Network Design: Firewall, IDS/IPS

resources.infosecinstitute.com/network-design-firewall-idsips/

Introduction

There are many different types of devices and mechanisms within the security environment to provide a layered approach of defense so that if an attacker is able to bypass one layer, another layer stands in the way to protect the network. Two of the most popular and significant tools used to secure networks are firewalls and intrusion detection systems. The rudimentary functionality of a firewall is to screen network traffic for the purpose of preventing unauthorized access between computer networks.

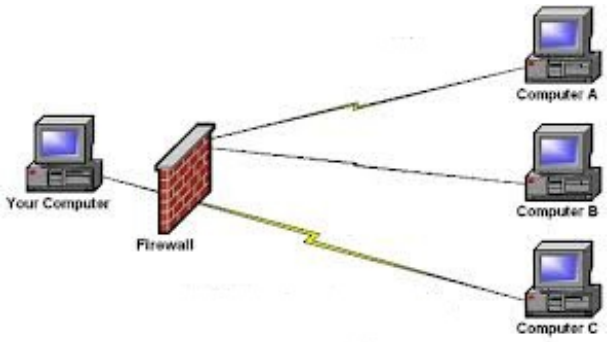
In this article, we will examine the various types of firewalls and intrusion detection systems, as well as understand the architecture behind these technologies. We will touch attack indications and the countermeasures that should be applied in order to secure the network from breach. This article describes the importance of intrusion detection and prevention, and why they must be a part of every network security administrator's defense plan.

Ethical Hacking Training – Resources (InfoSec)

What is a Firewall?

A firewall is a device installed between the internal network of an organization and the rest of the network. It is designed to forward some packets and filter others. For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP or it can be used to deny access to a specific host or a service in the organization. The following image depicts a firewall installation in the network.

Firewalls are a set of tools that monitors the flow of traffic between networks. Placed at the network level and working closely with a router, it filters all network packets to determine whether or not to forward them towards their destinations.



Working Architecture

A firewall is often installed away from the rest of the network so that no incoming requests get directly to the private network resource. If it is configured properly, systems on one side of the firewall are protected from systems on the other side. Firewalls generally filter traffic based on two methodologies:

- A firewall can allow any traffic except what is specified as restricted. It relies on the type of firewall used, the source, the destination addresses, and the ports.
- A firewall can deny any traffic that does not meet the specific criteria based on the network layer on which the firewall operates.
- The type of criteria used to determine whether traffic should be allowed through varies from one type to another.
- A firewall may be concerned with the type of traffic or with source or destination addresses and ports.
- A firewall may also use complex rules based on analyzing the application data to determine if the traffic should be allowed through.

Firewall Pros and Cons

Every security device has advantages and disadvantages and firewalls are no different. If we applied strict defensive mechanisms into our network to protect it from breach, then it might be possible that even our legitimate communication could malfunction, or if we allow entire protocol communications into our network, then it can be easily hacked by malicious users. So, we should maintain a balance between strictly-coupled and loosely-coupled functionalities.

Advantage

- A firewall is an intrusion detection mechanism. Firewalls are specific to an organization's security policy. The settings of firewalls can be altered to make pertinent modification to the firewall functionality.
- Firewalls can be configured to bar incoming traffic to POP and SNMP and to enable email access.
- Firewalls can also block email services to secure against spam.
- Firewalls can be used to restrict access to specific services. For example, the firewall can grant public access to the web server but prevent access to the telnet and the other non-public daemons.
- Firewall verifies the incoming and outgoing traffic against firewall rules. It acts as a router in moving data between networks.
- Firewalls are excellent auditors. Given plenty of disk or remote logging capabilities, they can log any and all traffic that passes through.

Disadvantage

- A firewall can't prevent revealing sensitive information through social engineering.
- Firewall can't protect against what has been authorized. Firewalls permit normal communications of approved applications, but if those applications themselves have flaws, a firewall will not stop the attack because to the firewall, the communication is authorized.
- Firewalls are only as effective as the rules they are configured to enforce.
- Firewalls can't stop attacks if the traffic does not pass through them.
- Firewalls also can't secure against tunneling attempts. Applications that are secure can be Trojaned. Tunneling bad things over HTTP, SMTP and other protocols is quite simple and easily demonstrated.

Firewall Classification

The way a firewall provides greater protection relies on the firewall itself, and on the policies that are configured on it. The main firewall technologies available today are:

- Hardware Firewall
- Software Firewall
- Packet-Filter Firewall
- Proxy Firewall
- Application Gateways
- Circuit-Level Gateways
- Stateful Packet-Inspection (SPI)

Hardware Firewall

A hardware firewall is preferred when a firewall is required on more than one machine. Hardware firewall provides

an additional layer of security to the physical network. The disadvantage of this approach is that if one firewall is compromised, all the machines that it serves are vulnerable.

Software Firewall

A software firewall is a second layer of security and secures the network from malware, worms and viruses, and email attachments. It looks like any other program and can be customized based on network requirements. Software firewall can be customized to include antivirus programs and to block sites and images.

