MODULE 4

NETWORK INFRASTRUCTURE SECURITY & CONNECTIVITY

FIREWALLS:

- ✓ A **firewall** in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the **untrusted network** (for example, the Internet), and the inside world, known as the **trusted network**.
- ✓ The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices.
- ✓ Firewalls can be categorized by processing mode, development era, or structure.

Firewall Processing Modes

Firewalls fall into five major **processing-mode** categories:

1. Packet-Filtering Firewalls,
2. Application Gateways,
3. Circuit Gateways
4. Mac Layer Firewalls,
5. Hybrids.

1. Packet-Filtering Firewalls

- ✓ simply called a filtering firewall
- ✓ Examines the header information of data packets that come into a network
- ✓ A packet-filtering firewall installed on a TCP/IP- based network typically functions at the IP level and determines whether to drop a packet (deny) or forward it to the next network connection (allow) based on the rules programmed into the firewall.
- ✓ Packet-filtering firewalls 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.
- ✓ The restrictions most commonly implemented in packet-filtering firewalls are based on a combination of the following:
  - IP source and destination address

- Direction (inbound or outbound)
- Protocol (for firewalls capable of examining the IP protocol layer)
- Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests (for firewalls capable of examining the TCP/UPD layer)

- ✓ Simple firewall models examine two aspects of the packet header: the destination and source address.
- ✓ They enforce **address restrictions**, rules designed to prohibit packets with certain addresses or partial addresses from passing through the device.
- ✓ They accomplish this through ACLs, which are created and modified by the firewall administrators

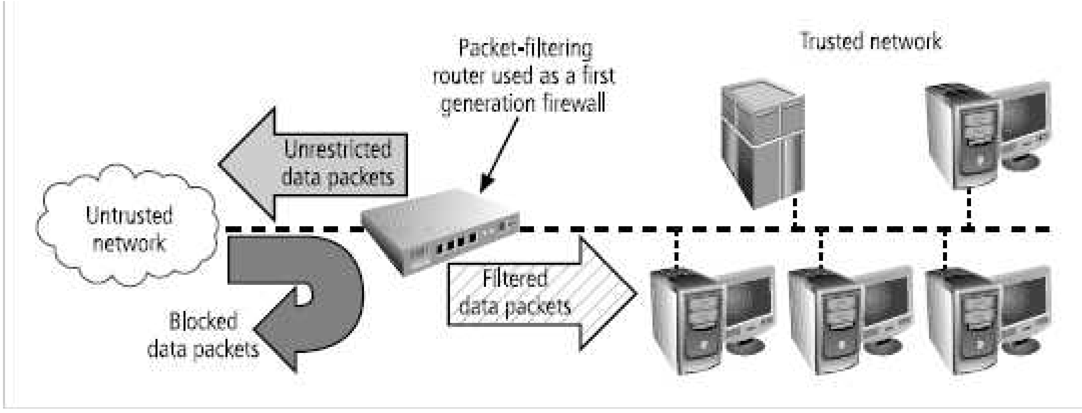
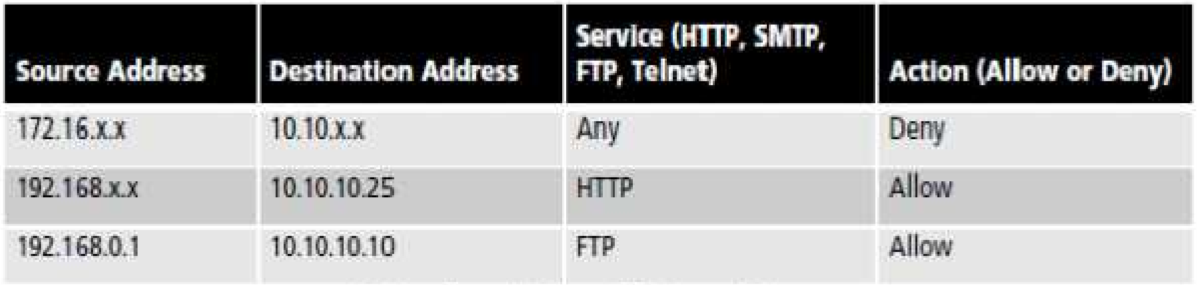

Packet-filtering router used as a first generation firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

Fig : Packet-Filtering Router



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 : Sample Firewall Rule and Format

There are three subsets of packet-filtering firewalls:

- **a. Static Filtering,**
- **b. Dynamic Filtering,**
- **c. Stateful Inspection.**

a. **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. Any changes to the rules require human intervention. This type of filtering is common in network routers and gateways.

