Network Security Technologies

Learning Objective

After studying this chapter, you should be able to:

- Examine some types of network security technologies
- Understand how these security technologies work
- Understand what type of threats can be stopped by each type
- Understand the limitation (what they cannot do) of each type

1.Introduction

There are tools and devices developed specifically for network security. These tools act as a wall between the internal network and any malicious activity. This wall will remain penetrable until you opt for the best solution to protect it. The following types of network security technologies help you understand which one suits your organization better than the others (based on your organization's requirements). The most important devices and tools for our course are firewalls and intrusion detection systems.

2.Firewalls

A Firewall is a network security device designed to restrict access to resources (information or services) according to security policy. Firewall is not a magic solution to network security problems, nor are they a complete solution for remote attacks or authorised access to data. Firewalls are used to separate two networks. Most often they are used to separate an internal corporate network from an external public network. Firewalls can also be used to separate internal networks. You may have certain areas of your network that you want to secure the general network traffic. You may want to separate your user network from your infrastructure network or your data network. Firewalls can be implemented using hardware or software. Many software firewalls come preinstalled on hardware with a hardened OS.

We can summarize what one can expect from a firewall. The following capabilities are within the scope of a firewall:

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.
2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
4. A firewall can serve as the platform for IPsec. Using the tunnel mode capability, described later in this course, the firewall can be used to implement virtual private networks.

Firewalls have their limitations, including the following:

1. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.
2. The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall.
4. A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally.

3.Types of Firewalls

A firewall can monitor network traffic at a number of levels, from low-level network packets either individually or as part of a flow, to all traffic within a transport connection, up to inspecting details of application protocols. The choice of which level is appropriate is determined by the desired firewall access policy. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria. The criteria implement the access policy for the firewall. Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. In this section, we look at the principal types of firewalls.

3.1.Packet Filtering Firewall

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- Source IP address: The IP address of the system that originated the IP packet (e.g., 192.178.1.1).
- Destination IP address: The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2).
- Source and destination transport-level address: The transport-level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET.
- IP protocol field: Defines the transport protocol.
- Interface: For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for.

The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. Two default policies are possible:

- Default discard: That which is not expressly permitted is prohibited
- Default forward: That which is not expressly prohibited is permitted

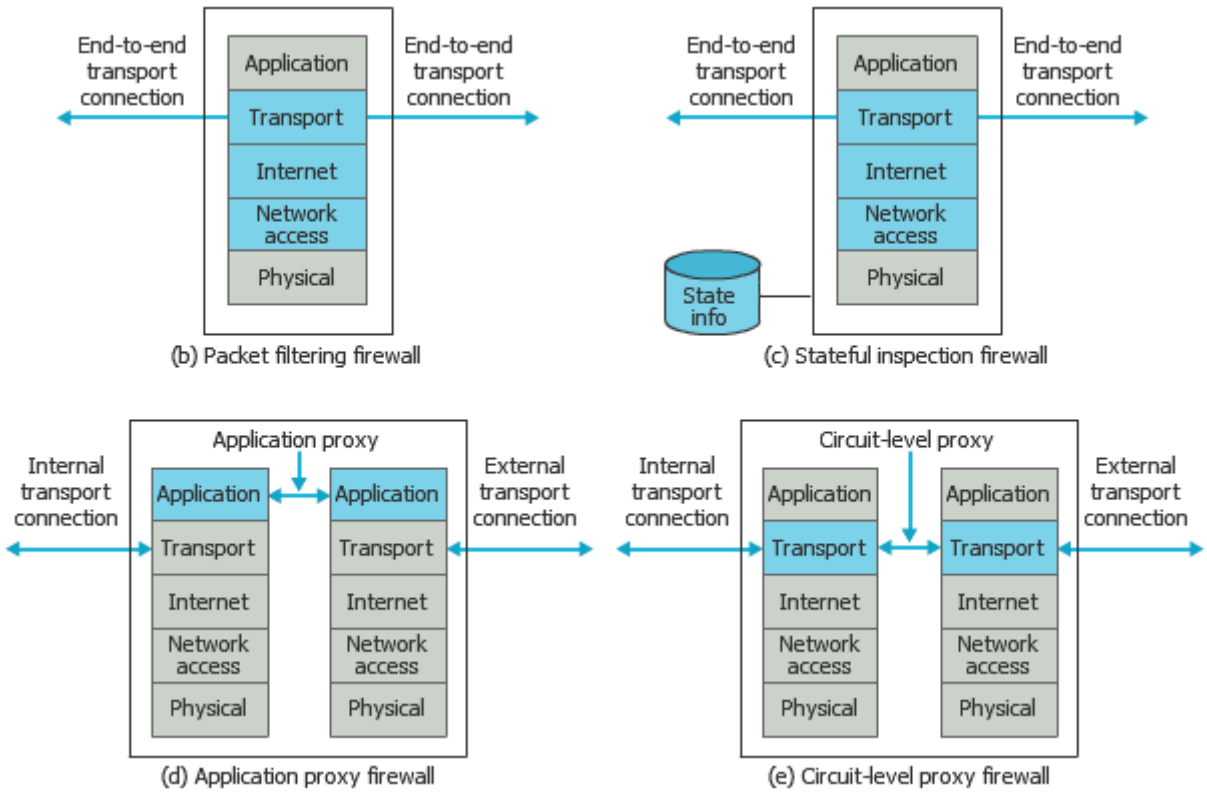
The default discard policy is more conservative. Initially, everything is blocked, and services must be added on a case-by-case basis. This policy is more visible to users, who are more likely to see the firewall as a hindrance. However, this is the policy likely to be preferred by businesses and government organizations. Further, visibility to users diminishes as rules are created. The default forward policy increases ease of use for end users but provides reduced security, the security administrator must, in essence, react to each new security threat as it becomes known. This policy may be used by generally more open organizations, such as universities.

