Service Name

AWS Firewall Manager

Service Overview

AWS Firewall Manager is a security management service that simplifies administration and maintenance tasks across multiple accounts and resources for various protections, including AWS WAF, AWS Shield Advanced, Amazon VPC security groups and network ACLs, AWS Network Firewall, and Amazon Route 53 Resolver DNS Firewall. The service enables centralized configuration and management of firewall rules and protections across accounts and applications within an AWS Organizations structure. Users set up protections once, and Firewall Manager automatically applies them across all accounts and resources, including newly added ones, ensuring consistent security policy enforcement organization-wide.

Key Use Cases

- Centralized security policy management: Deploy consistent firewall rules and protections across multiple AWS accounts in an organization from a single management point
- Compliance enforcement: Automatically monitor for new resources and ensure they comply with mandatory security policies from day one of deployment
- Multi-layer protection orchestration: Coordinate AWS WAF, Shield Advanced, Network Firewall, VPC security groups, and DNS Firewall rules across organizational boundaries
- Security audit and remediation: Audit existing security configurations for over-permissive rules and automatically remediate non-compliant resources

Features

- **Multi-service protection management**: Centrally manages AWS WAF, AWS Shield Advanced, VPC security groups, Network ACLs, AWS Network Firewall, and Route 53 Resolver DNS Firewall protections
- **Cross-account policy enforcement**: Applies security policies automatically across multiple AWS accounts within an AWS Organizations structure
- **Automatic resource protection**: Automatically applies protections to new resources as they are created, ensuring continuous compliance
- **Hierarchical rule management**: Supports hierarchical rule enforcement allowing common organizational rules while permitting account-specific customizations
- **Compliance dashboard**: Provides centralized visibility into compliance status with notifications for non-compliant resources and threat monitoring

- **Third-party firewall integration**: Supports integration with third-party firewall solutions from AWS Marketplace including Palo Alto Networks and Fortigate

Value Proposition

AWS Firewall Manager provides unparalleled centralized security management for organizations with multiple AWS accounts, eliminating the complexity of manually configuring security policies across accounts. The service automatically ensures consistent security posture as organizations scale, reducing administrative overhead and human error:

- Key advantages include automatic policy application to new resources, hierarchical rule management that balances central control with local flexibility, and comprehensive compliance monitoring
- Organizations benefit from reduced security management complexity, improved security consistency, and the ability to leverage managed rules from AWS Marketplace while maintaining centralized oversight of their entire AWS security infrastructure

Service Integration

AWS Firewall Manager deeply integrates with AWS Organizations as a prerequisite, requiring organizational structure for multi-account management. Core service integrations include AWS WAF for web application protection, AWS Shield Advanced for DDoS protection, AWS Network Firewall for network-level filtering, Amazon VPC for security groups and network ACLs, and Amazon Route 53 Resolver for DNS filtering:

- The service requires AWS Config for continuous resource monitoring and compliance tracking, and integrates with AWS Security Hub for centralized security findings management
- Additional integrations include AWS Resource Access Manager for cross-account resource sharing, AWS CloudTrail for API logging, and AWS Marketplace for third-party security solutions

Onboarding and Offboarding

Getting started with AWS Firewall Manager requires completing several prerequisite steps in sequence. First, organizations must join AWS Organizations and enable all features:

- Next, they must designate a Firewall Manager administrator account from either the management account or a delegated member account
- AWS Config must be enabled across all member accounts for continuous resource monitoring
- Optionally, customers can enable AWS Resource Access Manager for Network Firewall and DNS Firewall resource sharing

- Once prerequisites are complete, customers create their first security policy by selecting the protection type (WAF, Shield, Network Firewall, etc.), configuring rules and protections, defining policy scope including accounts and resources, and choosing between automatic or manual remediation modes

Getting Started Guide: https://docs.aws.amazon.com/waf/latest/developerguide/fms-prereq.html

Data Removal

Offboarding from AWS Firewall Manager involves deleting policies using the DeletePolicy API with the DeleteAllPolicyResources parameter set to true for complete cleanup. This removes rule groups, disassociates web ACLs from resources, deletes Firewall Manager-created security groups, and cleans up Network Firewall resources. For third-party firewall integrations, the DisassociateThirdPartyFirewall API removes all associated firewalls and tenant configurations. Customer data is removed when policies are deleted, though underlying service resources may require separate cleanup actions depending on the protection type.

Backup/Restore and Disaster Recovery

AWS Firewall Manager does not provide direct backup and disaster recovery capabilities as it is a management service for security policies rather than a data storage service. The service maintains policy configurations and compliance state information, but does not offer specific backup features. Disaster recovery relies on the underlying AWS infrastructure resilience, and policies can be recreated using infrastructure as code practices or by reconfiguring through the console or APIs.

Backup Capabilities

AWS Firewall Manager does not have built-in backup capabilities and does not integrate directly with AWS Backup service. As a security policy management service, it focuses on configuration management rather than data protection. Policy configurations should be backed up through infrastructure as code practices, version control systems, or by maintaining documented configurations that can be recreated.

Disaster Recovery

AWS Firewall Manager does not directly integrate with AWS Elastic Disaster Recovery as it is a management service rather than a compute or data service. Disaster recovery for Firewall Manager relies on AWS infrastructure resilience and the ability to recreate policies in alternate regions. The service operates regionally, so organizations must create separate policies in each region for comprehensive coverage.

Recovery Objectives

AWS Firewall Manager supports recovery objectives by enabling rapid policy recreation and deployment across multiple accounts and regions. While not directly providing RPO/RTO capabilities, the service can quickly restore security postures by reapplying policies to resources. Organizations can achieve low RTO by maintaining policy configurations in infrastructure as code and leveraging the service's automatic policy application capabilities for rapid security restoration.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/waf/latest/developerguide/fms-limits.html

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

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html

User Guide: https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html

API Reference: https://docs.aws.amazon.com/fms/2018-01-01/APIReference/Welcome.html

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/firewall-manager/pricing/

Cost Optimization

AWS Firewall Manager pricing is based on policy types and regional deployment, with charges primarily for underlying services rather than the management layer itself. Key cost optimization strategies include leveraging the fact that AWS Shield Advanced customers receive Firewall Manager WAF policies at no additional charge:

- Organizations can optimize costs by carefully scoping policies to avoid unnecessary resource inclusion and utilizing manual remediation mode during testing phases
- Consolidating similar protection requirements into fewer policies and leveraging managed rules from AWS Marketplace can provide cost-effective security coverage
- Understanding that charges are primarily from underlying services allows for targeted optimization of WAF, Network Firewall, and Config usage

Savings Considerations

Primary cost savings come from avoiding duplicate security configurations across multiple accounts and reducing administrative overhead through centralized management. Organizations save on operational costs by eliminating manual security policy deployment and maintenance across accounts:

- The service enables bulk purchasing efficiencies for Shield Advanced subscriptions across organizational accounts
- Automated compliance monitoring reduces the need for manual security auditing resources
- By preventing security misconfigurations through consistent policy application, organizations avoid potential costs associated with security incidents
- Leveraging AWS Marketplace managed rules through Firewall Manager can provide economies of scale compared to developing custom security rules for each account separately