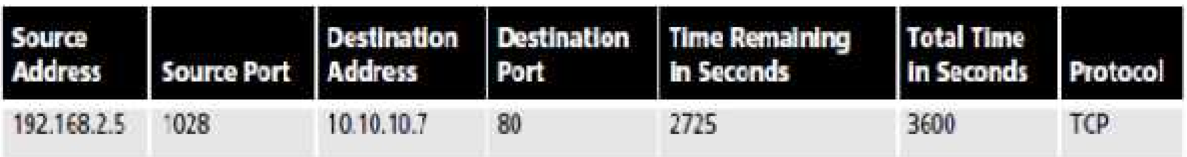
b. **Dynamic packet-filtering firewall** allows only a particular packet with a particular source, destination, and port address to enter. It does this by opening and closing "doors" in the firewall based on the information contained in the packet header.

c. **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 but they take it a step further. Whereas simple packet-filtering firewalls only allow or deny certain packets based on their address, a stateful firewall can expedite incoming packets that are responses to internal requests.

If the stateful firewall receives an incoming packet that it cannot match in its state table, it refers to its ACL to determine whether to allow the packet to pass.

- ✓ **The primary disadvantage** of this type of firewall is the additional processing required to manage and verify packets against the state table. This can leave the system vulnerable to a DoS or DDoS attack. In such an attack, the system receives a large number of external packets, which slows the firewall because it attempts to compare all of the incoming packets first to the state table and then to the ACL.



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 : State Table Entries

2. 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.
- ✓ For example, an organization that runs a Web server can avoid exposing the server to direct user traffic by installing a proxy server configured with the registered domain's URL.
- ✓ 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.**
- ✓ The benefits from this type of implementation are significant. The proxy server is placed in an unsecured area of the network or in the demilitarized zone (DMZ)—an intermediate area between a trusted network and an untrusted network—so that it, rather than the Web server, is exposed to the higher levels of risk from the less trusted networks.
- ✓ Additional filtering routers can be implemented behind the proxy server, limiting access to the more secure internal system, and thereby further protecting internal systems.
- ✓ 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.
- ✓ Since application firewalls work at the application layer (hence the name), they are typically restricted to a single application (e.g., FTP, Telnet, HTTP, SMTP, and SNMP).

3. Circuit Gateways

- ✓ The **circuit gateway firewall** operates at the transport layer.
- ✓ Again, connections are authorized based on addresses. Like filtering firewalls, circuit gateway firewalls 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.
- ✓ John Wack describes the operation of a circuit gateway as follows: "A circuit level gateway relays TCP connections but does no extra processing or filtering of the protocol i.e., since once the connection between the source and destination is established, the firewall simply passes bytes between the systems.

4. MAC Layer Firewalls

- ✓ MAC layer firewalls are designed to operate at the media access control sub layer 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.
- ✓ 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.

5. 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.

Firewall Architectures

- ✓ There are four common architectural implementations:

1. Packet-filtering routers
2. Screened host firewalls
3. Dual-homed firewalls
4. Screened subnet firewalls.

1. Packet Filtering Routers (Refer above PFF)

2. 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 prescreen 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** it can be a rich target for external attacks and should be very thoroughly secured.
- ✓ To its advantage, this configuration requires the external attack to compromise two separate systems before the attack can access internal data. In this way, the bastion host protects the data more fully than the router alone.

