Service Name

AWS Network Firewall

Service Overview

AWS Network Firewall is a stateful, managed network firewall and intrusion detection and prevention service for Amazon Virtual Private Cloud (VPC). It filters traffic at the perimeter of VPCs, including traffic to and from internet gateways, NAT gateways, or over VPN or Direct Connect connections. The service uses the open source intrusion prevention system Suricata for stateful inspection and supports Suricata-compatible rules. Network Firewall enables organizations to monitor and protect VPC traffic through deep packet inspection, domain filtering, custom rule definitions, and protocol detection capabilities.

Key Use Cases

- VPC perimeter security: Filter network traffic at VPC boundaries to protect against external threats and control access to internet resources
- Compliance and regulatory requirements: Meet security standards through centralized firewall management and detailed traffic monitoring and logging
- Advanced threat protection: Block malicious URLs, command-and-control channels, and other threat vectors using intrusion prevention system capabilities
- Domain-based filtering: Control outbound traffic by allowing only known good domains or blocking known malicious domains
- Deep packet inspection: Perform comprehensive analysis of network traffic entering or leaving VPCs for security threats
- Multi-account security governance: Centrally manage firewall policies across multiple AWS accounts using AWS Firewall Manager integration

Features

- **Stateful and Stateless Inspection**: Supports both stateful rules (context-aware traffic flow inspection) and stateless rules (individual packet inspection) for comprehensive traffic filtering
- **Suricata-based IPS**: Uses open source Suricata intrusion prevention system for advanced threat detection and prevention with compatible rule support
- **TLS Inspection**: Advanced inspection capability that decrypts and inspects SSL/TLS encrypted traffic for enhanced security analysis
- **Active Threat Defense**: Managed rule groups providing real-time threat intelligence and protection against emerging threats
- **Domain and URL Filtering**: Web filtering capabilities to control access to specific domains and URLs, including automated domain list generation

- **Flow Management**: Flow capture and flush operations for network visibility, troubleshooting, and security policy enforcement
- **Central Management**: Integration with AWS Firewall Manager for centralized configuration and management across multiple AWS accounts
- **Multi-VPC Support**: Support for multiple VPC endpoints and associations for scalable network security architecture
- **Transit Gateway Integration**: Native integration with AWS Transit Gateway for simplified centralized network security deployment

Value Proposition

AWS Network Firewall provides a fully managed solution that eliminates the need to deploy, maintain, or patch network security infrastructure. Unlike self-managed solutions, it offers automatic scaling up to 100 Gbps throughput per Availability Zone with built-in high availability:

- The service integrates natively with AWS services like Transit Gateway, VPC, and Firewall Manager, providing seamless deployment and centralized management
- Cost-effective NAT Gateway discounts are available when used in service chains
- The managed Suricata-based engine provides enterprise-grade threat protection with continuously updated threat intelligence, while flexible rule management supports both custom and AWS Marketplace partner rule groups

Service Integration

Network Firewall integrates deeply with core AWS networking and security services. It works natively with Amazon VPC for subnet-level protection and route table management:

- Transit Gateway integration enables centralized network security across multi-VPC architectures without dedicated inspection VPCs
- AWS Firewall Manager provides centralized policy management across multiple accounts and Organizations
- The service integrates with NAT Gateways for cost-optimized outbound traffic inspection, and supports VPC endpoint associations for multi-VPC deployments
- Additional integrations include Route 53 Resolver DNS Firewall, AWS PrivateLink, CloudWatch for monitoring and logging, CloudTrail for audit trails, and AWS Certificate Manager for TLS inspection certificate management

Onboarding and Offboarding

Getting started requires having a VPC with internet gateway and designated firewall subnets in each Availability Zone. The process involves creating stateless and stateful rule groups that define traffic filtering behavior, creating a firewall policy that combines rule groups and specifies default actions, creating the firewall resource and associating it with

the VPC and subnets, and updating VPC route tables to direct traffic through firewall endpoints:

