Comparison of Firewall, IDS, and Honeypot

Introduction

- An IDS attempts to identify intrusions, defined as unauthorized uses, misuses, or abuses of computer systems by either authorized or unauthorized users.
- Firewalls are the primary means of securing a private network against penetration from a public network
- A honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.

First Line of Defense: The Firewall

- Firewalls are systems that enforce an access control policy into a protected network.
- Core of enterprise's comprehensive security policy
- Can monitor all traffic entering and leaving the private network, and alert the IT staff to any attempts to circumvent security or patterns of inappropriate use

- A firewall uses two principal mechanisms:
  - One that blocks traffic
  - another that permits traffic, according to the organizational policy
- A number of firewalls can be deployed in the proper positions of the managed network for cooperative, integrated, and in-depth network security protection

- Each firewall has a rule set, commonly known as the Access Control List (ACL), that allows the administrator to decide which traffic will be allowed or denied.

Advantages of Firewalls

- Firewalls can prevent the traffic which is non-legitimate.
- Firewalls can filter those protocols and services that can be easily exploited.
- A firewall helps protecting the internal network by hiding names of internal systems from the outside hosts.

Disadvantages of Firewalls

- Firewalls use set of rules that are manually configured to differentiate legitimate traffic from non-legitimate traffic.
- The firewall can't react to a network attack nor can initiate effective counter-measures.
- Most firewalls do not analyze the contents of the data packets that make up network traffic.
- Firewalls cannot prevent attacks coming from Intranet.
- Filtering rules of the firewall cannot prevent attack coming from application layer

Types of Firewall

- **Packet-Filtering Router**
- **Application level gateways**
- **Circuit level gateways**

Packet-Filtering Router

- Set up as a list of rules based on matches to fields in the IP or TCP header.
- Applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.

Application level gateways

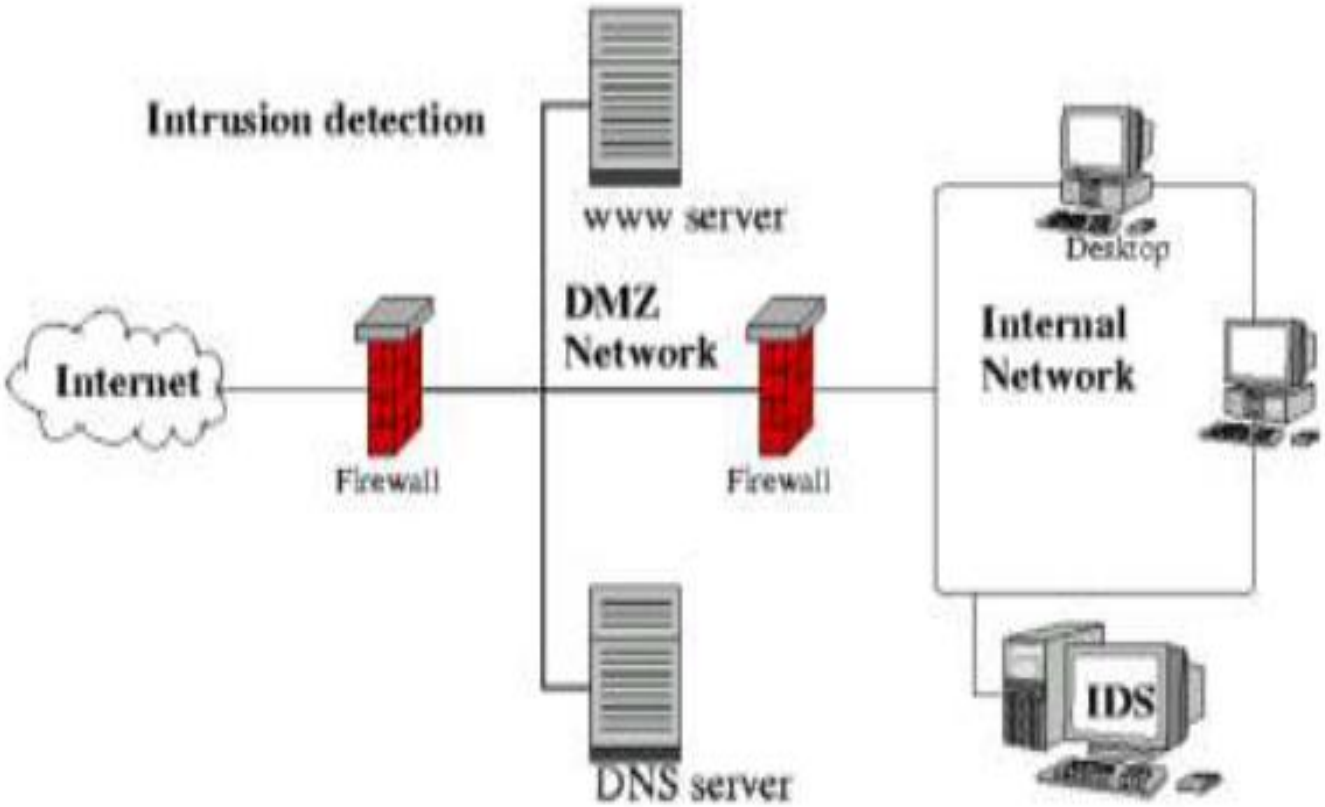
- It is also known as proxy server.
- Application-level gateways tend to be more secure than packet filters. It is easy to log and audit all incoming traffic at the application level.

