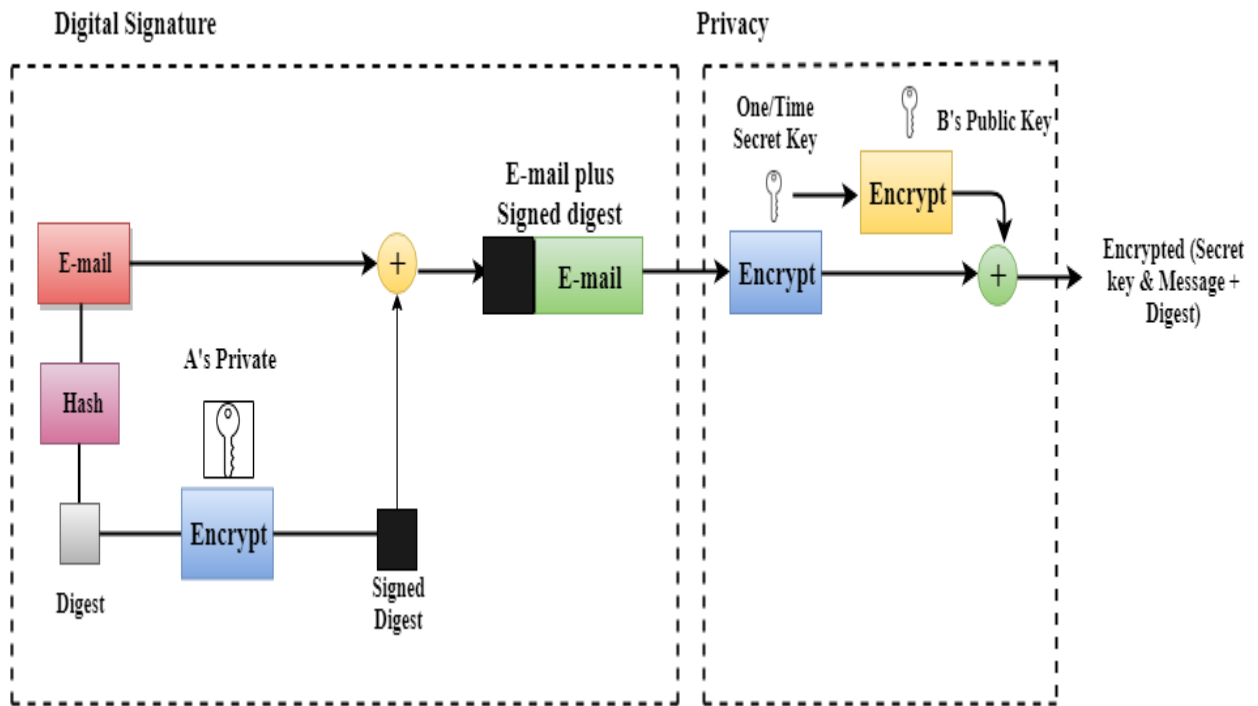
provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.

- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

Following are the steps taken by PGP to create secure e-mail at the sender site:

- The e-mail message is hashed by using a hashing function to create a digest.
- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.
- Both the encrypted secret key and the encrypted combination of message and digest are sent together.

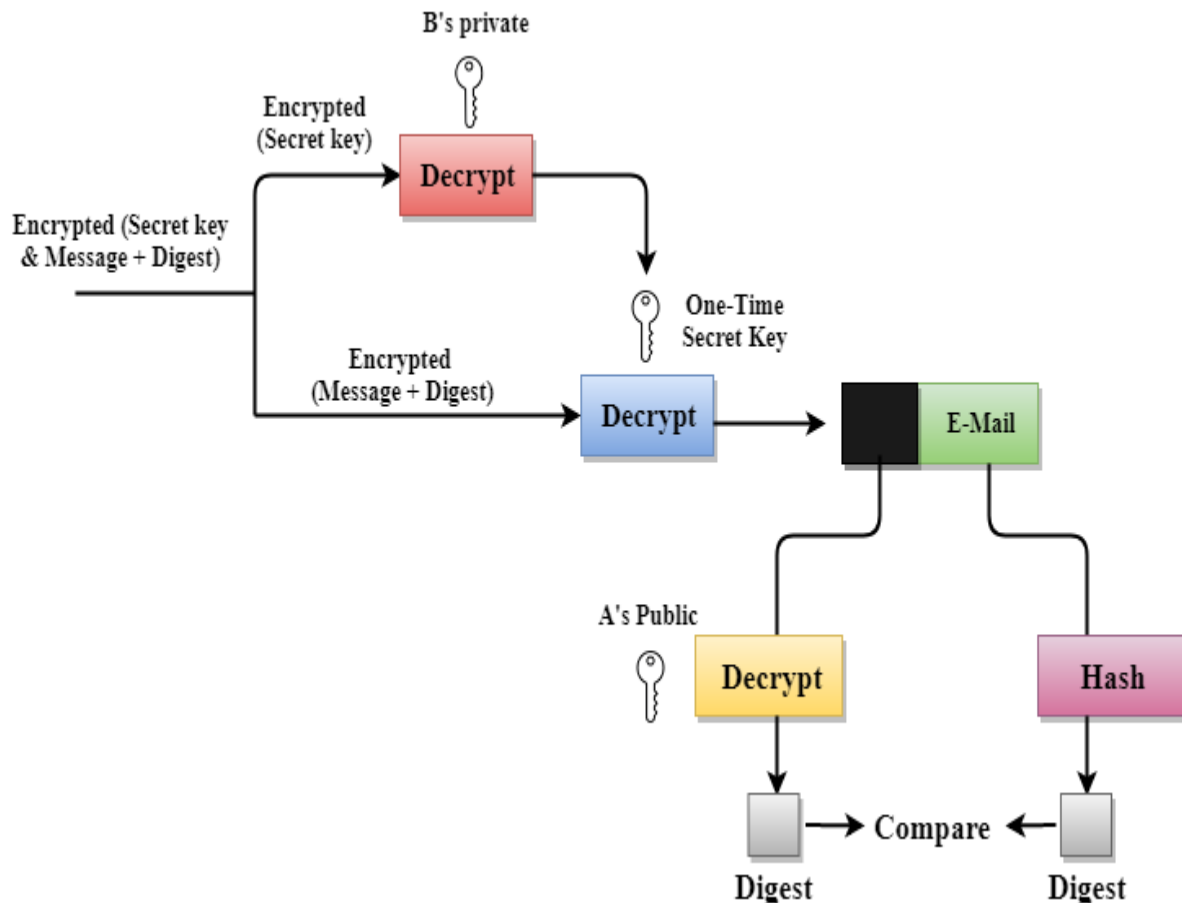
PGP at the Sender site (A)



Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

- The receiver receives the combination of encrypted secret key and message digest is received.
- The encrypted secret key is decrypted by using the receiver's private key to get the one-time secret key.
- The secret key is then used to decrypt the combination of message and digest.
- The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
- Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

PGP at the Receiver site (B)



Disadvantages of PGP Encryption

- **The Administration is difficult:** The different versions of PGP complicate the administration.
- **Compatibility issues:** Both the sender and the receiver must have compatible versions of PGP. For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.
- **Complexity:** PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.

- **No Recovery:** Computer administrators face the problems of losing their passwords. In such situations, an administrator should use a special program to retrieve passwords. For example, a technician has physical access to a PC which can be used to retrieve a password. However, PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.

TCP layer Security

Securing TCP Connections

Securing Socket Layer (SSL)

TCP layer Security

Transport layer security (TLS) is a critical feature that's essential to securing the internet's infrastructure. Learn how the TLS protocol works and how it helps to keep your connection safe wherever you go online. Then, get a VPN from the industry leaders in cybersecurity to help you protect your personal data and access the content you love.

What is transport layer security and what does it do?

Transport layer security (TLS) is a security protocol that encrypts data sent over a network like the internet — typically between a client device, such as a computer or smartphone, and a web server that hosts the content that device is accessing.

As well as connections between [web browsers](#) and websites, common examples of TLS implementation include internet applications like email and instant messaging, and VoIP (Voice over Internet Protocol) telephony.

TLS has become one of the [Internet Engineering Task Force's \(IETF\)](#) standard security protocols. It contains advanced, integrated encryption algorithms that provide an extra layer of security — essential for reducing the risk of [hackers](#) and [malware](#) hijacking connections between online devices.

What is datagram transport layer security (DTLS)?

Datagram transport layer security (DTLS) is a protocol based on TLS used to secure datagram-based applications, such as video conferencing, [VPNs](#), internet telephony (VoIP), and online gaming and [streaming](#).

DTLS works with the [user data protocol](#) (UDP) — which supports data transfers across networks — to provide a secure, rapid connection for live messaging and broadcasting.

So, what is the transport layer?

The transport layer is a part of networking and appears in both the OSI model (Open Systems Interconnection model) and the [TCP/IP model](#) (Transmission Control Protocol/Internet Protocol model).

In the OSI model, TLS operates on four layers: Application, Presentation, Session, and Transport; in the TCP/IP model, it operates only on the Transport layer.

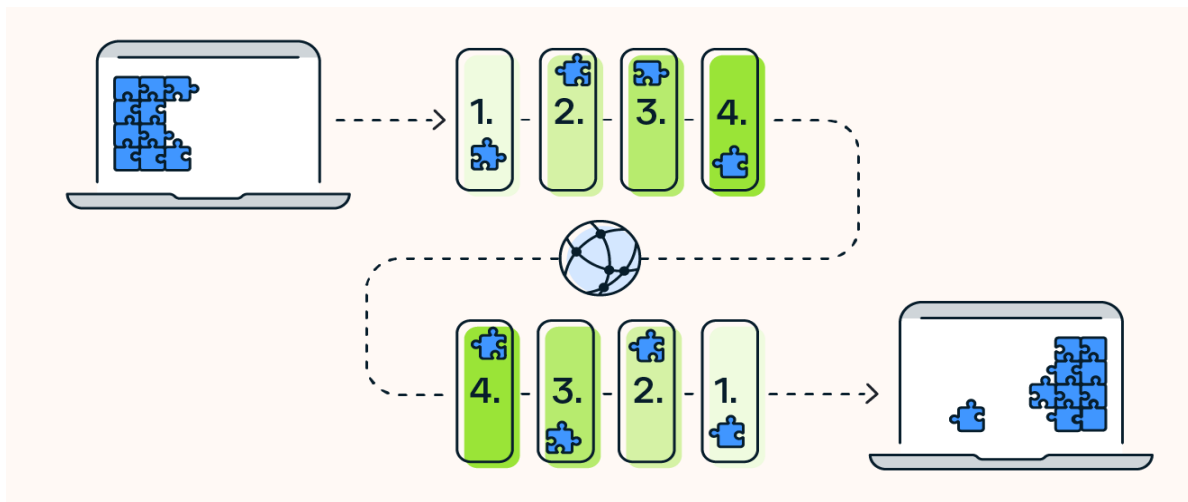
The OSI model is a framework that represents the following network communication methods:

- **Application:** Provides access to a network (e.g., a browser), including the internet.

- **Presentation:** Defines data type and formatting, alongside [encryption](#) capabilities.
- **Session:** Establishes a channel of communication between devices, manages the duration of sessions, and terminates sessions when applicable.
- **Transport:** Processes messages within the end-to-end connection.
- **Network:** Moves data packets and reassembles them when they reach their destination.
- **Data link:** Takes data packets from the network layer and puts them into individual frames, which are sent from one device to another.
- **Physical:** Transmits raw data (known as data bits) and handles the speed at which they are managed.

The TCP/IP model is a set of rules that enable computers to connect to the internet and other networks.

- **Application:** The user interface, like a browser or other web-enabled application.
- **Transport:** Ensures a reliable connection between devices.
- **Internet:** Also known as the network layer, it controls the movement of network data packets.
- **Data link:** Handles the physical parts of data movement.



The TCP/IP model splits data into packets and delivers it through 4 different layers.

What is the difference between SSL and TLS?

The purpose of [Secure Sockets Layer \(SSL\)](#) and TLS is the same: to establish a secure network connection between two computer systems online. TLS is the successor to SSL, and it was developed to fix vulnerabilities in SSL by using more advanced [cryptography](#).

- **Secure Sockets Layer (SSL)** was the first cryptographic protocol to authenticate and exchange data between client devices, applications, and servers. SSL had three versions (1.0, 2.0, and 3.0), although the first was never publicly released due to security flaws. All versions have now been deprecated, but some websites continue to use SSL.
- **Transport layer security (TLS)** offers higher levels of security. TLS 1.0 was established in 1999, TLS 1.1 in 2006, and TLS 1.2 in 2008. TLS 1.3 was released in 2018 and is now used by most websites. TLS uses 256-bit AES encryption, which is harder to decipher than other algorithms like RSA encryption, which early SSL versions used.

What is a TLS certificate?

A TLS certificate, still commonly called an SSL/TLS certificate, is a data file that certifies the ownership of a public key. It lets [web browsers](#) identify that it's

safe to establish a connection to websites. TLS certificates form part of the authentication process between a client device (like your computer or phone) and the server that stores and delivers the content you're accessing.

Individuals and organizations providing websites and apps for public use must obtain an SSL/TLS certificate from an approved certificate authority, such as IdenTrust, DigiCert, or Sectigo.

An SSL/TLS certificate contains the following information:

- Domain name
- SSL/TLS version
- Issue date and expiration date
- Server public key information
- Issuing certification authority and digital signature

What is the difference between TLS and HTTPS?

TLS and HTTPS are both protocols. HTTP (Hypertext Transfer Protocol) allows a connection between an internet browser and a web server, while TLS and SSL are encryption protocols. When TLS or SSL is added on top of HTTP, this is known as HTTPS (Hypertext Transfer Protocol Secure).

Put simply, **the 'S' part of HTTPS refers to SSL/TLS**. HTTPS websites encrypt the data sent between your device and the web server, which is why you shouldn't use HTTP sites for making purchases or entering other sensitive data.

How does TLS work?

TLS works by establishing a secure connection between a client device like your computer or phone and a web server that holds the content you're accessing. TLS authenticates a connection before encrypting the data that travels over that connection.

