Firewall 

Understanding Firewall as a security mechanism

Momik Shrestha
Masters of Computer Science, Lincoln College University.
LIC00015002679

Jan 27, 2023

Contents

What is firewall ?

Definition
A firewall is a security system, either hardware or software, that monitors and controls incoming and outgoing network traffic based on predefined security rules.

Purpose:

- Protects devices and networks from unauthorized access.
- Blocks malicious traffic such as viruses, malware, or hackers.

A simple way to explain how a firewall works is to think of it as a security guard with intimate knowledge of millions of potential criminals. If the guard sees one, he or she keeps the criminal out of the building.

The firewall shields your network by acting as a 24/7 filter, scanning the data that attempts to enter your network and preventing anything that looks suspicious from getting through.

When to use firewall ?

Default Firewalls :

- Many systems (e.g., Windows, macOS) include basic firewalls for general protection.

  The warnings you see on your Windows system before downloading or visiting certain sites are often related to security features that involve a firewall or other protective systems

- Network routers often have built-in firewall capabilities.

  Routers are often the first line of defense between your internal network (e.g., your home Wi-Fi or office network) and the internet. The built-in firewall on the router helps block unauthorized access from external sources, such as hackers or malicious websites.

When to use firewall ?

Custom Firewalls :

- **Handling Sensitive Data**: Financial, healthcare, or personal information.
- **Large/Complex Networks**: Businesses with multiple users and devices.
- **Specific Threat Protection**: Targeted attacks, ransomware, or DDoS threats.
- **Remote Work**: Securing employees connecting to company resources via public networks.
- **Compliance Requirements**: Industries with strict security regulations (e.g., PCI DSS, HIPAA).

Why to use firewall ?

Key Benefits:

1. **Prevent Unauthorized Access:** Stops hackers and intruders from entering the network.
2. **Block Malware and Cyber Threats:** Filters malicious traffic to prevent data breaches and infections.
3. **Traffic Monitoring and Control:** Allows businesses to prioritize and regulate network usage.
4. **Protect Privacy:** Prevents unauthorized monitoring or data theft.
5. **Supports Compliance:** Ensures adherence to legal and industry security standards.

Real-Life Importance:
Without firewalls, networks are vulnerable to attacks, data theft, and operational downtime. A well-configured firewall forms the foundation of any robust cybersecurity strategy.

Types of Firewall

Based on Deployment:

Hardware Firewalls

Description: These are physical devices that are placed between the internal network and external networks (like the internet) to control traffic. They often come with dedicated processing power and specialized components for traffic filtering and monitoring.

Deployment: Typically deployed at the network perimeter to protect the entire network infrastructure.

Use Case: Ideal for large organizations, data centers, or businesses with high network traffic requiring robust, dedicated protection.

Types of Firewall

Based on Deployment:

Software Firewalls

Description: These are firewalls implemented through software that runs on operating systems. They can be installed on individual devices (such as personal computers or servers) and offer more granular control over specific device-level traffic.

Deployment: Installed on individual devices or within network infrastructure, such as on servers or virtual machines.

Use Case: Suitable for protecting individual devices, securing servers, or managing network traffic within smaller setups.

Types of Firewall

Based on Deployment:

Software Firewalls

Description: These are firewalls implemented through software that runs on operating systems. They can be installed on individual devices (such as personal computers or servers) and offer more granular control over specific device-level traffic.

Deployment: Installed on individual devices or within network infrastructure, such as on servers or virtual machines.

Use Case: Suitable for protecting individual devices, securing servers, or managing network traffic within smaller setups.

Types of Firewall

Based on Functionality:

1. Packet Filtering Firewall
2. Stateful Inspection Firewall
3. Proxy Firewall (Application-Level Gateway)
4. Next-Generation Firewall (NGFW)
5. Circuit-Level Gateway
6. Hybrid Firewall
7. Web Application Firewall (WAF)

Types of Firewall

1. Packet Filtering Firewall

Description: Inspects packets of data based on predefined rules, such as IP address, port number, and protocol. It allows or blocks traffic based on these filters without tracking the state of the connection.
Use Case: Suitable for basic network protection where detailed inspection isn't required, such as for smaller networks or home routers.

2. Stateful Inspection Firewall

Description: Monitors the state of active connections and makes decisions based on both the predefined rules and the state of the connection. It tracks the state of traffic to ensure it is part of a legitimate session.
Use Case: Used in enterprise networks where the need to track the state of connections adds an extra layer of security, such as for internal networks.

