Firewalls :

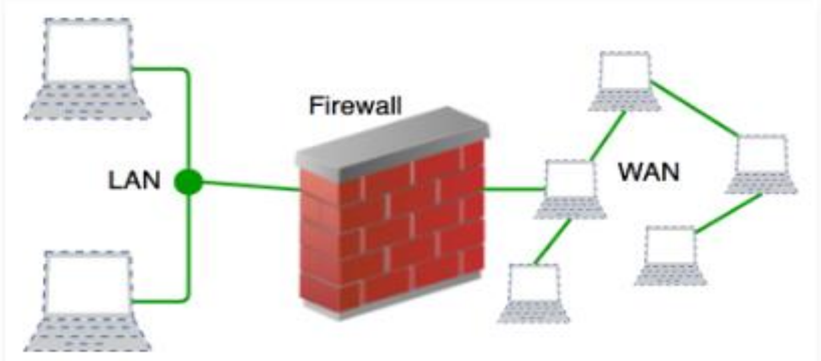
Introduction, Identification, Authentication, Authorization, Accountability:

Introduction of Firewall :

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.

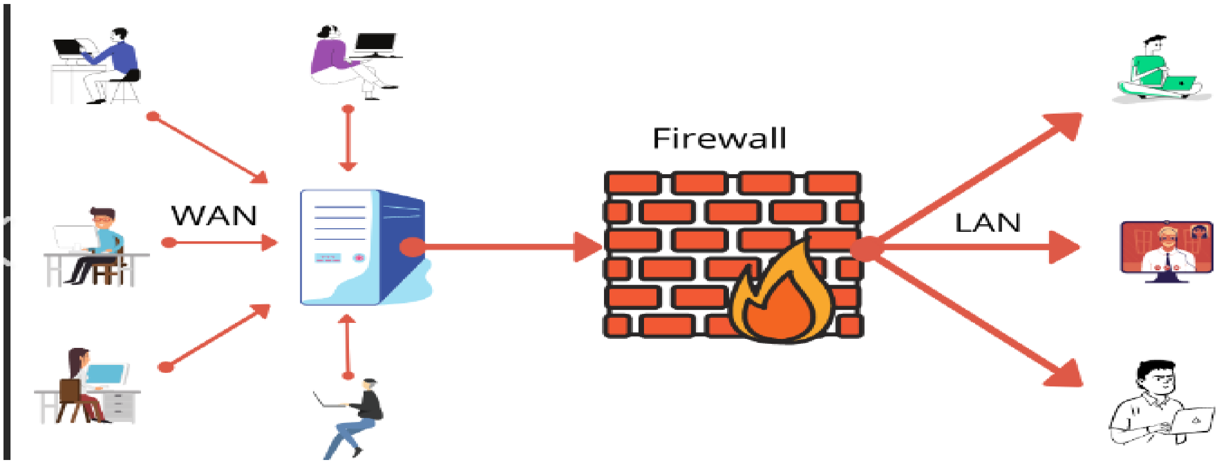
Accept : allow the traffic
Reject : block the traffic but reply with an “unreachable error”
Drop : block the traffic with no reply

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



What is the purpose of a firewall?

- It acts as a barrier between internal private networks and external sources (such as the public Internet). The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.
- Firewalls are generally of two types: *Host-based* and *Network-based.*



- ✓ Whenever you log in to most of the websites, you submit a username. In case you create an account, you are asked to choose a username which identifies you. This username which you provide during login is "Identification". It is simply a way of claiming your identity.

- ✓ From an information security point of view, identification describes a method where you claim whom you are. If you notice, you share your username with anyone. Your email id is a form of identification and you share this identification with everyone to receive emails. This means that identification is a public form of information.

OR

- ✓ Identification is a mechanism whereby an unverified entity—called a supplicant—that seeks access to a resource proposes a label by which they are known to the system. The label applied to the supplicant (or supplied by the supplicant) is called an identifier (ID), and must be mapped to one and only one entity within the security domain. Some organizations use composite identifiers, concatenating elements—department codes, random numbers,

or special characters—to make unique identifiers within the security domain. Other organizations generate random IDs to protect the resources from potential attackers. Most organizations use a single piece of unique information, such as a complete name or the user's first initial and surname.

Firewalls: Authentication :

So now you have entered your username, what do you enter next? The password. This is what authentication is about. Here you authenticate or prove yourself that you are the person whom you are claiming to be. Authentication can be done through various mechanisms. Let's understand these types.

There are commonly 3 ways of authenticating:

- something you know,
- something you have and
- something you are.

- Something You Know: Here the authentication happens with your knowledge or what you know. This can be a PIN, password, key, pet's name etc. This is the most common authentication implemented today. This is also one of the cheapest authentication mechanisms.
- **Something You Have**: Here the authentication happens with ownership, i.e. something you have or own. An access id card, credit card, RSA token, security badge are all examples of things you can own and authenticate yourself with. In case this badge is stolen or lost, this could be an issue in those cases.
- **Something You Are:** Here the authentication happens with YOU (characteristic). Your physical attribute is used to authenticate you. Characteristics such as fingerprints, voice print, iris scan, palm print etc. are examples of characteristics or biometrics. An issue with this can be you can never change your characteristics if someone gets hold of your biometrics, unlike a password which can be changed.

- Authorization is the matching of an authenticated entity to a list of information assets and corresponding access levels.

In general, authorization can be handled in one of three ways:

- Authorization for each authenticated user, in which the system performs an authentication process to verify each entity and then grants access to resources for only that entity. This quickly becomes a complex and resource-intensive process in a computer system.

- Authorization for members of a group, in which the system matches authenticated entities to a list of group memberships, and then grants access to resources based on the group's access rights. This is the most common authorization method.

- Authorization across multiple systems, in which a central authentication and authorization system verifies entity id

- Accountability, also known as auditability, ensures that all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Accountability is most often accomplished by means of system logs and database journals, and the auditing of these records.

- Systems logs record specific information, such as failed access attempts and systems modifications. Logs have many uses, such as intrusion detection, determining the root cause of a system failure, or simply tracking the use of a particular resource.

PROCESSING MODES OF FIREWALLS :

Firewalls fall into five major processing-mode categories:

- packet-filtering firewalls,
- application gateways,
- circuit gateways,
- layer firewalls, and
- hybrids

Packet-Filtering Firewall :

- examines the header information of data packets that come into a network.
- determines whether to drop a packet (deny) or forward it to the next network connection (allow) based on the rules programmed into the firewall.
- examine every incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet type, and other key information.
- scan network data packets looking for compliance with or violation of the rules of the firewall's database.

- If the device finds a packet that matches a restriction, it stops the packet from traveling from one network to another.
- The restrictions most commonly implemented in packet-filtering firewalls are based on a combination of the following:
    - IP source and destination address