Packet-Filtering Firewall

Packet-Filtering firewall filters at the network or transport layer. It provides network security by filtering network communications based on the information contained in the TCP/IP header of each packet. The firewall examines these headers and uses the information to decide whether to accept and route the packets along to their destinations or deny the packet by dropping them. A Packet-Filter firewall is a router that uses a filtering table to decide which packets must be discarded.

Packet-Filtering makes decisions based upon the following header information:

- The Source IP address
- The Destination IP address
- The Network protocol in use (TCP ,ICMP or UDP)
- The TCP or UDP source port
- The TCP or UDP destination port
- If the protocol is ICMP, then its message type

Proxy Firewall

The Packet-Filter firewall is based on information available in the network and transport layer header. However, sometimes we need to filter a message based on the information available in the message itself (at the application layer). For example, assume that an organization only allows those users who have previously established business relations with the company, then access to other users must be blocked. In this case, Packet-Filter firewall is not feasible because it can't distinguish between different packets arriving at TCP port 80.

Here *proxy firewall* came into light as a solution: install a proxy computer between the customer and the corporation computer. When the user client process sends a message, the *proxy firewall* runs a server process to receive the request. The server opens the packet at the application level and confirms whether the request is legitimate or not. If it is, the server acts as a client process and sends the message to the real server, otherwise the message is dropped. In this way, the requests of the external users are filtered based on the contents at the application layer.

Application Gateways

These firewalls analyze the application level information to make decisions about whether or not to transmit the packets. Application gateways act as an intermediary for applications such as e-mail, FTP, Telnet, HTTP and so on. An application gateway verifies the communication by asking for authentication to pass the packets. It can also perform conversion function on data if necessary.

For example, an application gateway can be configured to restrict FTP commands to allow only *get* commands and deny *put* command.

Application gateways can be used to protect vulnerable services on protected systems. A direct communication between the end user and destination service is not permitted. These are the common disadvantages when

implementing application gateway:

- Slower performance
- Lack of transparency
- Need for proxies for each application
- Limits to application awareness

Circuit-Level Gateways

Circuit-level gateways work at the sessions layer of the OSI model or the TCP layer of the TCP/IP. They forward data between the networks without verifying it. It blocks incoming packets on the host, but allows the traffic to pass through itself. Information passed to remote computers through it appears to have originated from gateway. Circuit-level gateways operate by relaying TCP connections from the trusted network to the untrusted network. This means that a direct connection between the client and server never occurs.

The main advantage of circuit-level gateway is that it provides services for many different protocols and can be adapted to serve an even greater variety of communications. A SOCK proxy is a typical implementation of circuit-level gateway.

Stateful Packet Inspection

A stateful packet-inspection (SPI) firewall permits and denies packets based on a set of rules very similar to that of a packet filter. However, when a firewall is state-aware, it makes access decisions not only on IP addresses and ports but also on the SYN, ACK, sequence numbers and other data contained in the TCP header. Whereas packet filters can pass or deny individual packets and require permissive rules to permit two-way TCP communications, SPI firewalls track the state of each session and can dynamically open and close ports as specific sessions require.

Firewall Identification

Normally, firewalls can be identified for offensive purposes. Because firewalls are usually a first line of defense in the virtual perimeter, to breach the network from a hacker perspective, it is required to identify which firewall technology is used and how it’s configured. Some popular tactics are:

Port scanning

- Hackers use it for investigating the ports used by the victims.
- Nmap is probably the most famous port-scanning tool available.

Firewalking

- The process of using traceroute-like IP packet analysis in order to verify if a data packet will be passed through the firewall from source to host of the attacker to the destination host of the victim.

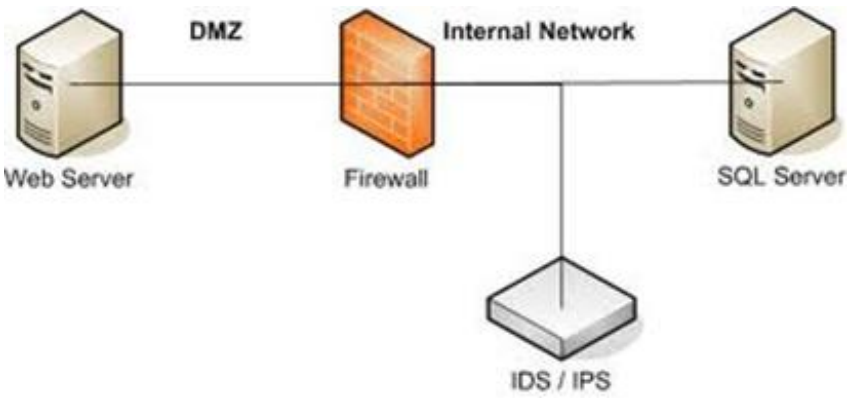
Banner grabbing

- This is a technique to enable a hacker to spot the type of operation system or application running on a target server. It works through a firewall by using what looks like legitimate connections.