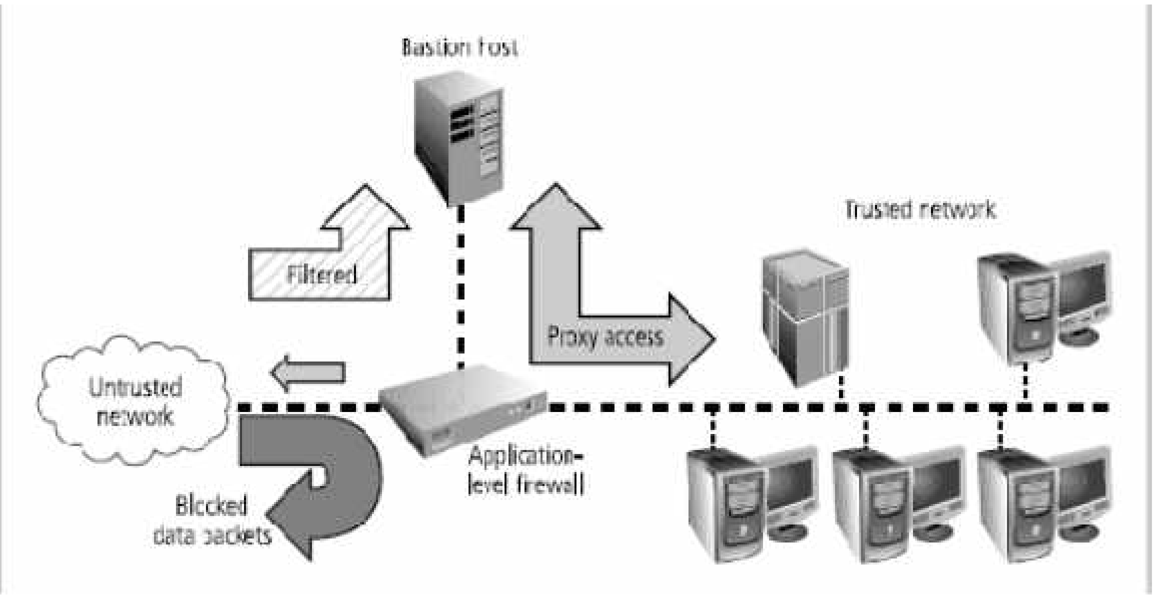


Fig : Screened Host Firewall

3. Dual-Homed Host Firewalls

- ✓ The next step up in firewall architectural complexity is the dual-homed host.
- ✓ When this architectural approach is used, the bastion host contains two NICs (network interface cards) rather than one, as in the bastion host configuration.
- ✓ One NIC is connected to the external network, and one is connected to the internal network, providing an additional layer of protection.
- ✓ 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 nonroutable internal IP addresses, thereby creating yet another barrier to intrusion from external attackers.
- ✓ Another benefit of a dual-homed host is its ability to translate between many different protocols at their respective data link layers, including Ethernet, token ring, Fiber Distributed Data Interface (FDDI), and asynchronous transfer mode (ATM).
- ✓ On the downside, if this dual-homed host is compromised, it can disable the connection to the external network, and as traffic volume increases it can become overloaded. However, compared to more complex solutions this architecture provides strong overall protection with minimal expense.