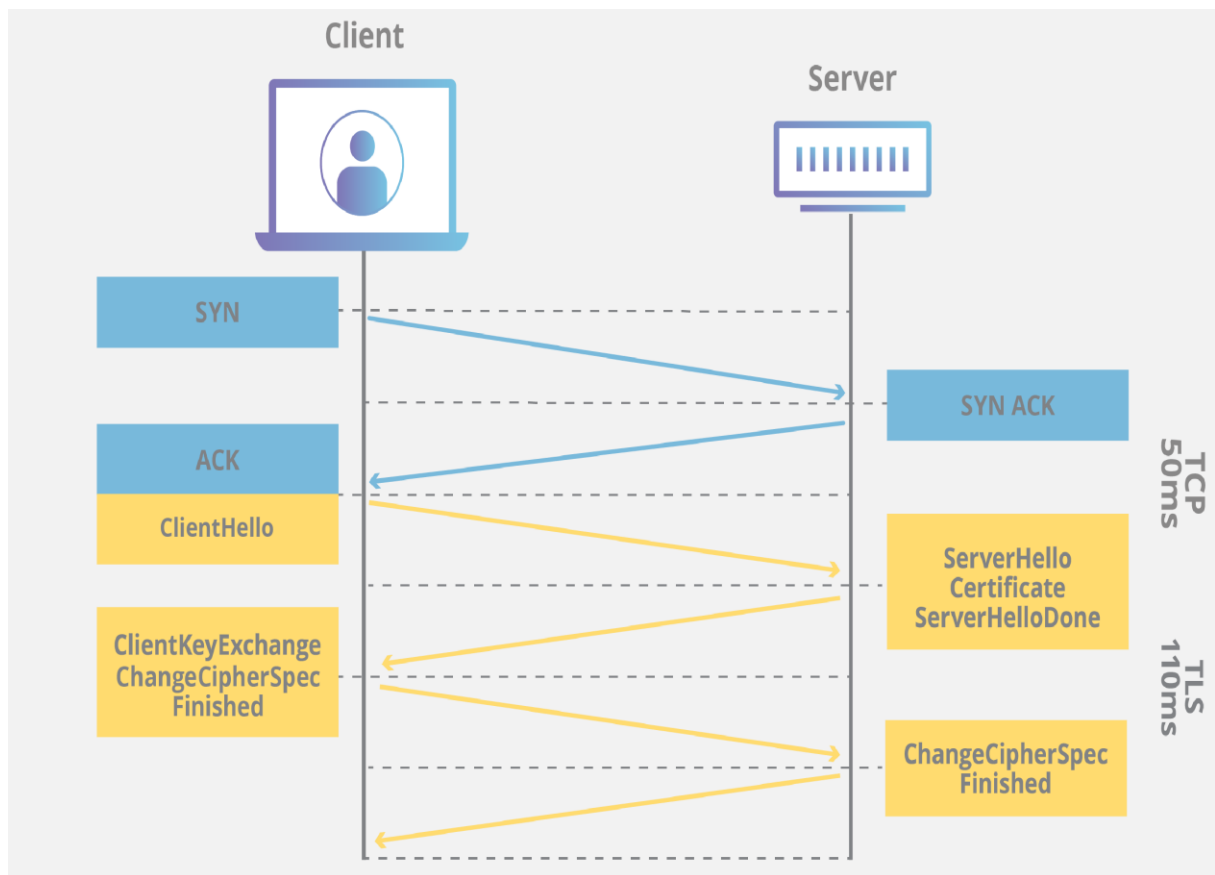
To understand how TLS authenticates connections, you need to understand the handshake protocol, which is an important part of how cryptography secures communications.

How is a TLS handshake done?

The TLS “handshake” establishes an authenticated connection between a client device and a server. Here’s how the TLS handshake works:

1. The client device sends an initial message (**Client Hello**) to the destination server. It includes the version of TLS it supports as well as the cryptographic algorithms it supports (cipher suite).
2. The server responds with a **Server Hello** message that includes its corresponding certificate with its public key.
3. The client device verifies the server’s **TLS certificate**.
4. The client device then **creates a pre-master secret** that’s encrypted using the public key.
5. The server **decrypts the pre-master secret** with its own private key.
6. Both the client device and server confirm that the process has been completed and have a **symmetric (master) key** that can now be used for encryption and decryption.

So while the handshake uses asymmetric encryption, once the process is complete, symmetric encryption is used to send data safely and securely.



The pros and cons of TLS technology

TLS is certainly a big improvement over legacy web encryption protocols, but it's not perfect. Here's a summary of the main advantages and disadvantages of TLS technology:

Pros

- **End-to-end encryption:** Sensitive data can be sent securely to the intended device or user.
- **Trusted:** An HTTPS website secured by TLS is recognized to be safer by users when browsing, allowing them to choose safe websites.
- **Increased control:** If there are issues in the TLS connection, users are alerted immediately.
- **Reduction in MITM attacks:** TLS helps to prevent man-in-the-middle attacks and potential [data breaches](#) as a result.

Cons

- **Incompatibility:** Some older versions of TLS, such as TLS 1.0 or TLS 1.1, are no longer supported by common applications, and some servers can't yet support TLS 1.3.

Transport Layer Security (TLS) is designed to provide security at the transport layer. TLS was derived from a security protocol called [Secure Socket Layer \(SSL\)](#). TLS ensures that no third party may eavesdrop or tamper with any message. There are several benefits of TLS:

Encryption:

TLS/SSL can help to secure transmitted data using encryption.

- **Interoperability:**
TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Securing TCP Connections

What are the best TCP connection security practices?

2. [Use encryption](#)
3. [Implement firewalls](#)
4. [Use strong authentication](#)

5. [Apply patches and updates](#)
6. [Monitor and audit](#)

TCP, or Transmission Control Protocol, is a widely used protocol for reliable and ordered data transmission over the internet. However, TCP connections are also vulnerable to various attacks, such as SYN flooding, session hijacking, and data tampering. Therefore, it is essential to apply some best practices to secure your TCP connections and protect your network. In this article, we will discuss some of the best TCP connection security practices that you can implement to enhance your network security.

1. Use encryption

One of the most basic and effective ways to secure your TCP connections is to use encryption. Encryption is the process of transforming data into an unreadable form that can only be decoded by authorized parties. Encryption can prevent attackers from eavesdropping, intercepting, or modifying your data in transit. You can use encryption protocols such as SSL/TLS, SSH, or IPsec to encrypt your TCP connections and ensure data confidentiality, integrity, and authenticity.

2. Implement firewalls

Another important practice to secure your TCP connections is to implement firewalls. Firewalls are devices or software that monitor and filter the incoming and outgoing network traffic based on predefined rules. Firewalls can block or allow TCP connections based on criteria such as source and destination IP addresses, ports, protocols, or application signatures. Firewalls can help you prevent unauthorized access, limit network exposure, and mitigate network attacks such as SYN flooding or port scanning.

3. Use strong authentication

A third practice to secure your TCP connections is to use strong authentication. Authentication is the process of verifying the identity of the parties involved in a

TCP connection. Authentication can prevent attackers from impersonating legitimate users or servers and gaining unauthorized access to your network resources or data. You can use authentication methods such as passwords, certificates, tokens, or biometrics to authenticate your TCP connections and ensure data authorization and accountability.

4. Apply patches and updates

A fourth practice to secure your TCP connections is to apply patches and updates regularly. Patches and updates are software fixes that address bugs, vulnerabilities, or performance issues in your operating systems, applications, or network devices. Patches and updates can help you improve the security, stability, and functionality of your TCP connections and prevent attackers from exploiting known or unknown flaws in your software. You should always keep your software up to date and install patches and updates as soon as they are available.

5. Monitor and audit

fifth practice to secure your TCP connections is to monitor and audit them constantly. Monitoring and auditing are the processes of collecting, analyzing, and reporting on the performance, behavior, and activity of your TCP connections. Monitoring and auditing can help you detect and respond to anomalies, incidents, or breaches in your network security. You can use tools such as network analyzers, intrusion detection systems, or log management systems to monitor and audit your TCP connections and ensure data availability and compliance.

Securing 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. In this article, we are going to discuss SSL in detail, its protocols, the silent features of SSL, and the version of SSL.

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.

Why is SSL Important?

Originally, data on the web was transmitted in plaintext, making it easy for anyone who intercepted the message to read it. For example, if someone logged into their email account, their username and password would travel across the Internet unprotected.

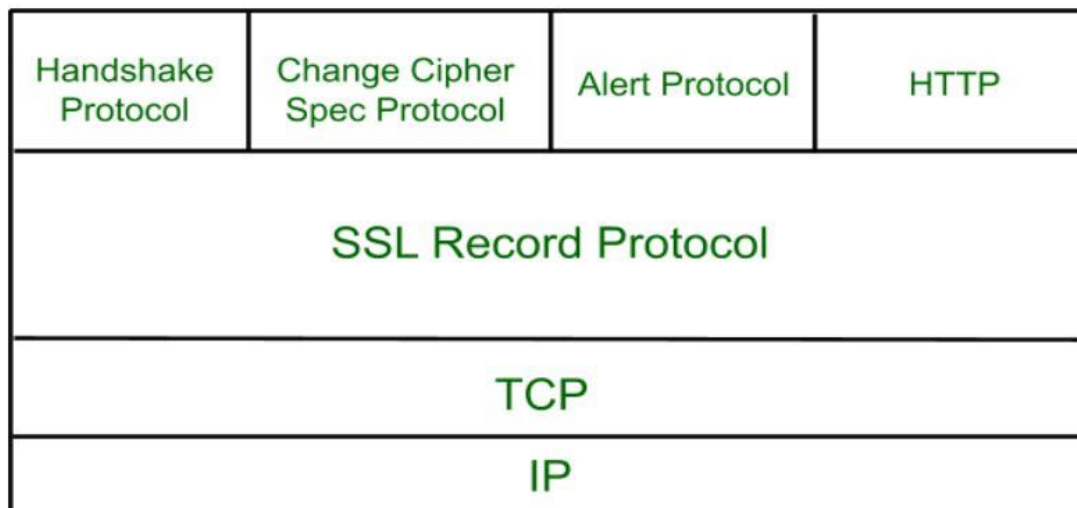
SSL was created to solve this problem and protect user privacy. By encrypting data between a user and a web server, SSL ensures that anyone who intercepts the data sees only a scrambled mess of characters. This keeps the user's login credentials safe, visible only to the email service.

Additionally, SSL helps prevent cyber attacks by:

- **Authenticating Web Servers:** Ensuring that users are connecting to the legitimate website, not a fake one set up by attackers.
- **Preventing Data Tampering:** Acting like a tamper-proof seal, SSL ensures that the data sent and received hasn't been altered during transit.

Secure Socket Layer Protocols

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

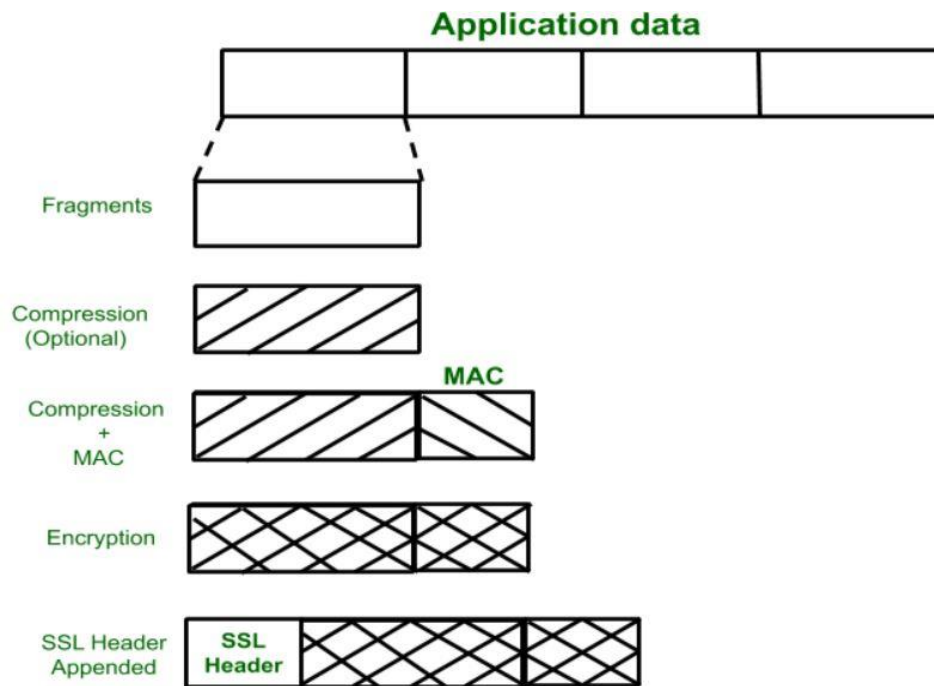


SSL Record Protocol

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

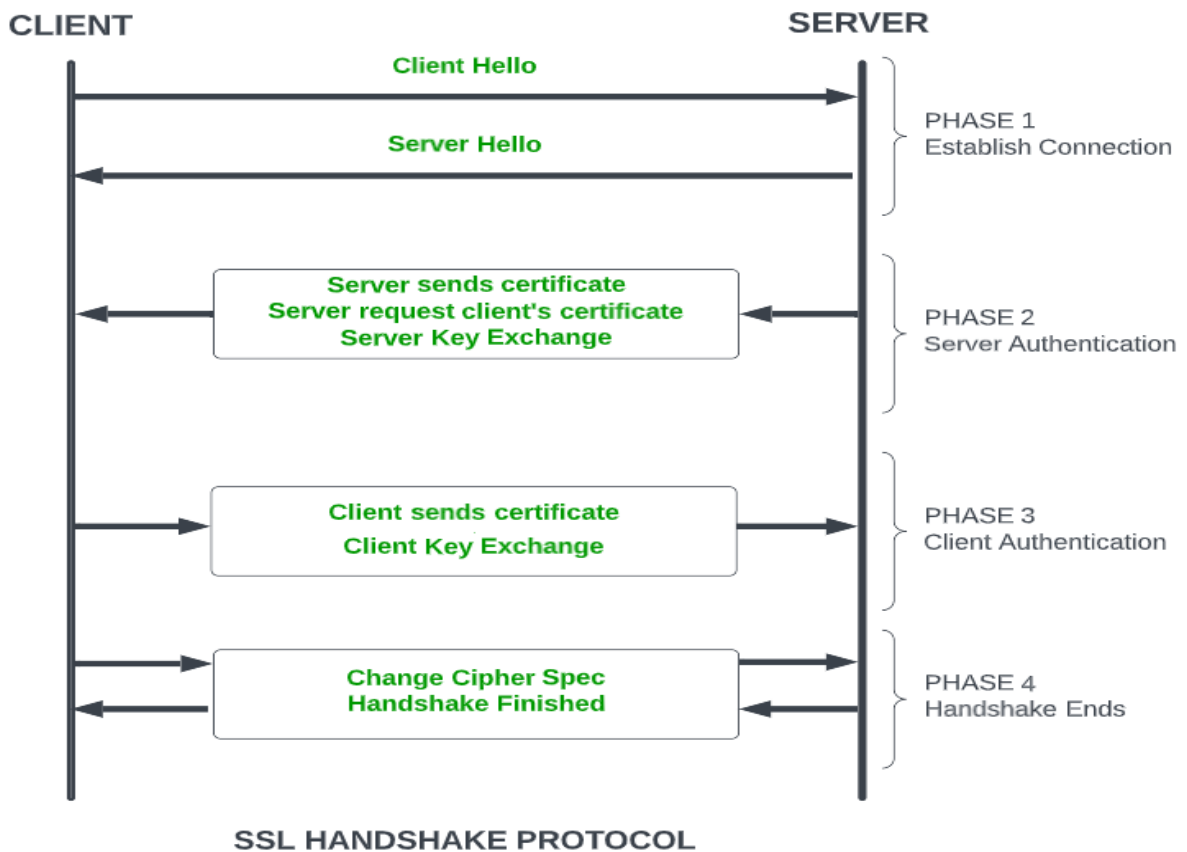
In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA ([Secure Hash Protocol](#)) and MD5 ([Message Digest](#)) is appended. After that encryption of the data is done and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



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.



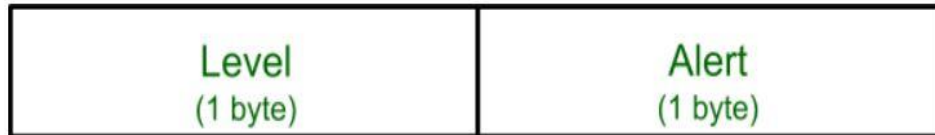
Change-Cipher Protocol

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.



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.
- **Certificate Revoked:** The certificate received is in revocation list.

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.

Salient Features of Secure Socket Layer

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is a two-layered protocol.

Versions of SSL

SSL 1 – Never released due to high insecurity

SSL 2 – Released in 1995

SSL 3 – Released in 1996

TLS 1.0 – Released in 1999

TLS 1.1 – Released in 2006

TLS 1.2 – Released in 2008

TLS 1.3 – Released in 2018

SSL Certificate

SSL (Secure Sockets Layer) certificate is a digital certificate used to secure and verify the identity of a website or an online service. The certificate is issued by a trusted third-party called a Certificate Authority (CA), who verifies the identity of the website or service before issuing the certificate.

