Firewall and Basic Network Security

Student: Nuray Beydullayeva

OUTLINE

1. INTRODUCTION TO NETWORK SECURITY
2. UNDERSTANDING FIREWALLS
3. TYPES OF FIREWALLS
4. STATELESS VS. STATEFUL FIREWALLS
5. REAL-LIFE FIREWALL APPLICATIONS
6. BASIC NETWORK SECURITY PRACTICES
7. FIREWALL AS PART OF A COMPLETE SECURITY STRATEGY
8. SUMMARY & CONCLUSION

WHAT IS NETWOK SECURITY?

Definition

Network security refers to the policies, practices, and technologies used to protect the integrity, confidentiality, and availability of computer networks and data. It involves preventing unauthorized access, misuse, or theft of information and resources within a network.

KEY COMPONENTS

- Firewalls: Control incoming and outgoing network traffic based on security rules.
- Antivirus and anti-malware software: Detect and remove harmful software.
- Intrusion Detection and Prevention Systems (IDPS): Monitor for suspicious activity.
- Encryption: Protect data during transmission.
- Access control: Ensure only authorized users can access certain data or systems.
- Virtual Private Networks (VPNs): Secure remote connections.

WHY NETWORK SECURITY IS IMPORTANT?

Network security is crucial because it protects systems, data, and devices from a wide range of real-world threats.

DATA THEFT AND IDENTITY FRAUD

- Risk: Hackers can steal personal or business data, including credit card numbers, social security numbers, and login credentials.
- Real Example: In the 2017 Equifax breach, hackers stole data from over 147 million people, including SSNs and financial info.

RANSOMWARE ATTACKS

- Risk: Malicious software locks systems or files until a ransom is paid.
- Real Example: The 2017 WannaCry ransomware attack affected over 200,000 computers in 150+ countries, disrupting hospitals, banks, and businesses.

BUSINESS DISRUPTION

- Risk: Cyberattacks can shut down networks, websites, and services, leading to revenue loss and reputational damage.
- Real Example: In 2021, a cyberattack on Colonial Pipeline caused fuel shortages across the U.S. East Coast.

FINANCIAL LOSS

- Risk: Phishing, fraud, and other attacks can lead to massive financial losses.
- Real Example: In 2020, Twitter was hacked through social engineering, and attackers made over $100,000 through fake Bitcoin giveaways.

Common Network Threats

Viruses - Malicious software that attaches to files or programs and spreads when the file is executed. Can damage data, steal information, or render systems unusable.

Phishing - Fraudulent attempts to obtain sensitive information (passwords, credit card numbers) by pretending to be a trustworthy entity (e.g., fake emails or websites). Often leads to identity theft or financial loss.

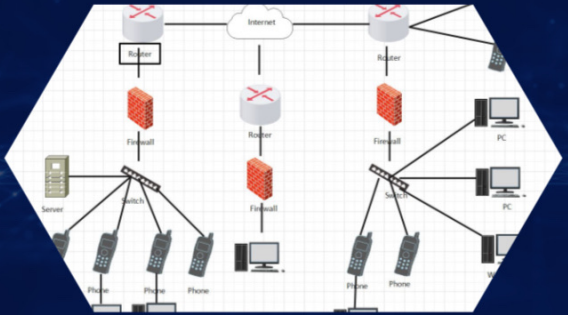
DDoS (Distributed Denial of Service) Attacks - Overwhelms a server, network, or website with massive traffic from multiple sources to make it unavailable. Can cause prolonged downtime and damage reputation.

Malware - Broad term for malicious software (includes viruses, worms, trojans, spyware, etc.). Can steal, encrypt, or delete data, monitor user activity, or disrupt system operations.

Man-in-the-Middle (MitM) Attacks - Attacker secretly intercepts and possibly alters communication between two parties. Can lead to stolen data or credentials.

Ransomware - Malware that encrypts the victim's files and demands payment for the decryption key. Can paralyze entire organizations.

WHAT IS A FIREWALL?



Definition

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to create a barrier between a trusted internal network (like your home or company network) and untrusted external networks (like the internet), helping to block malicious traffic such as hackers, viruses, or unauthorized access attempts.

- Hardware firewalls: Physical devices that sit between your network and the internet.
- Software firewalls: Programs installed on individual computers or servers.