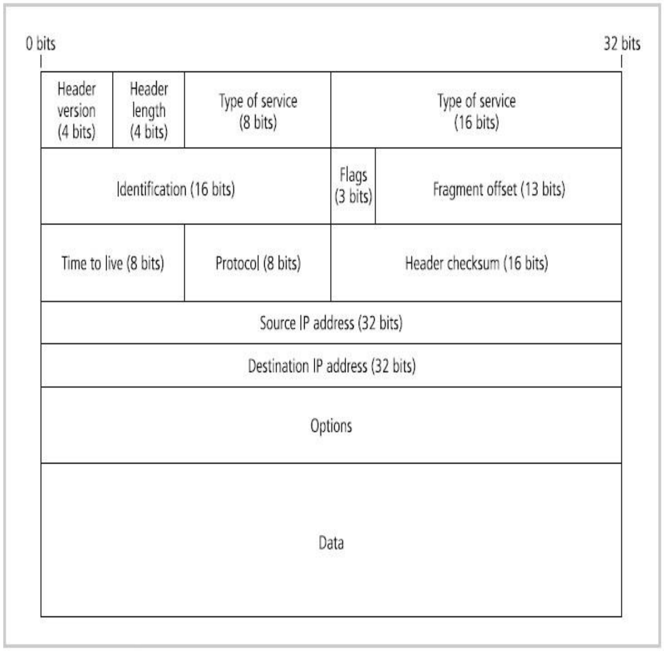


Figure 6-2 IP Packet Structure

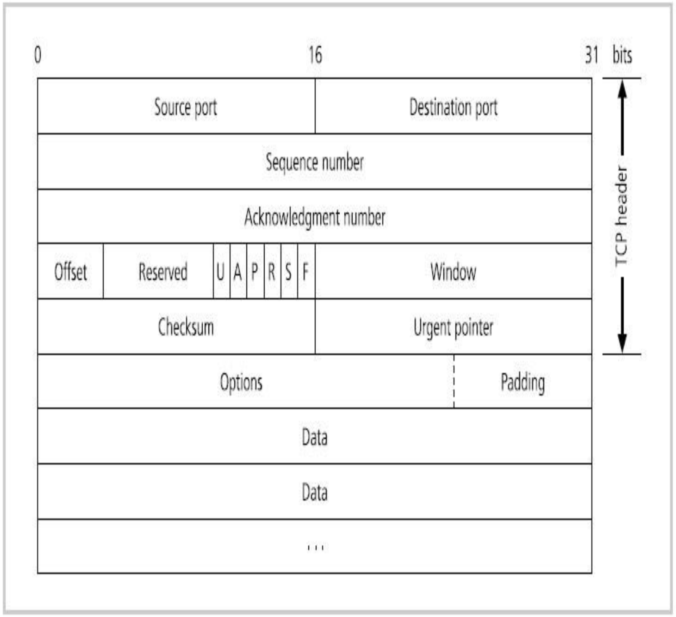


Figure 6-3 TCP Packet Structure

Packet structure varies depending on the nature of the packet. The two primary service types are TCP and UDP (as noted above). Figures 6-3 and 6-4 show the structures of these two major elements of the combined protocol known as TCP/IP.

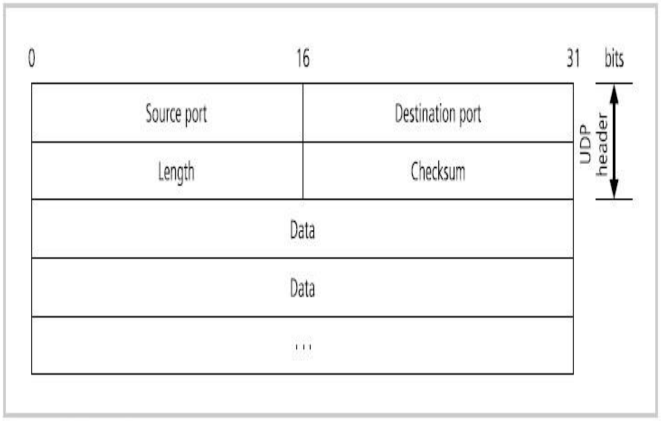


Figure 6-4 UDP Datagram Structure

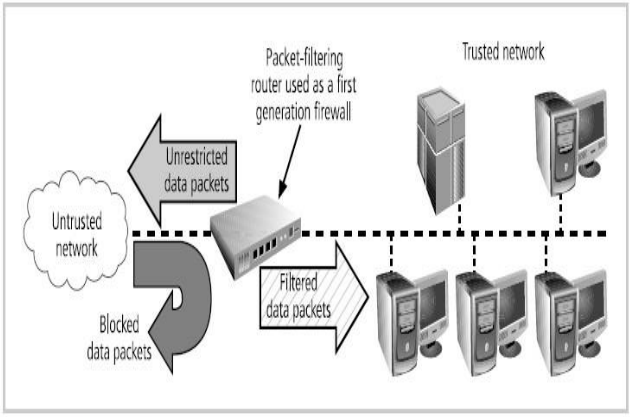
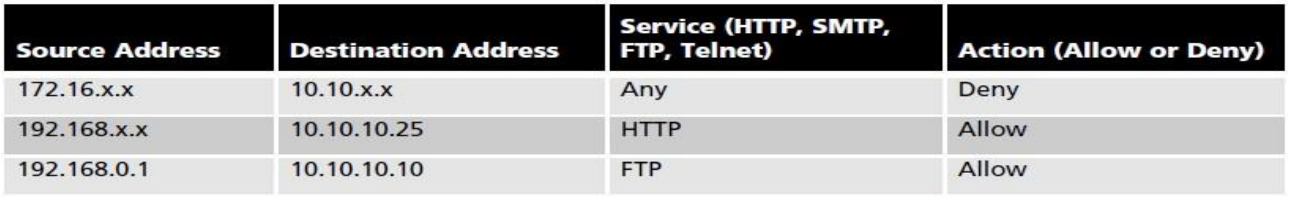

Packet-filtering router used as a first generation firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

Figure 6-5 Packet-Filtering Router

Simple firewall models examine two aspects of the packet header: the destination and source address. They enforce address restrictions. Figure 6-5 shows how a packet-filtering router can be used as a simple firewall to filter data packets from inbound connections and allow outbound connections unrestricted access to the public network



Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Table 6-1 Sample Firewall Rule and Format

There are three subsets of packet-filtering firewalls:

♠ static filtering,

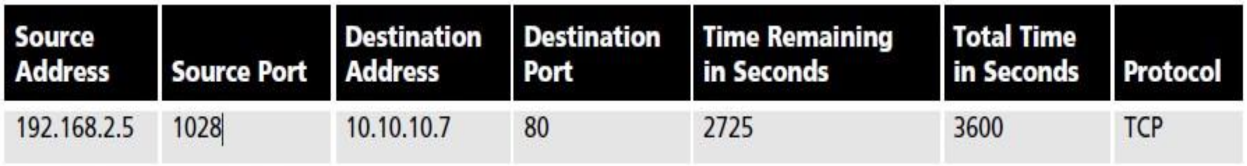
♠ dynamic filtering, and

♠ stateful inspection.

↔ Static filtering requires that the filtering rules be developed and installed with the firewall. The rules are created and sequenced either by a person directly editing the rule set, or by a person using a programmable interface to specify the rules and the sequence.

↔ A dynamic filtering firewall can react to an emergent event and update or create rules to deal with that event. While static filtering firewalls allow entire sets of one type of packet to enter in response to authorized requests, the dynamic packet-filtering firewall allows only a particular packet with a particular source, destination, and port address to enter. It does this by opening and closing "doors" in the firewall based on the information contained in the packet header.

↔ Stateful inspection firewalls, also called stateful firewalls, keep track of each network connection between internal and external systems using a state table. A state table tracks the state and context of each packet in the conversation by recording which station sent what packet and when



Source Address	Source Port	Destination Address	Destination Port	Time Remaining in Seconds	Total Time in Seconds	Protocol
192.168.2.5	1028	10.10.10.7	80	2725	3600	TCP

Table 6-2 State Table Entries

Application Gateways

♣ The application gateway, also known as an application-level firewall or application firewall, is frequently installed on a dedicated computer, separate from the filtering router, but is commonly used in conjunction with a filtering router.

♣ The application firewall is also known as a proxy server since it runs special software that acts as a proxy for a service request.

♣ This proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users. These servers can store the most recently accessed pages in their internal cache, and are thus also called cache servers.

♣ One common example of an application-level firewall (or proxy server) is a firewall that blocks all requests for and responses to requests for Web pages and services from the internal computers of an organization, and instead makes all such requests and responses go to intermediate computers (or proxies) in the less protected areas of the organization's network.

♣ The primary disadvantage of application-level firewalls is that they are designed for one or a few specific protocols and cannot easily be reconfigured to protect against attacks on other protocols.

Circuit Gateways

♣ The circuit gateway firewall operates at the transport layer.

♣ They do not usually look at traffic flowing between one network and another, but they do prevent direct connections between one network and another.

♣ They accomplish this by creating tunnels connecting specific processes or systems on each side of the firewall, and then allowing only authorized traffic, such as a specific type of TCP connection for authorized users, in these tunnels.

MAC Layer Firewalls

♣ MAC layer firewalls are designed to operate at the media access control sublayer of the data link layer (Layer 2) of the OSI network model.

♣ This enables these firewalls to consider the specific host computer's identity, as represented by its MAC or network interface card (NIC) address in its filtering decisions.