The SSL certificate has several important characteristics that make it a reliable solution for securing online transactions:

- **Encryption:** The SSL certificate uses encryption algorithms to secure the communication between the website or service and its users. This ensures that the sensitive information, such as login credentials and credit card information, is protected from being intercepted and read by unauthorized parties.
- **Authentication:** The SSL certificate verifies the identity of the website or service, ensuring that users are communicating with the intended party

and not with an impostor. This provides assurance to users that their information is being transmitted to a trusted entity.

- **Integrity:** The SSL certificate uses message authentication codes (MACs) to detect any tampering with the data during transmission. This ensures that the data being transmitted is not modified in any way, preserving its integrity.
- **Non-repudiation:** SSL certificates provide non-repudiation of data, meaning that the recipient of the data cannot deny having received it. This is important in situations where the authenticity of the information needs to be established, such as in e-commerce transactions.
- **Public-key cryptography:** SSL certificates use public-key cryptography for secure key exchange between the client and server. This allows the client and server to securely exchange encryption keys, ensuring that the encrypted information can only be decrypted by the intended recipient.
- **Session management:** SSL certificates allow for the management of secure sessions, allowing for the resumption of secure sessions after interruption. This helps to reduce the overhead of establishing a new secure connection each time a user accesses a website or service.
- **Certificates issued by trusted CAs:** SSL certificates are issued by trusted CAs, who are responsible for verifying the identity of the website or service before issuing the certificate. This provides a high level of trust and assurance to users that the website or service they are communicating with is authentic and trustworthy.

In addition to these key characteristics, SSL certificates also come in various [levels of validation](#), including Domain Validation (DV), Organization Validation (OV), and Extended Validation (EV). The level of validation determines the amount of information that is verified by the CA before issuing the certificate, with EV certificates providing the highest level of assurance and

trust to users. For more information about SSL certificates for each Validation level type, please refer to [Namecheap](#).

Overall, the SSL certificate is an important component of online security, providing encryption, authentication, integrity, non-repudiation, and other key features that ensure the secure and reliable transmission of sensitive information over the internet.

What Are The Types of SSL Certificates?

There are different types of SSL certificates, each suited for different needs:

- **Single-Domain SSL Certificate:** This type covers only one specific domain. A domain is the name of a website, like `www.geeksforgeeks.org`. For instance, if you have a single-domain SSL certificate for `www.geeksforgeeks.org`, it won't cover any other domains or subdomains.
- **Wildcard SSL Certificate:** Similar to a single-domain certificate, but it also covers all subdomains of a single domain. For example, if you have a wildcard certificate for `*.geeksforgeeks.org`, it would cover `www.geeksforgeeks.org`, `blog.www.geeksforgeeks.org`, and any other subdomain under `example.com`.
- **Multi-Domain SSL Certificate:** This type can secure multiple unrelated domains within a single certificate.

These certificates vary in scope and flexibility, allowing website owners to choose the appropriate level of security coverage based on their needs. SSL certificates have different validation levels, which determine how thoroughly a business or organization is vetted:

- **Domain Validation (DV):** This is the simplest and least expensive level. To get a DV certificate, a business just needs to prove it owns the domain (like `www.geeksforgeeks.org`).
- **Organization Validation (OV):** This involves a more hands-on verification process. The [Certificate Authority](#) (CA) directly contacts the

organization to confirm its identity before issuing the certificate. OV certificates provide more assurance to users about the legitimacy of the organization.

- **Extended Validation (EV):** This is the most rigorous level of validation. It requires a comprehensive background check of the organization to ensure it's legitimate and trustworthy. EV certificates are recognized by the green address bar in web browsers, indicating the highest level of security and trustworthiness.

These validation levels help users understand the level of security and trust they can expect when visiting websites secured with SSL certificates.

Are SSL and TLS the Same thing?

SSL is the direct predecessor of TLS (Transport Layer Security). In 1999, the [Internet Engineering Task Force](#) (IETF) proposed an update to SSL. Since this update was developed by the IETF without Netscape's involvement, the name was changed to TLS. The changes between the last version of SSL (3.0) and the first version of TLS were not significant; the name change mainly signified new ownership. Because SSL and TLS are so similar, people often use the terms interchangeably. Some still call it SSL, while others use "SSL/TLS encryption" since SSL is still widely recognized.

SSL (Secure Sockets Layer) hasn't been updated since SSL 3.0 back in 1996 and is now considered outdated. It has known vulnerabilities, so security experts advise against using it. Most modern web browsers no longer support SSL.

TLS (Transport Layer Security) is the current encryption protocol used online. Despite this, many still refer to it as "SSL encryption," causing confusion when people look for security solutions. Nowadays, any vendor offering "SSL" is likely providing TLS protection, which has been the standard for over 20 years. The term "SSL protection" is still used widely on product pages because many users still search for it.

Network Layer Security
IPsec and Virtual Private Networks
The AH and ESP Protocols
IKE: Key Management in IPsec

Network Layer Security

Network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet because they can provide protection for many applications at once without modifying them.

In the earlier chapters, we discussed that many real-time security protocols have evolved for network security ensuring basic tenets of security such as privacy, origin authentication, message integrity, and non-repudiation.

Most of these protocols remained focused at the higher layers of the OSI protocol stack, to compensate for inherent lack of security in standard Internet Protocol. Though valuable, these methods cannot be generalized easily for use with any application. For example, SSL is developed specifically to secure applications like HTTP or FTP. But there are several other applications which also need secure communications.

This need gave rise to develop a security solution at the IP layer so that all higher-layer protocols could take advantage of it. In 1992, the Internet Engineering Task Force (IETF) began to define a standard ‘IPsec’.

In this chapter, we will discuss how security is achieved at network layer using this very popular set of protocol IPsec.

Security in Network Layer

Any scheme that is developed for providing network security needs to be implemented at some layer in protocol stack as depicted in the diagram below –

Layer	Communication Protocols	Security Protocols
Application Layer	HTTP FTP SMTP	PGP. S/MIME, HTTPS
Transport Layer	TCP /UDP	SSL, TLS, SSH
Network Layer	IP	IPsec

The popular framework developed for ensuring security at network layer is Internet Protocol Security (IPsec).

Features of IPsec

- IPsec is not designed to work only with TCP as a transport protocol. It works with UDP as well as any other protocol above IP such as ICMP, OSPF etc.
- IPsec protects the entire packet presented to IP layer including higher layer headers.
- Since higher layer headers are hidden which carry port number, traffic analysis is more difficult.
- IPsec works from one network entity to another network entity, not from application process to application process. Hence, security can be adopted without requiring changes to individual user computers/applications.
- Though widely used to provide secure communication between network entities, IPsec can provide host-to-host security as well.
- The most common use of IPsec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway).

Security Functions

The important security functions provided by the IPsec are as follows –

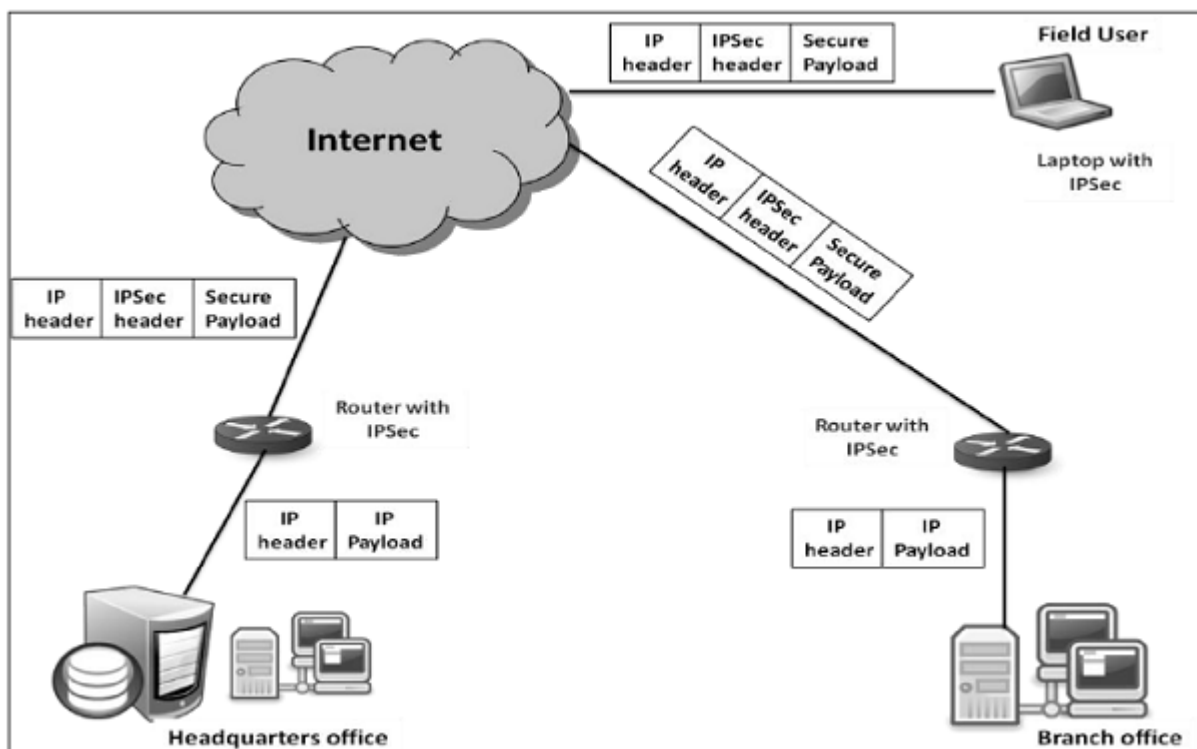
- Confidentiality
 - Enables communicating nodes to encrypt messages.
 - Prevents eavesdropping by third parties.
- Origin authentication and data integrity.

- Provides assurance that a received packet was actually transmitted by the party identified as the source in the packet header.
- Confirms that the packet has not been altered or otherwise.
- Key management.
 - Allows secure exchange of keys.
 - Protection against certain types of security attacks, such as replay attacks.

Virtual Private Network

Ideally, any institution would want its own private network for communication to ensure security. However, it may be very costly to establish and maintain such private network over geographically dispersed area. It would require to manage complex infrastructure of communication links, routers, DNS, etc.

IPsec provides an easy mechanism for implementing Virtual Private Network (VPN) for such institutions. VPN technology allows institution's inter-office traffic to be sent over public Internet by encrypting traffic before entering the public Internet and logically separating it from other traffic. The simplified working of VPN is shown in the following diagram –



Overview of IPsec

IPsec is a framework/suite of protocols for providing security at the IP layer.

In early 1990s, Internet was used by few institutions, mostly for academic purposes. But in later decades, the growth of Internet became exponential due to expansion of network and several organizations using it for communication and other purposes.

With the massive growth of Internet, combined with the inherent security weaknesses of the TCP/IP protocol, the need was felt for a technology that can provide network security on the Internet. A report entitled "Security in the Internet Architecture" was issued by the Internet Architecture Board (IAB) in 1994. It identified the key areas for security mechanisms.

The IAB included authentication and encryption as essential security features in the IPv6, the next-generation IP. Fortunately, these security capabilities were defined such that they can be implemented with both the current IPv4 and futuristic IPv6.

Security framework, IPsec has been defined in several 'Requests for comments' (RFCs). Some RFCs specify some portions of the protocol, while others address the solution as a whole.

Operations Within IPsec

The IPsec suite can be considered to have two separate operations, when performed in unison, providing a complete set of security services. These two operations are IPsec Communication and Internet Key Exchange.

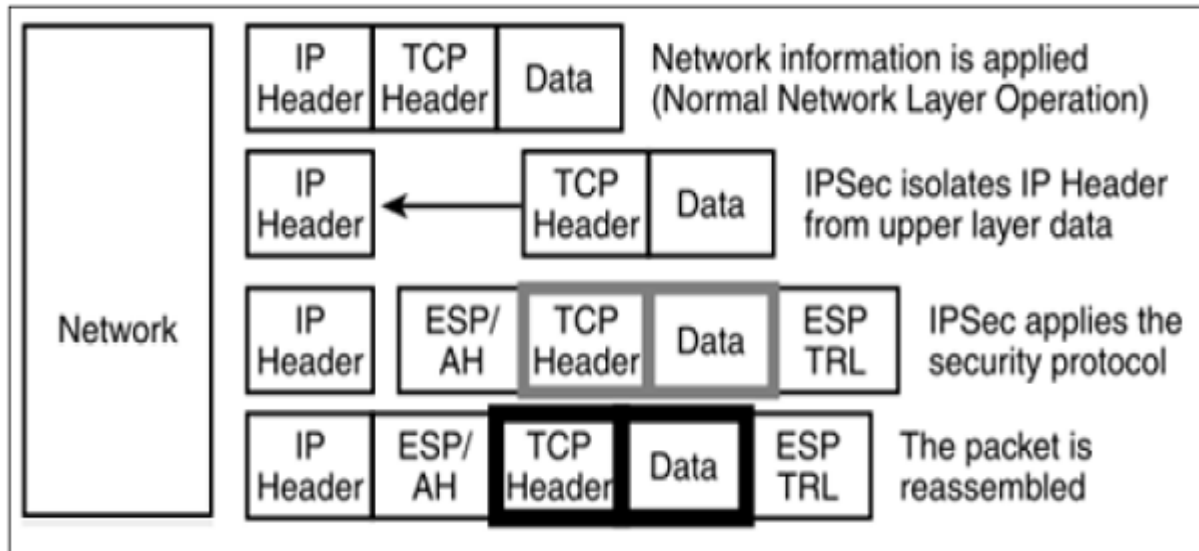
- IPsec Communication
 - It is typically associated with standard IPsec functionality. It involves encapsulation, encryption, and hashing the IP datagrams and handling all packet processes.
 - It is responsible for managing the communication according to the available Security Associations (SAs) established between communicating parties.

- It uses security protocols such as Authentication Header (AH) and Encapsulated SP (ESP).
- IPsec communication is not involved in the creation of keys or their management.
- IPsec communication operation itself is commonly referred to as IPsec.
- Internet Key Exchange (IKE)
 - IKE is the automatic key management protocol used for IPsec.
 - Technically, key management is not essential for IPsec communication and the keys can be manually managed. However, manual key management is not desirable for large networks.
 - IKE is responsible for creation of keys for IPsec and providing authentication during key establishment process. Though, IPsec can be used for any other key management protocols, IKE is used by default.
 - IKE defines two protocol (Oakley and SKEME) to be used with already defined key management framework Internet Security Association Key Management Protocol (ISAKMP).
 - ISAKMP is not IPsec specific, but provides the framework for creating SAs for any protocol.

