IMPLEMENTING NETWORK SECURITY

AUTHENTICATION, AUTHORIZATION AND AUDITING (AAA)

Roles played within an AAA system.

Core Components of AAA

- *Client:* The client is the device attempting to access the network. Either the client authenticates itself, or it acts as a proxy to authenticate a user.
- *Policy Enforcement Point (Authenticator):* The Policy Enforcement Point (PEP) is sometimes called the *authenticator* or *dial-in server*. The PEP is responsible for enforcing the terms of a client's access. This enforcement varies based on the capabilities of the PEP and the defined policies
- *Policy Information Point:* The *Policy Information Point* (PIP) is a repository of information to help make the access decision. It could be a database of device IDs, a user directory such as the *Lightweight Directory Access Protocol* (LDAP), a *one-time password* (OTP) or any other system that houses data relevant to a device or user access request.
- *Policy Decision Point (AAA Server):* The Policy Decision Point (PDP) is the brain of the AAA decision. It collects the access request from the client through the PEP. It also queries any relevant *PIPs* to gather the information it needs to make the access decision. The PDP, as its name implies, is the entity that makes the final decision around network access. It also can send specific authorizations back to the PEP that apply settings or constraints to the client's network traffic.
- *Accounting and Reporting System:* Whether on a dedicated system or built as part of a PDP, tracking use of the network with accounting is one of the best features of *AAA*. With all forms of network access now offering controlled access, the AAA service can tell you who got on the network, from where, and what that person was granted access to.

It is important to note that the preceding categories are logical containers of functions and not necessarily dedicated physical devices. Often elements are combined, such as PEP with PDP, and PDP with PIP.

1. AUTHENTICATION

Authentication, Authorization, and Accounting (*AAA*) is a technology that is used to check whether a user has permission to access a network, authorizes exactly what a user is allowed to access, and makes records regarding the network resources used by a user.

MODES OF AUTHENTICATION

AAA supports three authentication modes.

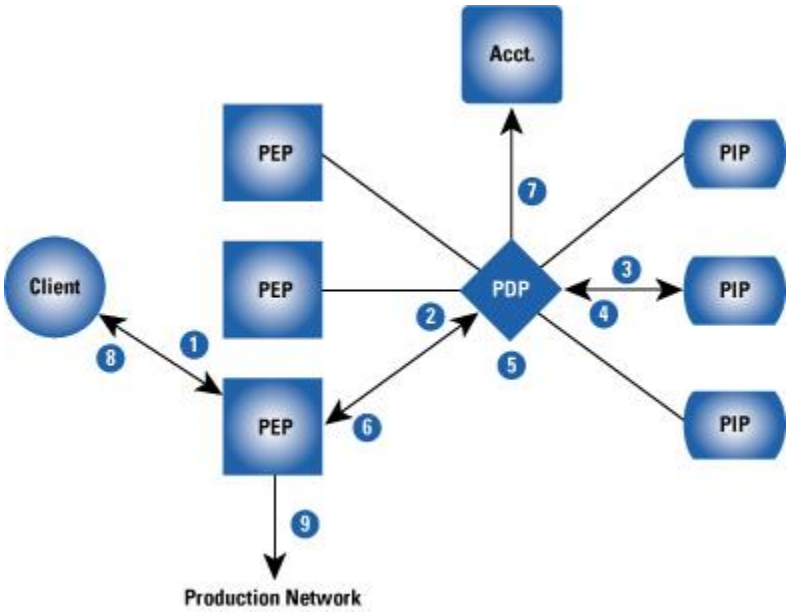
a) Non-authentication completely trusts users and does not check their validity. This is seldom used for obvious security reasons.

b) Local authentication configures user information, including the username, password, and attributes of local users, on a *Network Access Server (NAS)*. Local authentication has advantages such as fast processing.

c) Remote authentication configures user information including the username, password, and attributes on the authentication server.

Example of AAA Flow

Now that we have examined the components of an AAA solution, let's look at an example. The Figure below shows an example of a client attempting to gain access to the network.



