**How Firewalls Filter Traffic: Concepts and Mechanisms**

**Introduction**

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Understanding how firewalls filter traffic is essential for effective network security management.

**Basic Firewall Concepts**

**What is Traffic Filtering?**

Traffic filtering is the process of examining network packets and making decisions about whether to allow, block, or modify them based on predefined rules and criteria.

**Key Components of Network Packets**

Every network packet contains:

* **Source IP Address**: Where the packet originated
* **Destination IP Address**: Where the packet is going
* **Source Port**: The application port on the sender
* **Destination Port**: The application port on the receiver
* **Protocol**: TCP, UDP, ICMP, etc.
* **Payload**: The actual data being transmitted

**Types of Firewall Filtering**

**1. Packet Filtering (Stateless)**

**How it works:**

* Examines each packet independently
* Makes decisions based on header information only
* No memory of previous packets or connections

**Filtering Criteria:**

Source IP: 192.168.1.100  
Destination IP: 10.0.0.1  
Source Port: 45678  
Destination Port: 80  
Protocol: TCP  
Action: ALLOW/DENY

**Example Rule:**

# Allow HTTP traffic from internal network  
iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 80 -j ACCEPT

**2. Stateful Filtering**

**How it works:**

* Tracks connection states and sessions
* Remembers previous packets in a connection
* Makes decisions based on connection context

**Connection States:**

* **NEW**: First packet of a new connection
* **ESTABLISHED**: Packets belonging to an existing connection
* **RELATED**: Packets related to an established connection
* **INVALID**: Packets that don't match any known connection

**3. Application Layer Filtering (Deep Packet Inspection)**

**How it works:**

* Examines the actual content of packets
* Understands application protocols (HTTP, FTP, SMTP)
* Can filter based on URLs, file types, or content

**Traffic Flow and Decision Process**

**Typical Firewall Processing Steps**

1. **Packet Reception**
   * Firewall receives network packet
   * Extracts header information
2. **Rule Matching**
   * Compares packet against rule list
   * Processes rules in order (first match wins)
   * Checks source/destination IPs, ports, protocols
3. **State Checking** (for stateful firewalls)
   * Verifies connection state
   * Updates connection tracking table
4. **Action Execution**
   * **ACCEPT**: Allow packet to pass
   * **DROP**: Silently discard packet
   * **REJECT**: Discard packet and send error response
   * **LOG**: Record packet information

**Linux Netfilter/iptables Architecture**

* **PREROUTING**: Before routing decisions
* **INPUT**: Packets destined for local system
* **FORWARD**: Packets being routed through system
* **OUTPUT**: Packets generated by local system
* **POSTROUTING**: After routing decisions

**Windows Firewall Architecture**

Network Layer:  
Application Layer  
 ↓  
Transport Layer (TCP/UDP)  
 ↓  
Windows Filtering Platform (WFP)  
 ↓ (Rules Processing)  
Network Layer (IP)  
 ↓  
Data Link Layer