One advantage of a packet filtering firewall is its simplicity. Also, packet filters typically are transparent to users and are very fast. The main weaknesses of packet filter firewalls are:

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions.

For example, if a packet filter firewall allows a given application, all functions Available within that application will be permitted.

- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing.
- Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet filter firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy.



Figure(3.1): Type of Firewalls [1]

3.2.Stateful Inspection Firewalls (Dynamic Packet Filtering)

A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher-layer context. The main idea of stateful inspection is to guide the filtering to connection, allowing the filtering mechanism to know the connections and based on this it would legitimize a packet or not. This auxiliary feature is known as connection table or status table.

With the status table, every connection start is properly registered (a new status is created). When the packet returns, before starting the process of evaluating the access rules, the stateful firewall checks the status table, validating if there is any associated connection and, if it does, accepts the connection without processing the rules. Otherwise, discard the package.

The security of the environment is substantially increased by using of a stateful firewall, considering that there is traceability of parameters used to validate an active connection in the structure.

A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections. Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking. Some even inspect limited amounts of application data for some well-known protocols like FTP, IM and SIPS commands, in order to identify and track related connections.

As the connection evolves in terms of packet exchanges, the status table is always updated with the information, in order to ensure continuity of security and integrity. This process also guarantees the validity of the connection, without it being necessary to evaluate the access rules defined by the administrator.

The main advantages of stateful inspection firewalls are:

- A stateful firewall provides full protocol inspection, thereby eliminating additional attacks surface.
- A stateful firewall acts a building block for more advanced application layer firewalls or gateways.
- A stateful firewall understands the network flow and can identify data packets of a flow, thereby enabling simple rule writing for bidirectional connections or pseudo state networking protocols.

- Since a stateful firewall can look deeper into packet payloads, it can understand complex protocols that negotiate communication port and protocol at runtime and apply firewall policies accordingly. Examples of such protocols are: FTP, P2P protocols, etc.

3.3.Application Level Proxy

An application level firewall evaluates network packets for valid data at the application layer before allowing a connection. The firewall examines the data in all network packets at the application layer and maintains complete connection state and sequencing information. Other security items such as user password and service requests that appear in the application layer data can be validated by the firewall. Specialized application software and proxy services are included in most application layer firewalls. Proxy services manage traffic through a firewall for a specific service such as HTTP or FTP. Proxy services can provide increased access control, detailed checks for valid data, and generate audit records about the traffic they transfer because the proxy services are specific to the protocol that they are designed to forward. The proxy determines whether to accept or deny the packet based on the results of the rules comparison. Based on how it was configured, the proxy may also perform other functions such as URL filtering, data modification, authentication logging, and HTTP object caching.

A proxy service consists of the proxy server, proxy client and protocol analysis modes of operation. A proxy server and a proxy client are two components that are typically implemented as a single executable for each application proxy. A proxy server acts as the end server for all connection requests originated on a trusted network by a real client. Rather than allowing users to communicate directly with the other servers on the Internet, all communication between the internal users on the trusted network and the Internet passes through the proxy server.

When the internal users want to connect to an external service such as FTP or Telnet:

- They send a request to the proxy server for the connection.
- The proxy server decides whether to permit or deny the request based on an evaluation of a set of rules that is managed for the individual network service.

- Proxy servers only allow those packets through that comply with the protocol definitions because the servers understand the protocol of the service they are evaluating.
- The proxy client is the component that talks to the server on the external network on behalf of the real client on the trusted network.
- The proxy server evaluates a real client's request for a service against the policy rules defined for that proxy and determines whether to approve the request.
- The proxy server forwards the request to the proxy client if the request is approved.
- The proxy client contacts the real server on the external network on behalf of the client.
- The proxy client relays requests from the proxy server to the real server and relays responses from the real server to the proxy server.
- Then the proxy server relays the requests and responses between the proxy client and the real client.

Proxy services never allow direct connection between the real client on the trusted network and the real server on the external network. Proxy services force all network packets to be examined and filtered for suitability. All communication between the real user and the real service are handled by the proxy service. The proxy service is transparent to the user on the trusted network and the real service on the external network.

Proxy services are slower than packet filtering because each packet in a session is subjected to an examination process. Once in the application space the proxies perform a thorough inspection of the packet headers and packet data. Additional checks can be performed by application level firewalls to ensure that a network packet has not been spoofed.

Application level firewall technology using proxy services has several advantages such as:

- Proxy services enforce high level protocols such as HTTP and FTP.
- Information about the communications passing through the firewall server is maintained by the proxy service.