1. The client attempts to connect to the network, is challenged for identity information, and sends this information to the PEP. In this example, let's assume the client is a laptop with a worker attempting to access an organization's VPN from a remote location. Additionally, we'll assume this is a valid, permitted use of the network.
2. The PEP sends the collected identity information to the PDP. In some cases since the PEP cannot see the specific identity information provided but instead relays the information directly to the PDP.
3. The PDP queries any configured PIPs for information about the client and validates that the credential provided by the client is valid. In this example, the PIP is an LDAP directory.
4. The PIP returns a success or failure message from the credential validation step and sends additional information about the client to the PDP for evaluation. This information could include the role of the user, the location for the user, and so on.
5. The PDP evaluates information learned about the client through the client, PEP, and PIP; the role of the PEP and PIP that serviced the request; and any contextual information (such as time of day) against its configured policies. Based on this information, the PDP makes an authorization decision.
6. The PDP sends the PEP the authentication result and any authorizations specific to the client. These authorizations trigger specific PEP actions to apply to the client. For example, the authorization data might trigger specific *Access Control Lists* (ACLs) or IP pool assignments for the client.
7. The PDP also sends the result of this transaction to the accounting system.
8. The PEP applies the authorization profile learned from the PDP and sends the "authentication successful" message to the client. The PEP can also be configured to send accounting information on this new connection to the accounting and reporting system.
9. The client accesses the production network through the PEP.

Elements of Authentication

When performing authentication, numerous elements can be evaluated before a PDP reaches its access decision. At a high level, these elements can be broken down into three categories:

- *Principal itself (the user, device, or service requesting access)*

The principal is the entity requesting authorization. It is generally some combination of user, device, or service. When concerned with a user, the PIP can provide attributes about the user

such as role or group affiliations, job title, e-mail address, physical address, and so on. In specific applications, it can include much more granular information. For example, a higher-education facility might be interested in knowing a student's class schedule when servicing the student's authentication request.

When the principal is a device, the same thinking applies. The PIP can inform the PDP if the device is a managed asset, what its basic usage parameters are, and so on. User and device authentication can be carried out sequentially for the same transaction, often involving device authentication first and then user authentication. Lastly, a service such as a network management process can authenticate. In this case, the service almost always looks like a user to the AAA infrastructure and is handled accordingly.

- *Credential the principal submits (shared key, one-time password, digital certificate, or biometric credential)*

The next element the PDP considers is the credential the user or device submits as proof of identity. There are four main types of credentials: shared key (password), *one-time password* (OTP), digital certificate, and biometric credential. This section examines each of these types.

The first and most widely used form of credential is the shared key, typically a user password. AAA deployments that use shared keys can be subdivided based on the protocol the system uses to verify the password, including the:-

- *Password Authentication Protocol* (PAP)

PAP authentication is a plaintext authentication method that is not recommended for use in security-sensitive environments.

However, many newer protocols provide a secure transport for PAP, making its use in AAA still quite common.

- *Challenge Handshake Authentication Protocol* (CHAP)

CHAP improves on the security of PAP by not sending the password in the clear but rather a challenge based on a hash of the password.

- *Contextual information describing the transaction*

  This include details like location of access, time of day, software state, and so on

2. AUTHORIZATION

The AAA Authorization function is used to determine the permission for users to gain access to specific networks or devices; as such AAA supports various authorization modes.

In non-authorization mode users are not authorized. Local authorization however authorizes users according to the related attributes of the local user accounts configured on the Network Access Server.

AAA Authorization Methods

- If-Authenticated—the user is allowed to access the requested function provided the user has been authenticated successfully.
- None—the network access server does not request authorization information; authorization is not performed.
- Local—the router or access server consults its local database, as defined by the **username** command, for example, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.
- RADIUS—the network access server requests authorization information from the RADIUS security server. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server.

3. ACCOUNTING

Accounting is an increasingly critical step in the overall AAA process. Regulatory controls are starting to mandate better auditing of network access. The last stage of AAA, accounting simply records which clients accessed the network, what they were granted access to, and when they disconnected from the network.

Accounting has always been widely used in the *Internet Service Provider* (ISP) space because auditing network access is the basis for billing ISP customers.

Increasingly, accounting is being used as a way to correlate *client attribute information* (username, IP address, etc.) with actions and events on the network. This correlation can make other systems that are not user-aware more intelligent in the security decisions that they make.

For example, a network *Intrusion Detection System* (IDS) can learn a lot about the behavior of a given IP address. However, when that information is correlated with the user assigned to that IP address—and the permissions that user should have—the relevance of the IDS data increases dramatically.

