AWS WAF (Web Application Firewall)

ver the past couple of years, security has become a crucial concern for most companies. Fortunately, there are many services available to help you improve the overall security of your AWS environment. **AWS WAF (Web Application Firewall)** is a firewall that helps you to **protect your web application server** against a range of Internet threats.

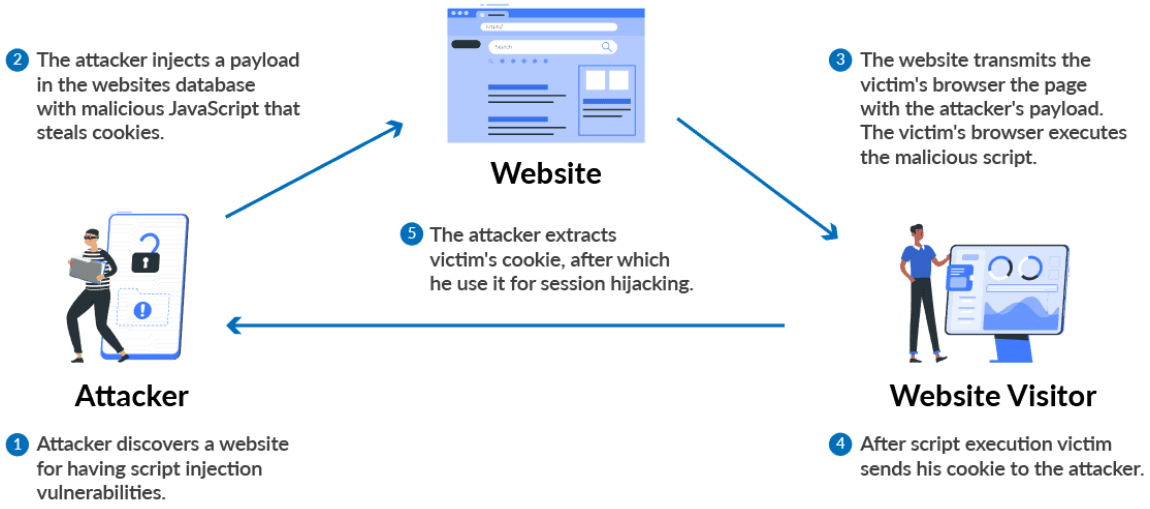
What is AWS WAF

AWS Web Application Firewall (WAF) is a security tool that helps you to protect the application against web attacks. WAF monitors and controls unusual bot traffic, and blocks common attack patterns, such as **SQL Injection or Cross-site scripting**, etc. It also lets you monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront, or an Application Load Balancer.

- Amazon WAF allows you to control your content by using an IP address from where the request originates.
- Three things make Amazon WAF work – **Access control lists (ACL), Rules, and Rule Groups**.
- Amazon WAF manages Web ACL capacity units (WCU) for rules, rule groups, and web ACLs.
- Amazon WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of security rules.

Common Web Attacks

Before protecting your applications, you need to know the most common web attacks mentioned below.



DDoS(Denial-Of-Service) attacks: This is probably the most common attack. Attackers overload an application by sending bulk requests to the web servers. Thousands of hosts infected with malware

are used in this attack, which utilizes more than one unique IP address or machine. This slows down the application and significantly hurt the value of a brand.
SQL injections: SQL injection is a code injection procedure that might destroy your SQL database. Attackers can run malicious SQL queries on your web applications.
Cross-Site Scripting: If your application is vulnerable to cross-site scripting, then the attacker can run or inject malicious scripts, generally in the form of a browser side script. These scripts can even rewrite the content of the HTML pages.

AWS WAF Features

Amazon Web Application Firewall offers lots of features to its users mentioned below.

- **Protection Against Web Attacks:** With minimum latency impact on incoming traffic, WAF AWS offers many rules to inspect any element of a web request. WAF AWS protects web applications against threats by filtering traffic according to the rules created.
- **Establish Rules Accordingly:** WAF AWS is a versatile and valuable tool for protecting the infrastructures of applications. And this is because it allows users to establish rules according to their needs and vulnerabilities that they wish to stop. We can consider it a great solution to protect any web application environment at the enterprise level.
- **Web traffic filtering:** WAF allows users to create rules to filter web traffic. It filters IP addresses, HTTP headers, HTTP bodies, or URI strings from a web request.
- **Flexible Integration With AWS Services:** AWS Firewall offers easy integration with other AWS services like Amazon EC2, CloudFront, Load balancer, etc.
- **Monitor Rules:** Web Application Firewall AWS allows us to create rules and review and customize them to prevent unknown attracts.