♣ Thus, MAC layer firewalls link the addresses of specific host computers to ACL entries that identify the specific types of packets that can be sent to each host, and block all other traffic

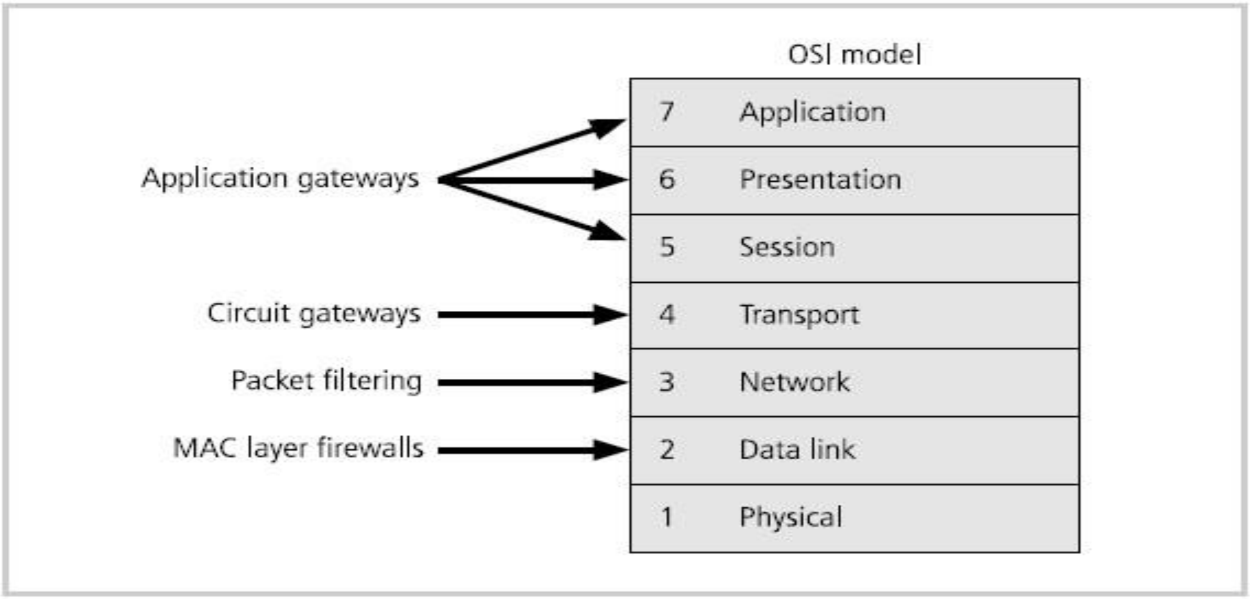


Figure 6-6 Firewall Types and the OSI Model

Hybrid Firewalls

♣ Hybrid firewalls combine the elements of other types of firewalls—that is, the elements of packet filtering and proxy services, or of packet filtering and circuit gateways.

♣ A hybrid firewall system may actually consist of two separate firewall devices; each is a separate firewall system, but they are connected so that they work in tandem.

♣ An added advantage to the hybrid firewall approach is that it enables an organization to make a security improvement without completely replacing its existing firewalls

FIREWALLS CATEGORIZED BY GENERATION

↔ First generation firewalls are static packet-filtering firewalls—that is, simple networking devices that filter packets according to their headers as the packets travel to and from the organization's networks.

↔ Second generation firewalls are application-level firewalls or proxy servers—that is, dedicated systems that are separate from the filtering router and that provide intermediate services for requestors.

↔ Third generation firewalls are stateful inspection firewalls, which, as described previously, monitor network connections between internal and external systems using state tables.

↔ Fourth generation firewalls, which are also known as dynamic packet-filtering firewalls, allow only a particular packet with a particular source, destination, and port address to enter.

↔ Fifth generation firewalls include the kernel proxy, a specialized form that works under Windows NT Executive, stack which is the kernel of Windows NT. This type of firewall evaluates packets at multiple layers of the protocol, by checking security in the kernel as data is passed up and down the stack.

FIREWALLS CATEGORISED BY STRUCTURE

Firewalls can also be categorized by the structures used to implement them.

- Commercial-Grade Firewall Appliances : Firewall appliances are stand-alone, self contained combinations of computing hardware and software. These devices frequently have many of the features of a general-purpose computer with the addition of firmware based instructions that increase their reliability and performance and minimize the likelihood of their being compromised. These variant operating systems are tuned to meet the type of firewall activity built into the application software that provides the firewall functionality.

- Commercial-Grade Firewall Systems : A commercial-grade firewall system consists of application software that is configured for the firewall application and run on a general-purpose computer. Organizations can install firewall software on an existing general purpose computer system, or they can purchase hardware that has been configured to specifications that yield optimum firewall performance.

- Small Office/Home Office (SOHO) Firewall Appliances : As more and more small businesses and residences obtain fast Internet connections with digital subscriber lines (DSL) or cable modem connections, they become more and more vulnerable to attacks. One of the most effective methods of improving computing security in the SOHO setting is by means of a SOHO or residential-grade firewall. These devices, also known as broadband gateways or DSL/cable modem routers, connect the user's local area network or a specific computer system to the Internetworking device—in this case, the cable modem or DSL router provided by the Internet service provider (ISP). The SOHO firewall serves first as a stateful firewall to enable inside-to-outside access and can be configured to allow limited TCP/IP port forwarding and/or screened subnet capabilities.

- Residential-Grade Firewall Software: Another method of protecting the residential user is to install a software firewall directly on the user's system. Many people have implemented these residential-grade software-based firewalls (some of which also provide antivirus or intrusion detection capabilities), but, unfortunately, they may not be as fully protected as they think. The most commonly used of residentialgrade software-based firewalls are McAfee Internet Security, Microsoft Windows Firewall etc.

FIREWALL ARCHITECTURES :

The configuration that works best for a particular organization depends on three factors:

The objectives of the network,

the organization's ability to develop and implement the architectures,

and The budget available for the function.

Although literally hundreds of variations exist, there are four common architectural implementations: Packet filtering routers, screened host firewalls, dual-homed firewalls, and screened subnet firewalls.

Packet-Filtering Routers :

♣ Most organizations with an Internet connection have some form of a router at the boundary between the organization’s internal networks and the external service provider.

♣ Many of these routers can be configured to reject packets that the organization does not want to allow into the network.

♣ This is a simple but effective way to lower the organization’s risk from external attack.

♣ The drawbacks to this type of system include a lack of auditing and strong authentication.

♣ Also, the complexity of the ACLs used to filter the packets can degrade network performance.

Screened Host Firewalls :

♣ Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server.

♣ This approach allows the router to pre-screen packets to minimize the network traffic and load on the internal proxy.

♣ The application proxy examines an application layer protocol, such as HTTP, and performs the proxy services. This separate host is often referred to as a bastion host.

♣ Compromise of the bastion host can disclose the configuration of internal networks and possibly provide attackers with internal information. Since the bastion host stands as a sole defender on the network perimeter, it is commonly referred to as the sacrificial host.

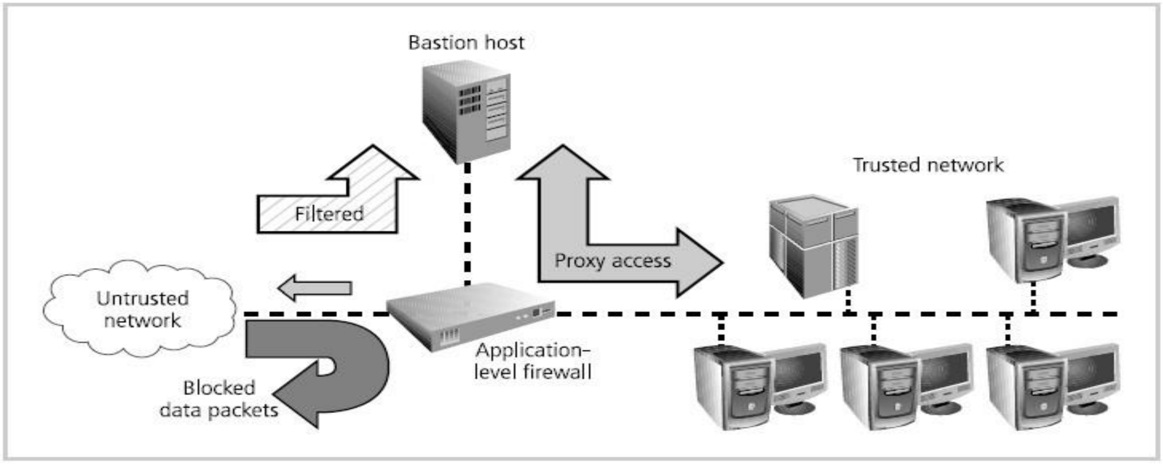


Figure 6-12 Screened Host Firewall

Dual-Homed Firewall :

♣ One NIC is connected to the external network, and

♣ another NIC is connected to the internal network, providing an additional layer of protection.

