Dunder-Mifflin Network Security Configuration with NFtables

Saturday, December 7, 2024 5:57 PM

Dunder-Mifflin Network Security Configuration with NFTables

This repository contains the configuration files and setup instructions to implement network security policies for a corporate network, as per the specifications given by **Dunder-Mifflin Corporate Headquarters**.

Objective

The goal is to configure firewalls using **nftables** on multiple machines within the corporate network, enforcing strict security policies to prevent access to unauthorized resources (such as Facebook), restrict incoming and outgoing traffic to only necessary services, and ensure all critical systems are properly secured.

Key Tasks Completed

1. **General Firewall Configuration (All Machines)**
    - Blocked all inbound traffic by default and only allowed explicitly permitted connections.
    - Allowed all outbound traffic by default.
    - Allowed all traffic on the local loopback interface (lo), enabling the machine to communicate with itself.
    - Allowed inbound ICMP traffic for echo-request, echo-reply (ping), time-exceeded (traceroute), and destination-unreachable messages.
    - Allowed incoming TCP traffic on port 4113 for the grading script.
    - Denied access to Facebook by blocking the IP address of facebook.com.
    - Allowed SSH access from the LAN, DMZ, WAN subnet, and VPN.
2. **Machine-Specific Configuration**
    - **Machine B (dns0)**: Configured to allow incoming DNS requests and zone transfers while allowing all outgoing traffic by default.
    - **Machine F (dns1)**: Configured to allow incoming DNS requests but not zone transfers and allowed outgoing traffic by default.
    - **Machine C (web0) and Machine D (web1)**: Configured to allow incoming HTTP traffic. Outbound traffic is denied by default, except for:
        - Outgoing DHCP and NTP traffic to Machine A's DMZ interface.
        - Outgoing DNS to Machines B and F.
        - Outgoing NFS to Machine E.
        - Outgoing SSH to the DMZ subnet.
        - Outgoing HTTP/HTTPS for package management (apt/dnf).
        - Allowed ping to all networks except the LAN subnet.
    - **Machine E (nfs)**: Configured to allow incoming NFS traffic from the DMZ and all outgoing traffic by default.
3. **Security Focus for Web Servers**
    - Tightened security specifically on the web servers (Machine C and Machine D) to limit potential attack vectors by restricting unnecessary services and ensuring only essential communication is allowed.
4. **Network Monitoring and Verification**
    - Ensured that all firewall rules are applied correctly by testing the firewall with various network tools (such as nmap, ping, and netstat) to verify open/closed ports and the proper functioning of critical services.
    - Used nft list ruleset to list the complete firewall rules and nft -f to load custom

rule configurations from the nftables.conf file.

5. **Additional Considerations**
    - Configured to prevent locking out of the machine via the network by ensuring correct use of return path rules (tracked with connection tracking ct).
    - Took measures to ensure all machines can survive a reboot without losing the applied firewall configuration.
    - Applied rules incrementally to ensure proper service functionality and avoid misconfigurations.