How It Works

AWS Web Application Firewall protects the applications from malicious attacks. The working of WAF in AWS mentioned below.

- **AWS Firewall Manage:** It Manages multiple AWS Web Application Firewall Deployments
- **AWS WAF:** Protect deployed applications from common web exploits.
- **Create a Policy:** Now you can build your own rules using the visual rule builder.
- **Block Filter:** Block filters protect against exploits and vulnerabilities attacks.
- **Monitor:** Use Amazon CloudWatch for incoming traffic metrics & Amazon kinesis firehose for request details, then tune rules based on metrics and log data.

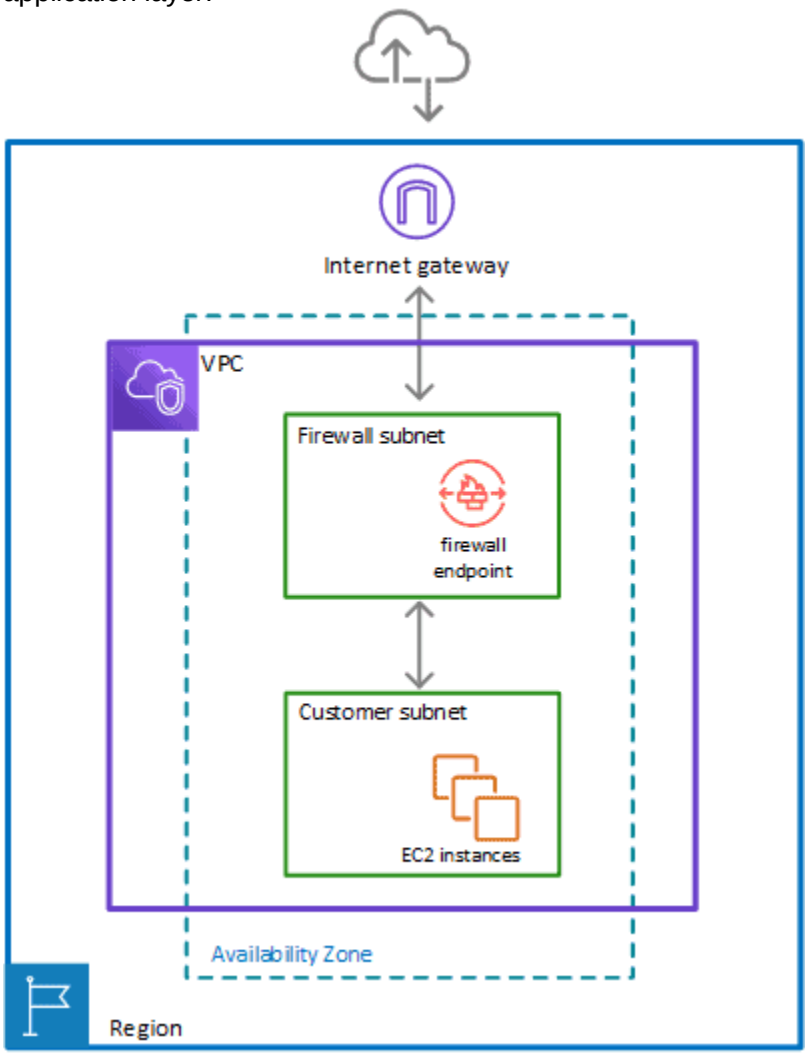
AWS Network Firewall

> ***AWS Network Firewall***, in simple terms, is ***an additional layer of security to protect your infrastructure*** against dangerous ***threats like malware, botnets, and DDoS attacks*** while getting advanced access control.

Overview of AWS Network Firewall

AWS Network Firewall is a **highly available**, scalable firewall service from AWS, with **fully managed infrastructure.** This firewall service allows you to apply blanket protections across your entire VPC, regardless of the application type or protocol. This means you can inspect traffic at