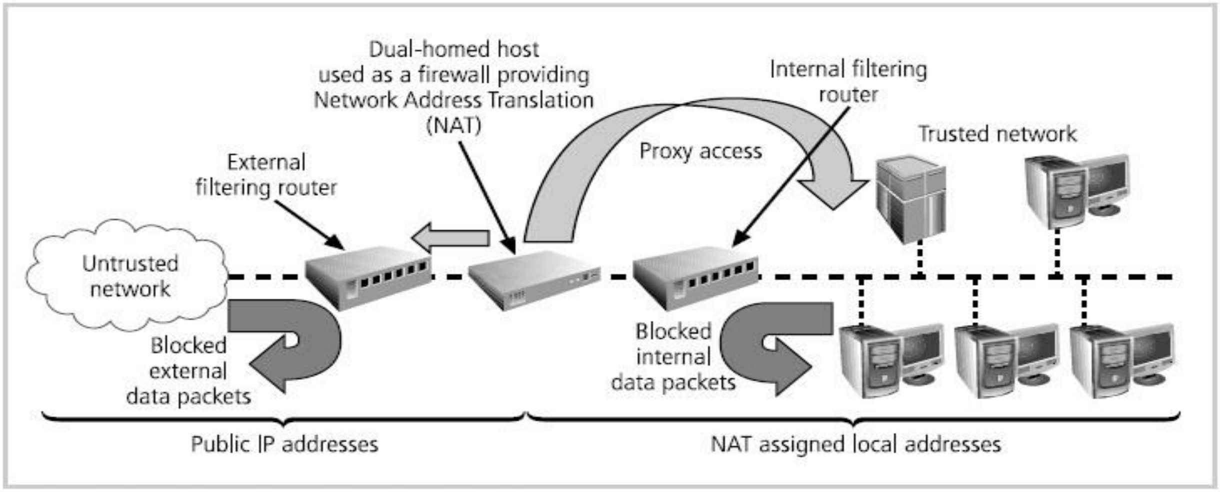

Dual-homed host used as a firewall providing Network Address Translation (NAT)
Internal filtering router
Trusted network
Proxy access
External filtering router
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT assigned local addresses

Figure 6-13 Dual-Homed Host Firewall

♣ With two NICs, all traffic must physically go through the firewall to move between the internal and external networks.

♣ Implementation of this architecture often makes use of NAT.

♣ NAT is a method of mapping real, valid, external IP addresses to special ranges of non-routable internal IP addresses, thereby creating yet another barrier to intrusion from external attackers.

Screened Subnet Firewalls (with DMZ):

♣ The architecture of a screened subnet firewall provides a DMZ.

♣ The DMZ can be a dedicated port on the firewall device linking a single bastion host, or it can be connected to a screened subnet, as shown in Figure 6-14.

♣ Connections from the outside or untrusted network are routed through an external filtering router.

♣ Connections from the outside or untrusted network are routed into—and then out of—a routing firewall to the separate network segment known as the DMZ.

♣ Connections into the trusted internal network are allowed only from the DMZ bastion host servers.

♣ The screened subnet is an entire network segment that performs two functions: o it protects the DMZ systems and information from outside threats by providing a network of intermediate security o It protects the internal networks by limiting how external connections can gain access to them.

♣ Another facet of the DMZ is the creation of an area known as an extranet.

♣ An extranet is a segment of the DMZ where additional authentication and authorization controls are put into place to provide services that are not available to the general public.

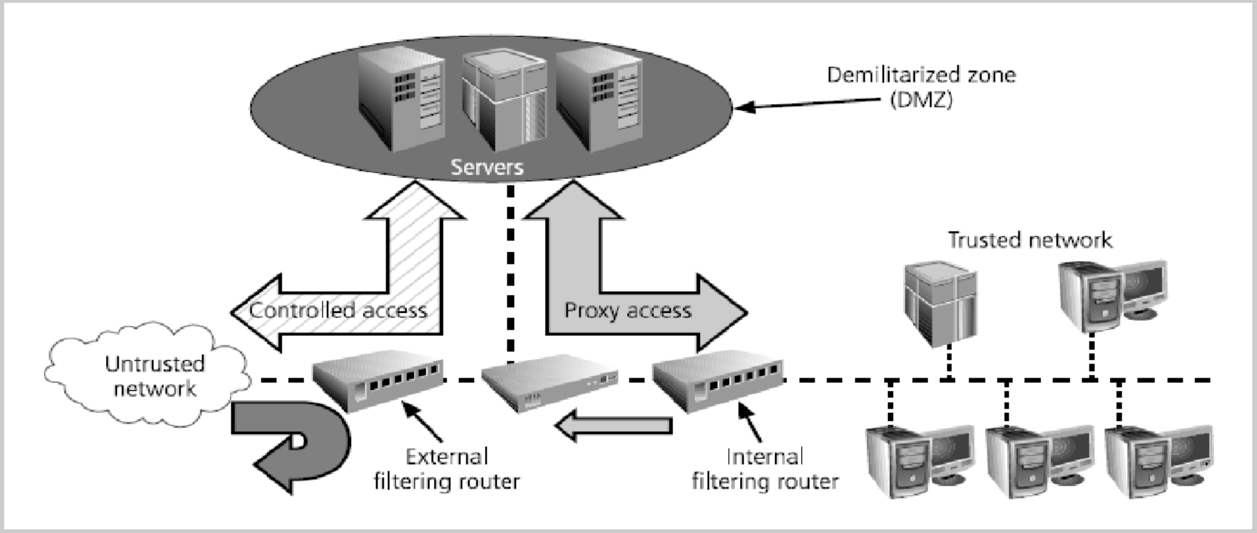


Figure 6-14 Screened Subnet (DMZ)

SOCKS Servers:

♣ SOCKS is the protocol for handling TCP traffic via a proxy server.

♣ The SOCKS system is a proprietary circuit-level proxy server that places special SOCKS client-side agents on each workstation.

♣ A SOCKS system can require support and management resources beyond those of traditional firewalls since it entails the configuration and management of hundreds of individual clients, as opposed to a single device or small set of devices.

SELECTING THE RIGHT FIREWALL:

When trying to determine which the best firewall for an organization is, you should consider the following questions:

1. Which type of firewall technology offers the right balance between protection and cost for the needs of the organization?

2. What features are included in the base price? What features are available at extra cost? Are all cost factors known?

3. How easy is it to set up and configure the firewall? How accessible are the staff technicians who can competently configure the firewall?

4. Can the candidate firewall adapt to the growing network in the target organization?

The most important factor is, of course, the extent to which the firewall design provides the required protection. The second most important factor is cost.

CONTENT FILTERS:

♥ Content filter is another utility that can help protect an organisation's systems from misuse and unintentional denial-of-service problems, and which is often closely associated with firewalls.

♥ Content filters are also called reverse firewalls because their primary purpose is to restrict internal access to external material.

♥ Content filters has two components: Rating is like a set of firewall rules for websites and is common in residential content filters.

It can be:

♣ complex, with multiple access control settings for different levels of the organization.

♣ simple, with a basic allow/deny scheme like that of a firewall. The filtering is a method used to restrict specific access requests to the identified resources, which may be websites, servers, or whatever resources the content filter administrator configures.

♥ The most common content filters restrict users from accessing Web sites with obvious non-business related material, such as pornography, or deny incoming spam e-mail.

♥ Content filters can be small add-on software programs for the home or office, such as NetNanny or SurfControl, or corporate applications, such as the Novell Border Manager.

♥ The benefit of implementing content filters is the assurance that employees are not distracted by nonbusiness material and cannot waste organizational time and resources.

♥ The downside is that these systems require extensive configuration and ongoing maintenance to keep the list of unacceptable destinations or the source addresses for incoming restricted e-mail up-to-date.

VIRTUAL PRIVATE NETWORKS

VPN is defined as “a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures.” The VPNC defines three VPN technologies: o A trusted VPN, also known as a legacy VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits. The organization must trust the service provider, who provides contractual assurance that no one else is allowed to use these circuits and that the circuits are properly maintained and protected—hence the name trusted VPN. o Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet. o A hybrid VPN combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network. A VPN that proposes to offer a secure and reliable capability while relying on public networks must accomplish the following, regardless of the specific technologies and protocols being used:

♥ Encapsulation of incoming and outgoing data, wherein the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network and be usable by the server network environment.

♥ Encryption of incoming and outgoing data to keep the data contents private while in transit over the public network, but usable by the client and server computers and/or the local networks on both ends of the VPN connection.

