Firewall Fundamentals

Introduction

This lab covers the fundamentals of firewall technologies and their practical application in both Windows and Linux environments. We explore different types of firewalls, including stateless, stateful, proxy, and next-generation firewalls, as well as how rules control network traffic. The lab provides hands-on exercises using Windows Defender Firewall and Linux firewalls such as iptables, nftables, firewalld, and ufw, highlighting rule creation, management, and testing.

Objectives

- The types of firewalls
- The firewall rules and its components
- Hands-on Windows built-in firewall
- Hands-on Linux built-in firewall

By:Fábio Vieira

Provided: TryHackMe

Types of Firewalls

Stateless Firewall

Operates at OSI layers 3 and 4, filtering packets based only on predefined rules. It does not track the state of previous connections, treating each packet independently. Fast but cannot apply policies based on connection history.

Stateful Firewall

Also operates at layers 3 and 4, but maintains a connection state table. Allows or blocks future packets based on the history of the connection, providing stronger security than stateless firewalls.

Proxy Firewall (Application-Level Gateway)

Operates at layer 7, inspecting packet content. Acts as an intermediary between the internal network and the Internet, masking internal IPs and applying content-based filtering policies.

Next-Generation Firewall (NGFW)

Operates from layers 3 to 7, offering deep packet inspection, intrusion prevention, heuristic analysis, and SSL/TLS inspection. Integrates threat intelligence to make more accurate security decisions.

Rules in Firewalls

Firewalls control traffic through rules that define how packets are handled. Each rule typically includes:

- Source address: IP sending the traffic
- Destination address: IP receiving the traffic
- Port: Target port number
- Protocol: Communication protocol (e.g., TCP, UDP)
- Action: What the firewall does with matching traffic
- Direction: Whether the rule applies to inbound or outbound traffic

Rule Actions

- Allow: Permits traffic matching the rule
  Example: Allow outbound HTTP (port 80) from network 192.168.1.0/24
- Deny: Blocks traffic matching the rule
  Example: Deny inbound SSH (port 22) to critical servers
- Forward: Redirects traffic to another device or segment
  Example: Forward inbound HTTP (port 80) to web server 192.168.1.8

Rule Directionality

- Inbound: Applied to incoming traffic
- Outbound: Applied to outgoing traffic
- Forward: Redirects traffic within the network

Windows Defender Firewall

Windows Defender Firewall

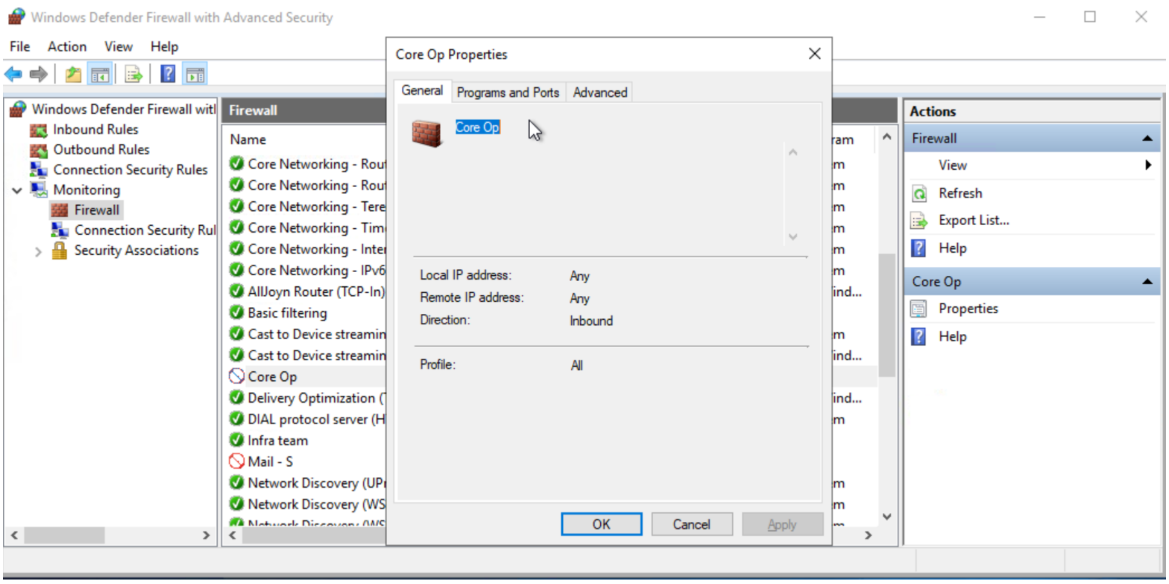
Windows Defender Firewall is the built-in firewall in Windows OS. It allows creating, allowing, or blocking programs and custom rules to control incoming and outgoing traffic. The main dashboard displays Network Profiles and firewall options, accessible by searching for "Windows Defender Firewall" in Windows.

Exercise

The security team noticed suspicious incoming and outgoing traffic on their critical Windows system. They created rules on their Windows Defender Firewall to block some of their specific network traffic. You are tasked to answer a few questions given at the end of this task by looking at the created rules.

Q1.What is the name of the rule that was created to block all incoming traffic on the SSH port?

Core Op



Windows Defender Firewall with Advanced Security

Core Op Properties

Core Op

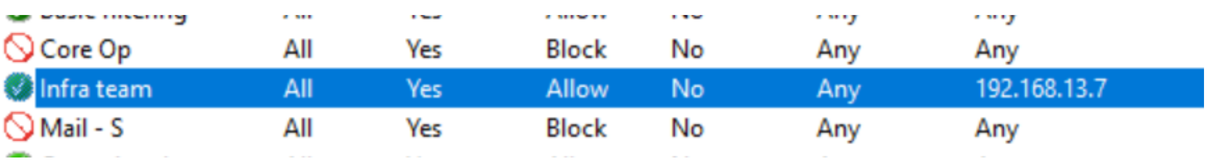
Local IP address: Any
Remote IP address: Any
Direction: Inbound

Profile: All

Name
Core Networking - Rou
Core Networking - Rou
Core Networking - Tere
Core Networking - Tim
Core Networking - Inte
Core Networking - IPv6
AllJoyn Router (TCP-In)
Basic filtering
Cast to Device streamin
Cast to Device streamin
Core Op
Delivery Optimization (
DIAL protocol server (H
Infra team
Mail - S
Network Discovery (UP
Network Discovery (WS

Q2. A rule was created to allow SSH from one single IP address. What is the rule name?

Infra team



⊘ Core Op	All	Yes	Block	No	Any	Any
✓ Infra team	All	Yes	Allow	No	Any	192.168.13.7
⊘ Mail - S	All	Yes	Block	No	Any	Any

Q3.Which IP address is allowed under this rule?

As seen below **192.168.13.7.**

Linux Firewalls Overview

Linux has built-in firewall functionality via the Netfilter framework, which handles packet filtering, NAT, and connection tracking. Common utilities based on Netfilter include:

- iptables – widely used, full-featured firewall utility.
- nftables – successor to iptables with improved filtering and NAT.
- firewalld – uses predefined rule sets and network zones.
- ufw (Uncomplicated Firewall) – beginner-friendly interface to define rules easily.

Basic ufw Commands:

- Check status: `sudo ufw status`
- Enable firewall: `sudo ufw enable`
- Allow all outgoing traffic: `sudo ufw default allow outgoing`
- Deny incoming SSH traffic: `sudo ufw deny 22/tcp`
- List rules: `sudo ufw status numbered`
- Delete a rule: `sudo ufw delete <rule_number>`