Fundamentals of Unix and Linux System Administration Training

Security Principles
Firewalls

Caroline Gachuhi
System Administrator , KENET
cgachuhi@kenet.or.ke

Learning Objectives

- Understand the concept of Firewalls
- Identify the types of Firewalls
- Understand the concept of IPtables
- Learn how to install and configure IPtables

Key Terms

- Firewall
- Network Packets
- OSI Model/ Layers
- Iptables
- Putty/ Terminal

What is a Firewall?

- A **firewall** is a network security device or software that is designed to monitor, filter, and control network traffic, allowing or blocking data packets based on a set of predetermined security rules and policies.

- Firewalls act as a barrier between a trusted internal network and untrusted external networks, such as the internet, to protect against unauthorized access, cyberattacks, and the spread of malicious software.

Types Of Firewalls

Packet Filtering Firewalls

Packet filtering firewalls operate at the network layer (Layer 3) of the OSI model and filter network packets based on criteria such as source and destination IP addresses, port numbers, and protocol type.

Examples include iptables (Linux), Windows Firewall (Windows), and routers with access control lists (ACLs)

Stateful Inspection Firewalls

Stateful inspection, or dynamic packet filtering, firewalls keep track of the state of active connections and make decisions based on the state information.

They are more intelligent than packet filtering firewalls and can inspect the context of traffic.

Examples include Cisco ASA and Check Point Firewall.

Types Of Firewalls

Proxy Firewalls

Proxy firewalls act as intermediaries between a user's device and the target server.

They examine traffic at the application layer (Layer 7) and may modify or cache data.

Examples include Squid (for web traffic) and application-specific proxies.

Application Layer Firewalls

Application layer firewalls are designed to filter and control traffic at the application layer.

They are often used for specific applications or services.

Examples include web application firewalls (WAFs) and email security gateways.

Types Of Firewalls

Next-Generation Firewalls (NGFW):

NGFWs combine traditional firewall features with advanced security capabilities, such as intrusion detection and prevention (IDS/IPS), antivirus, content filtering, and application awareness.

Examples include Palo Alto Networks, Fortinet, and Cisco Firepower.

Unified Threat Management (UTM) Firewalls

UTM firewalls are comprehensive security appliances that integrate various security functions into a single device, including firewall, antivirus, intrusion prevention, VPN, and content filtering.

Examples include Sophos UTM and WatchGuard.

Types Of Firewalls

Cloud Firewalls

Cloud firewalls are specifically designed to protect cloud-based infrastructure and applications.

Examples include AWS WAF (Amazon Web Services), Azure Firewall

(Microsoft Azure), and Google Cloud Firewall (Google Cloud Platform).

Host-Based Firewalls

Host-based firewalls are installed on individual computers or servers to control incoming and outgoing traffic at the host level.

Examples include Windows Firewall (built into Windows operating systems) and iptables (Linux).

Importance of firewalls

Why do we need Firewalls?

Importance of firewalls

- ✓ **Access Control:** Firewalls control and restrict network traffic based on predefined rules and policies
- ✓ **Protection from Cyberattacks** by enforcing Intrusion Prevention firewalls to detect and block known attack patterns.
- ✓ **Content Filtering:** Firewalls can be configured to filter and block specific sites and content categories.
- ✓ **Network Segmentation:** Firewalls can be used to segment networks into isolated zones, creating additional layers of security.
- ✓ **Encryption and VPNS Support:** firewalls include support for Virtual Private Network(VPNs) to encrypt data traffic between remote locations ensuring confidentiality.
- ✓ **Logging and Monitoring:** firewalls generate logs and

IPTABLES

- **Background**

- Iptables is an opensource command-line utility for configuring firewall rules in a Linux-based operating system. Its primary purpose is to filter/manipulate network packets based on a set of predefined rules.
- It operates by organizing rules into tables and chains.

The Iptables Inbuilt chains

a) **INPUT CHAIN**: This processes all packets destined for our server.

b) **OUTPUT CHAIN**: This is responsible for processing network packets originating from the local server itself.

c) **FORWARD CHAIN:** This is responsible for handling packets that are being forwarded between network interfaces on the system.

The Filter Table

- The Filter Table is responsible for filtering and controlling network traffic based on specific criteria.

- **IPtable Filter options**
-

a) **Source/Destination IP Address:** One can filter packets based on their source or destination IP addresses using options like **-s** for source IP address and **-d** for destination IP address.

b) **Protocol:** This filters packets based on the protocol they use, such as TCP, UDP, ICMP, etc. The **-p** option is used to specify the protocol.

c) **Port:** This filters packets based on source or destination ports using options like **--sport** for source port and **--dport** for destination port.

d) **State**: This filters packets based on their connection state, such as established, related, or new connections. The **-m** state module is used along with options like **--state** to specify the desired state.

1. Installation and configuration of iptables

- To install IPtables
  - $ ***sudo apt install iptables-persistent***
- *the IPv4 rules are written to and read from /etc/iptables/rules.v4*
- To view/list the rules
  - ***$ sudo iptables -L –v***

- **Setting rules on iptables**

- There are two ways of setting up a firewall:

i. Setting the default rule to accept and then blocking any undesired traffic
ii. Utilizing rules to specify authorized traffic and blocking everything else

2. Adding rules for authorized inbound traffic.

To enable established connections to continue

$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

To permit SSH connections

$ sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT

To allow traffic to a HTTP server

$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Saving the rules on iptables

 # iptables-save > /etc/iptables/rules.v4

Confirm if the rules were added.

$ sudo iptables -L

3. Flushing the rules

To clear the input chain

$ sudo iptables -F INPUT

To flush the entire Iptables

$ sudo iptables -F

Saving the rules on iptables

 # iptables-save > /etc/iptables/rules.v4

Display the file contents in the terminal window, to confirm the iptables rules were flushed

$ sudo cat /etc/iptables/rules.v4

kenet
Kenya Education Network

Thank You!

Transforming education through ICT

kenet
Kenya Education Network

THANK YOU!

www.kenet.or.ke
support@kenet.or.ke
Jomo Kenyatta Memorial Library, University of Nairobi
P. O Box 30244-00100,
Nairobi.
0733 150 500 / 0703 044 500

Transforming learning, research and working environments with ICT