SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

AN AUTONOMOUS INSTITUTION

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

Department of Computer Science and Engineering

Firewalls , Firewall Design Principles in Network Security

What is Firewall?

- A firewall in network security is a pr**otective barrier or security system that is designed to monitor and control incoming and outgoing network** traffic based on a set of predetermined security rules.
- Its primary purpose is to act as a filter or gatekeeper for data packets
- , allowing or blocking them based on criteria such as source and destination IP addresses, port numbers, and the type of network protocol being used.

How Firewalls Work?

- A firewall acts as a virtual barrier between your computer network and potential threats from the internet.
- Think of it as a **security checkpoint that filters incoming and outgoing data**,
- allowing only authorized and safe information to pass through while blocking malicious elements.
- Firewalls work by examining data packets and comparing them against a set of predefined rules to determine their legitimacy.

Types of Firewalls

- Packet Filtering Firewalls
- Stateful Inspection Firewalls
- Proxy Firewalls
- Next-Generation Firewalls (NGFW)

Packet Filtering Firewalls

- Packet filtering firewalls are the simplest form of firewalls.
- They analyze individual data packets and decide whether to allow or block them based on predefined rules.
- While effective, they can sometimes lack the granularity needed to combat more sophisticated attacks.
- **Example:** A **packet filtering firewall** may be configured to block incoming traffic on port 80 (HTTP) to prevent unauthorized access to web services.
- Packet filtering firewalls have low overhead as they operate at the network layer (Layer 3) and make filtering decisions based on packet headers.
- Packet filtering is often implemented in network routers to enforce basic security policies.

Stateful Inspection Firewalls

- Stateful inspection firewalls go beyond packet filtering by keeping track of active connections and the state of network traffic.
- This enables them to make more informed decisions about allowing or denying data packets.
- **Example:** A stateful inspection firewall monitors TCP connections, ensuring that incoming packets belong to established, legitimate sessions.
- Stateful inspection provides enhanced security by considering the state of network connections,
- such as TCP handshakes, to make more informed filtering decisions.
- They have some application layer (Layer 7) awareness, enabling deeper inspection of protocols like HTTP and FTP.

Proxy Firewalls

- Proxy firewalls act as intermediaries between a user's device and the internet.
- They retrieve and forward data on behalf of the user, adding an extra layer of security by shielding the internal network from direct exposure.
- **Example:** A web proxy firewall intercepts and inspects web requests from clients,
- filtering out malicious or unauthorized content before forwarding requests to web servers.
- They provide enhanced privacy and anonymity for internal clients by hiding client IP addresses from external servers.
- Proxy firewalls can cache frequently accessed content, reducing bandwidth usage and improving performance for clients.

Next-Generation Firewalls (NGFW)

- NGFWs combine traditional firewall functionalities with advanced features such as **intrusion detection and prevention,** , and application awareness.
- **Example:** An NGFW inspects not only packet headers but also packet payloads to detect and block advanced threats, such as zero-day exploits and malware.
- NGFWs can identify and control applications, allowing granular control over application-level traffic.
- They include intrusion prevention system (IPS) capabilities to detect and block known and unknown threats in real time.
- NGFWs provide a unified approach to network security, combining firewalling and VPN capabilities in a single platform.

Intrusion Detection and Prevention Systems (IDPS)

- IDPS capabilities allow firewalls to detect unauthorized attempts to access a network.
- These systems monitor for suspicious activity, such as unusual login patterns and respond in real time to prevent breaches.
- IDPSs monitor network traffic and system activities to detect abnormal behavior or patterns that may indicate a security threat or intrusion.
- They use predefined detection signatures or rulesets to identify known attack patterns, such as malware, denial-of-service (DoS) attacks, and unauthorized access attempts.
- IDPSs provide real-time monitoring and alerting capabilities, notifying administrators or security teams.

- **Example:** Imagine an IDPS installed on a company's network. It continuously monitors incoming and outgoing network traffic,
- looking for signs of malicious activities , If the IDPS detects a suspicious pattern, such as multiple failed login attempts from an external IP address,
- it triggers an alert for further investigation by security personnel.

Virtual Private Networks (VPNs)

- A virtual private network (VPN) extends a private network over a public network,
- allowing users to access secure resources as if they were directly connected to the private network.
- VPNs encrypt traffic, enhancing privacy and security, making them an essential tool for remote work and maintaining secure communications.
- VPNs can bypass geo-restrictions imposed by websites or streaming services, allowing users to access region-locked content or services from anywhere in the world.
- for example: When working from a coffee shop, connecting to your company's VPN encrypts your data,
- ensuring confidentiality when accessing internal files and applications.

Identifying and Mitigating Threats

Intruders and Unauthorized Access

- Firewalls monitor incoming traffic for signs of unauthorized access attempts.
- They can detect and block IP addresses exhibiting suspicious behavior, effectively neutralizing potential threats.

Viruses, Malware, and Ransomware

- Malicious software often finds its way into systems through various channels.
- Firewalls equipped with advanced threat detection mechanisms can identify and block incoming malware, preventing potential infections.

Firewalls Design Principles

Designing an effective firewall strategy requires careful consideration of various principles:

Defense in Depth

- Employing multiple layers of security ensures that even if one layer is breached, others remain intact.
- This principle reduces the risk of a single point of failure compromising the entire network.

Default Deny

- Firewalls should adopt a "default deny" stance, meaning that all traffic is blocked by default unless explicitly allowed.
- This minimizes the attack surface and ensures that only necessary and trusted traffic is permitted.

Regular Updates

- Firewalls should be regularly updated to stay resilient against new threats.
- Keeping rule sets and firmware up to date ensures that emerging vulnerabilities are addressed promptly.

Testing and Validation

- Conduct regular security assessments and firewall rule reviews to validate the effectiveness of firewall configurations,
- and ensure compliance with security policies and regulatory requirements.