Intrusion Detection System (IDS)

Intrusion Detection (ID) is the process of monitoring for and identifying attempted unauthorized system access or manipulation. An ID system gathers and analyzes information from diverse areas within a computer or a network to identify possible security breaches which include both intrusions (attack from outside the organization) and misuse

(attack from within the organization).



An Intrusion Detection System (IDS) is yet another tool in the network administrator's computer security arsenal. It inspects all the inbound and outbound network activity. The IDS identifies any suspicious pattern that may indicate an attack the system and acts as a security check on all transactions that take place in and out of the system.

Types of IDS

For the purpose of dealing with IT, there are four main types of IDS:

Network intrusion detection system (NIDS)

It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems gain access to network traffic by connecting to a network hub, a network switch configured for port mirroring, or a network tap. In a NIDS, sensors are placed at choke points in the network to monitor, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of a NIDS is Snort.

Host-based intrusion detection system (HIDS)

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. In a HIDS, sensors usually consist of a software agent. Some application-based IDS are also part of this category. An example of a HIDS is OSSEC.

Intrusion detection systems can also be system-specific using custom tools and honeypots. In the case of physical building security, IDS is defined as an alarm system designed to detect unauthorized entry.

Perimeter Intrusion Detection System (PIDS)

Detects and pinpoints the location of intrusion attempts on perimeter fences of critical infrastructures. Using either electronics or more advanced fiber optic cable technology fitted to the perimeter fence, the PIDS detects disturbances on the fence, and if an intrusion is detected and deemed by the system as an intrusion attempt, an alarm is triggered.

VM based Intrusion Detection System (VMIDS)

It detects intrusions using virtual machine monitoring. By using this, we can deploy the Intrusion Detection System with Virtual Machine Monitoring. It is the most recent type and it's still under development. There's no need for a separate intrusion detection system since by using this, we can monitor the overall activities.

Comparison with Firewall

Though they both relate to network security, an intrusion detection system (IDS) differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking action to alert operators. A system that terminates connections is called an intrusion prevention system, and is another form of an application layer firewall.

Anomaly Detection Model

All Intrusion Detection Systems use one of two detection techniques:

Statistical anomaly-based IDS

A statistical anomaly-based IDS establishes a performance baseline using normal network traffic evaluations. It will then sample current network traffic activity to this baseline in order to detect whether or not it is within baseline parameters. If the sampled traffic is outside baseline parameters, an alarm will be triggered.

Signature-based IDS

Network traffic is examined for preconfigured and predetermined attack patterns known as signatures. Many attacks today have distinct signatures. In good security practice, a collection of these signatures must be constantly updated to mitigate emerging threats.

Indication of Intrusions

System Intrusions

- System failure in identifying valid user
- Active access to unused logins
- Login during non-working hours
- New user account created automatically
- Modification in system software or configuration files
- System logs are deleted
- System performance decreased drastically
- Unusual display of graphics, pop-ups
- System crashes suddenly and reboots without user interventions

File Intrusions

- Identifications of unknown files and program on your system
- File permission modifications
- Unexplained modifications in file size
- Identifications of strange file presence into system directories
- Missing files

Network Intrusions

- Identifications of repeated attempts to log in from remote locations

- Sudden increase in bandwidth consumptions
- Repeated probes of the existing services
- Arbitrary log data in log files

Defense against IDS attacks

The network security administrator must perform various precautions and initiatives in order to defend the network from external or internal attacks. Some of these are:

- Frequently update antivirus Signature database.
- Configure the firewall to filter out IP address of an intruder.
- Beep or play .WAV file as an indication.
- Force a TCP FIN or RST packet to force a connection termination.
- Save a trace file of raw packets for future analysis.
- Save the attack information (Intruder IP, victim IP, timestamp).
- Send intimation to Administrator about attack.

Intrusion Prevention System

The traditional Intrusion Detection System is a detective technology; it only detects the anomaly in the network and sends intimation to the concerned person whereas an IPS is both detective and preventive technology. However, an IDS just makes a database of irregularities occurring in the inner network executed by the malicious hacker; it is not able to block the particular kind of attack. The Intrusion Prevention System's goal is to detect malicious activity and not allow the traffic to gain access to its target network.

Conclusion

This article provided an in-depth overview of firewalls and IDS, and their roles in protecting the corporate network. There are four main types of firewalls: packet-filters, application gateways, circuit-level gateways, and other firewalls. Though some have predicted the end of the firewall, its strategic location in the network makes it an indispensable tool for protecting assets. Good security practices dictate that firewalls should be deployed between any two networks of differing security requirements.

This article illustrates the importance of IDS and its various types. IDS monitor hosts for system alteration or sniffs network packets off the wire, seeking for malicious contents. Security Administrators should contemplate using combinations of HIDS and NIDS, with both signature-detection and anomaly-based engines. IDS can be configured purely as monitoring and detection devices or it can participate as an inline device and prevent threats. Its biggest weaknesses are the high number of false-positives and the maintenance effort needed to keep signatures up to date and fine-tuned.