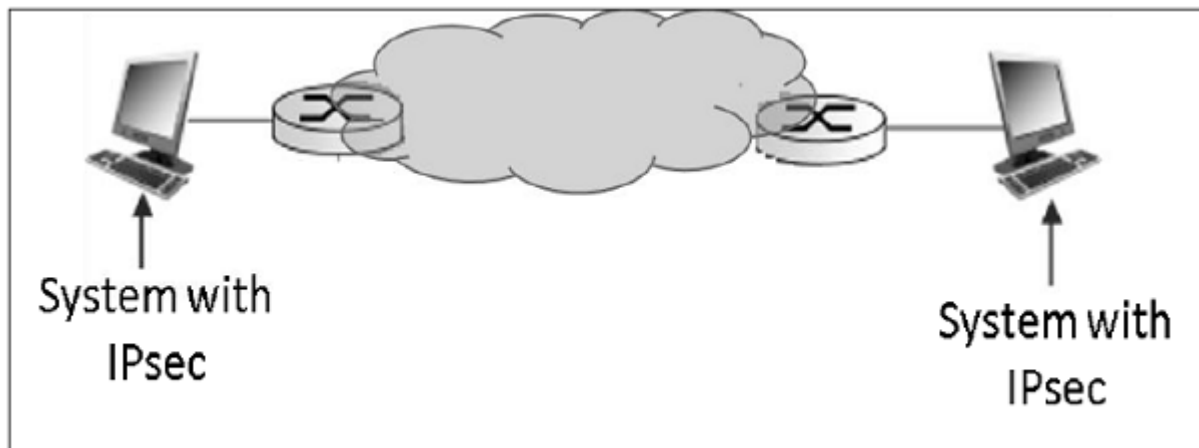
IPsec Communication has two modes of functioning; transport and tunnel modes. These modes can be used in combination or used individually depending upon the type of communication desired.

Transport Mode

- IPsec does not encapsulate a packet received from upper layer.
- The original IP header is maintained and the data is forwarded based on the original attributes set by the upper layer protocol.
- The following diagram shows the data flow in the protocol stack.

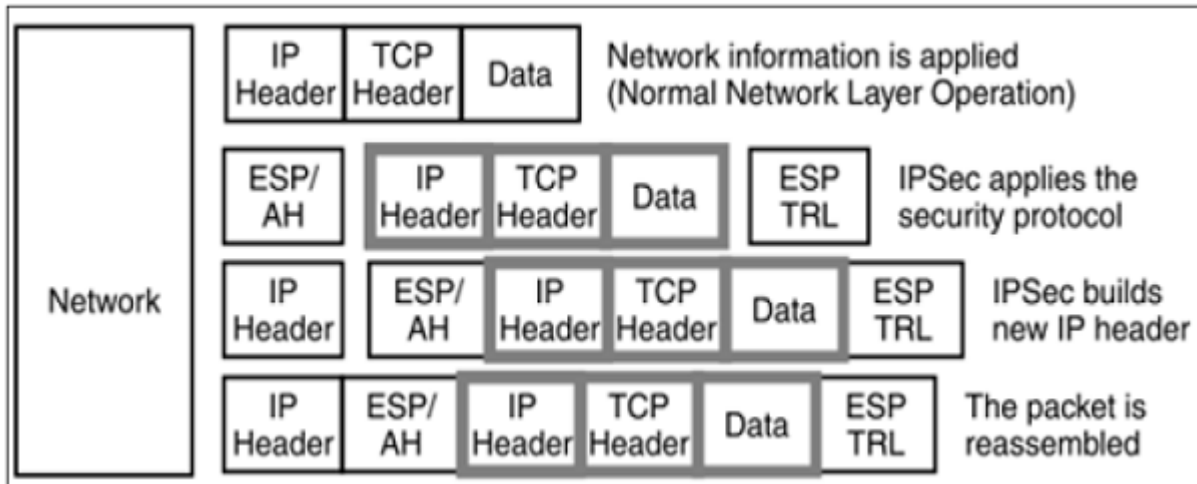


- The limitation of transport mode is that no gateway services can be provided. It is reserved for point-to-point communications as depicted in the following image.

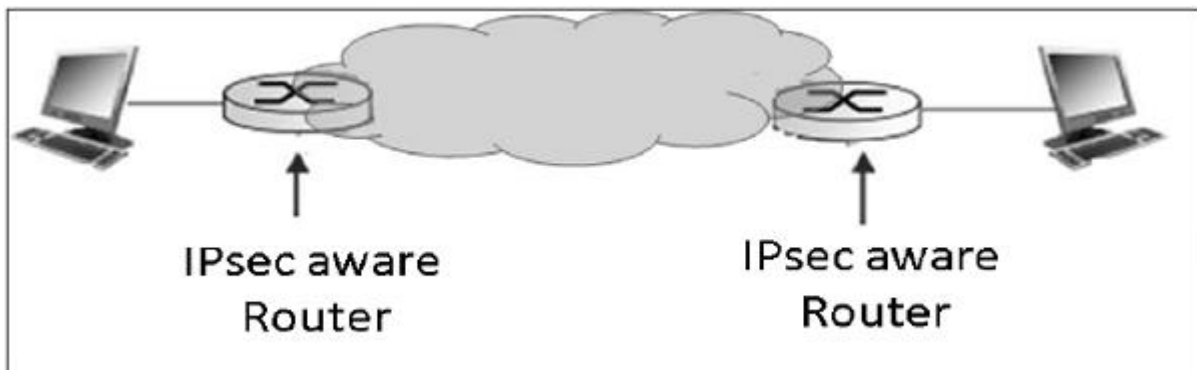


Tunnel Mode

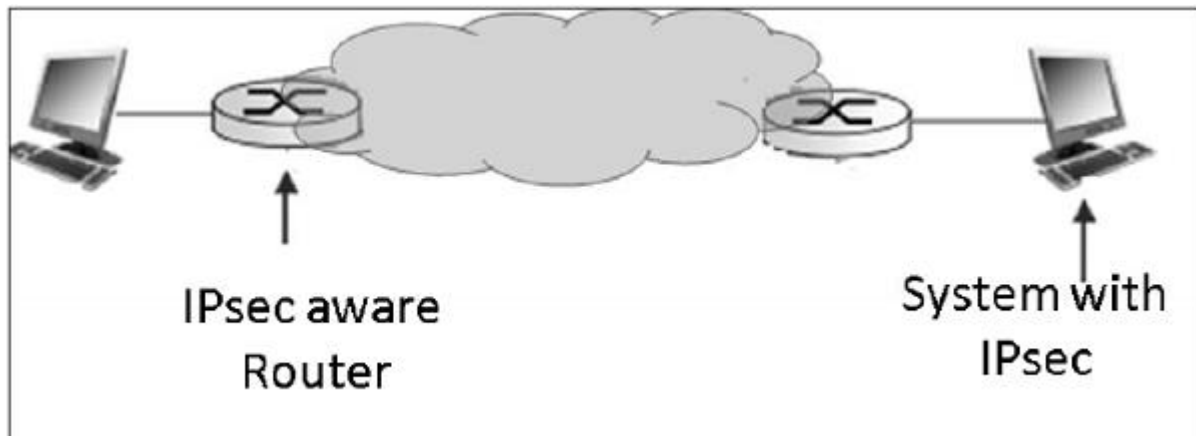
- This mode of IPsec provides encapsulation services along with other security services.
- In tunnel mode operations, the entire packet from upper layer is encapsulated before applying security protocol. New IP header is added.
- The following diagram shows the data flow in the protocol stack.



- Tunnel mode is typically associated with gateway activities. The encapsulation provides the ability to send several sessions through a single gateway.
- The typical tunnel mode communication is as depicted in the following diagram.



- As far as the endpoints are concerned, they have a direct transport layer connection. The datagram from one system forwarded to the gateway is encapsulated and then forwarded to the remote gateway. The remote associated gateway de-encapsulates the data and forwards it to the destination endpoint on the internal network.
- Using IPsec, the tunneling mode can be established between the gateway and individual end system as well.



IPsec Protocols

IPsec uses the security protocols to provide desired security services. These protocols are the heart of IPsec operations and everything else is designed to support these protocol in IPsec.

Security associations between the communicating entities are established and maintained by the security protocol used. There are two security protocols defined by IPsec — Authentication Header (AH) and Encapsulating Security Payload (ESP).

Authentication Header (AH)

The AH protocol provides service of data integrity and origin authentication. It optionally caters for message replay resistance. However, it does not provide any form of confidentiality.

AH is a protocol that provides authentication of either all or part of the contents of a datagram by the addition of a header. The header is calculated based on the values in the datagram. What parts of the datagram are used for the calculation, and where to place the header, depends on the mode cooperation (tunnel or transport).

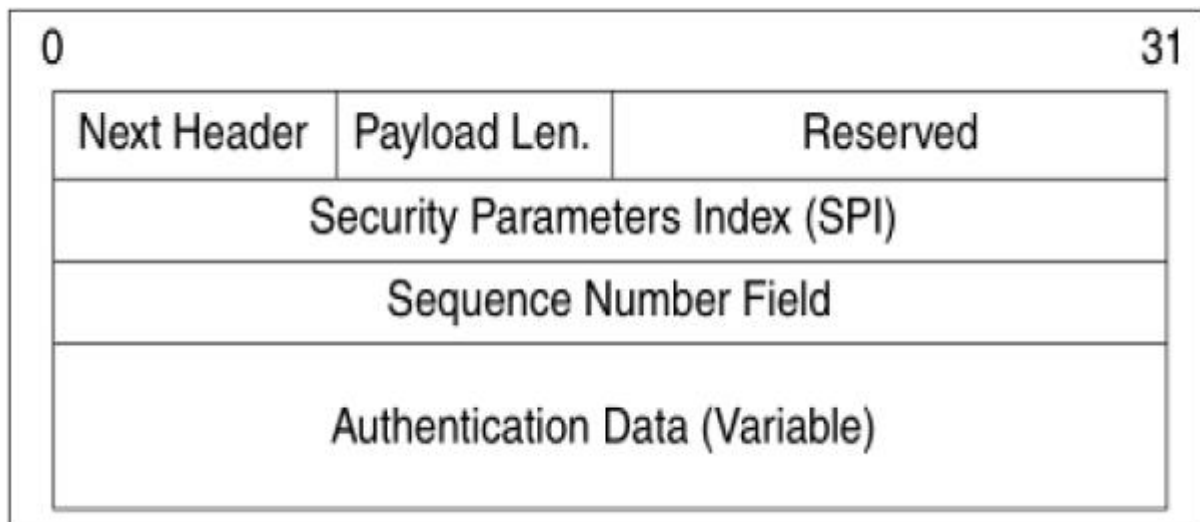
The operation of the AH protocol is surprisingly simple. It can be considered similar to the algorithms used to calculate checksums or perform CRC checks for error detection.

The concept behind AH is the same, except that instead of using a simple algorithm, AH uses special hashing algorithm and a secret key known only to

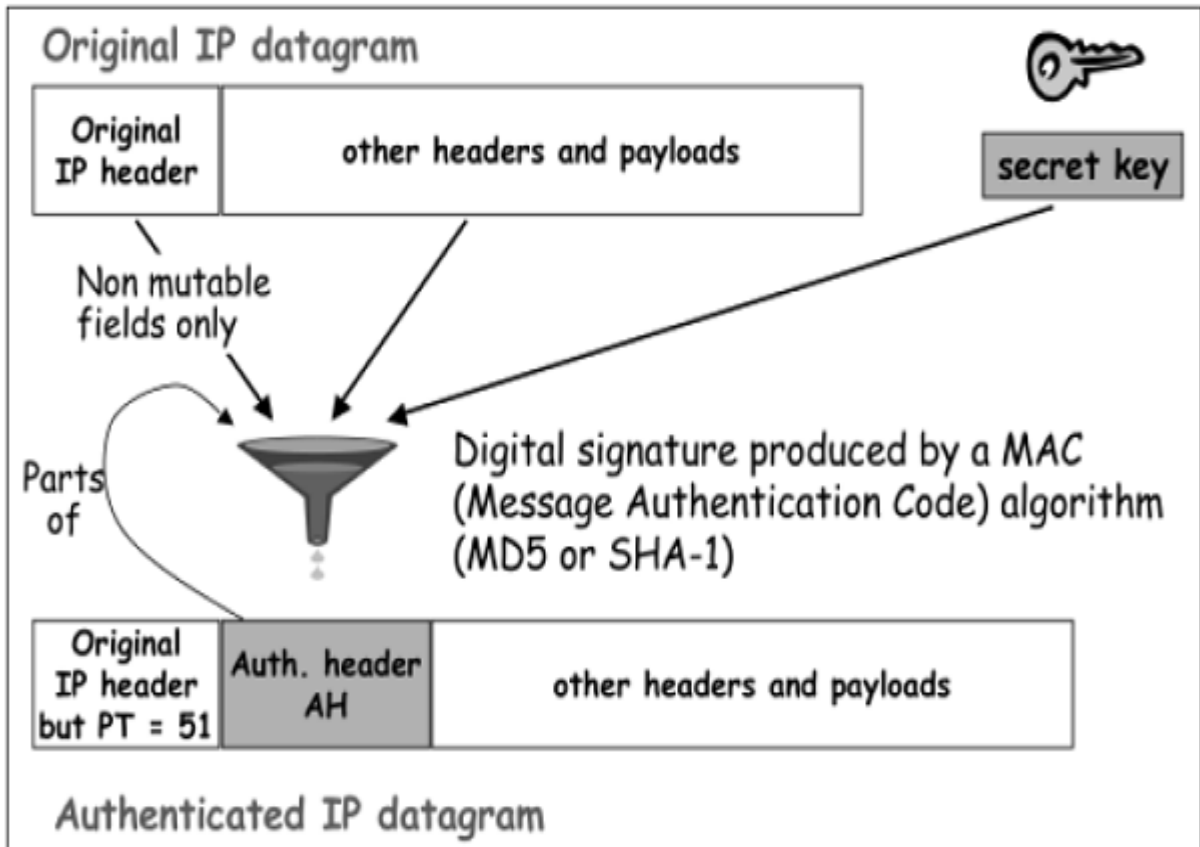
the communicating parties. A security association between two devices is set up that specifies these particulars.

The process of AH goes through the following phases.

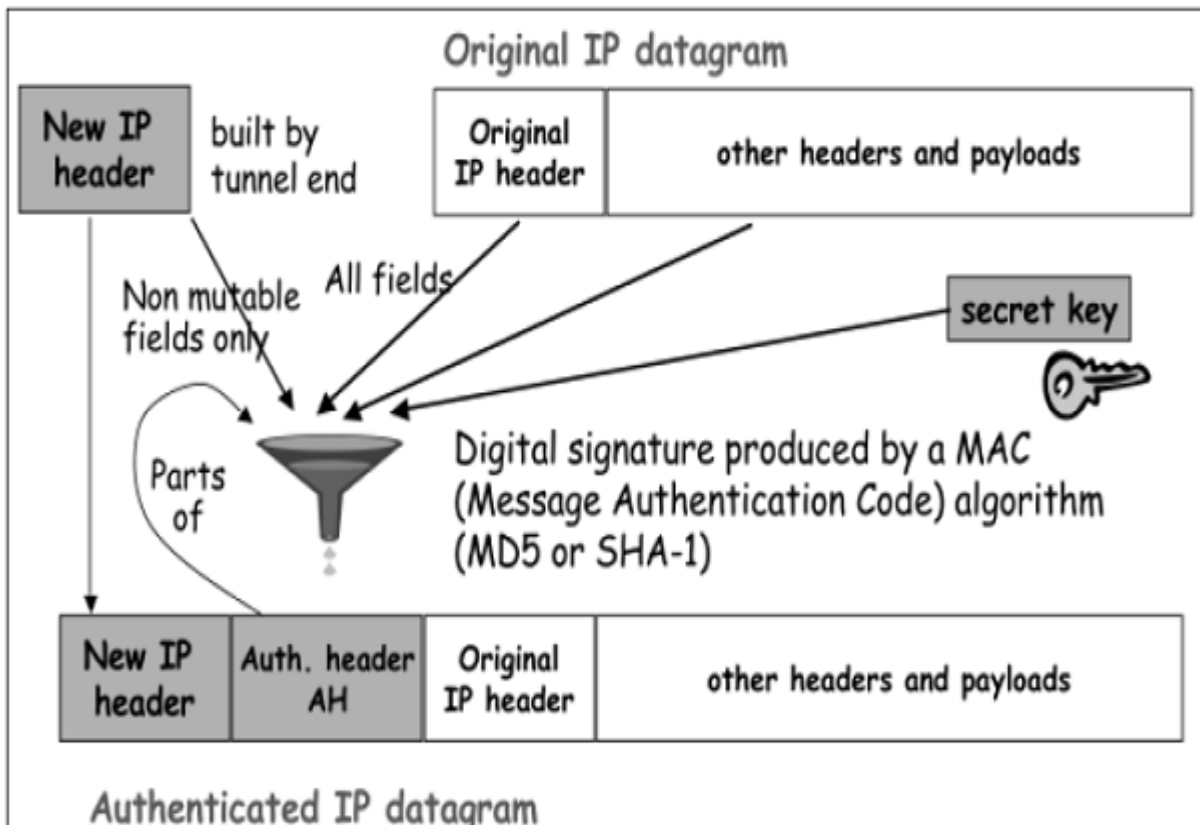
- When IP packet is received from upper protocol stack, IPsec determine the associated Security Association (SA) from available information in the packet; for example, IP address (source and destination).
- From SA, once it is identified that security protocol is AH, the parameters of AH header are calculated. The AH header consists of the following parameters –



- The header field specifies the protocol of packet following AH header. Sequence Parameter Index (SPI) is obtained from SA existing between communicating parties.
- Sequence Number is calculated and inserted. These numbers provide optional capability to AH to resist replay attack.
- Authentication data is calculated differently depending upon the communication mode.
- In transport mode, the calculation of authentication data and assembling of final IP packet for transmission is depicted in the following diagram. In original IP header, change is made only in protocol number as 51 to indicated application of AH.