One of the design considerations of accounting systems is that, given the *centralized* nature of audit and the *decentralized* nature of access makes them excellent resources to refer to when the network administrator wants to know when the client connected and what the client was granted access to.

This information can be learned by the network by coordinating the AAA accounting information with the rest of the network enforcement and monitoring systems. Accounting method lists are specific to the type of accounting being requested.

AAA supports six different types of accounting:

- *Network*—Provides information for all Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or Address Resolution Protocol (ARP) sessions, including packet and byte counts.
- EXEC—Provides information about user EXEC terminal sessions of the network access server.
- Commands—Provides information about the EXEC mode commands that a user issues. Command accounting generates accounting records for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- Connection—Provides information about all outbound connections made from the network access server, such as Telnet
- System—Provides information about system-level events.
- Resource—Provides "start" and "stop" records for calls that have passed user authentication, and provides "stop" records for calls that fail to authenticate.

4. IPSEC

IPsec Overview

A secure network starts with a strong security policy that defines the freedom of access to information and dictates the deployment of security in the network.

IPsec offers many technology solutions for building a custom security solution for Internet, extranet, intranet, and remote access networks.

IPsec is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPsec ensures confidentiality, integrity, and authenticity of data communications across a public network.

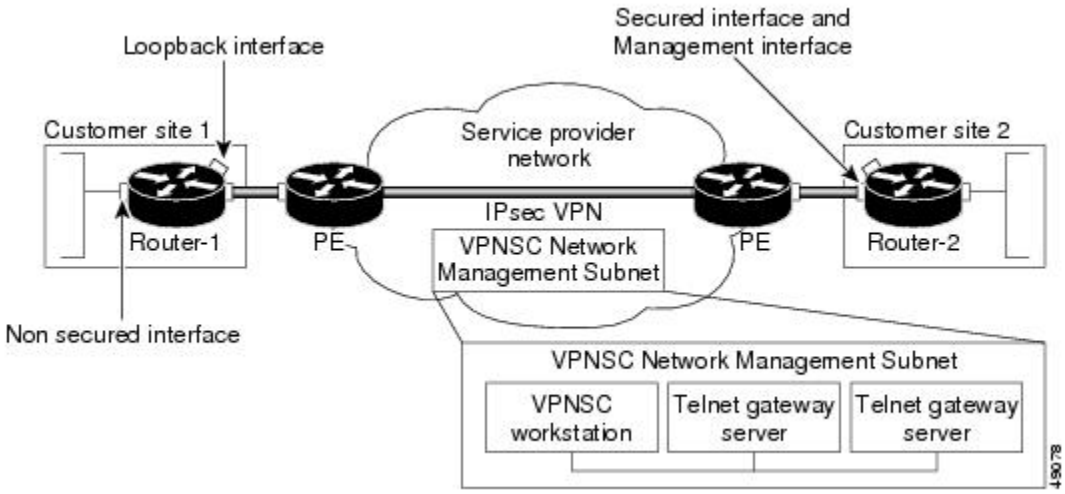
IPsec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

IPsec's method of protecting IP datagrams takes the following forms:-

- Data origin authentication
- Connectionless data integrity authentication
- Data content confidentiality
- Anti-replay protection
- Limited traffic flow confidentiality

IPsec protects IP datagrams by defining a method of specifying the traffic to protect, how that traffic is to be protected, and to whom the traffic is sent.

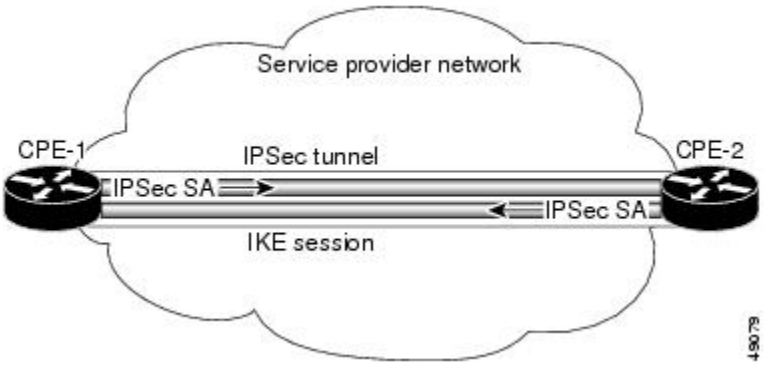
Typical IPsec usage scenario in a Cisco IPsec Solutions environment



How IPsec Works

IPsec provides secure *tunnels* between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters which should be used to protect these sensitive packets, by specifying characteristics of these tunnels.