Types of Firewall

3. Proxy Firewall (Application-Level Gateway)

Description: Intercepts traffic between the internal network and external network and performs deep packet inspection at the application layer. It acts as an intermediary between the client and the server.
Use Case: Suitable for high-security environments where you need to inspect and control traffic for specific applications (e.g., HTTP, FTP, DNS).

4. Next-Generation Firewall (NGFW)

Description: Combines traditional firewall features (stateful inspection) with advanced security functions like intrusion prevention, application control, and deep packet inspection, offering comprehensive protection.
Use Case: Ideal for modern enterprise environments where protection against sophisticated threats like malware, botnets, and advanced persistent threats (APTs) is critical.

Types of Firewall

5. Circuit-Level Gateway

Description: Monitors the TCP handshake and ensures that packets involved in the connection are valid. Once the session is established, it allows the data to flow freely between the client and the server.
Use Case: Useful in legacy systems where minimal inspection is needed, but connection legitimacy must be validated.

7. Web Application Firewall (WAF)

Description: Specifically designed to protect web applications by filtering and monitoring HTTP traffic to prevent attacks such as SQL injection, cross-site scripting (XSS), and other web-based threats.
Use Case: Used by organizations with web applications, such as e-commerce sites, to safeguard against common web attacks.


THE GREAT FIREWALL OF CHINA
Gmail
Gmail

Exploring the Great Firewall of China

WHAT is the Great Firewall of China (GFW):
The **GFW** refers to a set of **internet censorship and surveillance measures** employed by the Chinese government to control and monitor internet traffic coming in and out of the country. It's a complex system designed to regulate access to foreign websites and content, restrict access to certain types of information, and enforce the government's policies on digital content.

Setting asides the ethical concern, the **GFW** showcases a very large scale adoption and implementation of firewall technology and is a technological feat.

Exploring the Great Firewall of China

Why the GFW exists:

1. **Control Information**: The Chinese government uses the GFW to limit the flow of foreign information and prevent citizens from accessing content deemed politically sensitive or harmful to the state.
2. **Maintain National Security**: The GFW is designed to prevent the spread of information that could lead to political unrest, civil disobedience, or opposition movements, effectively controlling discourse in the country.
3. **Protect Local Industry**: By blocking international services like Google, Facebook, and Twitter, the Chinese government encourages domestic companies to fill those roles, promoting local technological growth and services (e.g., Baidu, WeChat, and Weibo).
4. **Social Control**: It ensures that the population remains exposed to government-approved narratives, limiting dissenting voices and encouraging conformity.

Exploring the Great Firewall of China

Why the GFW exists:

1. **Control Information**: The Chinese government uses the GFW to limit the flow of foreign information and prevent citizens from accessing content deemed politically sensitive or harmful to the state.
2. **Maintain National Security**: The GFW is designed to prevent the spread of information that could lead to political unrest, civil disobedience, or opposition movements, effectively controlling discourse in the country.
3. **Protect Local Industry**: By blocking international services like Google, Facebook, and Twitter, the Chinese government encourages domestic companies to fill those roles, promoting local technological growth and services (e.g., Baidu, WeChat, and Weibo).
4. **Social Control**: It ensures that the population remains exposed to government-approved narratives, limiting dissenting voices and encouraging conformity.

Exploring the Great Firewall of China

How the GFW works (The Gist):

1. **IP Blocking**: The firewall blocks access to IP addresses of websites that are deemed harmful or restricted by the government. For example, websites like Google, YouTube, and Facebook have their IP addresses blocked within the country.
2. **DNS Spoofing**: The GFW uses DNS poisoning, or DNS spoofing, to redirect users attempting to access blocked websites. When users try to visit a restricted site, the DNS query is intercepted and manipulated, leading to a non-existent or "dead" site.
3. **Packet Filtering**: The GFW inspects internet traffic at the packet level, looking for keywords or patterns related to banned content (e.g., topics like Tiananmen Square or references to the Dalai Lama). It can block or restrict packets that contain specific content.
4. **Deep Packet Inspection (DPI)**: DPI is used to examine the data contained within network packets, not just the headers. This allows the firewall to block communications that contain specific content or violate censorship rules, even if they use encrypted channels (e.g., VPNs or HTTPS).
5. **VPN and Proxy Blocking**: To prevent citizens from bypassing censorship via VPNs or proxies, the GFW aggressively monitors and blocks VPN services and uses techniques like **traffic analysis** to detect and disrupt VPN connections.
6. **Throttling and Filtering**: It can reduce the speed of foreign websites to make them unusable or block access completely. Filtering is also applied to ensure that sensitive terms and websites are inaccessible.