- In Tunnel mode, the above process takes place as depicted in the following diagram.



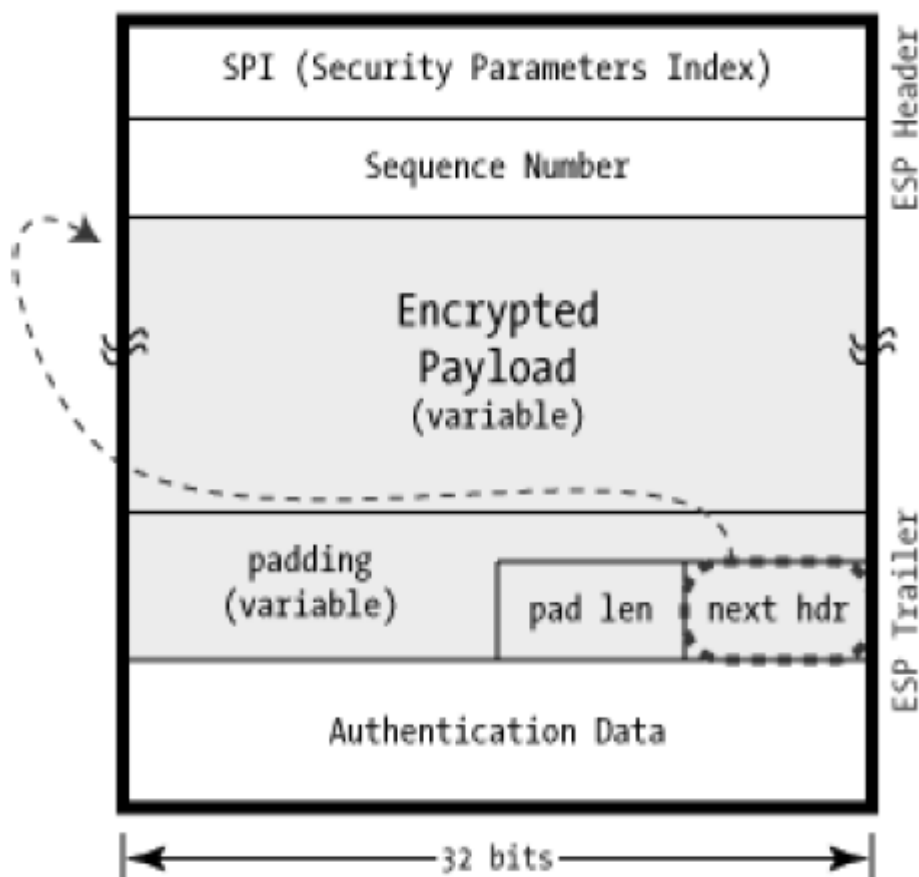
Encapsulation Security Protocol (ESP)

ESP provides security services such as confidentiality, integrity, origin authentication, and optional replay resistance. The set of services provided depends on options selected at the time of Security Association (SA) establishment.

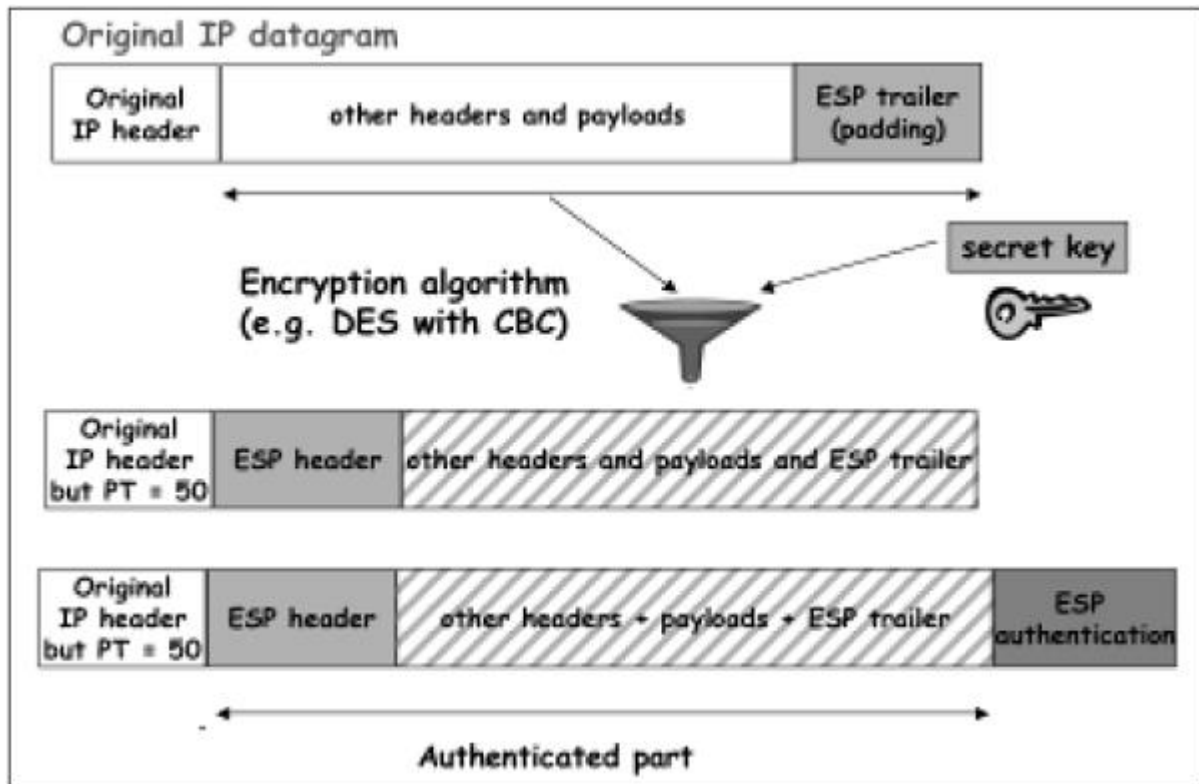
In ESP, algorithms used for encryption and generating authenticator are determined by the attributes used to create the SA.

The process of ESP is as follows. The first two steps are similar to process of AH as stated above.

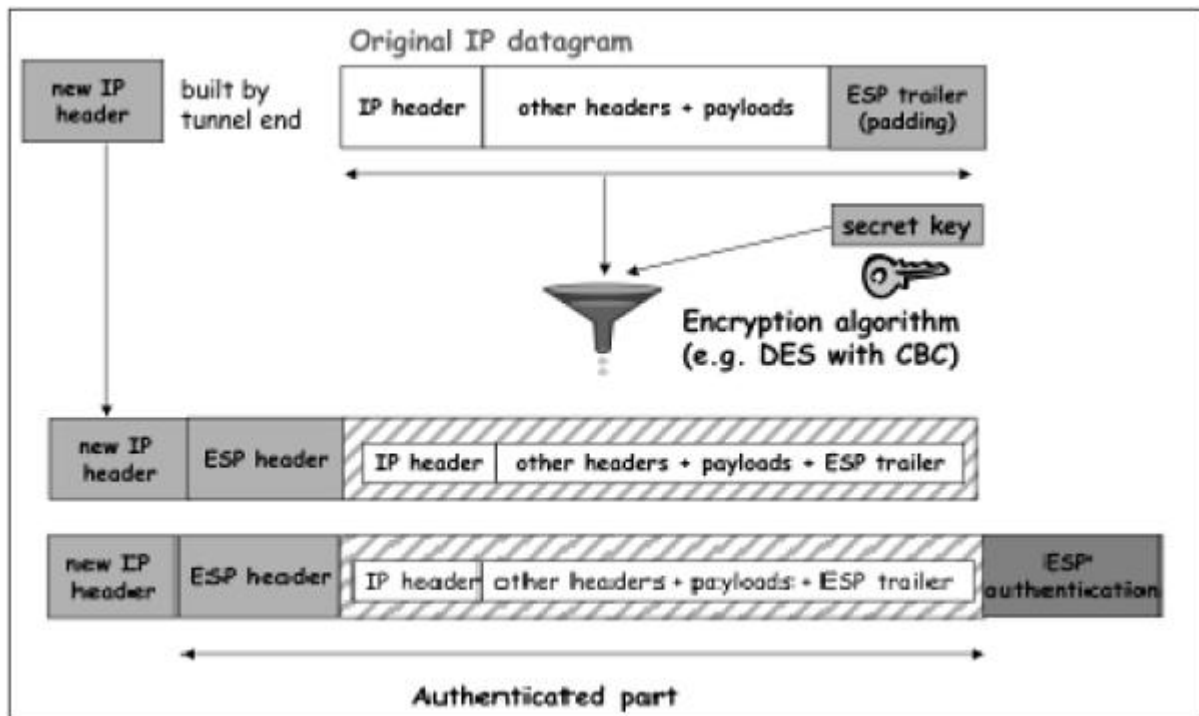
- Once it is determined that ESP is involved, the fields of ESP packet are calculated. The ESP field arrangement is depicted in the following diagram.



- Encryption and authentication process in transport mode is depicted in the following diagram.



- In case of Tunnel mode, the encryption and authentication process is as depicted in the following diagram.



Although authentication and confidentiality are the primary services provided by ESP, both are optional. Technically, we can use NULL encryption without

authentication. However, in practice, one of the two must be implemented to use ESP effectively.

The basic concept is to use ESP when one wants authentication and encryption, and to use AH when one wants extended authentication without encryption.

Security Associations in IPsec

Security Association (SA) is the foundation of an IPsec communication. The features of SA are –

- Before sending data, a virtual connection is established between the sending entity and the receiving entity, called “Security Association (SA)”.
- IPsec provides many options for performing network encryption and authentication. Each IPsec connection can provide encryption, integrity, authenticity, or all three services. When the security service is determined, the two IPsec peer entities must determine exactly which algorithms to use (for example, DES or 3DES for encryption; MD5 or SHA-1 for integrity). After deciding on the algorithms, the two devices must share session keys.
- SA is a set of above communication parameters that provides a relationship between two or more systems to build an IPsec session.
- SA is simple in nature and hence two SAs are required for bi-directional communications.
- SAs are identified by a Security Parameter Index (SPI) number that exists in the security protocol header.
- Both sending and receiving entities maintain state information about the SA. It is similar to TCP endpoints which also maintain state information. IPsec is connection-oriented like TCP.

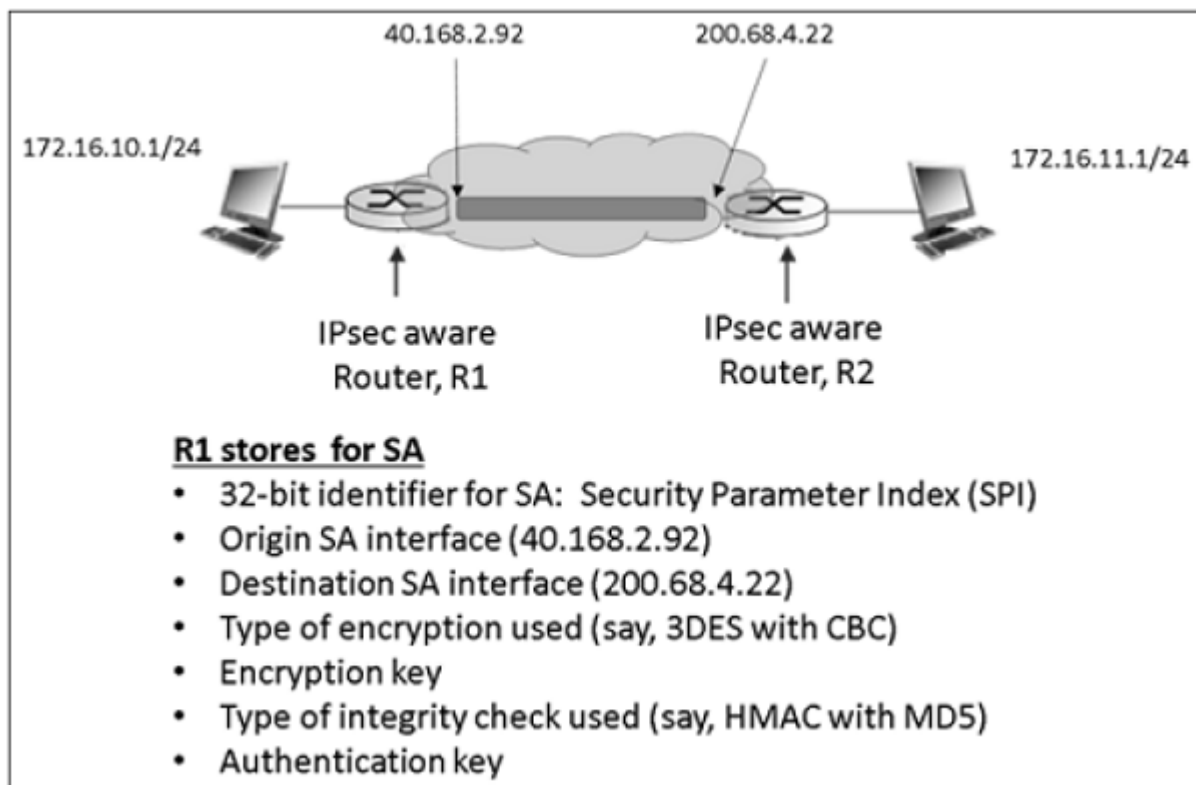
Parameters of SA

Any SA is uniquely identified by the following three parameters –

- Security Parameters Index (SPI).

- It is a 32-bit value assigned to SA. It is used to distinguish among different SAs terminating at the same destination and using the same IPsec protocol.
- Every packet of IPsec carries a header containing SPI field. The SPI is provided to map the incoming packet to an SA.
- The SPI is a random number generated by the sender to identify the SA to the recipient.
- **Destination IP Address** – It can be IP address of end router.
- **Security Protocol Identifier** – It indicates whether the association is an AH or ESP SA.

Example of SA between two router involved in IPsec communication is shown in the following diagram.



Security Administrative Databases

In IPsec, there are two databases that control the processing of IPsec datagram. One is the Security Association Database (SAD) and the other is the Security

Policy Database (SPD). Each communicating endpoint using IPsec should have a logically separate SAD and SPD.