Then, when the IPsec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.



More accurately, these tunnels are sets of *security associations* (SAs) that are established between two IPsec peers. The security associations define which protocols and algorithms should be applied to sensitive packets, and also specify the keying material to be used by the two peers. Security associations are unidirectional and are established per security protocol (AH or ESP).

With IPsec you define what traffic should be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces by way of *crypto map sets.*

Therefore, traffic can be selected based on source and destination address, and optionally Layer 4 protocol, and port. The access lists used for IPsec only determine which traffic should be protected by IPsec, not which traffic should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.

Once established, the set of security associations (outbound, to the peer) is then applied to the triggering packet as well as to subsequent applicable packets as those packets exit the router.

Multiple IPsec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of security associations. For example, some data streams might be just authenticated while other data streams must both be encrypted and authenticated.

The Benefits of IPsec Technology

The benefits of IPsec are as follows:-

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.
- IPsec is below the transport layer (TCP, UDP), so is transparent to applications.

  There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper layer software, including applications, is not affected.
- IPsec can provide security for individual users if needed. This feature is useful for offsite workers and also for setting up a secure virtual subnetwork within an organization for sensitive applications.

5. ENCRYPTION

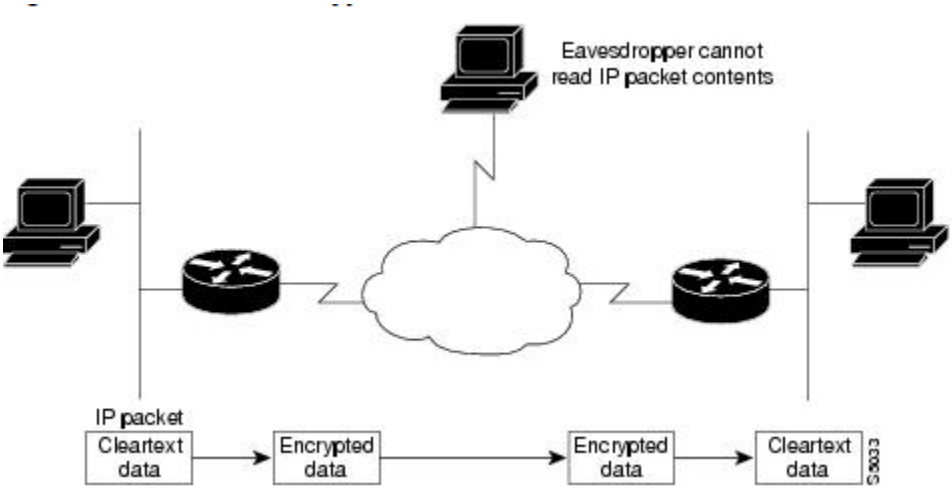
In the computing world, *encryption* is the conversion of data from a readable format into an encoded format that can only be read or processed after it's been decrypted.

Encryption is the basic building block of data security and is the simplest and most important way to ensure a computer system's information can't be stolen and read by someone who wants to use it for nefarious means.

Why Encryption?

Data that traverses unsecured networks is open to many types of attacks. Data can be read, altered, or forged by anybody who has access to the route that your data takes. For example, a protocol analyzer can read packets and gain classified information. Or, a hostile party can tamper with packets and cause damage by hindering, reducing, or preventing network communications within your organization.

Encryption provides a means to safeguard network data that travels from one device to another across unsecured networks. Encryption is particularly important if classified, confidential, or critical data is being sent.



What Gets Encrypted?

Network data encryption is provided at the IP packet level—*only IP packets* can be encrypted. (If you wish to encrypt a network protocol other than IP, you must encapsulate the protocol within an IP packet.)

An IP packet is encrypted/decrypted only if the *packet meets criteria* you establish when you configure a router for encryption.

When encrypted, individual IP packets can be detected during transmission, but the IP packet contents (payload) *cannot be read*. Specifically, the IP header and upper-layer protocol headers (for example, TCP or UDP) are not encrypted, but all payload data within the TCP or UDP packet will be encrypted and therefore not readable during transmission.

Where Are Packets Encrypted and Decrypted in the Network?

