Please identify different types of Firewalls. Also include Network Address Translation (NAT) and how it could be used to restrict access.

Firewalls

-Firewall: Hardware or software that is designed to prevent malicious packets from entering or leaving computers. Also called packet filter.

-Host-Based Application Firewall: A firewall that runs as a program on a local system.

-Packet Filter: Hardware or software that is designed to prevent malicious packets from entering or leaving computers. Also called firewall.

-Web Application Firewall: A special type of application-aware firewall that looks at the applications using HTTP.

-Network Firewall: Designed to protect an entire network; their functions are essentially the same: to inspect packets and either accept or deny entry;

-Rule-Based Firewall: Uses a set of individual instructions to control actions, called firewall rules. These rules are a single line of textual information containing such information as: Source address, Destination address, Source port, Destination port, Protocol, Direction, and Action.

-Application-Aware Firewall: “Intelligent” firewall; Sometimes called a next-generation firewall (NGFW); Operate at a higher level by identifying the applications that send packets through the firewall and then make decisions about the application instead of filtering packets based on granular rule settings like the destination port or protocol;

-Web Application Firewall: A special type of application-aware firewall; A firewall that looks at the applications using HTTP.

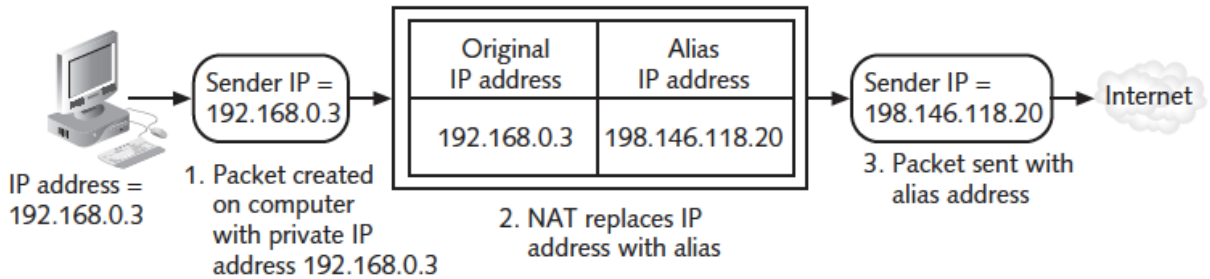
NAT

-Network address translation (NAT) is a technique that allows private IP addresses to be used on the public Internet; Strictly speaking, NAT is not a specific device, technology, or protocol. It is a technique for substituting IP addresses.

A device using NAT, such as a NAT router, also can provide a degree of security. Because all outgoing traffic flows through the NAT router, it knows which packets were sent out and what it expects to receive.

If the initial request did not come through the NAT router, the router will discard all unsolicited packets so that they never enter the internal network. In this way the NAT router acts like a firewall by discarding unwanted packets.

Another element of security that NAT provides is masking the IP addresses of internal devices. An attacker who captures the packet on the Internet cannot determine the actual IP address of the sender. Without that address, it is more difficult to identify and attack a computer.



NAT replaces a private IP address with a public IP address. As a packet leaves a network, NAT removes the private IP address from the sender's packet and replaces it with an alias IP public address. The NAT software maintains a table of the private IP addresses and alias public IP addresses. When a packet is returned to NAT, the process is reversed. A variation of NAT is port address translation (PAT). Instead of giving each outgoing packet a different IP address, each packet is given the same IP address but a different TCP port number. This allows a single public IP address to be
used by several users.

Private IP Addresses

Class	Beginning Address	Ending Address
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

- CompTIA® Security+ Guide to Network Security Fundamentals,