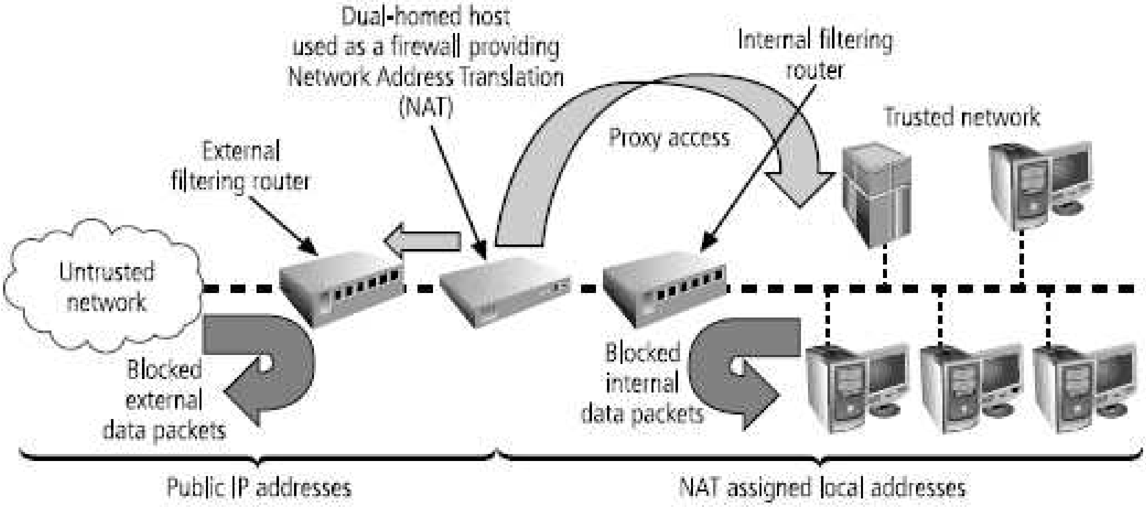

Dual-homed host used as a firewall providing Network Address Translation (NAT)
Internal filtering router
Trusted network
Proxy access
External filtering router
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT assigned local addresses

Fig: Dual-Homed Host Firewall

4. Screened Subnet Firewalls (with DMZ)

- ✓ The dominant architecture used today is the screened subnet firewall.
- ✓ 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 .
- ✓ Until recently, servers providing services through an untrusted network were commonly placed in the DMZ.
- ✓ Examples of these include Web servers, file transfer protocol (FTP) servers, and certain database servers.
- ✓ More recent strategies using proxy servers have provided much more secure solutions.

- ✓ A common arrangement finds the subnet firewall consisting of two or more internal bastion hosts behind a packet-filtering router, with each host protecting the trusted network.
- ✓ There are many variants of the screened subnet architecture. The first general model consists of two filtering routers, with one or more dual-homed bastion hosts between them.

- ✓ In the second general model, the connections are routed as follows:
- 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.

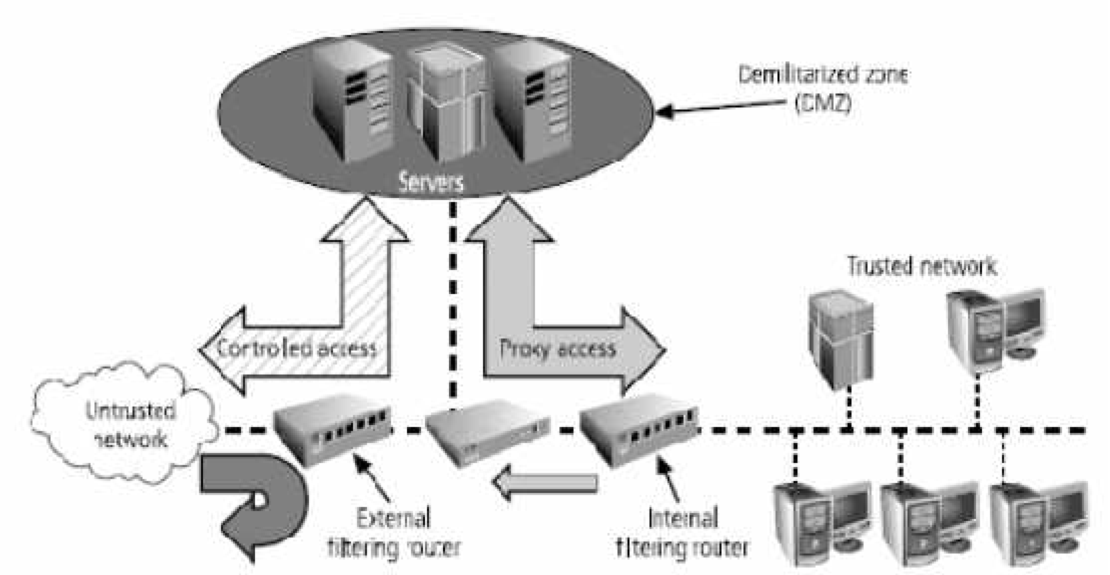


Fig : Screened Subnet (DMZ)

- ✓ The **screened subnet** is an entire network segment that performs two functions: it protects the DMZ systems and information from outside threats by providing a network of intermediate security (more secure than the general public networks but less secure than the internal network)
- ✓ 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.
- ✓ An example is an online retailer that allows anyone to browse the product catalog and place items into a shopping cart, but requires extra authentication and authorization when the customer is ready to check out and place an order.

Intrusion Detection and Prevention Systems

- ✓ **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.
- ✓ **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.
- ✓ **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.
- ✓ 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 systems can also be configured—again like a burglar alarm—to notify an external security service organization of a “break-in.”