- Proxy services can permit access to certain network services, while denying access to others.
- Packet data can be processed and manipulated by proxy services.
- Internal IP addresses are shielded from the external world because proxy services do not allow direct communications between external server and internal computers.
- Administrators are able to monitor attempts to violate the firewall's security policies using the audit records that proxy services can generate.

Although application level firewalls provide increased security over other type of firewalls there are some disadvantages to using an application level firewall such as:

- Application level firewalls are slower since inbound data is processed by the application and by its proxy.
- A new proxy usually must be written for each protocol that is to pass through the firewall. This can cause the number of available network services and their scalability to be limited.
- Proxy services are vulnerable to operating system and application level bugs.
- Most application level firewalls require extensive support from the operating system to run correctly.
- The security of the firewall server can be effected by problems in these operating system components.
- Most application level firewalls require licenses and update from its manufacturer.

3.4.Circuit-Level Gateway

A fourth type of firewall is the circuit-level gateway or circuit-level proxy. This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection, rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

3.5.Choosing a Firewall

When determining which firewall technology to use the system administrator needs to evaluate several opposing aspects. There is a tradeoff between performance and security. The performance and security tradeoff is based on how far up the network stack the packet must travel, as well as what level of security checks are being performed on each packet. Generally packet filter firewalls provide the highest level of performance, followed by stateful packet filtering and then application level firewalls. The level of security checks normally follows a reverse order of performance because as network packets pass through more protocol layers, they are inspected in more detail. Therefore, application level firewalls are considered more secure than stateful packet filtering firewalls, which are more secure than packet filtering firewalls. In an application level firewall all the network packets are sent up one network stack and down a different stack resulting in two separate network sessions. This makes application level firewalls generally the slowest firewall technology. The processing time required for network packet movement is greater with application level firewalls because these firewalls implement the broadest set of security checks. Application level firewalls are considered to generally provide the best security. When implementing a firewall solution an organization needs to evaluate the advantages and disadvantages of each firewall technology and apply the best solution to meet the organization's security requirements.

4.Firewall Location and Configuration

A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network. With that general principle in mind, a security administrator must decide on the location and on the number of firewalls needed. In this section, we look at some common options.

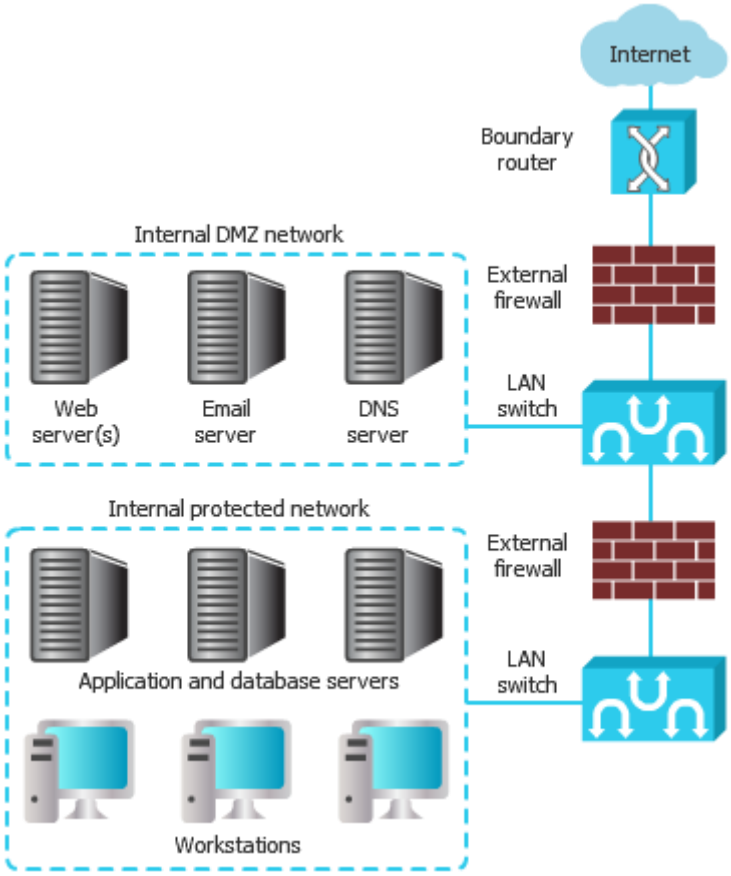
4.1.DMZ Networks

The most common distinction, that between an internal and an external firewall. An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server.

The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. The external firewall also provides a basic level of protection for the remainder of the enterprise network. In this type of configuration, internal firewalls serve three purposes:

- The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.
- The internal firewall provides two-way protection with respect to the DMZ.
- First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Such attacks might originate from worms, rootkits, bots, or other malware lodged in a DMZ system. Second, an internal firewall can protect the DMZ systems from attack from the internal protected network.
- Multiple internal firewalls can be used to protect portions of the internal network from each other. For example, firewalls can be configured so that internal servers are protected from internal workstations and vice versa. A

common practice is to place the DMZ on a different network interface on the external firewall from that used to access the internal networks.



Figure(3.2): Firewall Networking [2]

5.What Do not Firewalls Do?