♥ Authentication of the remote computer and, perhaps, the remote user as well. Authentication and the subsequent authorization of the user to perform specific actions are predicated on accurate and reliable identification of the remote system and/or user. VPN can be implemented using either Transport mode or Tunnel mode. [Look at the diagrams & explain something]

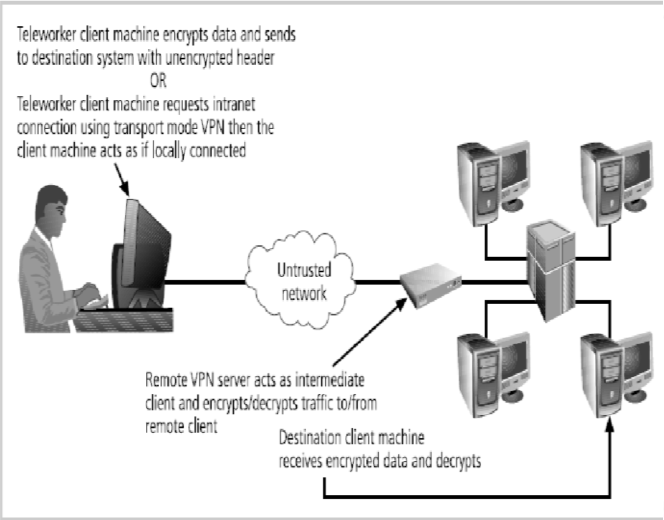

Teleworker client machine encrypts data and sends to destination system with unencrypted header
OR
Teleworker client machine requests intranet connection using transport mode VPN then the client machine acts as if locally connected
Untrusted network
Remote VPN server acts as intermediate client and encrypts/decrypts traffic to/from remote client
Destination client machine receives encrypted data and decrypts

Figure 6-19 Transport Mode VPN

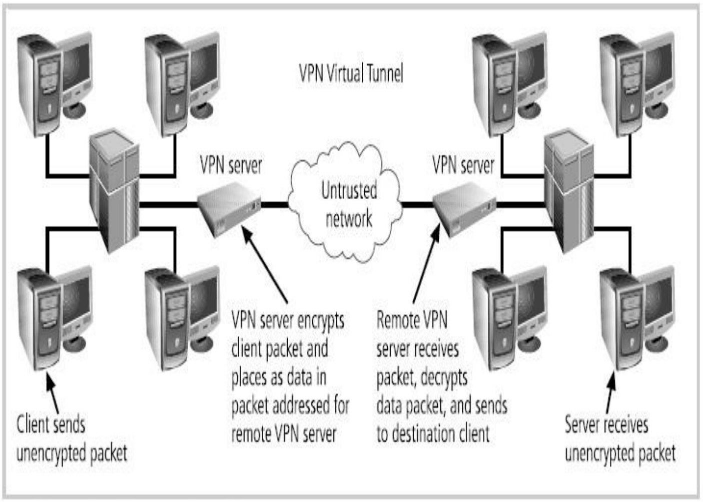

VPN Virtual Tunnel
VPN server
Untrusted network
VPN server
Client sends unencrypted packet
VPN server encrypts client packet and places as data in packet addressed for remote VPN server
Remote VPN server receives packet, decrypts data packet, and sends to destination client
Server receives unencrypted packet

Figure 6-20 Tunnel Mode VPN

INTRUSION DETECTION AND PREVENTION SYSTEMS :

♥ An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm.

♥ Even when such attacks are self-propagating, as in the case of viruses and distributed denial-of-service attacks, they are almost always instigated by someone whose purpose is to harm an organization.

♥ Intrusion prevention consists of activities that deter an intrusion.

♥ Some important intrusion prevention activities are writing and implementing good enterprise information security policy, planning and executing effective information security programs, installing and testing technology-based information security countermeasures (such as firewalls and intrusion detection systems), and conducting and measuring the effectiveness of employee training and awareness activities.

♥ Intrusion detection consists of procedures and systems that identify system intrusions.

♥ Intrusion reaction encompasses the actions an organization takes when an intrusion is detected.

♥ These actions seek to limit the loss from an intrusion and return operations to a normal state as rapidly as possible.

♥ Intrusion correction activities finalize the restoration of operations to a normal state and seek to identify the source and method of the intrusion in order to ensure that the same type of attack cannot occur again—thus reinitiating intrusion prevention.

↔ Information security intrusion detection systems (IDSs) became commercially available in the late 1990s.

↔ An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm. ↔ This alarm can be audible and/or visual (producing noise and lights, respectively), or it can be silent (an e-mail message or pager alert).

↔ With almost all IDSs, system administrators can choose the configuration of the various alerts and the alarm levels associated with each type of alert.

↔ Many IDSs enable administrators to configure the systems to notify them directly of trouble via e-mail or pagers.

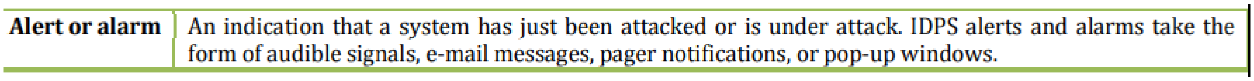
↔ The configurations that enable IDSs to provide customized levels of detection and response are quite complex.

↔ A current extension of IDS technology is the intrusion prevention system (IPS), which can detect an intrusion and also prevent that intrusion from successfully attacking the organization by means of an active response.

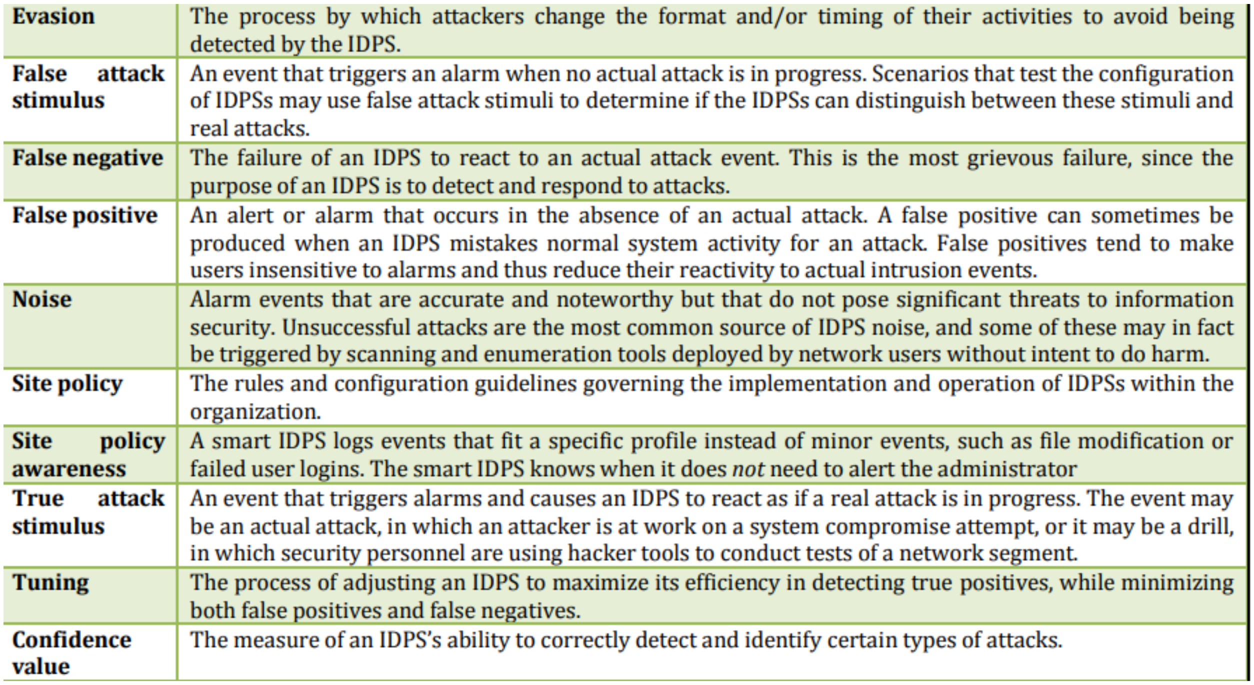
↔ Because the two systems often coexist, the combined term intrusion detection and prevention system (IDPS) is generally used to describe current anti-intrusion technologies.