- ✓ 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.

IDPS Terminology

1. **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.
2. **Evasion:** The process by which attackers change the format and/or timing of their Activities to avoid being detected by the IDPS.
3. **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.
4. **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.
5. **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.
6. **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.
7. **Site policy**: The rules and configuration guidelines governing the implementation and operation of IDPSs within the organization.
8. **Site policy awareness**: An IDPS's ability to dynamically modify its configuration in response to environmental activity. A so-called smart IDPS can adapt its

reactions in response to administrator guidance over time and circumstances of the current local environment. 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—for example, when an attack is using a known and documented exploit that the system is protected from.

9. **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.
10. **Tuning:** The process of adjusting an IDPS to maximize its efficiency in detecting true positives, while minimizing both false positives and false negatives.
11. **Confidence value**: The measure of an IDPS's ability to correctly detect and identify certain types of attacks. The confidence value an organization places in the IDPS is based on experience and past performance measurements. The confidence value, which is based upon fuzzy logic, helps an administrator determine how likely it is that an IDPS alert or alarm indicates an actual attack in progress. For example, if a system deemed 90 percent capable of accurately reporting a denial-of-service attack sends a denial-of-service alert, there is a high probability that an actual attack is occurring.
12. **Alarm filtering**: The process of classifying IDPS alerts so that they can be more effectively managed. An IDPS administrator can set up alarm filtering by running the system for a while to track what types of false positives it generates and then adjusting the alarm classifications. For example, the administrator may set the IDPS to discard alarms produced by false attack stimuli or normal network operations. 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.
13. **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.

Why Use an IDPS?

1. To prevent problem behaviours by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system.
2. To detect attacks and other security violations that are not prevented by other security Measures.
3. To detect and deal with the preambles to attacks (commonly experienced as network probes and other "doorknob rattling" activities)
4. To document the existing threat to an organization.
5. To act as quality control for security design and administration, especially in large and complex enterprises
6. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.
7. If internal and external users know that an organization has an intrusion detection and prevention system, they are less likely to probe or attempt to compromise it, just as criminals are much less likely to break into a house that has an apparent burglar alarm.

Types of IDPS

- ★ IDPSs operate as **network- or host-based systems.**
  1. **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 Behaviour 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.
  2. A host-based IDPS protects the server or host's information assets.
     - ✓ The example shown in fig monitors both network connection activity and current information states on host servers.

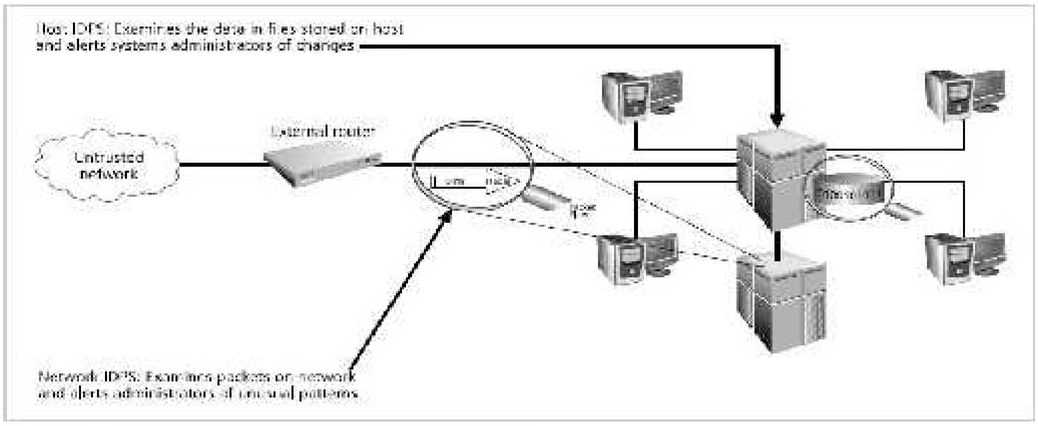

Host IDPS: Examines the data in files stored on host and alerts systems administrators of changes
External router
Untrusted network
Network IDPS: Examines packets on network and alerts administrators of unusual patterns

Figure 7-1 Intrusion Detection and Prevention Systems

1. 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 mconfiguration 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 specifically 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.