Even with a firewall, there are still many areas of risk for your network. The most important ones are:

- Malicious use of authorized services: A firewall cannot, for instance, prevent someone from using an authenticated Telnet session to compromise your internal machines or from tunneling an unauthorized protocol through another, authorized protocol.
- Users not going through the firewall: A firewall can only restrict connections that go through it. It cannot protect you from people who can go around the firewall, for example, through a dial-up server behind the firewall. It also

cannot prevent an internal intruder from hacking an internal system. To detect and thwart these kinds of threats, you may need a properly configured intrusion detection/prevention system.

- Social engineering: If intruders can somehow obtain passwords they are not authorized to have or otherwise compromise authentication mechanisms through social engineering mechanisms, the firewall won't stop them. For example, a hacker could call your users pretending to be a system administrator and ask them for their passwords to "fix some problem".
- Flaws in the host operating system: A firewall is only as secure as the operating system on which it is installed. There are many flaws present in operating systems that a firewall cannot protect against. This is why it is important to properly secure the operating system and apply the necessary security patches before you install the firewall and on a periodic basis thereafter.
- Packet filter, circuit level, and stateful firewalls do not check content. Even Application-Proxy Firewalls may not perform thorough checks on content. An increasing number of services are being offered across the Internet using TCP port 80, (HTTP) no longer just Web page access. This makes it increasingly difficult for Firewalls to allow or block access to different services.

Encrypted data is a problem for Firewalls. Encryption is becoming more widespread. SSH, TLS etc are end-to-end client to server, any system in between cannot decode data. Users can visit unknown Websites, i.e. non-productive business time and download cannot be anti-virus checked.

6.Firewalls in Context

Firewalls protect against network threats, whithout understanding of operating system or application vulnerably. Firewall must be between the good guy and the bad guy if they are to be any help. A good Firewall is good for network security. A strong Firewall needs to be supported by strong security elsewhere Such as network intrusion detection systems, internal and external detectors. Host intrusion detection system on internal machines, secure application on internal clients and servers, and strong passwords on user accounts.

7.Intrusion Detection System (IDS)

Perimeter security devices (e.g. Firewalls) and computer security mechanisms (e.g. application and OS security) can only offer best effort at preventing attacks. They may fail to do so: a Firewall may be mis-configured, a password may be sniffed off the network, a new attack type may emerge (Zero-day attacks), they do not detect when an attack is underway or has taken place, and they do not react to attacks.

An Intrusion Detection System (IDS) is a network security system designed to identify intrusive or malicious behavior via monitoring of network activity. The IDS identifies suspicious patterns that may indicate an attempt to attack, break in to, or otherwise compromise a system. An IDS can be network-based or host-based, passive or reactive, and can rely on either misuse detection or anomaly detection. Although Intrusion Detection Systems are a valuable addition to an organization's security infrastructure, there are things they do well, and other things they do not do well. As you plan the security strategy for your organization's systems, it is important for you to understand what IDSs should be trusted to do and what goals might be better served by other types of security mechanisms.

The following capabilities are within the scope of Intrusion detection 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.

Intrusion detection systems have their limitations, including the following:

- Compensating for weak or missing security mechanisms in the protection infrastructure. Such mechanisms include firewalls, identification and authentication, link encryption, access control mechanisms, and virus detection and eradication.
- Directly 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 attacks that are intended to defeat or circumvent them.
- Compensating for problems with the fidelity of information sources.
- Dealing effectively with switched networks.

8.IDS vs Firewalls

Firewall and IDS both work to protect against attacks and network intrusions threats. The firewall's job is to keep intruders from breaking into the network, the IDS doesn't keep them out, but it keeps track of attempts to break in. A firewall restricts access to the network by screening traffic and deciding which packets should be allowed in, according to the security policy. We can compare it to a security guard deciding who can get clearance. The firewall monitors the ports that connect the network to the Internet and checks data packets before allowing them to pass through. If firewalls are security guards, IDSs are security cameras. An IDS monitors traffic and spots patterns of activity, and alerts if it concludes that the network is under attack.

9.Intrusion Detection Approach

There are two primary approaches to analyzing events to detect attacks: signature based detection and anomaly detection. Signature based detection, in which the analysis targets something known to be “bad”. Anomaly detection, in which the analysis looks for abnormal patterns of activity.

Signature Based Detection

This approach is often referred to “knowledge based” or “Misuse detection” or “Signature Detection”. It is based on the search for evidence of attacks based on the incremental knowledge from known attacks. It uses information such as: Security policy, Known vulnerabilities of particular Operating System and applications, Known attacks on systems. This type of IDS can only detect attacks which it has the signature. They are only as good as the information in the database of attack signatures. New vulnerabilities not in the database are constantly being discovered and exploited. Vendors need to keep up to date with latest attacks and issue database updates, customers need to install these large number of vulnerabilities and different exploitation methods, so effective database difficult to build, large database makes IDS slow to use.

The efficiency of this approach depends on the precision of the signatures. That is why this system can be bypassed by attackers who use evasion techniques, to make their attacks undetectable. An exploit code can often easily change (polymorphic buffer overflow for example), and this attack will not be detected. It is possible to create generic signatures that can detect more variants of the same attack, but it is necessary to have a good understanding of attacks, and network components in order to block malicious activities, and not deny valid traffic.