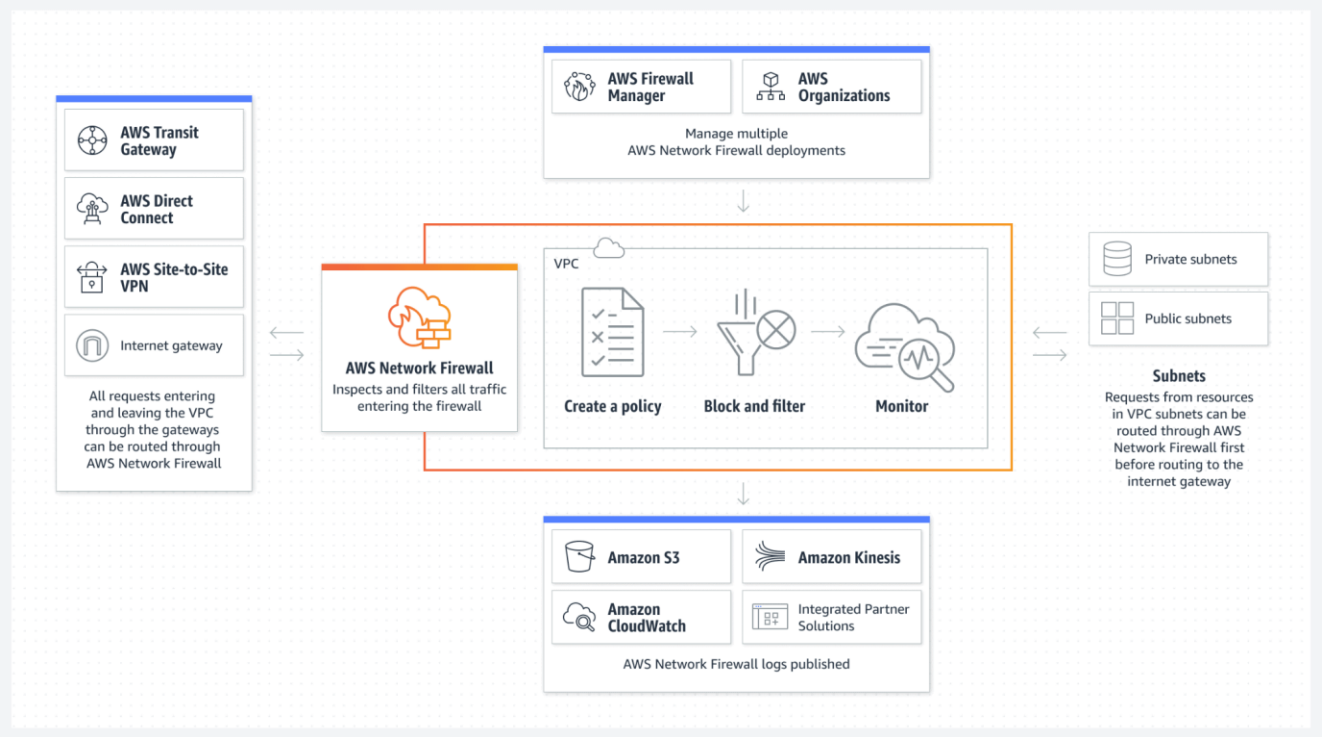
layers three through seven of the OSI model, both at the network layer and up through the application layer.



How Does It Work?

AWS Network Firewall is a service that allows you to create **stateful firewalls for your VPCs.** It uses rules that you define to control **inbound and outbound traffic** at the subnet level. The firewall can also inspect and analyze network traffic and can be used in conjunction with security groups and network ACLs to provide additional layers of security.