IDPS TERMINOLOGY:

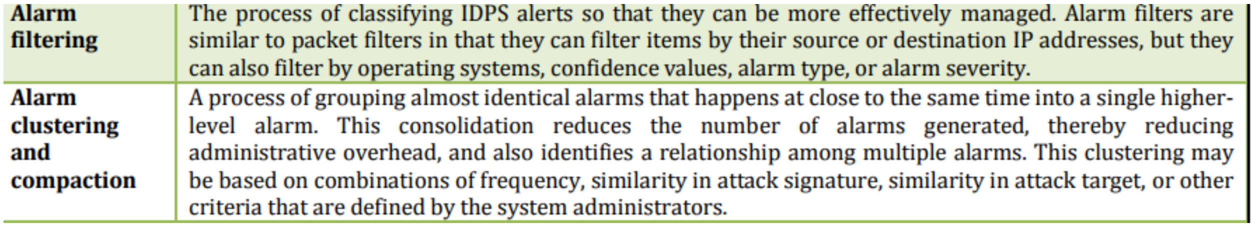
Alert or alarm An indication that a system has just been attacked or is under attack. IDPS alerts and alarms take the form of audible signals, e-mail messages, pager notifications, or pop-up windows



Alert or alarm	An indication that a system has just been attacked or is under attack. IDPS alerts and alarms take the form of audible signals, e-mail messages, pager notifications, or pop-up windows.



Evasion	The process by which attackers change the format and/or timing of their activities to avoid being detected by the IDPS.
False attack stimulus	An event that triggers an alarm when no actual attack is in progress. Scenarios that test the configuration of IDPSs may use false attack stimuli to determine if the IDPSs can distinguish between these stimuli and real attacks.
False negative	The failure of an IDPS to react to an actual attack event. This is the most grievous failure, since the purpose of an IDPS is to detect and respond to attacks.
False positive	An alert or alarm that occurs in the absence of an actual attack. A false positive can sometimes be produced when an IDPS mistakes normal system activity for an attack. False positives tend to make users insensitive to alarms and thus reduce their reactivity to actual intrusion events.
Noise	Alarm events that are accurate and noteworthy but that do not pose significant threats to information security. Unsuccessful attacks are the most common source of IDPS noise, and some of these may in fact be triggered by scanning and enumeration tools deployed by network users without intent to do harm.
Site policy	The rules and configuration guidelines governing the implementation and operation of IDPSs within the organization.
Site policy awareness	A smart IDPS logs events that fit a specific profile instead of minor events, such as file modification or failed user logins. The smart IDPS knows when it does *not* need to alert the administrator
True attack stimulus	An event that triggers alarms and causes an IDPS to react as if a real attack is in progress. The event may be an actual attack, in which an attacker is at work on a system compromise attempt, or it may be a drill, in which security personnel are using hacker tools to conduct tests of a network segment.
Tuning	The process of adjusting an IDPS to maximize its efficiency in detecting true positives, while minimizing both false positives and false negatives.
Confidence value	The measure of an IDPS's ability to correctly detect and identify certain types of attacks.



Alarm filtering	The process of classifying IDPS alerts so that they can be more effectively managed. Alarm filters are similar to packet filters in that they can filter items by their source or destination IP addresses, but they can also filter by operating systems, confidence values, alarm type, or alarm severity.
Alarm clustering and compaction	A process of grouping almost identical alarms that happens at close to the same time into a single higher-level alarm. This consolidation reduces the number of alarms generated, thereby reducing administrative overhead, and also identifies a relationship among multiple alarms. This clustering may be based on combinations of frequency, similarity in attack signature, similarity in attack target, or other criteria that are defined by the system administrators.

USE OF AN IDPS :

i. To prevent problem behaviours by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system

ii. To detect attacks and other security violations that are not prevented by other security measures

iii. To detect and deal with the preambles to attacks (commonly experienced as network probes and other
“doorknob rattling” activities)

iv. To document the existing threat
to an organization

v. To act as quality control for security design and administration, especially in large and complex enterprises

vi. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.

- IDPSs can also help administrators detect the preambles to attacks.
- Most attacks begin with an organized and thorough probing of the organization’s network environment and its defenses.
- This initial estimation of the defensive state of an organization’s networks and systems is called ***doorknob rattling*** and is accomplished by means of ***footprinting*** (activities that gather information about the organization and its network activities and assets) and ***fingerprinting*** (activities that scan network locales for active systems and then identify the network services offered by the host systems).
- A system capable of detecting the early warning signs of footprinting and fingerprinting functions like a neighbourhood watch that spots would-be burglars testing doors and windows, enabling administrators to prepare for a potential attack or to take actions to minimize potential losses from an attack.
- Data collected by an IDPS can also help management with quality assurance and continuous improvement; IDPSs consistently pick up information about

attacks that have successfully compromised the outer layers of information security controls such as a firewall.

- The IDPS can also provide forensic information that may be useful should the attacker be caught and prosecuted or sued.

TYPES OF IDP SYSTEMS:

 IDPSs operate as network- or host-based systems. o A network-based IDPS is focused on protecting network information assets.

- Two specialized subtypes of network-based IDPS are the wireless IDPS and the network behavior analysis (NBA) IDPS.
    - The wireless IDPS focuses on wireless networks
    - NBA IDPS examines traffic flow on a network in an attempt to recognize abnormal patterns like DDoS, malware, and policy violations.
- A host-based IDPS protects the server or host’s information assets; the example shown in Figure 7-1 monitors both network connection activity and current information states on host servers. The application-based model works on one or more host systems that support a single application and defends that specific application from special forms of attack.

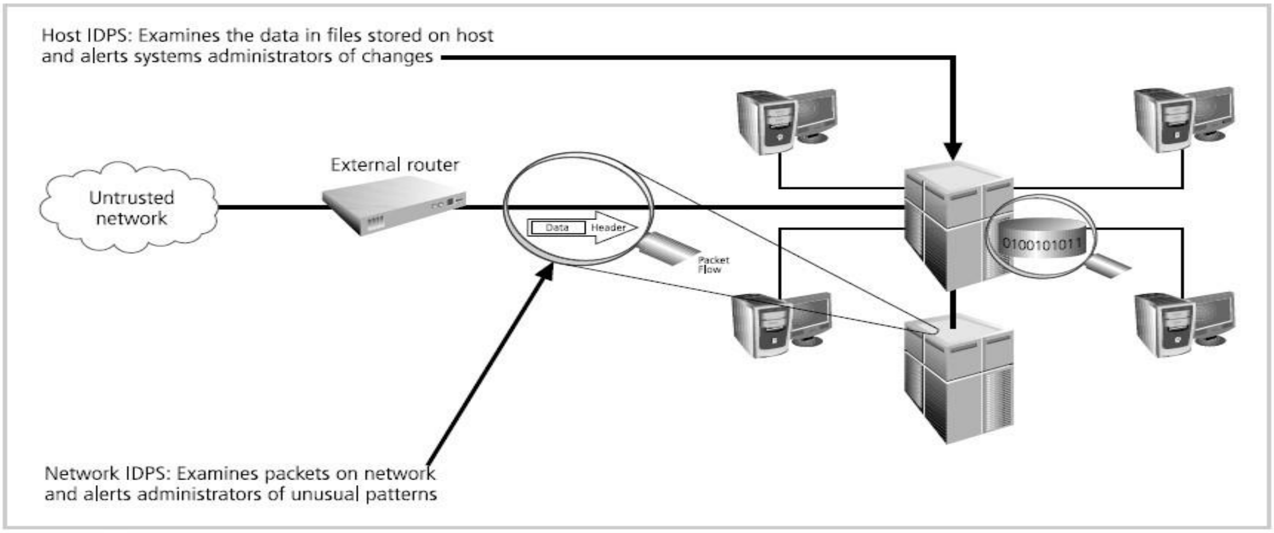

Host IDPS: Examines the data in files stored on host and alerts systems administrators of changes
External router
Untrusted network
Data
Header
Packet Flow
0100101011
Network IDPS: Examines packets on network and alerts administrators of unusual patterns

Figure 7-1 Intrusion Detection and Prevention Systems

Network-Based IDPS:

↔ A network-based IDPS (NIDPS) resides on a computer or appliance connected to a segment of an organization’s network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks.

↔ When the NIDPS identifies activity that it is programmed to recognize as an attack, it responds by sending notifications to administrators.

↔ An NIDPS can detect many more types of attacks than a host-based IDPS, but it requires a much more complex configuration and maintenance program.

↔ A NIDPS is installed at a specific place in the network from where it is possible to monitor the traffic going into and out of a particular network segment.

↔ The NIDPS can be deployed to monitor a specific grouping of host computers on a specific network segment, or it may be installed to monitor all traffic between the systems that make up an entire network.