A signature defines the characteristics of an attack (protocol, service, source, and pattern). Example signatures might include:

- A number of recent failed login attempts on a sensitive host
- A certain pattern of bits in an IP packet, indicating a buffer overflow attack
- Certain types of TCP SYN packets, indicating a SYN flood DoS attack

Statistical Anomaly Detection

Statistical Anomaly Detection (or behavior-based detection) is a methodology where statistical techniques are used to detect penetrations and attacks. It begins by establishing base-line statistical behavior: what is normal for this system. Then gather new statistical data and measure the deviation from the base-line. If a threshold is exceeded, issue an alarm.

The study of anomaly detection was prefaced by the assumption that it would be possible to distinguish between a usurper and a legitimate user by identifying

deviation from historical system usage. It was hoped that an audit analysis approach would be useful to identify not only crackers who had acquired identification and authentication information to allow masquerading as legitimate users, but also legitimate users who were performing unauthorized actions. Example of unauthorized actions are: monitor the number of failed login attempts at a sensitive host over a period, if a burst of failures occurs, an attack may be under way, Abnormally high CPU load combined with other metrics can indicate an intrusion in progress.

This model of IDS does not need to know about security vulnerabilities in a particular system the base-line defines normality, for example, it does not need to know the details of the construction of a buffer overflow packet. As a sequence, this model has the advantage of detecting new types of attacks, though, frequently adjustments are necessary to upgrade the reference model in order to reflect the normal user's behavior and reduce among of false positive. However, if the base-line is adjusted dynamically and automatically, a patient attacker may be able to gradually shift the base-line over time so that his attack does not generate an alarm.

Some disadvantages of this model are: Normal behavior may overlap with forbidden behavior, legitimate users may deviate from the base-line, causing false positives (e.g. user goes on holiday, or works late in the office, or forgets password, or starts to use new application). This raises the issue of false positives (an attack is flagged when one was not taking place – a false alarm) and false negatives (an attack was missed because it fell within the bounds of normal behavior). This issue does also apply to systems. But, a tool based on knowledge-based system is less impacted by false positive because all abnormal activities are described in signature database. However, if a pattern matching quality is too bad, it can be lead to generate many of false positive. In case of a new attack, the signature database may not contain the signature, therefore the attack will not be detected.

10.Types of IDS

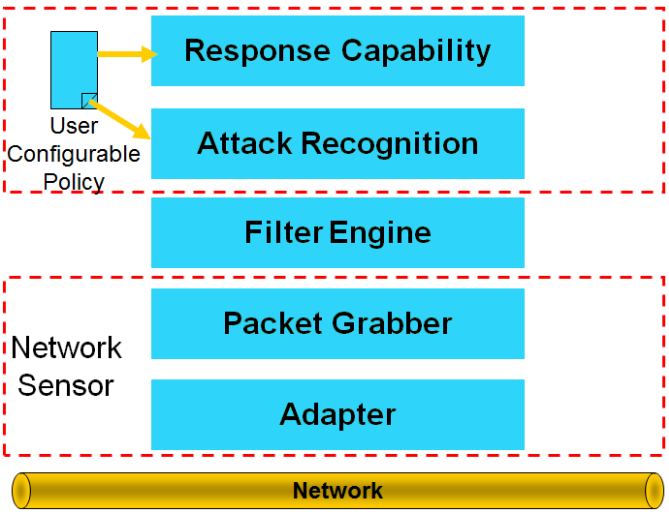
There are mainly two types of Intrusion Detection Systems, When an IDS looks for attack signatures in network traffic, it is called a network-based IDS (NIDS). When an IDS looks for attack signatures in log files of hosts, it is called a host-based IDS (HIDS). Naturally, the most effective Intrusion Detection System will make use of both kinds of information.

Network Intrusion Detection System (NIDS)

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It uses network packets as the data source. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.

NIDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode (sniffer) and a separate management interface. The attack recognition module uses three common techniques to recognize attack signatures:

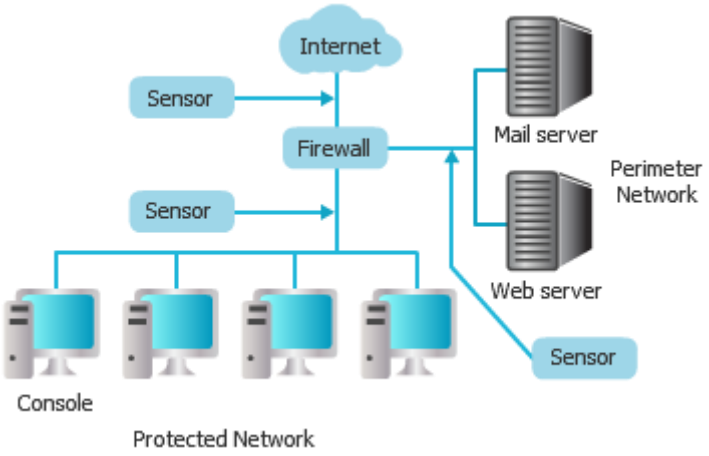
- Pattern, expression or byte code matching.
- Frequency or threshold crossing (eg detect port scanning activity).
- Correlation of lesser events (in reality, not much of this in commercial systems).