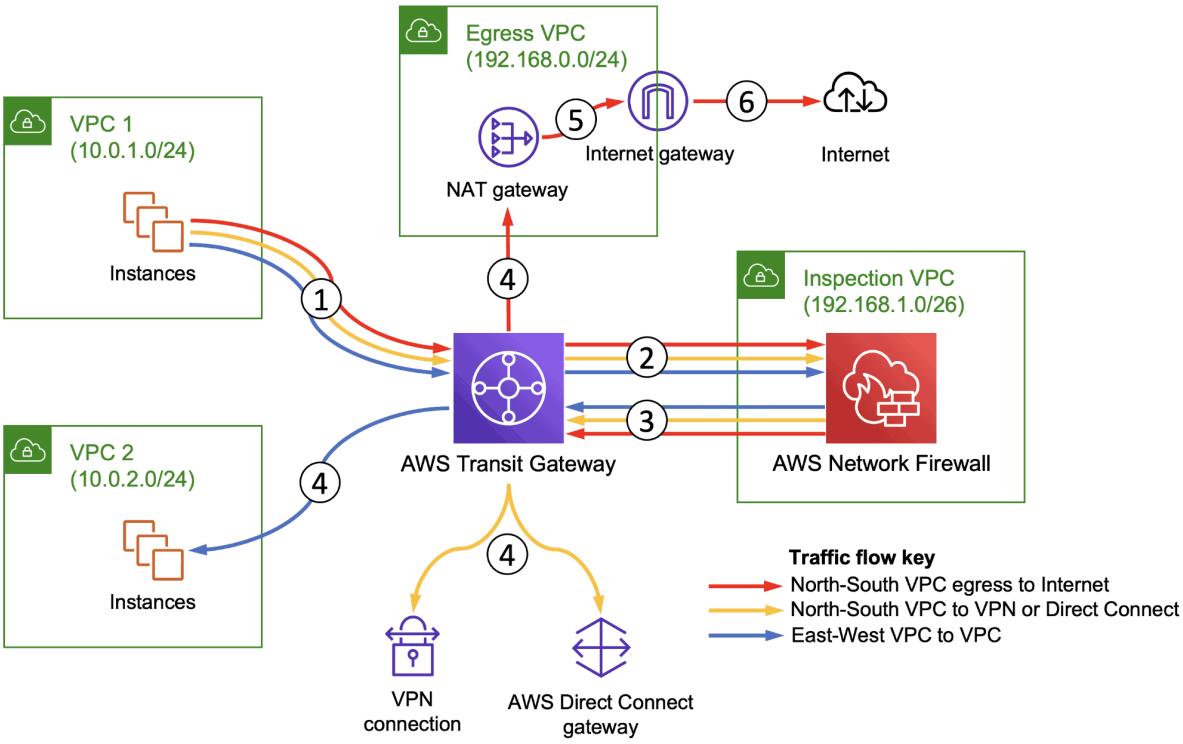
Network Firewall provides a set of pre-configured rule groups, you can also create your own custom rule groups. And, it also supports integration with AWS resource tagging, AWS Identity and Access Management (IAM), and AWS Resource Access Manager (RAM) for added security and management capabilities.



Key Benefits

- **Fully Managed:** With a fully managed service like AWS Network Firewall, the service automatically handles tasks such as rule updates and traffic monitoring. This means that you don't have to worry about manually updating your firewall rules or monitoring your network traffic, which can free up time and resources for other important tasks.
- **Flexible Deployments:** The service can be used in a variety of different deployment scenarios, depending on your specific requirements. One of the most popular deployment options for AWS Network Firewall is using it as a **VPC (Virtual Private Cloud) firewall.** This can be useful for protecting your resources within the VPC. Another deployment option for AWS Network Firewall is to use it as a **Transit Gateway firewall.**
- **Fine-Grained Controls:** When it comes to securing your network, having fine-grained controls is a key benefit of using a firewall. Fine-grained controls allow you to set precise rules for incoming and outgoing network traffic, which can help you protect your resources from unwanted access while also allowing legitimate traffic to pass through.
- **Partner Integrated:** AWS Network Firewall can be integrated with partners. This integration allows you to leverage the expertise and capabilities of these partners to enhance the security of your network traffic.
  AWS works with several other partners like **Cisco, Check Point, Palo Alto Networks, Fortinet,** etc. Allowing these vendors to provide network firewall devices that integrate with

Network Firewall to leverage the power of its fully managed service.