HOW FIREWALLS WORK?

Firewalls act as a barrier between trusted internal networks and untrusted external networks (like the internet). They filter traffic using a set of rules and policies that define what is allowed or denied.

TRAFFIC FILTERING LOGIC

PACKET INSPECTION

When data travels over a network, it's broken into packets. A firewall inspects each packet to decide whether it should be allowed or blocked.

RULE-BASED FILTERING

Firewalls follow a set of rules that define what traffic is allowed. These rules can be based on:

- IP Addresses (source or destination)
- Port Numbers (e.g., 80 for HTTP, 443 for HTTPS)
- Protocols (e.g., TCP, UDP, ICMP)
- Application type (for next-gen firewalls)

DEFAULT ACTION

If no rule matches, firewalls usually apply a default policy (e.g., deny all or allow all).

TYPES OF FILTERING LOGIC

Stateless Filtering:
Each packet is treated independently.
Rules are applied to individual packets without considering the connection state.

Stateful Filtering:
Tracks the state of active connections.
Only allows packets that are part of a valid, established session.

Deep Packet Inspection (DPI):
Analyzes packet contents, not just headers.
Used in advanced firewalls to detect malware, application usage, etc.

HISTORY OF FIREWALLS

The history of firewalls can be divided into four main generations. The first generation, developed in the late 1980s, used packet filtering to inspect basic information like IP addresses and port numbers, but lacked connection awareness. The second generation, emerging in the early 1990s, introduced stateful inspection, which allowed the firewall to monitor active connections and filter traffic more intelligently. In the mid to late 1990s, the third generation brought application-layer firewalls, also known as proxy firewalls, which could inspect traffic at the application level (e.g., HTTP, FTP). Finally, the fourth generation, starting in the 2000s, led to next-generation firewalls (NGFW) that integrated deep packet inspection, intrusion prevention systems, and application/user awareness, offering much more advanced security capabilities.

Benefits of Using a Firewall

Using a firewall offers several key benefits for both individuals and organizations. First and foremost, it provides essential protection by preventing unauthorized access to your network, acting as a barrier between your internal systems and potential threats from the internet. Firewalls also monitor incoming and outgoing traffic, allowing you to control what data enters or leaves your system. This helps in blocking harmful content, malicious software, and suspicious activities. Additionally, firewalls can prevent hackers from exploiting system vulnerabilities and protect sensitive data from being exposed. For organizations, they support regulatory compliance by ensuring secure communication and protecting confidential information. Overall, firewalls are a critical component of any cybersecurity strategy, enhancing both security and control over digital environments.

Limitations of Firewalls

Firewalls are a key part of network security, but they have limitations. They can't protect against internal threats or remove malware, so antivirus tools are still needed. Firewalls also can't stop social engineering attacks like phishing, and they lose control once data leaves the network.

Encrypted traffic can hide threats from basic firewalls, and poor configuration can lead to vulnerabilities. Attackers may also bypass firewalls using VPNs or tunneling. Lastly, firewalls aren't effective against zero-day or advanced persistent threats. To stay secure, they should be used alongside other security tools.

FIREWALL IN REAL LIFE

HOME FIREWALL SETUP:

In a typical home, the internet connection comes through a modem provided by the ISP (Internet Service Provider). This modem is often connected to a Wi-Fi router, which usually has a built-in firewall. This home firewall blocks unauthorized incoming connections from the internet and allows safe outgoing connections, like browsing or streaming.

For example, if someone tries to hack into your home network from the internet, the router's firewall will block that traffic. Parents might also set rules (like blocking certain websites or setting time limits), which are managed through the firewall settings on the router.

COMPANY FIREWALL SETUP:

In a company, the firewall setup is more advanced. The internet first reaches a hardware firewall or UTM (Unified Threat Management) device at the network's edge. This firewall filters traffic, blocks known threats, manages VPN connections, and enforces company policies.

For instance, a company might use the firewall to block access to social media during work hours, protect sensitive data by monitoring outgoing traffic, and allow remote workers to securely access the network through a VPN. Large businesses may also use internal firewalls to segment departments and add another layer of protection.