Figure(3.3) Network-based IDS

The IDS is placed along a network segment or boundary and monitors all traffic on that segment. It is placed mostly at important points in the network so that it can keep an eye on the traffic traveling to and from the different devices on the network. The IDS is placed along the network boundary or between the network and the server. An advantage of this system is that it can be deployed easily and at low cost, without having to be loaded for each system. The most used places for sensors are (see figure 3.4):

- Outside Firewall and Just inside Firewall. Combination of both will detect attacks getting through Firewall and may help to refine Firewall rule set.
- Behind remote access server.
- Between Business Units.
- Between Corporate Network and Partner Networks.

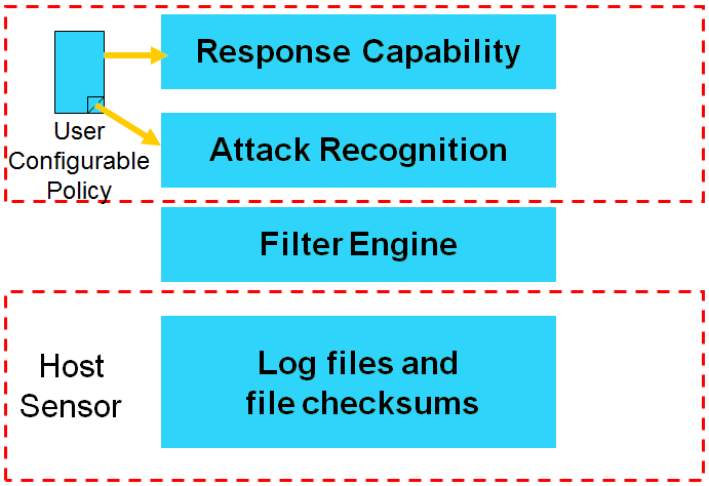


Figure(3.4): Placement of Network-based IDS

Host Intrusion Detection System (HIDS)

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. These systems are deployed locally on each host computer and monitor only the host on which it is installed. The HIDS operates by monitoring changes to a number of variables on the host system. These controls may include: System processes, registry entries, CPU Usage, file access and integrity checking, audit policies, user

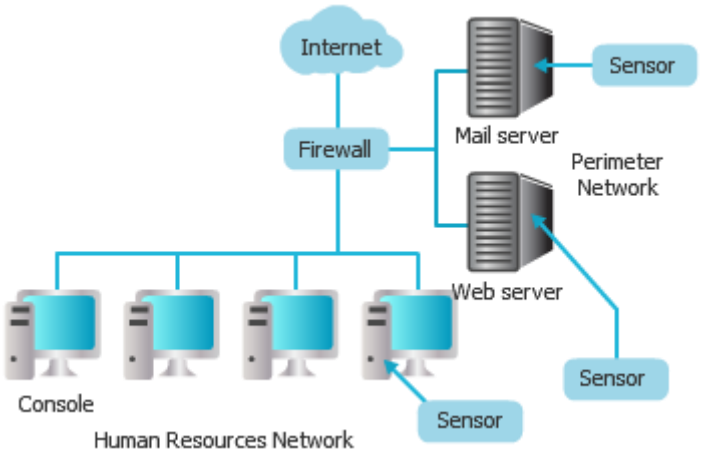
accounts, events logs. An example use: can check integrity of index.html files by regularly comparing a checksum computed over the file on the server with a checksum for the original file – this checksum is held securely on the console. Likewise, can maintain integrity of mail server configuration and protect it against attacks via eg, sendmail application. Can check for suspicious account activity on human resources network. Exceeding the threshold or suspicious integrity changes will send an alert to administrators.



Figure(3.5): Host-based IDS

HIDS can help to detect abnormal behavior on a computer that might have been compromised, but an administrator system must spend enough time to analyze the HIDS output regularly, and suppress all false positive alerts. They are typically placed on business critical hosts and on servers in a DMZ that are likely to be compromised. The most Deployment options are (see figure 3.6):

- Key servers that contain mission-critical and sensitive information
- Web servers
- FTP and DNS servers
- E-commerce database servers, etc



Figure(3.6): Placement of Host-based IDS

Network-based IDS vs. Host-based IDS

Of course each of the two technologies have their own strengths and weak points, Some of the advantages of NIDS comparing to HIDS are:

- NIDS systems are easy to deploy and cost effective since a single device is capable of protecting the entire network or at least its certain segments as compared to host based systems which require as many instances of the system as the number of systems to be protected.
- NIDS systems are easily scalable since addition or deletion of new hosts in the network does not necessarily mean increasing the hardware and so forth. Even if new appliances have to be added, they are relatively easier to install and configure.
- This also means that the hardware and the operating system can be hardened for providing the best possible level of security.
- Concentrating on one point of security (in NIDS systems) is easier than concentrating on hundreds or thousands of protection points at every host in the network (HIDS systems).
- NIDS systems have no impact on endpoint performance, and they are transparent to system users.
- Network-based monitoring can listen to all endpoints, regardless of type, no specific sensor is needed. While in a host-based sensor must be provided for each endpoint type, such as Windows, Linux, or Android.