The actual encryption and decryption of IP packets occur only at routers that you configure for *Control-flow Enforcement Technology* (CET). Such routers are considered to be *peer encrypting routers* (or simply *peer routers*). Intermediate hops do not participate in encryption/decryption.

Often, peer routers are situated at the *edges of unsecured networks* (such as the Internet), in order to provide secure communications between two secured networks that are physically separated.

Clear text (not encrypted) traffic that enters a peer router from the secure network side is encrypted and forwarded across the unsecure network. When the encrypted traffic reaches the remote peer router, the router decrypts the traffic before forwarding it into the remote secure network. Packets are encrypted at one peer router's outbound interface and decrypted at the other peer router's inbound interface.

When Can Encrypted Packets Be Exchanged?

Encrypted packets can be exchanged between peer routers only during encrypted sessions. When a peer router detects a packet that should be encrypted, an encrypted session must first be established. After an encrypted session is established, encrypted traffic can pass freely between peer routers. When the session expires, a new session must be established before encrypted traffic can continue to be sent.

How Does an Encrypting Router Identify Other Peer Encrypting Routers?

During the setup of every encrypted session, both participating peer routers attempt to authenticate each other. If either authentication fails, the encrypted session will not be established, and no encrypted traffic will pass. Peer authentication ensures that only known, trusted peer routers

exchange encrypted traffic, and prevents routers from being tricked into sending sensitive encrypted traffic to illegitimate or fraudulent destination routers.

6. ACCESS CONTROL LISTS

Routers provides basic traffic filtering capabilities with access control lists (also referred to as *access lists*). Access lists can be configured for all routed network protocols to filter the packets of those protocols as the packets pass through a router.

You can configure access lists at your router to control access to a network: access lists can prevent certain traffic from entering or exiting a network.

What Access Lists Do

Access lists filter network traffic by controlling whether routed packets are *forwarded* or *blocked* at the router's interfaces. Your router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria you specified within the access lists.

Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

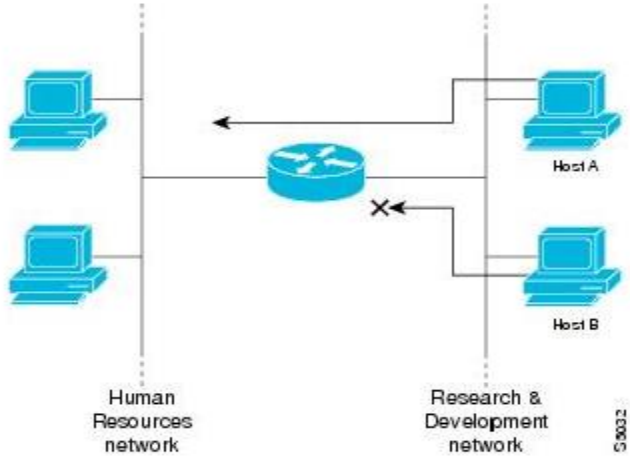
Why You Should Configure Access Lists

There are many reasons to configure access lists; for example, you can use access lists *to restrict contents of routing updates* or to *provide traffic flow control*. One of the most important reasons to configure access lists is to provide security for your network.

You should use access lists to *provide a basic level of security* for accessing your network. If you do not configure access lists on your router, all packets passing through the router could be allowed onto all parts of your network.

Access lists can allow one host to access a part of your network and prevent another host from accessing the same area. In example below host A is allowed to access the Human Resources network, and host B is prevented from accessing the Human Resources network.

Using Traffic Filters to Prevent Traffic from Being Routed to a Network



When to Configure Access Lists

Access lists should be used in "firewall" routers, which are often positioned between your internal network and an external network such as the Internet. You can also use access lists on a router positioned between two parts of your network, to control traffic entering or exiting a specific part of your internal network.

To provide the security benefits of access lists, you should at a minimum configure access lists on border routers—routers situated at the edges of your networks. This provides a basic buffer from the outside network, or from a less controlled area of your own network into a more sensitive area of your network.

On these routers, you should configure access lists for each network protocol configured on the router interfaces. You can configure access lists so that *inbound traffic* or *outbound traffic* or both are filtered on an interface.

Access lists must be defined on a *per-protocol basis.* In other words, you should define access lists for every protocol enabled on an interface if you want to control traffic flow for that protocol.