Circuit level gateways

- A circuit-level gateway does not permit an end-to-end TCP connection, instead the gateway sets up two TCP connections.
- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.

Intrusion Detection System (IDS)

- An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches


Intrusion detection
www server
Desktop
DMZ
Network
Internal
Network
Internet
Firewall
Firewall
IDS
DNS server

Advantages of IDS

- IDS are easier to deploy as it does not affect existing systems or infrastructure.
- Network based IDS sensors can detect many attacks by checking the packet headers for any malicious attack like TCP SYN attack, fragmented packet attack etc.
- IDS monitor traffic on a real time. So, network based IDS can detect malicious activity as they occur.
- IDS sensor deployed outside the firewall can detect malicious attacks on resources behind the firewall

Firewalls Vs. IDS

- Firewalls cannot respond to malicious activity; they see only host addresses, network addresses, and ports, then either allow or deny connections.
- IDSs do respond to malicious activity, but I haven't seen an IDS that deals with network traffic control better than a firewall does.

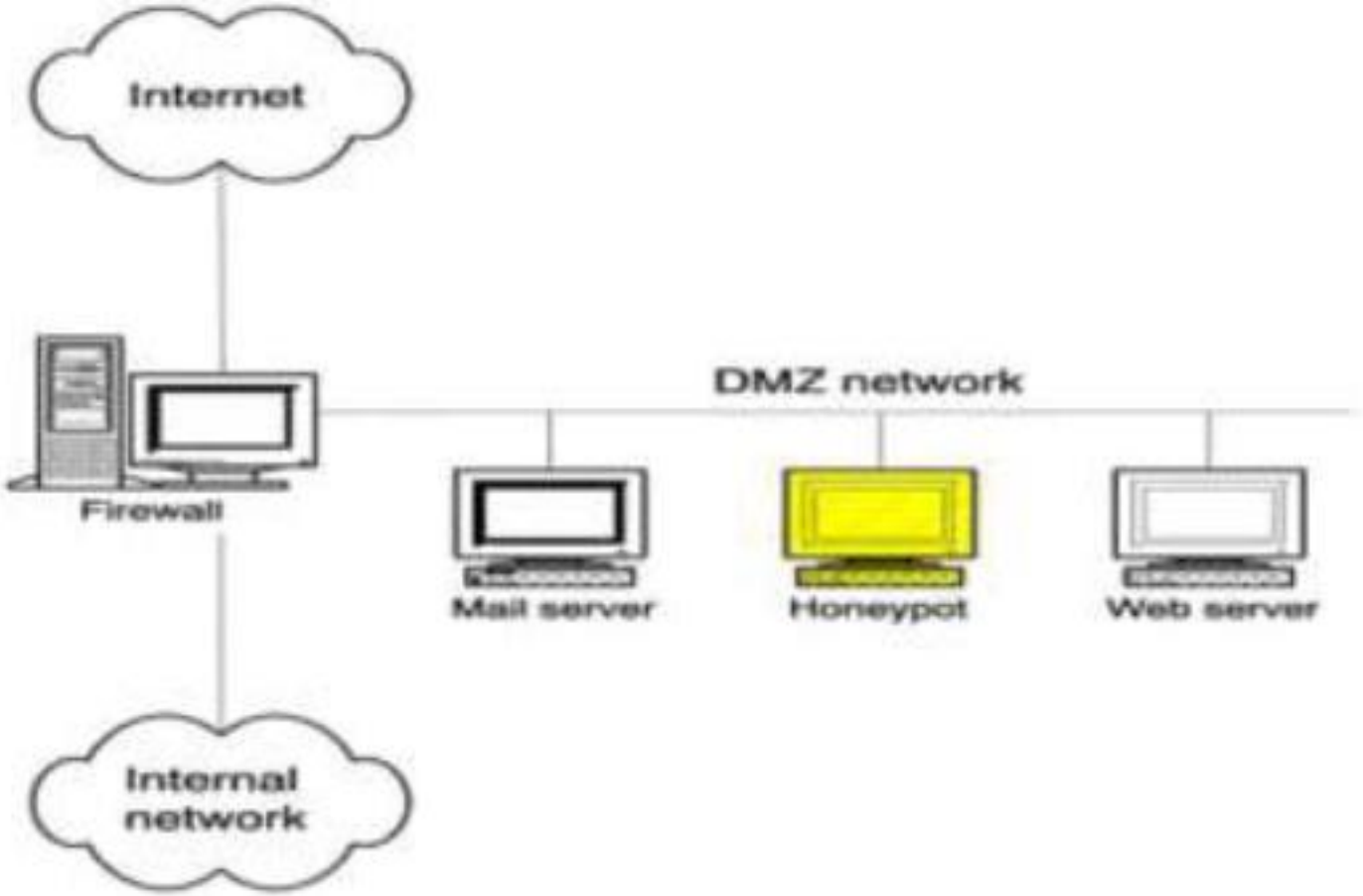
- Firewalls are designed to block or allow traffic. Intrusion Detection Systems are designed to detect intrusions.

