FORTINET

SOLUTION BRIEF

Secure Your Migration to AWS with a Cloud-Native Managed Firewall Service

Executive Summary

Most organizations now run more than half of their workloads on public clouds, leveraging the agility and scalability of the cloud to meet rapidly evolving business demands. However, as you move your workloads to the cloud, your network becomes more decentralized—which means the traditional methods used to secure your on-premises data centers are no longer enough. Ensuring consistent protection and visibility across distributed environments requires an enterprise-class network security solution with cloud-native benefits. Today's cloud-first companies are looking for simplified security operations integrated with native cloud service provider services to stop zero-day security threats while removing barriers to delivering essential business outcomes.

FortiGate Cloud-Native Firewall (FortiGate CNF) combines next-generation firewall capabilities with distinct cloud-based service advantages. FortiGate CNF is underpinned by FortiOS, our powerful security operating system designed to run consistently in any environment. This unique approach ensures a common network security experience across AWS cloud and on-premises environments. It also natively incorporates FortiGuard artificial intelligence (AI)-powered Security Services for real-time detection of and protection against malicious external and internal threats.

58% of 823 cybersecurity professionals polled say they will run more than 50% of their workloads on public clouds in the next 12–18 months.[1]

Securing AWS Deployments Can Be Very Challenging

One of the biggest challenges to operating cloud workloads is applying legacy network security operations—including configuration, provisioning, and firewall software maintenance—to the cloud. And the need to constantly scale the infrastructure and ensure availability as needs grow compounds those issues even further. Another challenge is multiple user accounts operating in diverse environments across AWS without consistent or adequate security protections.

Most organizations also require more than the basic security available by default on AWS. The AWS Network Firewall requires additional custom security packages to ensure proper protection. But many companies don't have the security and cloud expertise or resources needed to build and maintain them.

Finally, organizations want solutions that integrate into cloud workflows to avoid the runaway costs typically associated with cloud usage.

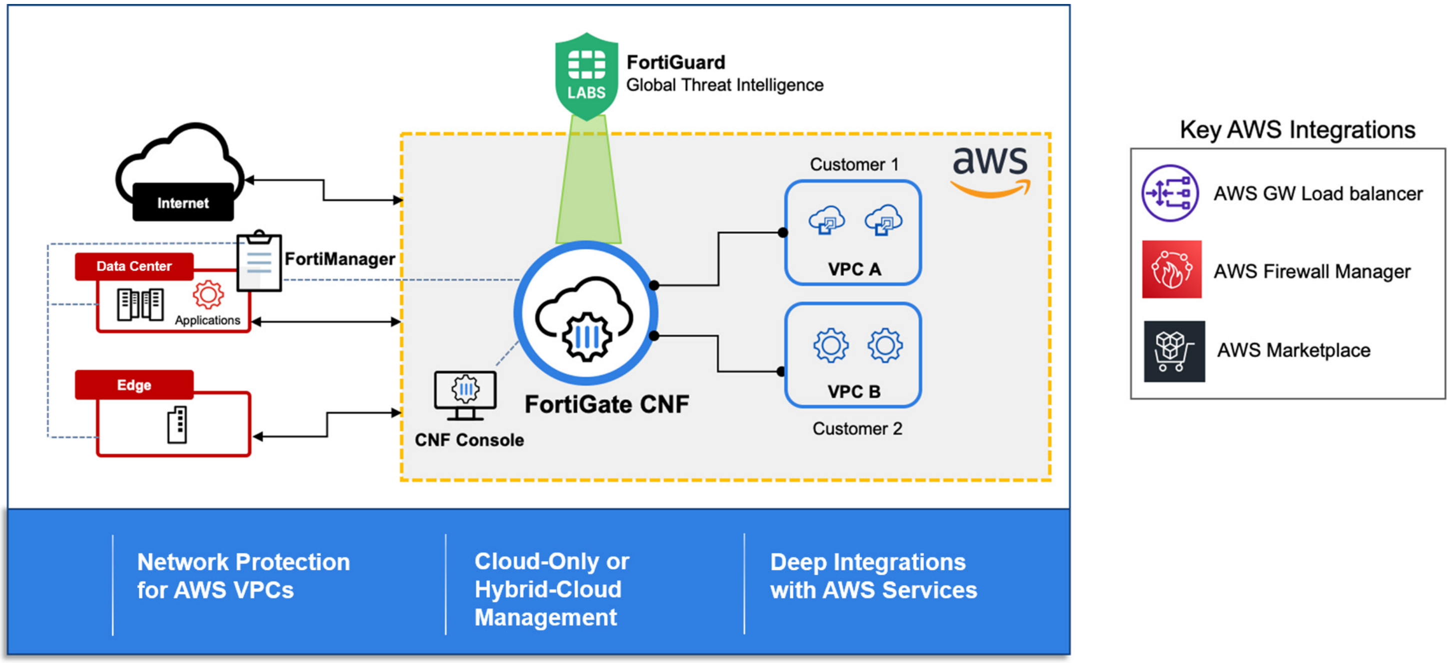
FortiGate CNF Ensures Consistent Protections Across Your AWS Environments

