How Firewalls Filter Network Traffic

Firewalls act as security gatekeepers that monitor and control incoming and outgoing network traffic based on predetermined security rules. Here's a concise summary of how they filter traffic:

Core Filtering Mechanisms

1. Packet Filtering:

- Examines individual data packets

- Filters based on:

* Source/destination IP addresses

* Port numbers

* Protocol types (TCP/UDP/ICMP)

- Fast but limited to basic information

2. Stateful Inspection:

- Tracks active connections and their states

- Makes decisions based on connection context

- Recognizes legitimate reply packets

- More secure than simple packet filtering

3. Application-Level Filtering:

- Analyzes traffic at the application layer

- Can filter specific content (e.g., websites, services)

- Understands application protocols (HTTP, FTP, etc.)

Common Filtering Criteria

1. Direction-based:

- Inbound rules: Control incoming traffic (from external networks)

- Outbound rules: Control outgoing traffic (to external networks)

2. Port-based:

- Allows/blocks specific ports (e.g., block port 23/TCP for Telnet)

- Common examples:

* Allow 22/TCP (SSH)

* Allow 80,443/TCP (HTTP/HTTPS)

* Block 135-139,445/TCP (Windows shares)

3. Protocol-based:

- Filters by protocol type (TCP, UDP, ICMP)

- Can allow ping (ICMP) while blocking other protocols

4. IP Address-based:

- Whitelist/blacklist specific IPs or ranges

- Example: Allow only your office IP to access SSH

Advanced Filtering Techniques

1. Deep Packet Inspection (DPI):

- Examines packet contents beyond headers

- Can detect and block specific patterns or malware

2. Rate Limiting:

- Controls bandwidth usage
- Prevents denial-of-service (DoS) attacks

3. NAT (Network Address Translation):

- Hides internal network structure
- Allows multiple devices to share a public IP

Decision-Making Process

When traffic arrives at a firewall:

1. Checks if it matches any explicit allow/deny rules
2. Verifies connection state (for stateful firewalls)
3. Applies default policy (usually "deny all" for incoming)
4. Logs the decision (if logging is enabled)

Key Benefits

- Prevents unauthorized access
- Blocks malicious traffic
- Controls application access
- Protects against network attacks
- Logs suspicious activity

Firewalls implement these filtering techniques through either software (like UFW/iptables) or dedicated hardware appliances, providing essential network security at various levels.