- Some examples of attacks that are prevented by NIDS and cannot be prevented by HIDS are: IP Spoofing, denial-of-service attacks, arp cache poisoning, DNS name corruption, and man-in-the-middle attacks.

In the other hands, HIDS systems have some advantages comparing to NIDS:

- They are capable of verifying if an attack was successful or not, whereas a network based IDS only give an alert of the attack.
- They can monitor all users' activities which is not possible in a network based system.
- They are capable of identifying attacks that originate from inside the host.
- A host based system can analyze the decrypted traffic to find attack signature-thus giving them the ability to monitor encrypted traffic.
- They do not require any extra hardware since they can be installed in the existing host servers.
- They are cost effective for a small scale network having a few hosts.
- Some examples of attacks that are prevented by HIDS and cannot be prevented by NIDS are: Trojan login script, walk up to unattended keyboard attack, encrypted traffic,…

The best case is to use a judicious combination of host and network based protection systems, with the host version only used on critical points of the network, whilst the rest are covered under the network based protection system.

11.Response Options for IDSs

Once IDSs have obtained event information and analyzed it to find symptoms of attacks, they generate responses. Some of these responses involve reporting results and findings to a pre-specified location. Others involve more active automated responses. Commercial IDSs support a wide range of response options, often categorized as active responses, passive responses, or some mixture of the two.

Active Responses

Active IDS responses are automated actions taken when certain types of intrusions are detected. There are three categories of active responses.

1. Collect additional information: The most innocuous, but at times most productive, active response is to collect additional information about a suspected attack. This

might involve increasing the level of sensitivity of information sources (for instance, turning up the number of events logged by an operating system audit trail, or increasing the sensitivity of a network monitor to capture all packets, not just those targeting a particular port or target system.) Collecting additional information is helpful for several reasons. The additional information collected can help resolve the detection of the attack (assisting the system in diagnosing whether an attack did or did not take place). This option also allows the organization to gather information that can be used to support investigation and apprehension of the attacker, and to support criminal and civil legal remedies.

2. Change the Environment: Another active response is to halt an attack in progress and then block subsequent access by the attacker. Typically, IDSs do not have the ability to block a specific person's access, but instead block IP addresses from which the attacker appears to be coming. It is very difficult to block a determined and knowledgeable attacker, but IDSs can often deter expert attackers or stop novice attackers by taking the following actions:
   - Injecting TCP reset packets into the attacker's connection to the victim system, thereby terminating the connection.
   - Reconfiguring routers and firewalls to block packets from the attacker's apparent location (IP address or site).
   - Reconfiguring routers and firewalls to block the network ports, protocols, or services being used by an attacker.
   - In extreme situations, reconfiguring routers and firewalls to sever all connections that use certain network interfaces.
3. Take Action against the intruder: The most aggressive form of this response involves launching attacks against or attempting to actively gain information about the attacker's host or site. However, this response is ill advised. Due to legal ambiguities, this option can represent a greater risk than the attack it is intended to block. The first reason for approaching this option with a great deal of caution is that it may be illegal. Furthermore, as many attackers use false network addresses when attacking systems, it carries with it a high risk of causing damage to innocent Internet sites and users.

Passive Responses

Passive IDS responses provide information to system users, relying on humans to take subsequent action based on that information. Many commercial IDSs rely solely on passive responses.

1. Alarms and Notifications: Alarms and notifications are generated by IDSs to inform users when attacks are detected. Most commercial IDSs allow users a great deal of latitude in determining how and when alarms are generated and to whom they are displayed. The most common form of alarm is an onscreen alert or popup window. This is displayed on the IDS console or on other systems as specified by the user during the configuration of the IDS. The information provided in the alarm message varies widely, ranging from a notification that an intrusion has taken place to extremely detailed messages outlining the IP addresses of the source and target of the attack, the specific attack tool used to gain access, and the outcome of the attack. Another set of options that are of utility to large or distributed organizations are those involving remote notification of alarms or alerts. These allow organizations to configure the IDS so that it sends alerts to cellular phones and pagers carried by incident response teams or system security personnel. Some products also offer email as another notification channel.

SNMP Traps and Plug-ins: Some commercial IDSs are designed to generate alarms and alerts, reporting them to a network management system. These use SNMP traps and messages to post alarms and alerts to central network management consoles, where they can be serviced by network operations personnel. Several benefits are associated with this reporting scheme, including the ability to adapt the entire network infrastructure to respond to a detected attack, the ability to shift the processing load associated with an active response to a system other than the one being targeted by the attack, and the ability to use common communications channels.