Types of Access Control Lists

Types	Value Ranges	Parameters
Basic	2000-2999	Source IP
Advanced	3000-3999	Source & Destination IP, Protocol, Source & Destination Port
Layer 2 ACL	4000-4999	MAC Address

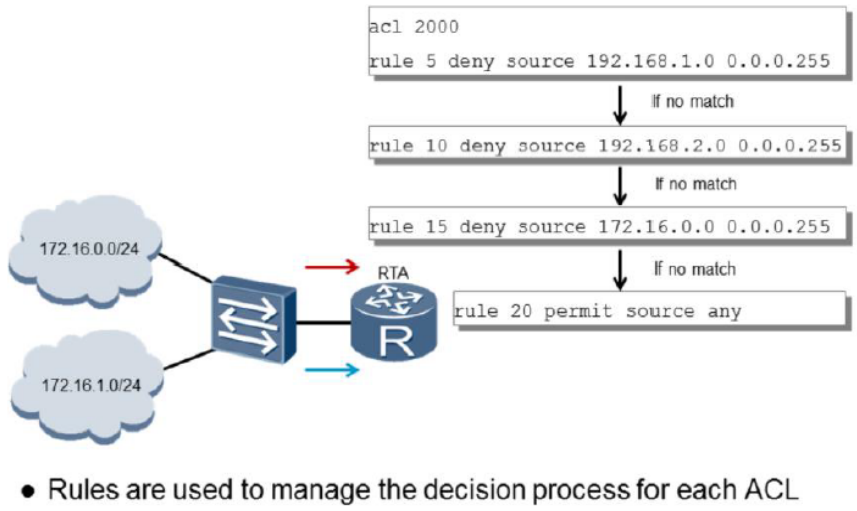
There are three general ACL types, including basic, advanced and layer2 access control list types.

- A basic ACL matches packets based on information such as source IP addresses, fragment flags, and time ranges, and is defined by a value in the range of 2000 -2999.
- An advanced ACL provides a greater means of accuracy in parameter association, and matches packets based on information such as source and destination IP addresses, source and destination port numbers, and protocol types. Advanced ACL are associated with a value range from 3000 -3999
- Lastly is the layer 2 ACL which matches packets based on packet based Layer2 information, such as source MAC addresses, destination MAC addresses, and Layer2 protocol types. Traffic is filtered based on rules containing the parameters defined by each type of ACL.

CREATING ACCESS LISTS

Create access lists for each protocol you wish to filter, per router interface. For some protocols, you create one access list to filter inbound traffic, and one access list to filter outbound traffic.

To create an access list, you specify the protocol to filter, you assign a unique name or number to the access list, and you define packet filtering criteria. A single access list can have multiple filtering criteria statements.



7. FIREWALLS

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.

Types of Firewalls

A) SOFTWARE FIREWALLS

i) Proxy firewall

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

ii) Stateful inspection firewall

Now thought of as a "traditional" firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed.

Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

iii) Microsoft's ISA Server

Microsoft's ISA Server (*Internet Security and Acceleration Server*) provides the two basic services of an enterprise firewall and a Web proxy/cache server.

ISA Server's firewall screens all *packet*-level, *circuit*-level, and *application*-level traffic.
ISA Server allows administrators to create policies for regulating usage based on user, group, application, destination, schedule, and content type criteria.

ISA Server comes in two editions, Standard Edition and Enterprise Edition.

- Standard Edition is a stand-alone server that supports a server with up to four processors.
- Enterprise Edition is for large-scale deployments, server array support, multi-level policy, and servers with more than four processors.

iv) pfSense

pfSense is an open source customized distribution of FreeBSD specifically tailored for use as a firewall and router that is entirely managed via web interface. pfSense is mostly used as a *router and firewall software*, and typically configured as DHCP server, DNS server, WiFi access point, VPN server, all running on the same hardware device.

v) Sophos

Sophos offers next-generation firewall (NGFW) features which protect a network while securing your web traffic. It protects against modern threats such as drive-by downloads and botnets, and securely connects people and offices using our flexible VPN options.

Sophos Firewall is a network security solution that fully identifies the source of an infection on your network and automatically limits the infected device's access to other network resources in response.

B) HARDWARE FIREWALLS

- Cyber Roam
- Fortinet
- Watch Guard
- Wi jungle (wireless)