↔ When placed next to a hub, switch, or other key networking device, the NIDPS may use that device’s monitoring port.

↔ The monitoring port also known as a switched port analysis (SPAN) port or mirror port, is a specially configured connection on a network device that is capable of viewing all of the traffic that moves through the entire device.

↔ To determine whether an attack has occurred or is underway, NIDPSs compare measured activity to known signatures in their knowledge base.

↔ In the process of protocol stack verification, the NIDPSs look for invalid data packets—that is, packets that are malformed under the rules of the TCP/IP protocol.

↔ In application protocol verification, the higher-order protocols (HTTP, FTP, and Telnet) are examined for unexpected packet behavior or improper use.

Advantages of NIDPSs

↔ Good network design and placement of NIDPS devices can enable an organization to use a few devices to monitor a large network.

↔ NIDPSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations.

↔ NIDPSs are not usually susceptible to direct attack and, in fact, may not be detectable by attackers.

Disadvantages of NIDPSs

↔ A NIDPS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected.

↔ NIDPSs require access to all traffic to be monitored.

↔ NIDPSs cannot analyze encrypted packets, making some of the network traffic invisible to the process.

↔ NIDPSs cannot reliably ascertain if an attack was successful or not.

↔ In fact, some NIDPSs are particularly vulnerable to malformed packets and may become unstable and stop functioning .

Wireless NIDPS ◊

A wireless IDPS monitors and analyzes wireless network traffic, looking for potential problems with the wireless protocols. Some issues associated with the implementation of wireless IDPSs include:

♠ Physical security: Many wireless sensors are located in public areas like conference rooms, assembly areas, and hallways in order to obtain the widest possible network range. Some of these locations may even be outdoors

♠ Sensor range: A wireless device’s range can be affected by atmospheric conditions, building construction, and the quality of both the wireless network card and access point. Some IDPS tools allow an organization to identify the optimal location for sensors by modeling the wireless footprint based on signal strength.

♠ Access point and wireless switch locations: Wireless components with bundled IDPS capabilities must be carefully deployed to optimize the IDPS sensor detection grid. The minimum range is just that; you must guard against the possibility of an attacker connecting to a wireless access point from a range far beyond the minimum.

♠ Wired network connections: Wireless network components work independently of the wired network when sending and receiving between stations and access points.

♠ Cost: The more sensors deployed, the more expensive the configuration. The wireless IDPS can also detect:

⎫ Unauthorized WLANs and WLAN devices

⎫ Poorly secured WLAN devices

⎫ Unusual usage patterns

⎫ The use of wireless network scanners

⎫ Denial of service (DoS) attacks and conditions

⎫ Impersonation and man-in-the-middle attacks

Wireless IDPSs are unable to detect certain passive wireless protocol attacks, in which the attacker monitors network traffic without active scanning and probing.

Network Behavior Analysis System ◊

NBA systems examine network traffic in order to identify problems related to the flow of traffic. They use a version of the anomaly detection method to identify excessive packet flows such as might occur in the case of equipment malfunction, DoS attacks, virus and worm attacks, and some forms of network policy violations. Typical flow data particularly relevant to intrusion detection and prevention includes:

Source and destination IP addresses

Source and destination TCP or UDP ports or ICMP types and codes.

Number of packets and bytes transmitted in the session

Starting and ending timestamps for the session

The types of events most commonly detected by NBA sensors include the following:

⎫ DoS attacks (including DDoS attacks)

⎫ Scanning

⎞ Worms

⎞ Unexpected application services (e.g., tunneled protocols, back doors, use of forbidden application protocols)

⎞ Policy violations

Host-based IDPS:

↔ A host-based IDPS (HIDPS) resides on a particular computer or server, known as the host, and monitors activity only on that system.

↔ HIDPSs are also known as system integrity verifiers because they benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files.

↔ An HIDPS has an advantage over an NIDPS in that it can access encrypted information travelling over the network and use it to make decisions about potential or actual attacks.

↔ Also, since the HIDPS works on only one computer system, all the traffic it examines traverses that system.

↔ An HIDPS is also capable of monitoring system configuration databases.

↔ The HIDPS triggers an alert when one of the following occurs: file attributes change, new files are created, or existing files are deleted.

↔ An HIDPS can also monitor systems logs for predefined events.

↔ The HIDPS maintains its own log file so that an audit trail is available even when hackers modify files on the target system to cover their tracks.

↔ The only time an HIDPS produces a false positive alert is when an authorized change occurs for a monitored file.

↔ An HIDPS classifies files into various categories and then sends notifications when changes occur.

↔ Managed HIDPSs can monitor multiple computers simultaneously by creating a configuration file on each monitored host.

Advantages of HIDPSs

↔ An HIDPS can detect local events on host systems and also detect attacks that may elude a networkbased IDPS.

↔ An HIDPS functions on the host system, where encrypted traffic will have been decrypted and is available for processing.

↔ The use of switched network protocols does not affect an HIDPS.

↔ An HIDPS can detect inconsistencies in how applications and systems programs were used by examining the records stored in audit logs.

Disadvantages of HIDPSs:

↔ HIDPSs pose more management issues because they are configured and managed on each monitored host.

↔ An HIDPS is vulnerable both to direct attacks and to attacks against the host operating system.

↔ An HIDPS is not optimized to detect multi-host scanning, nor is it able to detect the scanning of non-host network devices, such as routers or switches.

↔ An HIDPS is susceptible to some denial-of-service attacks.

↔ An HIDPS can use large amounts of disk space to retain the host OS audit logs; to function properly, it may be necessary to add disk capacity to the system.

↔ An HIDPS can inflict a performance overhead on its host systems, and in some cases may reduce system performance below acceptable levels.

IDPS DETECTION METHODS:

IDPSs use a variety of detection methods to monitor and evaluate network traffic. Three methods dominate: the signature-based approach, the statistical-anomaly approach, and the stateful packet inspection approach.

Signature-Based IDPS

♣ A signature-based IDPS (sometimes called a knowledge-based IDPS or a misuse-detection IDPS) examines network traffic in search of patterns that match known signatures—that is, preconfigured, predetermined attack patterns.

♣ Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures, for example: o footprinting and fingerprinting activities use ICMP, DNS querying, and e-mail routing analysis; o exploits use a specific attack sequence designed to take advantage of a vulnerability to gain access to a system; o DoS and DDoS attacks, during which the attacker tries to prevent the normal usage of a system, overload the system with requests so that the system's ability to process them efficiently is compromised or disrupted.

♣ A potential problem with the signature-based approach is that new attack strategies must continually be added into the IDPS's database of signatures; otherwise, attacks that use new strategies will not be recognized and might succeed.

♣ Another weakness of the signature-based method is that a slow, methodical attack might escape detection if the relevant IDPS attack signature has a shorter time frame.

♣ The only way a signature-based IDPS can resolve this vulnerability is to collect and analyze data over longer periods of time, a process that requires substantially larger data storage capability and additional processing capacity.

Statistical Anomaly-Based IDPS :

♣ The statistical anomaly-based IDPS (stat IDPS) or behavior-based IDPS collects statistical summaries by observing traffic that is known to be normal.

♣ This normal period of evaluation establishes a performance baseline.

♣ Once the baseline is established, the stat IDPS periodically samples network activity and, using statistical methods, compares the sampled network activity to this baseline.

♣ When the measured activity is outside the baseline parameters—exceeding what is called the clipping level—the IDPS sends an alert to the administrator.

♣ The baseline data can include variables such as host memory or CPU usage, network packet types, and packet quantities. ♣ The advantage of the statistical anomaly-based approach is that the IDPS can detect new types of attacks, since it looks for abnormal activity of any type.

♣ These systems require much more overhead and processing capacity than signature-based IDPSs, because they must constantly compare patterns of activity against the baseline.

♣ Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives.

♣ Because of its complexity and impact on the overhead computing load of the host computer as well as the number of false positives it can generate, this type of IDPS is less commonly used than the signature-based type.

Stateful Protocol Analysis IDPS:

♣ Stateful protocol analysis (SPA) is a process of comparing predetermined profiles of generally accepted definitions of benign activity for each protocol state against observed events to identify deviations.

♣ By storing relevant data detected in a session and then using that data to identify intrusions that involve multiple requests and responses, the IDPS can better detect specialized, multisession attacks.

♣ This process is sometimes called deep packet inspection because SPA closely examines packets at the application layer for information that indicates a possible intrusion.