- The AWS Management Console provides step-by-step guidance, while CloudFormation templates and APIs enable automated deployments
- Prerequisites include proper IAM permissions and network architecture planning for firewall subnet placement and routing configurations

Getting Started Guide: https://docs.aws.amazon.com/network-firewall/latest/developerguide/getting-started.html

Data Removal

Offboarding involves reversing VPC route table changes to remove traffic routing through firewall endpoints, deleting VPC endpoint associations if multiple VPCs are protected, and systematically removing Network Firewall resources including the firewall, firewall policy, and rule groups. All firewall logs stored in CloudWatch Logs and S3 must be manually deleted based on organizational data retention policies. Shared resources managed through AWS Firewall Manager require coordination across accounts for proper cleanup and policy removal.

Backup/Restore and Disaster Recovery

AWS Network Firewall is a managed service where AWS handles infrastructure backup and recovery. Customer-configured resources like firewall policies, rule groups, and configurations can be backed up using Infrastructure as Code approaches with CloudFormation templates or Terraform. The service provides automatic multi-Availability Zone deployment for high availability, but does not integrate with traditional backup services like AWS Backup since it manages infrastructure-level resources rather than data that requires backup and restoration.

Backup Capabilities

Network Firewall does not have traditional backup capabilities or integration with AWS Backup since it manages infrastructure resources rather than data. Configuration backup is achieved through Infrastructure as Code practices, exporting resource configurations to CloudFormation templates, or using AWS Config for configuration history tracking. AWS manages the underlying infrastructure backup and recovery automatically, while customers are responsible for maintaining configuration templates and policies for disaster recovery scenarios.

Disaster Recovery

Network Firewall does not directly integrate with AWS Elastic Disaster Recovery as it is an infrastructure service rather than a data service. Disaster recovery is achieved through the service's built-in multi-Availability Zone deployment for high availability and Infrastructure as Code approaches for cross-region deployment. The managed nature of the service

means AWS handles underlying infrastructure recovery, while customers implement disaster recovery through automated deployment scripts, CloudFormation templates, and multi-region architecture patterns.

Recovery Objectives

Network Firewall supports aggressive RTO and RPO objectives through its multi-Availability Zone deployment architecture and Infrastructure as Code deployment capabilities. High availability across multiple AZs provides near-zero RTO for availability zone failures. Cross-region deployment using CloudFormation or Terraform can achieve RTO of minutes to hours depending on automation sophistication. RPO is effectively zero for configuration data when using Infrastructure as Code practices, as all configurations can be version-controlled and rapidly redeployed in disaster scenarios.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/network-firewall/latest/developerguide/quotas.html

FAQ: https://aws.amazon.com/network-firewall/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/network-firewall/latest/developerguide/what-is-aws-network-firewall.html

User Guide: https://docs.aws.amazon.com/network-firewall/latest/developerguide/

API Reference: https://docs.aws.amazon.com/network-firewall/latest/APIReference/

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/network-firewall/pricing/

Cost Optimization

Network Firewall offers several unique cost optimization opportunities. NAT Gateway hourly and data processing charges are waived when placed next to Network Firewall in the same region and Availability Zone service chain:

- Secondary VPC endpoints have reduced hourly rates compared to primary endpoints
- Advanced Inspection and Active Threat Defense features have separate pricing tiers, allowing customers to enable only required capabilities

- Flexible cost allocation through Transit Gateway attachments enables distributing inspection costs across AWS accounts based on actual usage rather than consolidating expenses in the firewall owner account

Savings Considerations

Primary cost savings come from the NAT Gateway discount when architecting service chains properly in the same AZ. Centralized deployment models reduce the need for multiple firewall instances across VPCs while maintaining security:

- Using Infrastructure as Code reduces operational overhead and management costs
- The managed service eliminates costs associated with self-managed firewall infrastructure, including patching, maintenance, and scaling operations
- Combining with VPC Lattice for non-critical HTTP/HTTPS traffic can significantly reduce Network Firewall processing costs while maintaining security
- Regional deployment optimization and right-sizing firewall endpoints based on actual throughput requirements prevent over-provisioning costs