***Firewall Comparison Report***

***Author : Vineeth M***

***Date : sep 17, 2025***

***1. Traditional Firewall***

***where it is used****: Computers, home routers, and simple networks.*

## ***What is a Traditional Firewall:***

*A traditional firewall is a solution where incoming as well as outgoing network traffic is controlled according to predefined security rules either through hardware or software product filtering at Layer 3 of OSI or blocking/allowing packets based on source/destination IP addresses, protocols, and ports.*

### ***Advantages of Traditional Firewall***

1. ***Simplicity****: Traditional firewalls are easier to set up and manage, offer very basic traffic filtering, and are relatively less complex.*
2. ***Cost-effective****: They usually charge reasonably good money, thereby ensuring that small networks with relatively few security concerns can afford them.*
3. ***Performance****: Since they do minimal packet inspection, traditional firewalls are generally fast-speed.*

### ***Disadvantages of Traditional Firewall***

1. ***Limited Security****: The traditional aged firewalls can only provide packet filtering. Packet filtering cannot detect applications-layer threats and the more advanced attacks like malware or APTs.*
2. ***No DPI(*Deep Packet Inspection*)****: DPI in case of a traditional firewall means they do not scan the actual content of data in transit, therefore less effective against latest threats .*
3. ***No application awareness****: It cannot identify applications and is hence unable to enforce app-level security policies.*

## 2.**Next Generation Firewall (NGFW)**

***where it is used****: Enterprise routers, dedicated firewall appliances, cloud network gateways, and some advanced home Wi-Fi routers.*

## *What is a Next Generation Firewall?*

*NGFW is more advanced than the traditional firewall, since it offers more layers of protection. A traditional firewall features packet filtering, but NGFW carries out DPI (***Deep Packet Inspection***), intrusion prevention, application control, and identity-based access (***who can access what*)****. It works on a few layers from Layer 3 to Layer 7 for quite granular view.*

### *Advantages of Next Generation Firewall*

1. *Advanced Threat Protection. NGFW can detect and stop the latest malware, ransomware, and advanced persistent threats using DPI, IDS/IPS, and sandboxing.*

***Example:***

* *A hacker sends a malicious email attachment:*
  1. *NGFW uses* ***DPI*** *to inspect the file*
  2. ***IDS/IPS*** *detects it as suspicious*
  3. *The file is opened in a* ***sandbox*** *to confirm it’s dangerous*
  4. *NGFW* ***blocks it*** *before it reaches users*

1. *Application Awareness. NGFW can discern and manage traffic based on applications, not IP address or ports, so it can be much more granular.*

***Example:***

***can allow, block, or limit specific apps instead of blocking an entire IP or port.***

1. *Unified Security. NGFW can tie in lots of security functions together, such as firewall, VPN, antivirus, etc.*

***Example:***

*A company uses an NGFW:*

* + *Employee tries to access a harmful website →* ***web filter blocks it***
  + ***Suspicious download → A****ntivirus detects it*****
  + *Remote worker connects →* ***VPN secures the connection***
  + *All handled by* ***one NGFW device***

1. *Identity Awareness: It can enforce security policies according to the identity of the users. This way, role-based access control can also be implemented.*

***Ex:***  *NGFW enforces user's role-based access control automatically.*

***Disadvantages of Next-Gen Firewalls (NGFW)***

***1. High Cost***

* ***NGFWs are expensive compared to traditional firewalls.***
* ***Small businesses may struggle to afford them***

***2.*  *Complex Setup and Management***

* ***They have many advanced features (deep inspection, identity-based access, IPS, etc.).***
* *Needs* ***skilled people*** *to configure correctly.*

***3.Performance Issues (Slower Speed)***

* ***Because NGFW checks everything deeply (packets, apps, users, content).***
* *This* ***can slow down the network*** *if hardware is not strong enough.*

***4. If firewall on same server Need more resources***

***Needs powerful hardware (CPU, memory).***

* *Consumes more electricity and resources than basic firewalls.*

***3.Web Application Firewall (WAF)***

***where it is used: WAF (Web Application Firewall) is used to protect web applications, so it sits on the web server or in front of the web server.***

## *****What is a WAF?*****

***Web application firewalls (WAFs) are a critical security defense for websites, mobile applications, and APIs. They monitor, filter, and block data packets to and from web applications, protecting them from threats. WAFs are designed (trained) to detect and protect against dangerous security flaws that are most common within web traffic. This makes them essential for online businesses like retailers, banks, healthcare, and social media, which need to protect sensitive data from unauthorized access. WAFs can be deployed as network-based, host-based, or cloud-based solutions, providing visibility into application data at the HTTP application layer.***

***Since web and mobile applications and APIs are prone to security risks that can disrupt operations or exhaust resources, web application firewalls are designed to counter common web exploits like malicious bots. WAFs safeguard against threats that compromise availability, security, or resources including zero-day exploits, bots, and malware.***

*****Advantages of WAF (Web Application Firewall)*****

***1.****Protects Web Applications from Attacks*****

* *Blocks threats like* ***SQL injection, cross-site scripting (XSS), and other web attacks***
* ***Keets your website and users safe***

***Example:***

* ***You use a banking website.***
* *Hacker tries to enter username=' OR '1'='1 in the login form* ***from their own computer****.*
* *The website server receives it.*
* *If the website has a vulnerability → hacker might get access.*
* *If WAF is installed → it blocks the request → website stays safe.*

***2.Monitors and Filters Traffic***

* *Inspects* ***all incoming requests*** *to the website*
* *Allows* ***safe traffic*** *and blocks* ***malicious requests***

*****Example:*** *waf blocks malicious requests from hackers***

***3.DDoS Protection (in Some WAFs)***

* *Can help* ***prevent denial-of-service attacks*** *that try to crash your website*

***Example***

*-A small online store is attacked by hundreds of fake requests per second.*

*-WAF detects that these requests are* ***not normal*** *→ blocks them.*

*-Customers can still browse and shop without interruption.*

*4.****Logging and Alerts***

* *Keeps track of attacks and suspicious activity*
* *Helps website owners* ***analyze and respond*** *to threats*

***Example***

*- A hacker tries SQL injection 50 times in one day.*

*- WAF blocks all attempts and* ***records them in the log****.*

*- Website admin gets an* ***alert****: “SQL Injection attempts detected from IP: 192.168.1.50”*

*-The admin can then block report that IP or strengthen defenses.*

*5.****Compliance***

* *Helps meet* ***security standards*** *like PCI DSS (*Payment Card Industry Data Security Standard) *for online payment security*

***Disadvantages of Web Application Firewalls (WAF)***

***1.****False Positives*

* *WAF sometimes bolcks normal requests, by mistake they are attacked*

***2.Performance Impact***

* *WAF checks every single web requests*
* *This slow down requests*

***3. High Cost***

* *Cloud WAF services (like Cloudflare, AWS WAF) can be expensive*
* ***Hardware WAF devices cost even more, so small businesses may struggle.***

***4.Complex Setup & Maintenance***

* *It’s need carefull configuration.*
* *It’s too strict may block real users.*
* *Need experts to keep maintain*

***5. Limited Protection***

* *WAF only protects web applications.*
* *Malware infections and Other attacks posiblie*