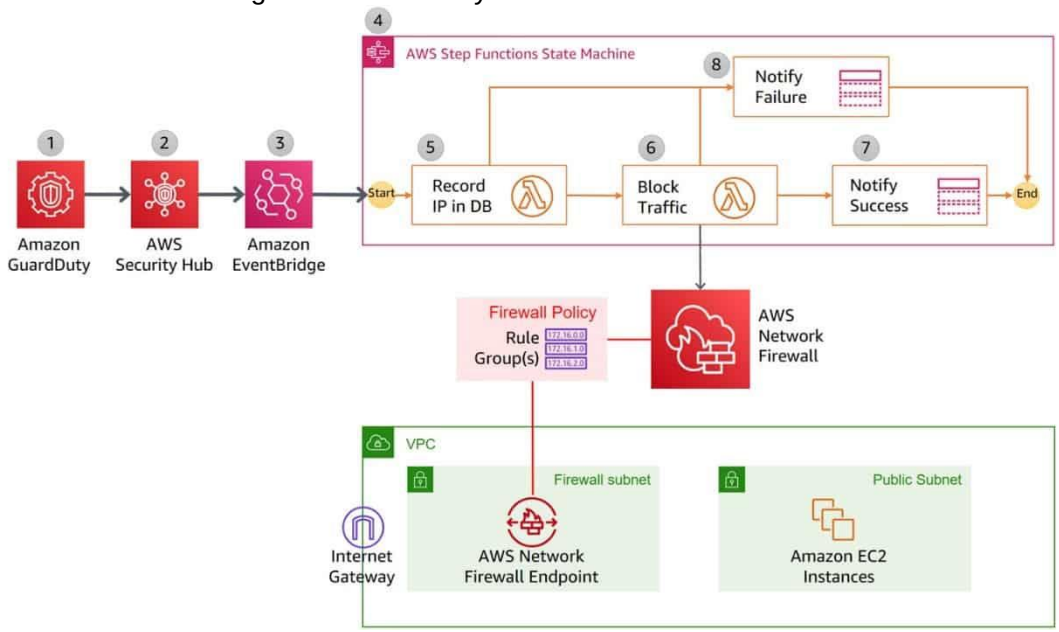


Features

AWS Network Firewall is a powerful service that provides a wide range of features to help you secure your network traffic. Some of the key features of the service include:

1. **Custom rules**: Allows you to define your own custom rules, which means you can create rules that are specific to your own network traffic, giving you more control over your network traffic and minimizing security risks.
2. **Automatic protections**: Provides automatic protections against common network threats, such as IP spoofing, SYN floods, and port scans, so you don't have to configure these protections manually.
3. **Integration with other services**: Integrates with other AWS security services such as Amazon GuardDuty, Amazon Inspector, and AWS WAF to provide a more comprehensive security strategy for your network traffic and infrastructure.
4. **Fully managed**: Automatically handles tasks such as rule updates and traffic monitoring, and includes high-availability and automatic failover capabilities to ensure your firewall is always available and that there is no disruption to your network traffic in case of failure.
5. **Analytics**: Network Firewall also includes analytics capabilities that allow you to monitor and troubleshoot network traffic, and can help you identify and resolve issues more quickly.

6. **Scale**: A network Firewall can handle large-scale traffic, so you don't have to worry about your firewall becoming a bottleneck for your network traffic.



By using these features, AWS Network Firewall can provide a powerful and flexible way to protect your network from unwanted access while also allowing legitimate traffic to pass through. It can also help you save time and resources by automating many of the operational tasks associated with running a firewall.

Pricing

AWS Network Firewall is priced on a ***pay-as-you-go basis***, which means that you only pay for the resources you use. The pricing for the service is based on the number of firewall rules and the amount of traffic that is processed by the firewall.
There are different prices for different types of traffic that are processed by the firewall, including:

1. **Internet traffic**: Traffic that enters or exits your VPC
2. **Transit traffic**: Traffic that enters or exits your Transit Gateway.

Additionally, prices also vary depending on the region you are using the service in. AWS provides a free tier for Network Firewall, which allows you to process up to **50GB of traffic per month for free**. This can be a great way to try out the service and see if it fits your needs before committing to spending any money.
It is always recommended to check the pricing page of the AWS Network Firewall service to have the most up-to-date and accurate pricing information.

Use Cases

AWS Network Firewall is a powerful and flexible service that can be used in a wide range of real-world scenarios. Here are a few examples of use cases for the service:

1. **Securing a VPC**: AWS Network Firewall can be used to create a firewall that is specific to your VPC. This allows you to control the traffic that enters and exits your VPC, which can help you protect your resources, such as EC2 instances or RDS instances, from unwanted access.

2. **Managing transit traffic**: With AWS, you can create a firewall that controls the traffic that flows between your Transit Gateway and your VPCs, on-premises data centers, and remote networks that are connected to your Transit Gateway.
3. **Compliance**: Network Firewall's fine-grained controls allow you to create rules that are specific to your own network traffic which means you can create rules that are compliant with security standards such as PCI-DSS or HIPAA, this can be particularly useful for organizations that are subject to regulatory requirements.
4. **Advanced threat protection**: Network Firewall can also be integrated with AWS security services like Amazon GuardDuty and Amazon Inspector, to provide advanced threat protection for your network and infrastructure.
5. **Multi-tier architecture**: Network Firewall can also support a multi-tier architecture, where you can have multiple layers of firewall, with each layer providing a different level of security.

These are just a few examples of the many use cases for AWS Network Firewall. The service's flexibility and wide range of features make it a valuable tool for securing network traffic in any environment.