Security Association Database

In IPsec communication, endpoint holds SA state in Security Association Database (SAD). Each SA entry in SAD database contains nine parameters as shown in the following table –

Parameters & Description

Sequence Number Counter

- 1 For outbound communications. This is the 32-bit sequence number provided in the AH or ESP headers.

Sequence Number Overflow Counter

- 2 Sets an option flag to prevent further communications utilizing the specific SA

32-bit anti-replay window

- 3 Used to determine whether an inbound AH or ESP packet is a replay

Lifetime of the SA

- 4 Time till SA remain active

Algorithm - AH

- 5 Used in the AH and the associated key

Algorithm - ESP Auth

- 6 Used in the authenticating portion of the ESP header

Algorithm - ESP Encryption

- 7 Used in the encryption of the ESP and its associated key information

IPsec mode of operation

- 8 Transport or tunnel mode

Path MTU(PMTU)

- 9 Any observed path maximum transmission unit (to avoid fragmentation)

All SA entries in the SAD are indexed by the three SA parameters: Destination IP address, Security Protocol Identifier, and SPI.

Security Policy Database

SPD is used for processing outgoing packets. It helps in deciding what SAD entries should be used. If no SAD entry exists, SPD is used to create new ones.

Any SPD entry would contain –

- Pointer to active SA held in SAD.
- Selector fields – Field in incoming packet from upper layer used to decide application of IPsec. Selectors can include source and destination address, port numbers if relevant, application IDs, protocols, etc.

Outgoing IP datagrams go from the SPD entry to the specific SA, to get encoding parameters. Incoming IPsec datagram get to the correct SA directly using the SPI/DEST IP/Protocol triple, and from there extracts the associated SAD entry.

SPD can also specify traffic that should bypass IPsec. SPD can be considered as a packet filter where the actions decided upon are the activation of SA processes.

Securing Wireless LANs

Firewalls

Intrusion Detection Systems

Securing Wireless LANs

In today's connected world, almost everyone has at least one internet-connected device. With the number of these devices on the rise, it is important to implement a security strategy to minimize their potential for exploitation (see [Securing the Internet of Things](#)). Internet-connected devices may be used by nefarious entities to collect personal information, steal identities, compromise financial data, and silently listen to—or watch—users. Taking a few precautions in the configuration and use of your devices can help prevent this type of activity.

What are the risks to your wireless network?

Whether it's a home or business network, the risks to an unsecured wireless network are the same. Some of the risks include:

Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. The typical indoor broadcast range of an access point is 150–300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could open your internet connection to many unintended users. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections available outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped

computer—sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is known as “wardriving.”

Evil Twin Attacks

In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker’s system, it’s easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

Wireless Sniffing

Many public access points are not secured and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted “in the clear,” malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers. Ensure that all the access points you connect to use at least WPA2 encryption.

Unauthorized Computer Access

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing. Ensure that when you connect your devices to public networks, you deny sharing files and folders. Only allow sharing on recognized home networks and only while it is necessary to share items. When not needed, ensure that file sharing is disabled. This will help prevent an unknown attacker from accessing your device’s files.

Shoulder Surfing

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information. Screen protectors that prevent shoulder-surfers from seeing your device screen can be purchased for little money. For smaller devices, such as phones, be cognizant of your surroundings while viewing sensitive information or entering passwords.

Theft of Mobile Devices

Not all attackers rely on gaining access to your data via wireless means. By physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts. Taking measures to protect your devices from loss or theft is important, but should the worst happen, a little preparation may protect the data inside. Most mobile devices, including laptop computers, now have the ability to fully encrypt their stored data—making devices useless to attackers who cannot provide the proper password or personal identification number (PIN). In addition to encrypting device content, it is also advisable to configure your device’s applications to request login information before allowing access to any cloud-based information. Last, individually encrypt or password-protect files that contain personal or sensitive information. This will afford yet another layer of protection in the event an attacker is able to gain access to your device.

What can you do to minimize the risks to your wireless network?

- **Change default passwords.** Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords is your first line of defense in protecting your device. (See [Choosing and Protecting Passwords](#).)

- **Restrict access.** Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the “guest” account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.
- **Encrypt the data on your network.** Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.
- **Protect your Service Set Identifier (SSID).** To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device’s SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer’s default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.
- **Install a firewall.** Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—

a host-based firewall will add a layer of protection to the data on your computer (see [Understanding Firewalls for Home and Small Office Use](#)).

- **Maintain antivirus software.** Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect against spyware and adware (see [Protecting Against Malicious Code](#) and [What is Cybersecurity?](#)).
- **Use file sharing with caution.** File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing (see [Choosing and Protecting Passwords](#)).
- **Keep your access point software patched and up to date.** The manufacturer of your wireless access point will periodically release updates to and patches for a device's software and firmware. Be sure to check the manufacturer's website regularly for any updates or patches for your device.
- **Check your internet provider's or router manufacturer's wireless security options.** Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.

Firewall Definition: What Is a Network Firewall?

A firewall is a network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules. The primary purpose of a firewall is to establish a barrier between a trusted internal network and untrusted external networks.

Firewalls come in both hardware and software forms, and they work by inspecting data packets and determining whether to allow or block them based on a set of rules. Organizations can configure these rules to permit or deny traffic based on various criteria, such as source and destination IP addresses, port numbers, and protocol type.

Understanding Firewalls and Network Security

Firewalls are the bedrock of network security, shielding the network from unauthorized access. They prevent bad actors — hackers, bots, and other threats — from overloading or infiltrating a private network to steal sensitive data.

Traditionally, firewalls regulate traffic by forming a secure perimeter around a network or computer. This prevents anyone from accessing network resources if they aren't authorized to do so. Without this protection, virtually anybody could enter and do as they please.

Today's cybersecurity landscape demands a layered approach. While firewalls remain a cornerstone of network defense, advanced threats require additional security measures. The rise of cloud computing and hybrid work environments further highlights the need for comprehensive security solutions.

Fortunately, cutting-edge firewall technologies with AI-powered services are bringing network security up to speed. Combining the strengths of traditional tools with the innovative capabilities of new solutions, modern firewall vendors help organizations defend against even the most complex attack strategies.

What Does a Firewall Do?

Firewalls protect against malicious traffic. They're strategically positioned at the network edge or in a data center, allowing them to closely monitor anything attempting to cross this boundary.

This visibility also allows a network firewall to granularly inspect and authenticate data packets in real time. This involves checking the data packet against predefined criteria to determine whether it poses a threat. If it fails to meet the criteria, the firewall blocks it from entering or leaving the network.

Firewalls regulate both inbound and outbound traffic, protecting the network from:

- **External threats** such as viruses, backdoors, phishing emails, and denial-of-service (DoS) attacks. Firewalls filter incoming traffic flows, preventing unauthorized access to sensitive data and thwarting potential malware infections.
- **Insider threats** like known bad actors or risky applications. A firewall can enforce rules and policies to restrict certain types of outgoing traffic, which helps identify suspicious activity and mitigate data exfiltration.

Firewall vs Antivirus Explained

What's the difference between firewall and antivirus software? Firewalls focus on controlling network traffic and preventing unauthorized access. By contrast, antivirus programs target and eliminate threats at the device level. More specifically, their key differences include:

- **Scope:** Antivirus software is primarily an endpoint solution, meaning it's installed on an individual device. Firewalls mainly deploy at the network level, but some organizations install hosted firewalls directly on an endpoint for extra protection.
- **Functionality:** Firewalls monitor traffic, blocking malicious data before it enters the network (or endpoint). Antivirus tools scan the local

environment for signs of malware, ransomware, and other infectious attacks.

Enterprises normally deploy both firewalls and antivirus programs. As complementary solutions, they each provide essential protective layers for safeguarding business assets.

Firewall Functions: NAT and VPN

Network Address Translation (NAT) and Virtual Private Network (VPN) are two distinct technologies, each with its own set of functions related to network security and connectivity. While NAT is primarily associated with address translation for routing purposes, VPNs are used to create secure, encrypted connections over the internet.

NAT

NAT changes the destination or source addresses of data packets as they pass through a firewall. This allows multiple devices to connect to the internet using the same IP address, which helps protect the private network from direct exposure to external threats.

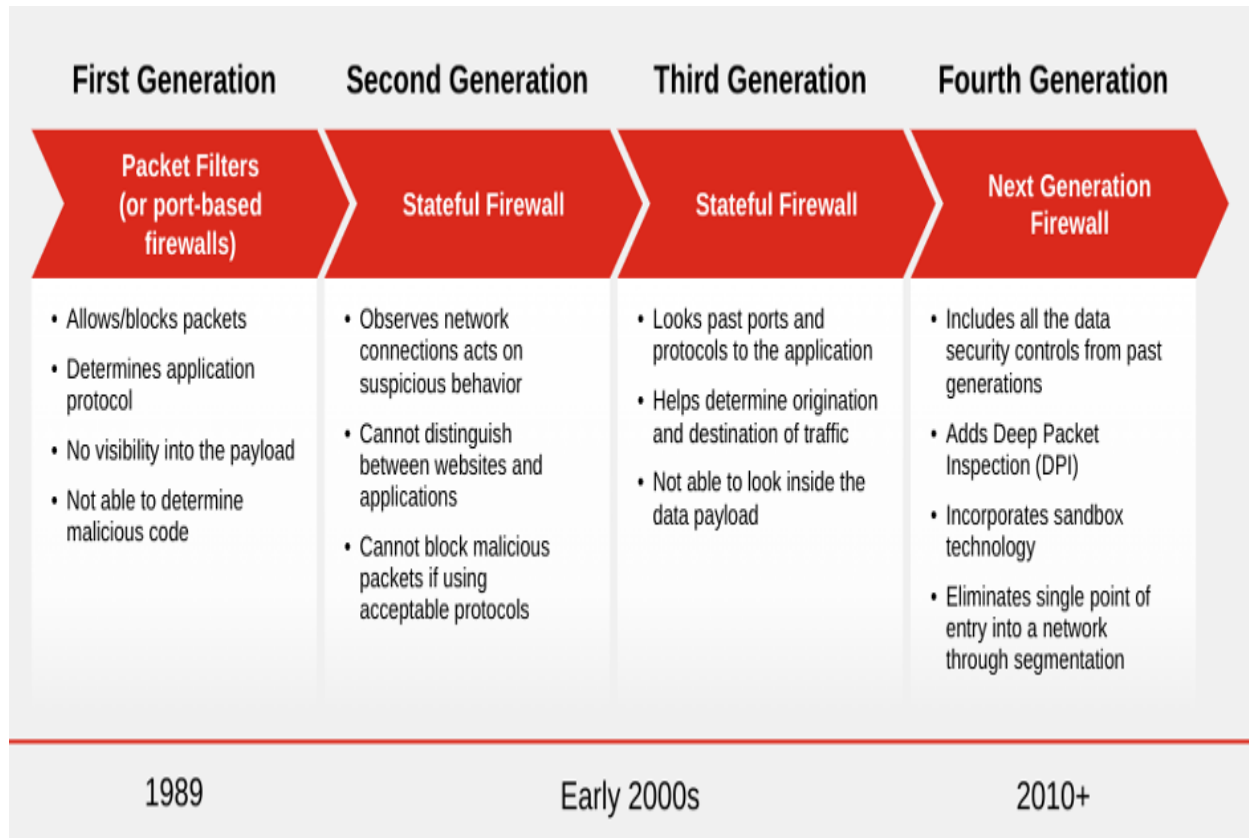
In an office environment, each employee uses their own computer or mobile device to access the internet for browsing, emailing, and accessing cloud services. Despite each device having its own private IP address within the company's internal network, all outbound traffic appears to external networks as originating from the same public IP address assigned to the company. As a result, it's harder for potential attackers to identify and target individual devices.

VPN

A VPN is a type of [proxy server](#). Therefore, it serves as a barrier between a computer or network and the internet, receiving all web requests before forwarding them to the network. VPNs are common and extend the private network across a public one, such as the internet. This allows users to securely transmit data as if their devices were directly connected to the private network.

The connection establishes an encrypted tunnel between remote devices and the corporate network, enabling secure access.

This function is especially useful in a hybrid environment. Remote employees can leverage VPNs to access corporate networks and critical applications regardless of where or how they're working.



Firewalls have evolved through four distinct phases:

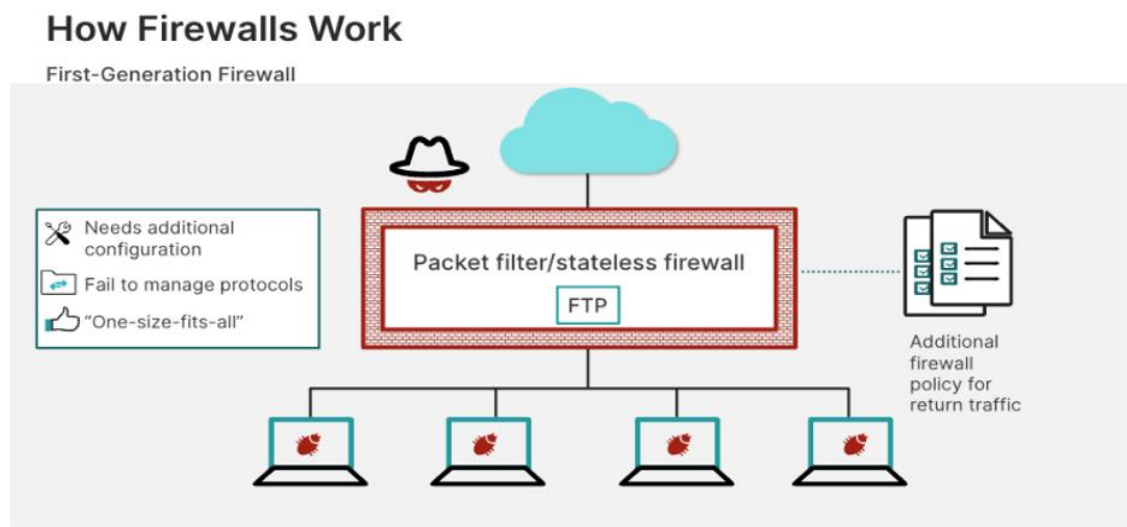
1. **First-generation firewalls** began in 1989 with the packet filtering approach. These firewalls examine individual data packets, making decisions to allow or block them based on predefined rules. However, these were unable to identify if those packets contained malicious code (i.e., malware).
2. **Second-generation firewalls** began in the early 2000s. Otherwise known as [stateful firewalls](#), these track the state of active connections. By

observing network traffic, they use context to identify and act on suspicious behavior. Unfortunately, this generation also has its limitations.

Third-generation firewalls emerged in the latter half of the early 2000s. Often called proxy firewalls or application-level gateways, these act as intermediaries between a client and server, forwarding requests and filtering responses.

3. **Fourth-generation firewall**, also known as next-generation firewall (NGFW), started in 2010. NGFWs combine traditional capabilities with new, advanced features such as intrusion prevention (IPS), application-layer filtering, and advanced threat detection.

Although each generation improved upon the last, many earlier iterations are still in use today. Let's review the [benefits of each firewall](#) in more detail.