♣ Stateful protocol analysis can also examine authentication sessions for suspicious activity as well as for attacks that incorporate “unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing a command upon which it is dependent, as well as ‘reasonableness’ for commands such as minimum and maximum lengths for arguments.”

♣ The models used for SPA are similar to signatures in that they are provided by vendors.

♣ It requires heavy processing overhead to track multiple simultaneous connections.

Log File Monitors :

♣ A log file monitor (LFM) IDPS is similar to a NIDPS.

♣ Using LFM, the system reviews the log files generated by servers, network devices, and even other IDPSs, looking for patterns and signatures that may indicate that an attack or intrusion is in process or has already occurred.

♣ LFM is able to look at multiple log files from a number of different systems.

♣ It requires considerable resources since it involves the collection, movement, storage, and analysis of very large quantities of log data.

IDPS RESPONSE BEHAVIOUR:

Each IDPS responds to external stimulation in a different way, depending on its configuration and function.

IDPS Response Options

♣ When an IDPS detects a possible intrusion, it has a number of response options, depending on the implementing organization’s policy, objectives, and system capabilities.

♣ When configuring an IDPS’s responses, the system administrator must exercise care to ensure that a response to an attack (or potential attack) does not inadvertently exacerbate the situation.

♣ IDPS responses can be classified as active or passive. o An active response is a definitive action automatically initiated when certain types of alerts are triggered and can include collecting additional information, changing or modifying the environment, and taking action against the intruders. o Passive response IDPSs simply report the information they have collected and wait for the administrator to act.

The following list describes some of the responses an IDPS can be configured to produce.

♣ Audible/visual alarm: The IDPS can trigger a .wav file, beep, whistle, siren, or other audible or visual notification to alert the administrator of an attack. The most common type of such notifications is the computer pop-up, which can be configured with color indicators and specific messages.

♣ SNMP traps and plug-ins: The Simple Network Management Protocol contains trap functions, which allow a device to send a message to the SNMP management console indicating that a certain threshold has been crossed, either positively or negatively.

♣ E-mail message: The IDPS can send e-mail to notify network administrators of an event. Many administrators use smart-phones and other e-mail enabled devices to check for alerts and other notifications frequently. Organizations should use caution in relying on e-mail systems as the primary means of communication between the IDPS and security personnel e-mail is inherently unreliable, and an attacker could compromise the e-mail system and block such messages.

♣ Page or phone message: The IDPS can be configured to dial a phone number and produce an alphanumeric pager or a modem noise.

♣ Log entry: The IDPS can enter information about the event (e.g., addresses, time, systems involved, and protocol information) into an IDPS system log file or operating system log file. These files can be stored on separate servers to prevent skilled attackers from deleting entries about their intrusions.

♣ Evidentiary packet dump: Organizations that require an audit trail of the IDPS data may choose to record all log data in a special way. This method allows the organization to perform further analysis on the data and also to submit the data as evidence in a civil or criminal case. Once the data has been written using a cryptographic hashing algorithm, it becomes evidentiary documentation—that is, suitable for criminal or civil court use.

♣ Take action against the intruder: Known as trap-and-trace, back-hacking, or traceback, this response option involves configuring intrusion detection systems to trace the data from the target system to the attacking system in order to initiate a counterattack. While this may sound tempting, it is ill-advised and may not be legal.

♣ Launch program: An IDPS can be configured to execute a specific program when it detects specific types of attacks. A number of vendors have specialized tracking, tracing, and response software that can be part of an organization’s intrusion response strategy.

♣ Reconfigure firewall: An IDPS can send a command to the firewall to filter out suspected packets by IP address, port, or protocol. An IDPS can block or deter intrusions via one of the following methods:

o Establishing a block for all traffic from the suspected attacker’s IP address o Establishing a block for specific TCP or UDP port traffic from the suspected attacker’s address or source network, blocking only the services that seem to be under attack. o Blocking all traffic to or from a network interface.

♣ Terminate session: Terminating the session by using the TCP/IP protocol specified packet TCP close is a simple process.

♣ Terminate connection: The last resort for an IDPS under attack is to terminate the organization’s internal or external connections. Smart switches can cut traffic to or from a specific port.

Reporting and Archiving Capabilities

Commercial IDPSs can generate routine reports and other detailed information documents, such as reports of system events and intrusions detected over a particular reporting period

Failsafe Considerations for IDPS Responses

Failsafe features protect an IDPS from being circumvented or defeated by an attacker. There are several functions that require failsafe measures. Encrypted tunnels or other cryptographic measures that hide and authenticate communications are excellent ways to secure and ensure the reliability of the IDPS

SELECTING IDPS APPROACHES AND PRODUCTS:

The following considerations and questions may help you prepare a specification for acquiring and deploying an intrusion detection product. [Since it is not very important, I have given brief notes.

For Extra info – refer text] Technical and Policy Considerations In order to determine which IDPS best meets an organization’s needs, first consider the organizational environment in technical, physical, and political terms.

ϖ **What Is Your Systems Environment?**

⎫ What are the technical specifications of your systems environment?

⎫ What are the technical specifications of your current security protections?

⎫ What are the goals of your enterprise?

⎫ How formal is the system environment and management culture in your organization?

ϖ **What Are Your Security Goals and Objectives?**

⎫ Is the primary concern of your organization protecting from threats originating outside your organization?

⎫ Is your organization concerned about insider attack?

⎫ Does your organization want to use the output of your IDPS to determine new needs?

⎫ Does your organization want to use an IDPS to maintain managerial control (non-security related) over network usage?

ϖ **What Is Your Existing Security Policy?**

⎫ How is it structured?

⎫ What are the general job descriptions of your system users?

⎫ Does the policy include reasonable use policies or other management provisions?

⎫ Has your organization defined processes for dealing with specific policy violations?

Organizational Requirements and Constraints:

Your organization’s operational goals, constraints, and culture will affect the selection of the IDPS and other security tools and technologies to protect your systems.

ϖ What Requirements Are Levied from Outside the Organization?

⎫ Is your organization subject to oversight or review by another organization?

⎫ If so, does that oversight authority require IDPSs or other specific system security resources?

⎫ Are there requirements for public access to information on your organization’s systems?

⎫ Do regulations or statutes require that information on your system be accessible by the public during certain hours of the day, or during certain date or time intervals?

⎫ Are there other security-specific requirements levied by law? Are there legal requirements for protection of personal information (such as earnings information or medical records) stored on your systems?

⎫ Are there legal requirements for investigation of security violations that divulge or endanger that information?

⎫ Are there internal audit requirements for security best practices or due diligence?

⎫ Do any of these audit requirements specify functions that the IDPSs must provide or support?

⎫ Is the system subject to accreditation?

⎫ If so, what is the accreditation authority’s requirement for IDPSs or other security protection?

⎫ Are there requirements for law enforcement investigation and resolution of security incidents?

⎫ Do they require any IDPS functions, especially having to do with collection and protection of IDPS logs as evidence?

ϖ What Are Your Organization’s Resource Constraints?

⎫ What is the budget for acquisition and life cycle support of intrusion detection hardware, software, and infrastructure?

⎫ Is there sufficient existing staff to monitor an intrusion detection system full time?

⎫ Does your organization have authority to instigate changes based on the findings of an intrusion detection system?

STRENGTHS AND LIMITATIONS OF IDPSs:

Strengths of Intrusion Detection and Prevention Systems

- Monitoring and analysis of system events and user behaviors
- Testing the security states of system configurations
- Baselining the security state of a system, then tracking any changes to that baseline
- Recognizing patterns of system events that correspond to known attacks
- Recognizing patterns of activity that statistically vary from normal activity
- Managing operating system audit and logging mechanisms and the data they generate
- Alerting appropriate staff by appropriate means when attacks are detected
- Measuring enforcement of security policies encoded in the analysis engine
- Providing default information security policies

- Allowing non-security experts to perform important security monitoring functions

Limitations of Intrusion Detection and Prevention Systems

- Compensating for weak or missing security mechanisms in the protection infrastructure, such as firewalls, identification and authentication systems, link encryption systems, access control mechanisms, and virus detection and eradication software.
- Instantaneously detecting, reporting, and responding to an attack when there is a heavy network or processing load
- Detecting newly published attacks or variants of existing attacks
- Effectively responding to attacks launched by sophisticated attackers
- Automatically investigating attacks without human intervention
- Resisting all attacks that are intended to defeat or circumvent them
- Compensating for problems with the fidelity of information sources
- Dealing effectively with switched networks .