The **advantages** of NIDPSs include the following:

- ★ 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 :

- ★ 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 analyse 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

1a. 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.

1b. 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 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

2. **Host-Based IDPS**
   - ✓ While a network-based IDPS resides on a network segment and monitors activities across that segment, 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 traveling 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.
   - ✓ HIDPSs work on the principle of configuration or change management, which means that they record the sizes, locations, and other attributes of system files.
   - ✓ 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 examines these files and logs to determine if an attack is underway or has occurred and if the attack is succeeding or was successful.
   - ✓ 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.
   - ✓ Once properly configured, an HIDPS is very reliable.
   - ✓ The only time an HIDPS produces a false positive alert is when an authorized change occurs for a monitored file.
   - ✓ This action can be quickly reviewed by an administrator, who may choose to disregard subsequent changes to the same set of files.
   - ✓ If properly configured, an HIDPS can also detect when users attempt to modify or exceed their access authorization level.

The advantages of HIDPSs include:

1. An HIDPS can detect local events on host systems and also detect attacks that may elude a network-based IDPS.

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

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

4. An HIDPS can detect inconsistencies in how applications and systems programs were used by examining the records stored in audit logs. This can enable it to detect some types of attacks, including Trojan horse programs.

The disadvantages of HIDPSs include:

1. HIDPSs pose more management issues because they are configured and managed on each monitored host. Operating an HIDPS requires more management effort to install, configure, and operate than does a comparably sized NIDPS solution.

2. An HIDPS is vulnerable both to direct attacks and to attacks against the host operating system. Either circumstance can result in the compromise and/or loss of HIDPS functionality.

3. An HIDPS is not optimized to detect multihost scanning, nor is it able to detect the scanning of non-host network devices, such as routers or switches. Unless complex correlation analysis is provided, the HIDPS will not be aware of attacks that span multiple devices in the network.

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

5. 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.

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:
  - footprinting and fingerprinting activities use ICMP, DNS querying, and e-mail

routing analysis;

- exploits use a specific attack sequence designed to take advantage of a vulnerability to gain access to a system;
- 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.

Honeypots, Honeynets, and Padded Cell Systems

- ✓ powerful security tools that go beyond routine intrusion detection is known variously as honeypots, honeynets, or padded cell systems.
- ✓ **Honeypots** are decoy systems designed to lure potential attackers away from critical systems.
- ✓ In the industry, they are also known as decoys, lures, and fly-traps. When a collection of honeypots connects several honeypot systems on a subnet, it may be called a **honeynet**.
- ✓ A honeypot system (or in the case of a honeynet, an entire subnetwork) contains pseudo-services that emulate well-known services, but is configured in ways that make it look vulnerable to attacks.
- ✓ This combination is meant to lure potential attackers into committing an attack, thereby revealing themselves—the idea being that once organizations have detected these attackers, they can better defend their networks against future attacks targeting real assets.
- ✓ In sum, honeypots are designed to do the following:
  - Divert an attacker from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps, respond
- ✓ A **padded cell** is a honeypot that has been protected so that that it cannot be easily
- ✓ compromised—in other words, a hardened honeypot. In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS.
- ✓ When the IDPS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm—the nature of this host environment is what gives the approach the name "padded cell."
- ✓ As in honeypots, this environment can be filled with interesting data,which can convince an attacker that the attack is going according to plan.
- ✓ Like honeypots, padded cells are well-instrumented and offer unique opportunities for a target organization to monitor the actions of an attacker.

Advantages:

- ✓ Attackers can be diverted to targets that they cannot damage.
- ✓ Administrators have time to decide how to respond to an attacker.
- ✓ Attackers' actions can be easily and more extensively monitored, and the records can be used to refine threat models and improve system protections.
- ✓ Honeypots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- ✓ The legal implications of using such devices are not well understood.
- ✓ Honeypots and padded cells have not yet been shown to be generally useful security technologies.
- ✓ An expert attacker, once diverted into a decoy system, may become angry and launch a more aggressive attack against an organization's systems.
- ✓ Administrators and security managers need a high level of expertise to use these systems.