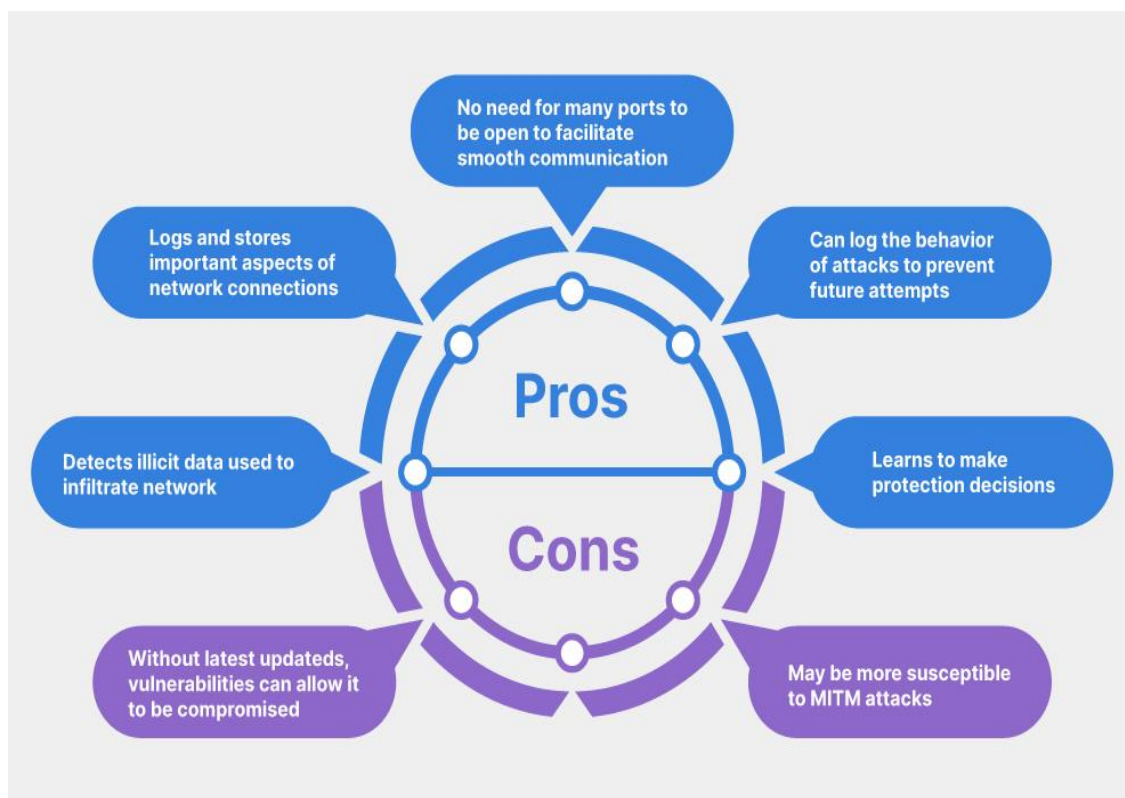
Stateless Firewalls

A [stateless firewall](#) protects the network by analyzing traffic in the transport layer protocol — the place where devices communicate with one another. Rather than store information about the state of the network connection, it inspects traffic on a packet-by-packet basis.

Then, it decides to block or allow the traffic based on the data located in the “packet header.” This may include source and destination IP addresses, port numbers, protocols, and other information. Altogether, this process is called packet filtering.

Despite being fast and inexpensive, stateless firewalls have their vulnerabilities. Critically, they have zero visibility into packet sequencing. That means they can’t detect illegitimate packets, which may contain attack vectors or not have a corresponding request.

Likewise, they only have insight into the packet header — not its actual contents. This makes it impossible for a stateless firewall to detect malware hidden within a packet’s payload.



Statefull Firewalls Stateful firewalls track the most recent or immediate status of active connections. Monitoring the state and context of network communications can help identify threats based on more insightful information.

For example, state-aware firewalls block or allow traffic by analyzing where it's coming from, where it's going, and the contents of its data packets. Moreover, they evaluate the behavior of data packets and network connections, cataloging patterns and using this information to improve future threat detection.

This approach offers more protection compared to packet filtering but takes a greater toll on network performance because it conducts a more in-depth analysis. Worse yet, attackers can trick stateful inspection firewalls into letting harmful connections sneak through. They exploit network rules and send malicious packets using protocols the firewall believes to be safe.







Application-Level Gateways

Application-level gateways, or proxy firewalls, act as an intermediary between internal and external systems. Notably, they operate at Layer 7 of the [Open Systems Interconnection \(OSI\) model](#) — the application layer. As the closest layer to the end-user, Layer 7 applications include web browsers, email clients, and instant messaging tools.

Proxy firewalls intercept and analyze all incoming and outgoing traffic, applying granular security policies to control access and protect the network. They offer packet filtering, application-level inspection, URL filtering, and more.

Next-Generation Firewall

Next-Generation Firewall (NGFW)

Controls applications by classification or users.			Helps protect web-browsing clients from attacks and threats.
Adopts various segmentation approaches.			Segregates users, devices, and applications that are aligned to business needs. Eliminates a single point of entry.
Has moved from reactive to proactive.			Uses artificial intelligence to enforce security policies.

NGFWs protect businesses against emerging cyber threats. They blend all the best parts of past firewall technologies with the advanced capabilities required to mitigate modern cyberattacks. For example, these include:

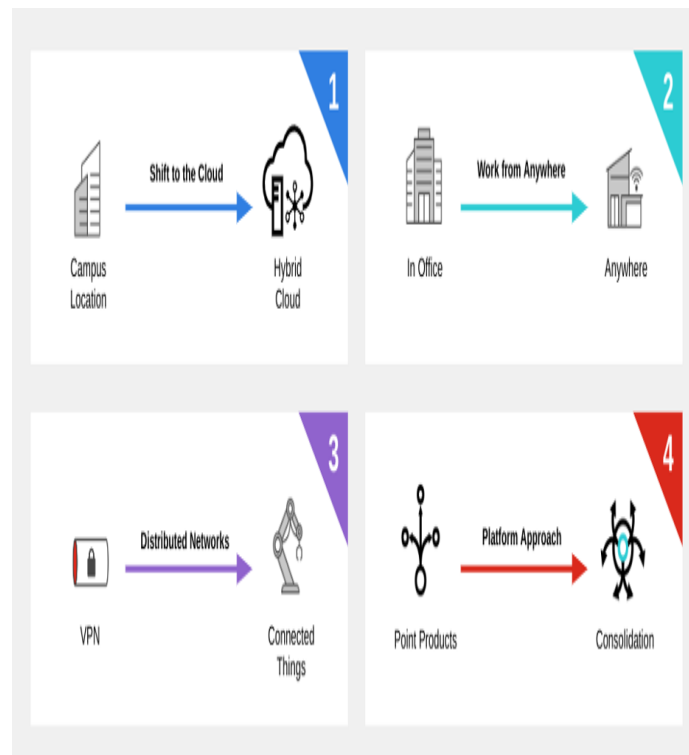
- **Deep Packet Inspection (DPI)**, a method of examining the contents of data packets as they pass through network checkpoints. DPI analyzes a larger range of information, allowing it to find otherwise hidden threats.
- **Intrusion Prevention (IPS)**, a system that monitors traffic in real time to proactively identify threats and automate response.
- **Data Loss Prevention (DLP)**, a cybersecurity solution that blocks intentional and accidental data disclosures.

NGFWs combine the protection of previous generations with the advanced security capabilities mentioned above. They can be deployed as software or hardware and can scale to any location: remote office, branch, campus, data center, and cloud. NGFWs can simplify, unify, and automate enterprise-grade protection with centralized management that extends across distributed environments. These capabilities include:

- **Internet of Things (IoT) security** to discover BYOD, rogue, or shadow IT devices.
- **Network sandboxing** to monitor and analyze suspicious objects in an isolated environment
- **Zero-trust network access (ZTNA)** to manage network access to users and applications based on identity and context
- **Operational technology (OT) security** to protect OT environments with threat intelligence, IPS, and SCADA applications and threat inspection
- **Domain Name System (DNS) security** to monitor, detect and prevent capabilities against DNS layer attacks
- **Software-defined wide-area network (SD-WAN)** architecture to deliver dynamic path selection, based on business or application policy,

centralized policy and management of appliances, virtual private network (VPN), and zero-touch configuration.

Firewall Trends: Hybrid Mesh Firewall

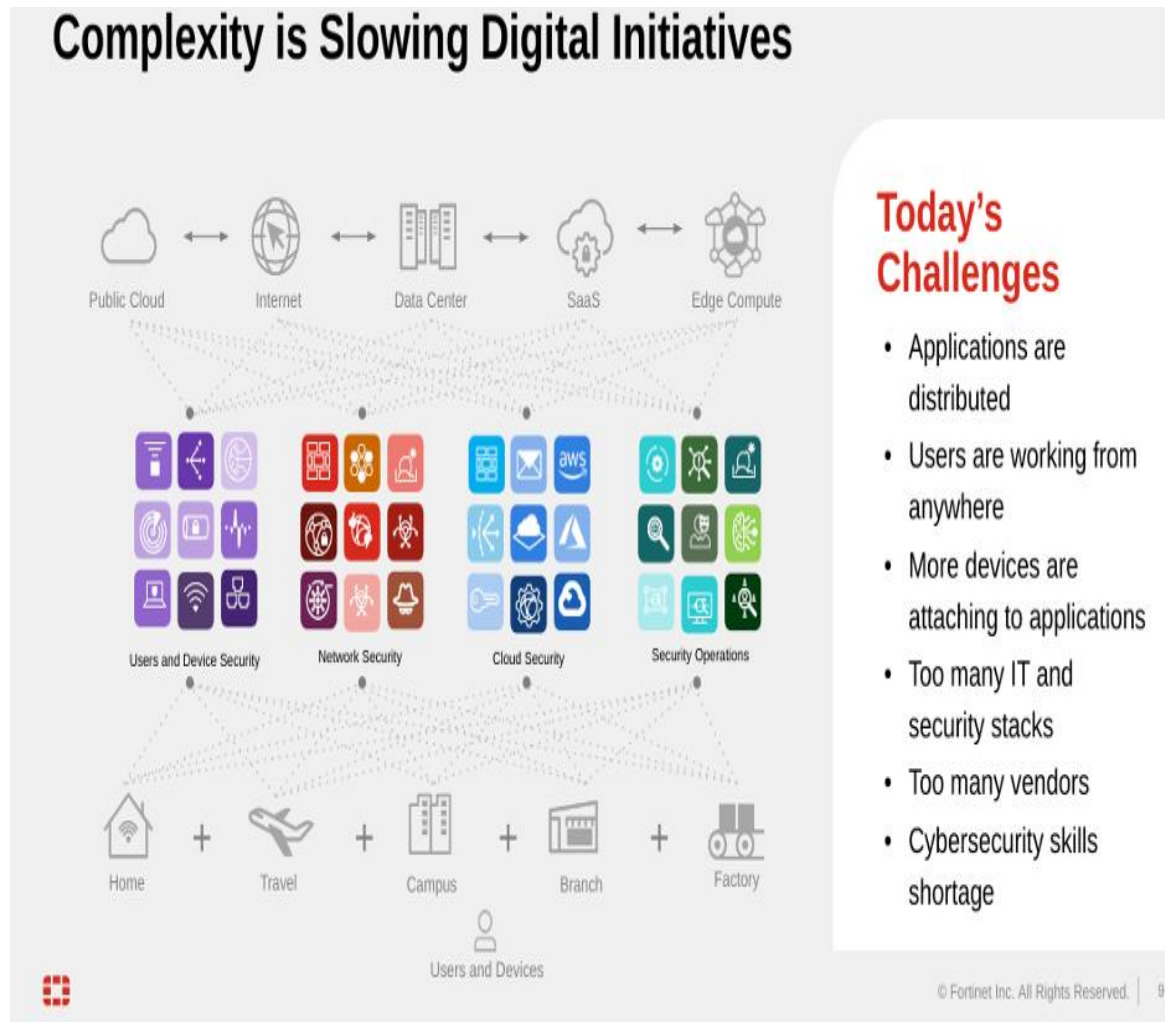


Hybrid mesh firewalls are emerging as the next frontier of network security. In brief, a hybrid mesh firewall is a security platform that provides centralized and unified management by combining the benefits of multiple firewall architectures. It simplifies cybersecurity operations and coordinates policies across firewalls of all form factors to create a comprehensive security posture.

With the rise of work-from-anywhere, employees are more distributed than ever before. And, to accommodate remote work setups, organizations have greatly accelerated their digital transformations. They've adopted hybrid cloud environments, stretching the network edge far past its former perimeter. Between cloud services, data centers, branch offices, and remote deployments, managing network traffic is exponentially more difficult.

Adding to the mix is the fact that enterprise attack surfaces are quickly expanding. Whether it be remote employees accessing corporate resources on unmanaged devices or a disjointed array of point solutions and cloud

applications, every new connection is another potential entry point bad actors can exploit. And, at a time when organizations are facing a significant cybersecurity skills gap, hackers only grow more sophisticated.



In turn, organizations must find a way to unify their cybersecurity approach and simplify risk management.

Why Hybrid Mesh Firewall?

By simplifying cybersecurity operations and coordinating security policies across all firewalls, hybrid mesh firewalls create a comprehensive security posture that is ideal to secure distributed network environments.

According to [Gartner](#), hybrid mesh firewall platforms address the growing complexity of implementing and managing firewalls across multiple use cases. Hybrid mesh firewalls offer mature, cloud-based, unified management with automation and orchestration capabilities. Features such as application connectivity mapping, visibility into cloud-native network security policies, policy fine-tuning, and recommendations facilitate the administration of all firewall complaints across hybrid environments. Integration with overlapping technologies such as micro segmentation and SASE provide mature visibility and risk management capabilities.

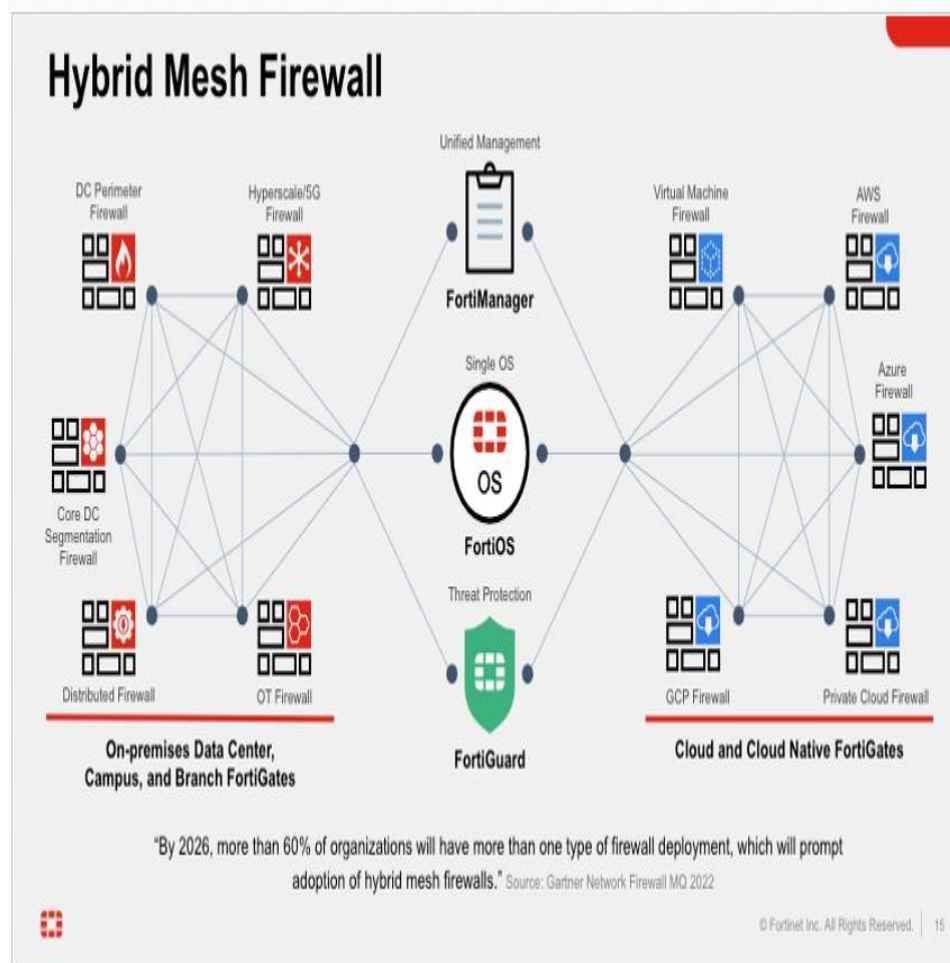
A hybrid mesh architecture spans distributed network environments unifying operations, security, and management of multi-deployment firewalls including hardware and virtual appliances, cloud-based, and as-a-service form factors. One of the most critical capabilities of an NGFW is to simplify the management of these dispersed network firewalls with consistent security across complex, hybrid environments.

