**Cryptography** is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure Communication refers to the scenario where the message or data shared between two parties can’t be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security. Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

1. **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2. **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
3. **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.
4. **Non-repudiation** refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

Consider two parties Alice and Bob. Now, Alice wants to send a message m to Bob over a secure channel. So, what happens is as follows. The sender’s message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of receival, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.

Alice (Sender) Bob (Receiver)

C = E (m, k) ----> m = D (C, k)

Here, C refers to the Ciphertext while E and D are the Encryption and Decryption algorithms respectively. Let’s consider the case of Caesar Cipher or Shift Cipher as an example. As the name suggests, in Caesar Cipher each character in a word is replaced by another character under some defined rules. Thus, if A is replaced by D, B by E and so on. Then, each character in the word would be shifted by a position of 3.

Components

There are various components of cryptography which are as follows −

Plaintext and Ciphertext

The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Cipher

We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

Types

There are two types of cryptography which are as follows −

Symmetric Key Cryptography

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

Asymmetric-Key Cryptography

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

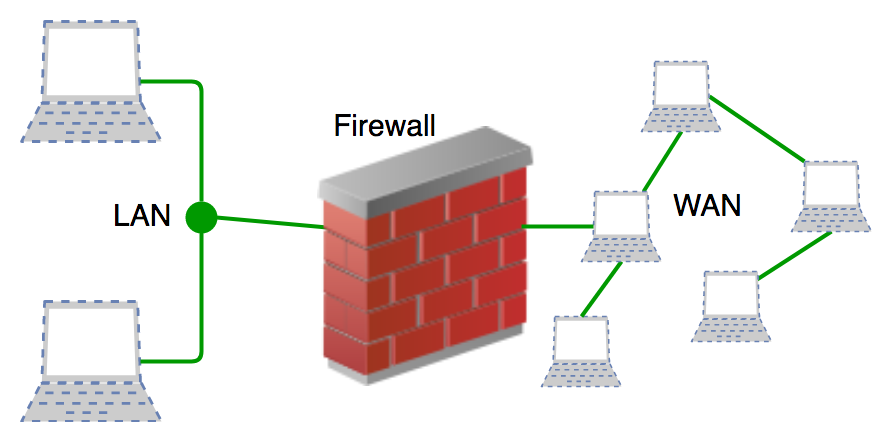
In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public, and the private key is available only to an individual.

# Introduction of Firewall in Computer Network

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

**Accept :** allow the traffic  
**Reject :** block the traffic but reply with an “unreachable error”  
**Drop :**block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



**How Firewall Works**

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.  
From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.  
Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.

**Default policy:** It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).  
Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to accept, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as drop (or reject) is always a good practice.

## Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., [hardware](https://www.javatpoint.com/hardware) and [software](https://www.javatpoint.com/software), though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a [computer network](https://www.javatpoint.com/computer-network-tutorial) and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

**Types of Firewall**

Firewalls are generally of two types: Host-based and Network-based.

1. **Host- based Firewalls :**Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :**Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Functions of Firewall

As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.

Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

* Network Threat Prevention
* Application and Identity-Based Control
* Hybrid Cloud Support
* Scalable Performance
* Network Traffic Management and Control
* Access Validation
* Record and Report on Events

An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and BitTorrent.

Application gateways

Application gateways provide high-level secure network system communication. For example, when a client requests access to server resources such as files, Web pages and databases, the client first connects with the proxy server, which then establishes a connection with the main server.

The application gateway resides on the client and server firewall. The proxy server hides Internet Protocol (IP) addresses and other secure information on the client’s behalf. A computer’s internal system may communicate with an external computer using firewall protection. The application gateway and external computer function without client information or knowledge of the proxy server IP address.

# Basic Network Attacks in Computer Network

Many people rely on the Internet for many of their professional, social and personal activities. But there are also people who attempt to damage our Internet-connected computers, violate our privacy and render inoperable the Internet services.

Given the frequency and variety of existing attacks as well as the threat of new and more destructive future attacks, network security has become a central topic in the field of computer networking.

**How are computer networks vulnerable? What are some of the more prevalent types of attacks today?**

**Malware** – short for malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. Much of the malware out there today is self-replicating: once it infects one host, from that host it seeks entry into other hosts over the Internet, and from the newly infected hosts, it seeks entry into yet more hosts. In this manner, self-replicating malware can spread exponentially fast.

**Virus** – A malware which requires some form of user’s interaction to infect the user’s device. The classic example is an e-mail attachment containing malicious executable code. If a user receives and opens such an attachment, the user inadvertently runs the malware on the device.

**Worm** – A malware which can enter a device without any explicit user interaction. For example, a user may be running a vulnerable network application to which an attacker can send malware. In some cases, without any user intervention, the application may accept the malware from the Internet and run it, creating a worm.

**Botnet** – A network of private computers infected with malicious software and controlled as a group without the owners’ knowledge, e.g. to send spam.

**DoS (Denial of Service)** – A DoS attack renders a network, host, or other pieces of infrastructure unusable by legitimate users. Most Internet DoS attacks fall into one of three categories :

• *Vulnerability attack*: This involves sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. If the right sequence of packets is sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash.

• *Bandwidth flooding*: The attacker sends a deluge of packets to the targeted host—so many packets that the target’s access link becomes clogged, preventing legitimate packets from reaching the server.

• *Connection flooding*: The attacker establishes a large number of half-open or fully open TCP connections at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

**DDoS (Distributed DoS)** – DDoS is a type of DOS attack where multiple compromised systems, are used to target a single system causing a Denial of Service (DoS) attack. DDoS attacks leveraging botnets with thousands of comprised hosts are a common occurrence today. DDoS attacks are much harder to detect and defend against than a DoS attack from a single host.

**Packet sniffer** – A passive receiver that records a copy of every packet that flies by is called a packet sniffer. By placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted! These packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages. some of the best defenses against packet sniffing involve cryptography.

**IP Spoofing** – The ability to inject packets into the Internet with a false source address is known as IP spoofing, and is but one of many ways in which one user can masquerade as another user. To solve this problem, we will need end-point authentication, that is, a mechanism that will allow us to determine with certainty if a message originates from where we think it does.

**Man-in-the-Middle Attack** – As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

**Compromised-Key Attack** – A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.

**Phishing** – The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

**DNS spoofing** – Also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver’s cache, causing the name server to return an incorrect IP address.

**Rootkit –** Rootkits are stealthy packages designed to benefit administrative rights and get the right of entry to a community tool. Once installed, hackers have complete and unrestricted get right of entry to the tool and can, therefore, execute any movement including spying on customers or stealing exclusive data with no hindrance.