PACKET-FILTERING FIREWALL

A packet-filtering firewall is a type of network security device that controls data flow to and from a network by examining individual packets. It applies a set of rules to incoming and outgoing packets based on information in the packet headers, such as:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol (TCP, UDP, ICMP, etc.)

HOW IT WORKS

1. A packet arrives at the firewall.
2. The firewall inspects the packet header.
3. It checks the header info against predefined rules (ACL – Access Control List).
4. Based on the rules, the firewall will either:
    - Allow the packet (forward it)
    - Deny the packet (drop it)

STATEFUL INSPECTION FIREWALL

A stateful firewall tracks the state of active connections and makes decisions based on the context of the traffic, not just individual packets.

Key Features:

- Remembers previous packets in a session.
- Allows only traffic that is part of an established connection.
- Offers better security than stateless firewalls.

How it works?

- Monitors TCP connections (SYN, ACK, FIN flags).
- Builds a state table to keep track of open sessions.
- Checks if incoming traffic matches an existing session.

SIMPLE DIAGRAM

[User] → [Stateful Firewall] → [Server]
| Keeps session info |
| Blocks unknown traffic |

CLOUD FIREWALLS

WHAT IS A CLOUD FIREWALL?

- A cloud firewall is a firewall delivered as a cloud-based service.
- It protects cloud infrastructure, applications, and data from cyber threats.
- Also known as Firewall-as-a-Service (FWaaS).

HOW IT WORKS

- Hosted in the cloud, not on-premises.
- Filters traffic between the internet and cloud resources (e.g., AWS, Azure).
- Can scale automatically with cloud infrastructure.

BENEFITS

- Scalability – Grows with your cloud environment.
- No hardware required – Fully managed by the provider.
- Easier updates and maintenance – Always up to date.

COMMON USE CASES

- Protecting web applications hosted in the cloud.
- Controlling access between virtual machines.
- Supporting remote teams and global access.

Basic Network Security Tips

1. Use Strong Passwords
   - Combine uppercase, lowercase, numbers, and symbols.
   - Avoid common words or personal information.

2. Keep Software Updated
   - Regularly install updates and patches for operating systems, firewalls, routers, and antivirus software.

3. Enable Firewalls
   - Use both hardware and software firewalls to protect your network.

4. Limit Access
   - Only allow necessary users and devices to access the network.
   - Use role-based access control where possible.

5. Regular Backups
   - Backup critical data frequently and store it securely.

6. Monitor Network Activity
   - Use monitoring tools to detect unusual traffic or unauthorized access.

Firewall as Part of a Security Strategy

Content (bullet points)

A firewall is just one layer of protection.
Strong security requires a combination of tools and policies.
Works best when combined with:
Antivirus software – to detect and remove malware.
Intrusion Detection/Prevention Systems (IDS/IPS) – to monitor for suspicious activity.
Virtual Private Networks (VPNs) – to secure remote access.
Access Control Policies – to limit who can access what.
Think of security as a layered “onion” – firewall is the outer layer.

OTHER TOOLS USED WITH FIREWALLS

INTRUSION DETECTION SYSTEM (IDS)

- Monitors network traffic for suspicious activity.
- Sends alerts if potential threats are detected.

INTRUSION PREVENTION SYSTEM (IPS)

- Similar to IDS, but can also block malicious traffic automatically.
- Often integrated into modern firewalls (NGFWs).

ANTIVIRUS/ANTI MALWARE SOFTWARE

- Protects devices from viruses, worms, and trojans.
- Works at the device level to scan and remove threats.

VIRTUAL PRIVATE NETWORK (VPN)

- Encrypts data between user and network.
- Ensures secure remote access.

Conclusion

In conclusion, firewalls play a crucial role in protecting networks by acting as a barrier between trusted and untrusted systems. They monitor and filter incoming and outgoing traffic based on predefined security rules. We explored different types of firewalls, including packet-filtering, stateful, and application-level firewalls, each serving different purposes in securing networks. However, a firewall alone is not enough. For complete protection, it should be combined with other security measures such as using strong passwords, keeping systems updated, and installing antivirus software. Understanding how firewalls work and how to configure them properly is essential to prevent unauthorized access, malware attacks, and data breaches. Overall, staying secure starts with being aware and proactive in protecting your digital environment.

THANK YOU