Hybrid mesh firewalls include multiple form factors, such as:

- **Virtual firewalls:** Software-based firewalls that run on virtualized infrastructure, such as hypervisors or cloud platforms. Protect virtualized environments and can be moved between clouds. Critically, they're flexible by nature, allowing organizations to deploy them to various public or private clouds.
- **Cloud-native firewalls:** Firewalls specifically created to operate in particular cloud environments. They're often tightly integrated with cloud service providers like Amazon Web Services, Azure, and Google Cloud. This reduces the workload for network security teams, as it eliminates the need to configure and maintain the software infrastructure.
- **Firewall-as-a-Service (FWaaS):** A deployment model where vendors deliver the firewall solution as a cloud-based service. This makes it easy

to scale across a growing network infrastructure and is easily configured to match an enterprise's unique security needs.

As network risk management becomes more complex, hybrid mesh firewalls stand to level the playing field for enterprises by unifying operations, security, and management across distributed network environments.



What to Look for in a Firewall Solution

Next-generation firewalls (NGFWs) serve as gatekeepers to safeguard an organization's compute resources with secure networking, advanced threat inspection and detection, and web filtering. Hybrid working models and the rapid adoption of cloud services are forcing network security to evolve to give

enterprises complete visibility and control across the entire distributed infrastructure.

When evaluating NGFW solutions, potential trade-offs between security and performance may be top of mind. The ability to provide consistent and consolidated security protection across all distributed edges with minimal performance impact is critical. Following are six criteria to consider when evaluating NGFWs for a distributed security edge to edge.

Choosing Your Firewall Deployment Use Cases

When choosing a firewall, consider the use case. Are you securing a branch office or ATM, a data center, or your headquarters on campus? Do you need to protect your network with work-from-anywhere access for remote users? Will your users need to access applications on multiple clouds? Do you need network segmentation to safeguard assets?

Branch—Protect and connect small offices or ATMs with AI/ML powered security and convergence with secure SD-WAN. Firewalls provide a first line of defense by protecting branch locations from unauthorized access, malicious traffic, and cyber threats with secure network operations, data integrity, and compliance with security policies.

Campus—Gain visibility and protection of enterprise headquarters with the ability to manage applications, users, devices, and access from a single dashboard. Firewalls provide campus networks with a multi-layered defense against cyber threats, ensure secure network operations, and enable compliance with security policies.

Data Center—Deploy hyperscale security with consistent, coordinated protection, rich interfaces, and decryption that scales to any environment. Firewalls act as a sophisticated security shield to control network traffic flow, identify and mitigate threats, enforce security policies, to protect critical IT infrastructure and sensitive data.

Segmentation—Protect your assets with rich macro- and micro-segmentation. By segmenting the network to isolate potential threats, create secure zones, and scale as needed, firewalls cater to the specific needs of larger and more complex network environments.

Multicloud—Integrate public and private cloud protection with easy-to-manage automation from a single console. Firewalls play secure remote work environments to protect sensitive data stored or accessed remotely by safeguarding access points, mitigating cyber threats, and controlling network traffic with centralized management.

Remote—Extend protection with converged networking and security services. Firewall-as-a-service, a component of a secure access service edge (SASE) cloud-native architecture extends security across hybrid work environments to protect data and applications with centralized management and advanced threat protection.

What is an Intrusion Detection System (IDS)?

An intrusion detection system (IDS) is an application that monitors network traffic and searches for known threats and suspicious or malicious activity. The IDS sends alerts to IT and security teams when it detects any security risks and threats.

Most IDS solutions simply monitor and report suspicious activity and traffic when they detect an anomaly. However, some can go a step further by taking action when it detects anomalous activity, such as blocking malicious or suspicious traffic.

IDS tools typically are software applications that run on organizations' hardware or as a network security solution. There are also cloud-based IDS solutions that protect organizations' data, resources, and systems in their cloud deployments and environments.

What is an Intrusion in Cybersecurity?

The answer to "what is intrusion" is typically an attacker gaining unauthorized access to a device, network, or system. Cyber criminals use increasingly sophisticated techniques and tactics to infiltrate organizations without being discovered. This includes common techniques like:

1. Address spoofing: The source of an attack is hidden using spoofed, misconfigured, and poorly secured proxy servers, which makes it difficult for organizations to discover attackers.
2. Fragmentation: Fragmented packets enable attackers to bypass organizations' detection systems.
3. Pattern evasion: Hackers adjust their attack architectures to avoid the patterns that IDS solutions use to spot a threat.
4. Coordinated attack: A network scan threat allocates numerous hosts or ports to different attackers, making it difficult for the IDS to work out what is happening.

Types of Intrusion Detection Systems (IDS)

IDS solutions come in a range of different types and varying capabilities. Common types of intrusion detection systems (IDS) include:

1. Network intrusion detection system (NIDS): A NIDS solution is deployed at strategic points within an organization's network to monitor incoming and outgoing traffic. This IDS approach monitors and detects malicious and suspicious traffic coming to and going from all devices connected to the network.
2. Host intrusion detection system (HIDS): A HIDS system is installed on individual devices that are connected to the internet and an organization's internal network. This solution can detect packets that come from inside the business and additional malicious traffic that a NIDS solution cannot. It can also discover malicious threats coming from the host, such as a host

being infected with malware attempting to spread it across the organization's system.

3. Signature-based intrusion detection system (SIDS): A SIDS solution monitors all packets on an organization's network and compares them with attack signatures on a database of known threats.
4. Anomaly-based intrusion detection system (AIDS): This solution monitors traffic on a network and compares it with a predefined baseline that is considered "normal." It detects anomalous activity and behavior across the network, including bandwidth, devices, ports, and protocols. An AIDS solution uses machine-learning techniques to build a baseline of normal behavior and establish a corresponding security policy. This ensures businesses can discover new, evolving threats that solutions like SIDS cannot.
5. Perimeter intrusion detection system (PIDS): A PIDS solution is placed on a network to detect intrusion attempts taking place on the perimeter of organizations' critical infrastructures.
6. Virtual machine-based intrusion detection system (VMIDS): A VMIDS solution detects intrusions by monitoring virtual machines. It enables organizations to monitor traffic across all the devices and systems that their devices are connected to.
7. Stack-based intrusion detection system (SBIDS): SBIDS is integrated into an organization's [Transmission Control Protocol/Internet Protocol \(TCP/IP\)](#), which is used as a communications protocol on private networks. This approach enables the IDS to watch packets as they move through the organization's network and pulls malicious packets before applications or the operating system can process them.

How Does an Intrusion Detection System Work? What Are Its Uses?

IDS solutions excel in monitoring network traffic and detecting anomalous activity. They are placed at strategic locations across a network or on devices themselves to analyze network traffic and recognize signs of a potential attack.

An IDS works by looking for the signature of known attack types or detecting activity that deviates from a prescribed normal. It then alerts or reports these anomalies and potentially malicious actions to administrators so they can be examined at the application and protocol layers.

This enables organizations to detect the potential signs of an attack beginning or being carried out by an attacker. IDS solutions do this through several capabilities, including:

1. Monitoring the performance of key [firewalls](#), files, routers, and servers to detect, prevent, and recover from cyberattacks
2. Enabling system administrators to organize and understand their relevant operating system audit trails and logs that are often difficult to manage and track
3. Providing an easy-to-use interface that allows staff who are not security experts to help with the management of an organization's systems
4. Providing an extensive database of attack signatures that can be used to match and detect known threats
5. Providing a quick and effective reporting system when anomalous or malicious activity occurs, which enables the threat to be passed up the stack
6. Generating alarms that notify the necessary individuals, such as system administrators and security teams, when a breach occurs
7. In some cases, reacting to potentially malicious actors by blocking them and their access to the server or network to prevent them from carrying out any further action

The increasingly connected nature of business environments and infrastructures means they demand highly secure systems and techniques to establish trusted lines of communication. IDS has an important role within modern [cybersecurity](#) strategies to safeguard organizations from hackers attempting to gain unauthorized access to networks and stealing corporate data.

Why Are Intrusion Detection Systems (IDS) Important?

An intrusion detection system provides an extra layer of protection, making it a critical element of an effective cybersecurity strategy. You can use it alongside your other cybersecurity tools to catch threats that are able to penetrate your primary defenses. So even if your main system fails, you are still alerted to the presence of a threat.

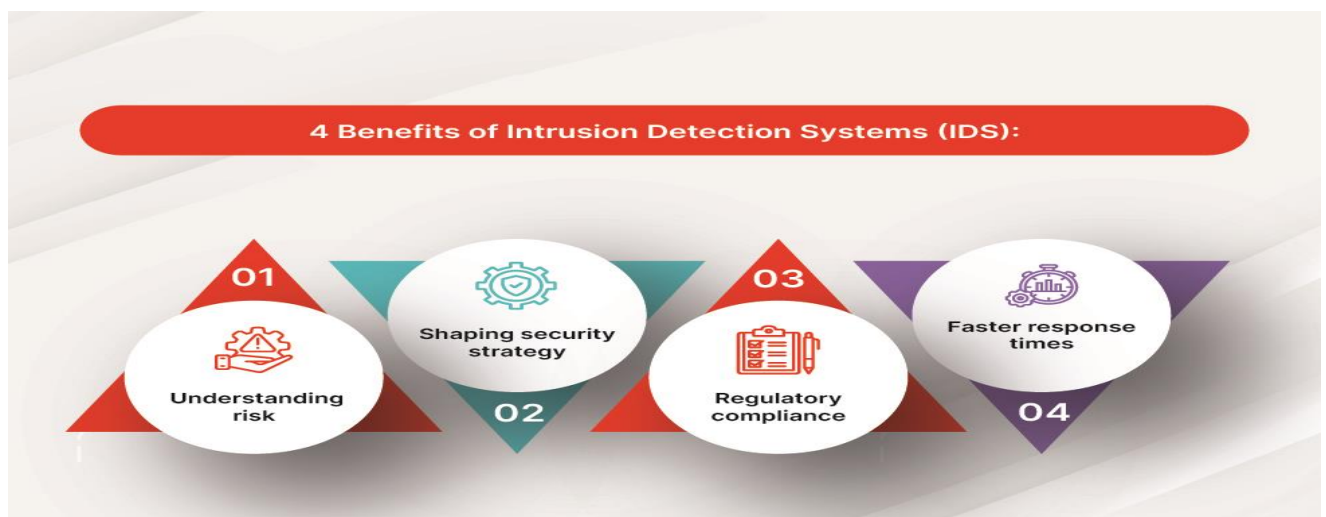
A healthcare organization, for example, can deploy an IDS to signal to the IT team that a range of threats has infiltrated its network, including those that have managed to bypass its firewalls. In this way, the IDS helps the organization to stay in compliance with data security regulations.

Benefits of intrusion detection systems

IDS solutions offer major benefits to organizations, primarily around identifying potential security threats being posed to their networks and users. A few common benefits of deploying an IDS include:

1. **Understanding risk:** An IDS tool helps businesses understand the number of attacks being targeted at them and the type and level of sophistication of risks they face.
2. **Shaping security strategy:** Understanding risk is crucial to establishing and evolving a comprehensive cybersecurity strategy that can stand up to the modern threat landscape. An IDS can also be used to identify bugs and potential flaws in organizations' devices and networks, then assess and adapt their defenses to address the risks they may face in the future.

3. Regulatory compliance: Organizations now face an ever-evolving list of increasingly stringent regulations that they must comply with. An IDS tool provides them with visibility on what is happening across their networks, which eases the process of meeting these regulations. The information it gathers and saves in its logs is also vital for businesses to document that they are meeting their compliance requirements.
4. Faster response times: The immediate alerts that IDS solutions initiate allow organizations to discover and prevent attackers more quickly than they would through manual monitoring of their networks. The sensors that an IDS uses can also inspect data in network packets and operating systems, which is also faster than manually collecting this information.



Intrusion detection system (IDS) challenges

While IDS solutions are important tools in monitoring and detecting potential threats, they are not without their challenges. These include:

1. False alarms: Also known as false positives, these leave IDS solutions vulnerable to identifying potential threats that are not a true risk to the organization. To avoid this, organizations must configure their IDS to

understand what normal looks like, and as a result, what should be considered as malicious activity.

2. False negatives: This is a bigger concern, as the IDS solution mistakes an actual security threat for legitimate traffic. An attacker is allowed to pass into the organization's network, with IT and security teams oblivious to the fact that their systems have been infiltrated.

As the threat landscape evolves and attackers become more sophisticated, it is preferable for IDS solutions to provide false positives than false negatives. In other words, it is better to discover a potential threat and prove it to be wrong than for the IDS to mistake attackers for legitimate users. Furthermore, IDS solutions increasingly need to be capable of quickly detecting new threats and signs of malicious behavior.

Intrusion Detection System vs. Intrusion Prevention System

An IDS solution is typically limited to the monitoring and detection of known attacks and activity that deviates from a baseline normal prescribed by an organization. The anomalies that an IDS solution discovers are pushed through the stack to be more closely examined at the application and protocol layer. Therefore, most IDS solutions are not capable of preventing or offering a solution for the threats that they discover.

An [intrusion prevention system \(IPS\)](#) goes beyond this by blocking or preventing security risks. An IPS can both monitor for malicious events and take action to prevent an attack from taking place.

IPS solutions help businesses take a more proactive cybersecurity approach and mitigate threats as soon as possible. They constantly monitor networks in search of anomalies and malicious activity, then immediately record any threats and prevent the attack from doing damage to the company's data, networks, resources, and users. An IPS will also send insight about the threat to system

administrators, who can then perform actions to close holes in their defenses and reconfigure their firewalls to prevent future attacks.

Deploying an IPS tool enables organizations to prevent advanced threats such as [denial-of-service \(DoS\) attacks](#), phishing, spam, and virus threats. They can also be used within security review exercises to help organizations discover vulnerabilities in their code and policies.

It is increasingly important for organizations to deploy tools capable of IDS and IPS, or a tool that can do both, to protect their corporate data and users. Integrating IDS and IPS in one product enables the monitoring, detection, and prevention of threats more seamlessly.

What Is the Difference between a Firewall and IDS?

[Firewalls](#) and intrusion detection systems (IDS) are cybersecurity tools that can both safeguard a network or endpoint. Their objectives, however, are very different from one another.

1. **IDS:** Intrusion detection systems are passive monitoring tools that identify possible threats and send out notifications to analysts in [security operations centers \(SOCs\)](#). In this way, incident responders can promptly look into and address the potential event.
2. **Firewall:** A firewall, on the other hand, analyzes the metadata contained in network packets and decides whether to allow or prohibit traffic into or out of the network based on pre-established rules. A firewall essentially creates a barrier that stops certain traffic from crossing through it.

An IDS is focused on detecting and generating alerts about threats, while a firewall inspects inbound and outbound traffic, keeping all unauthorized traffic at bay.