Response Type	Network-based	Host-based
Notification	Alarm to console	Alarm to console
	E-Mail notification	E-Mail notification
	SNMP trap	SNMP trap
	View active session	
Storage	Log summary	Log summary
	Log raw network data	
Active	Kill connection (TCP Reset)	Terminate user login
	Re-configure firewall	Disable user account
		Restore index.html

Table(3.1): IDS Response Options

Exercises:

Multiple Choice Questions

1. A firewall is a _____.
   A. wall built to prevent fires from damaging a corporate intranet
   B. security device deployed at the boundary of a company to prevent unauthorized physical access
   C. security device deployed at the boundary of a corporate intranet to protect it from unauthorized access
   D. device to prevent all accesses from the internet to the corporate intranet

2. What is the **MAIN** purpose of using firewalls?
   A. to apply security policy between the internal and external networks
   B. to apply security policy between the user and the Internet
   C. to apply security policy between internal networks
   D. to apply security policy between external networks

3. _____ detection focuses on characterizing the past behavior of individual users or related groups of users and then detecting significant deviations.
   A. Rule-based
   B. Statistical anomaly
   C. Threshold
   D. Profile-based anomaly

4. A _____ firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
   - **A.** Packet filtering
   - **B.** Distributed
   - **C.** Stateful inspection
   - **D.** Host-based
   - **E.** Network-based

5. In a normal multi-firewall configuration, which of the following is true of the DMZ?
   - **A.** It contains any machines you keep outside your outermost firewall
   - **B.** It is the area inside your innermost firewall
   - **C.** It is between your outermost firewall and innermost firewall
   - **D.** It contains portable machines that have not yet been validated to allow them any network access

6. List or table of stored by a router that controls access to and from a network.
   - **A.** State Table
   - **B.** Access Control List (ACL)
   - **C.** routing table
   - **D.** Packet Filter

7. Some _____ firewalls are able to examine the contents of packets as well as the headers for signs that they are legitimate.
   - **A.** Circuit level proxy
   - **B.** Stateful
   - **C.** Stateless
   - **D.** Application level proxy

8. Which of the following is true of signature-based IDSes ?
   A. They alert administrators to deviations from "normal" traffic behavior
   B. They identify previously unknown attacks
   C. The technology is mature and reliable enough to use on production networks
   D. They scan network traffic or packets to identify matches with attack-definition files

9. Which fields of information are used by a typical packet-filtering router in its security decisions?
   A. IP addresses, protocol, and port numbers
   B. Digital certificates, IP addresses, and IP header checksums
   C. URL addresses, IP addresses, and port numbers
   D. Mac addresses, IP addresses, and port number

10. A technique that focuses on characterizing the past behaviour of individual users or related groups of users and then detecting significant deviations is called:
   A. Statistical anomaly
   B. Profile - based anomaly
   C. Threshold
   D. Action condition
   E. Markov chain

11. _____ techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious.
   A. Rule-based
   B. Statistical-based
   C. Threshold-based
   D. Profile-based anomaly

12. The _____ by default policy increases ease of use for end users but provides reduced security because the security administrator must react to each new security threat as it becomes known.

A. Block
B. Check
C. Allow
D. Select

13. A _____firewall sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established TCP segments from one connection are relayed to the other without examining the contents.

A. packet filter
B. circuit-level gateway
C. stateful packet filter
D. application level proxy

14. Between an internal firewall and an external firewall are one or more networked devices in a region referred to as a _____ . Systems that are externally accessible but need some protection are usually located in this area.

A. Trusted zone
B. untrusted zone
C. DMZ (demilitarized zone)
D. Operation zone

15. Which of the following is true of anomaly detection based IDS?

A. They can only detect problems they are already aware of
B. They may be susceptible to training attacks
C. They are prone to false alarms more than signature based IDS
D. They are only usable for network-based intrusion detection, not host-based intrusion detection
E. B and C

16. A packet-filtering firewall does which of the following?

A. It analyzes network traffic at the network and transport protocol layers

B. It evaluates network packets for valid data at the application layer before allowing connections

C. It validates the fact that a packet is either a connection request or a data packet belonging to a connection

D. It keeps track of the actual communication process through the use of a state table

17. Which of the following is NOT a characteristics of a firewall?

A. Enforces the access control policy of an organization

B. Must be hardened against attacks

C. Must be the only transit point between networks

D. Completely eliminates the risk of network compromise

E. None of the above

18. Which of the following is true of firewalls?

A. An application gateway firewall will probably need more processing power than a filtering gateway firewall

B. If you use an application gateway firewall, you will not need to update it regularly

C. Circuit level proxy firewalls are able to stop Sync flood attacks

D. Transparency is an undesirable property for a firewall

E. A and C

19. A type of firewall closely related to a packet filter that can track the status of a connection through use of a state table that keeps track of connection activities.

A. Anomaly detection

B. Packet filter inspection

C. Stateful inspection

D. Knowledge based detection

20. When discussing signature-based IDS, what is a signature?

A. An electronic signature used to authenticate the identity of a user on the network

B. Attack-definition file

C. It refers to "normal" baseline network behavior

D. a digital signature for the software owner

References

1. Stallings, W.: Network Security essentials: application and standards, 6th edn. Pearson India Education Services Pvt. LTD (2017).
2. Stallings, W., Brown, L. : Computer Security: Principles and Practice 4th edn. Prentice Hall (2018).
3. https://www.ipa.go.jp/security/fy11/report/contents/intrusion/ids meeting/idsbg.pdf.
4. https://apps.dtic.mil/dtic/tr/fulltext/u2/a393326.pdf.

Number of the Question	Answer
1	C
2	A
3	B
4	A
5	C
6	B
7	D
8	D
9	A
10	A
11	A
12	C
13	B
14	C
15	E
16	A
17	D
18	A
19	C
20	B