Disadvantages of IDS

- IDS is not an alternative to strong user identification and authentication mechanism.
- IDS is not a solution to all security concerns.
- Human intervention is required to investigate the attack once it is detected and reported.
- False positives occur when IDS incorrectly identifies normal activity as being malicious.
- False negatives occur when IDS fails to detect the malicious activity

Honeypot

- Honey pots are systems used to lure hackers by exposing known vulnerabilities deliberately.
- Once a hacker finds a honey pot, it is more likely that the hacker will stick around for some time.
- During this time the admin can log hacker activities to find out his/her actions and techniques. Once these techniques are known, yo this information can be used later on to harden security on the actual servers.


Internet
DMZ network
Firewall
Mail server
Honeypot
Web server
Internal network

- It is a good idea to keep log files on some other machine so that when the honey pot is compromised, the hacker does not have the ability to delete these files.
- In general honeypots can be divided into two categories.
  - **Production Honeypots**
  - **Research Honeypots**

Production Honeypots

- Production honeypots are used to assist an organization in protecting its internal IT infrastructure.
- Useful in catching hackers with criminal intentions.
- The implementation and deployment of these honeypots are relatively easier than research honeypots

Research Honeypots

- Research honeypots are complex.
- They are designed to collect as much information as possible about the hackers and their activities.
- The information gathered by research honeypots will help the organization to better understand the hackers attack patterns

Advantages of Honeypot

- **Small Data Sets**
- **Reduced False Positives**
- **Catching False Negatives**
  - Honeypots can easily identify and capture new attacks against them.
  - Any activity with the Honeypot is an anomaly, making new or unseen attacks easily stand out.

- **Encryption**
  - It does not matter if an attack or malicious activity is encrypted, the Honeypot will capture the activity.
- **IPv6**
  - Honeypots work in any IP environment, regardless of the IP protocol, including IPv6.
  - Many current technologies, such as firewalls or IDS sensors, cannot handle IPv6.

- **Minimal Resources**
  - Honeypots require minimal resources, even on the largest of networks.

Disadvantages of Honeypots

- **Risk:**
- Attacker could use a honeypot to attack or harm other non-honeypot systems.
- **Limited Field of View**
  - Honeypots only see or capture that which interacts with them.
  - Can not capture activity to all other systems

Honeypots vs Firewalls

- A firewall is designed to keep the attackers out of the network whereas honeypots are designed to entice the hackers to attack the system.
- The firewall’s log contains 1000 entries of all the systems of the network whereas the honeypot,s log only contain 5-10 entries.

Honeypots vs IDS

- To detect malicious behavior, NIDS require signatures of known attacks and often fail to detect compromises that were unknown at the time it was deployed. On the other hand, honeypots can detect vulnerabilities that are not yet understood.
- Analysis of data collected from honeypots is less likely to lead to false positives than data collected by NIDS.