How to Configure AWS Firewalls to secure the Network Layer of AWS Environments

AWS primarily offers two Managed Firewalls, AWS Network Firewall and AWS WAF both offering different Security Benefits. Understanding the Difference between these two Firewalls, is crucial in securing your Cloud Environments.

AWS Network Firewall

AWS Network Firewall is AWS Managed Network Firewall, which primarily operates at Layer 3, 4, and 7 of the OSI Layer.

- Layer 3, 4 Security - It performs stateful inspection of IP Addresses, protocols and ports.
- Layer 7 Security - It provides Deep packet inspection (DPI) to filter traffic based on domain names (FQDN) or specific patterns within the application data (like HTTP headers), which is a significant step up from standard Security Groups.

Understanding these Features in Detail is important to justify its high monthly cost, and the Compliance Benefit :

- **Stateful Inspection:** Unlike standard Network ACLs, which are stateless, this firewall remembers the state of active connections. It can track the context of traffic flows to ensure that incoming return traffic is only allowed if it matches a legitimate outgoing request.
- **Deep Packet Inspection (DPI):** It can peer into the "payload" of the network packets. This allows you to block specific types of web traffic or identify malicious patterns that are hidden within legitimate-looking connections.
- **FQDN Filtering:** You can restrict outbound traffic to a specific list of domain names (e.g., only allowing `*.amazonaws.com`). This is critical for preventing "data exfiltration," where a compromised server tries to send data to an unauthorized external site.
- **Intrusion Prevention System (IPS):** It includes signature-based detection to identify and block known threats, such as malware, spyware, and command-and-control (C2) communications.
- **Suricata Rule Support:** It supports open-source Suricata rule sets, giving you the flexibility to write highly customized security rules or import rules from third-party security vendors.
- **Centralized Management:** Through AWS Firewall Manager, you can deploy and manage firewall policies across multiple AWS accounts and VPCs simultaneously, ensuring consistent security posture across your entire organization.

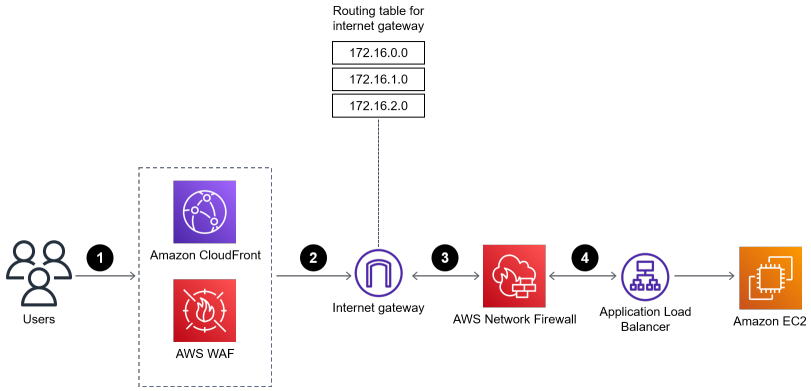

Figure 1: AWS WAF Placement

AWS Web Application Firewall

The primary benefit of AWS WAF is that malicious traffic **never** makes it to your network, and is built to block OWASP Top 10 common Web exploits at Layer 7 that Network Firewalls Typically Miss. This includes :

```
1. OWASP Top 10 Attacks - Internets top 10 exploits updated each year.
    1. SQL Injection Attacks - Where malicious code is injected into input fields to manipul
    2. XSS Attacks - Blocking Scripts injected into web pages, that could execute in malicio
    3. Path Traversal Attacks - Preventing attackers from accessing unauthorized files on se
2. DDoS Attacks - Rate Based traffic filtering, and carefully crafter attacks such as Slowlo
3. Vulnerability Exploitation - Managed rules are frequently updated to block exploits for v
4. Reconissance Attacks - Blocking tools which attackers use to "map" your applications vuln
```

Network Firwall Vs. AWS WAF

Feature	AWS Network Firewall (Managed)	AWS WAF (Web Application Firewall)
Primary Goal	VPC-level security & Egress filtering.	Protecting Web Apps & APIs (HTTP/S).
Protocol Support	TCP, UDP, ICMP, and more	HTTP, HTTPS, WebSockets
Bot Mitigation	Limited (IP-based).	**Advanced** (Behavioral analysis, CAPTCHAs).
SQL Injection	Not designed for this.	Specializes in detecting SQLi patterns.
Cross-Site Scripting (XSS)	Not designed for this.	Specializes in detecting XSS patterns.

Feature	AWS Network Firewall (Managed)	AWS WAF (Web Application Firewall)
VPC Traffic Control	**Yes** (Inter-VPC, Outbound to Internet).	No (Only inspects web traffic at the ALB/CloudFront).
DDoS Protection	L3/L4 (via Shield Standard).	L7 HTTP Floods (Rate-limiting & Geo-blocking).
Encryption (TLS)	Can inspect via TLS 1.3 decryption.	Inspects at the ALB where TLS is terminated.
Malware Signatures	Yes (IPS/Suricata)	No
Monthly Cost	~**$284 / month** (Bundled with NAT Gateway Waiver).	~**$25 / month** (Base fee + $0.60 per 1M requests).

Final Verdict

For complete security, use Both !

Key advantage of Network Firewall is that it also inspects traffic leaving a secure environment, which would mitigate cases of Leaked confidential data. Additionally, if an insider attack were to occur, it would detect that and automatically block it. Finally, Network Firewalls are non-negotiable if there is Non-WebApplication Traffic (SSH, IPSec Tunnel to External Environment or VPC-to-VPC, External Databases) and offers Intrusion Prevention Capabilities by looking for "fingerprints" of exploits that are not necessarily Web Based (Layer 7).

AWS WAF offers more security at Layer 7, detecting Bot Attacks, SQLi and Cross Site Scripting Attacks, Captcha Challenges to detect human traffic, body and Header Inspection . WAF is called a permiter Firewall because it can perform filtering at the Edge with Amazon Cloudfront. Wheras Network Firewall needs to run inside your VPC/Network.

Still there Exist use cases where Network Firewall might be overkill .

1. **Pure Serverless Architectures** (API Gateway and Lambda Only) - API Gateway only speaks HTTPS, and Lambda can be deployed on Managed Architecture (without a VPC, no SSH or RDP). Therefore there is no network to secure.
2. **Static Content Delivery** (CloudFront + S3) - S3 static websites are served at Layer 7 only, there is no networks, therefore no need for a Network firewall to defend a network.

3. **Public Facing Web Apps with Strict Security Groups** - A Web Application Sitting Infront of an ALB, and (Attached to a WAF, with only port 443 ingress), and Frontend and Backend (Fargate Tasks) with Strict Security Groups to only allow traffic between each other.
    - **Risks Involved** - Since a network firewall detects malicious outbound traffic, and WAF cannot. Compromised code (code libraries, docker vulnerabilities), and insider attacks can exfiltrate ePHI Data.
        - Container and Code Scanning, can reduce this risk, but Zero Day Exploits are still vulnerable.
        - Any protocol below Layer 7 can be compromised (SSH, RDP, FTP, exfiltrating data in ping packets, smb/nfs, syn flood attacks)
        - Attackers can exfiltrate data through DNS exfiltration (code exfiltrating data as dns traffic).

References

1. Deployment Models for AWS Network Firewall
2. Permiter Zone Architecture