FortiGate Cloud-Native Firewall is a managed firewall service that removes complexity while improving security efficacy and supporting consistent security policies across different AWS environments. With no infrastructure to manage, organizations can focus on their business operations on the cloud, easily deploying effective security policies to protect their business-critical applications and data.

FortiGate CNF is designed for three critical use cases:

- Outbound traffic inspection: Content inspection of outgoing traffic from AWS workloads to the internet
- Inbound traffic protection: Deep visibility into incoming traffic and advanced security measures to protect AWS workloads
- East-west traffic filtering: Inspection and control of traffic between AWS VPCs and preventing the lateral spread of threats

This CNF service delivers seamless scalability, implicit resiliency, streamlined workflows, and flexible consumption through deep cloud-native integrations with native AWS services like AWS Gateway Load balancer, AWS Firewall Manager, and AWS Marketplace. Through this service, Fortinet and AWS bring together the best of both worlds—deep security expertise and leading-edge cloud technology—in a simple-to-manage and easy-to-consume service.



FortiGate CNF Enterprise-Grade Protections

Cloud-native integrations: FortiGate CNF offers the robust inspection capabilities of a next-generation firewall. This includes support for security policies and deep visibility into the application layer—combined with advanced AI-powered detection and comprehensive protection, including geo-IP blocking, advanced filtering, threat protection, etc. It also supports metadata-based policies and dynamic objects to abstract away network dependencies and protect elastic workloads with changing IP addresses.

It simplifies security delivery to deliver zero operations overhead. Unlike other solutions, FortiGate CNF requires just one CNF instance with an appropriate policy set to secure an entire AWS region, including multiple accounts, sub-nets, VPCs, and availability zones.

Flexible management: The FortiGate CNF console provides a lightweight user interface and intuitive wizards to easily create, deploy, and manage security policies for AWS environments. For more sophisticated enterprise IT cases, a centralized management tool like FortiManager can define, deploy, and manage advanced security policies across multiple deployments and hybrid environments.

Optimal pricing: By aggregating security across a region into a single CNF instance, enterprises can avoid the extra costs entailed by other vendor offerings that charge by cloud networks or availability zones. FortiGate CNF also offers competitive hourly and linear traffic inspection costs. The service also utilizes AWS Graviton instances to deliver even better price performance.

Better Protection Everywhere

FortiGate CNF reduces the mean time to identify and remediate non-compliance issues. Its deeper traffic inspection reduces risks from attacks on AWS workloads caused by web-based threats, vulnerability exploits, and other external and internal threat vectors.

Integration with the AWS Gateway Load Balancer helps network security teams move at the speed and scale of applications teams. It eliminates do-it-yourself automation and easily secures Amazon VPC environments—while improving high availability and scale. And integration with the AWS Firewall Manager streamlines security workflows and automates security rollout, saving time and increasing efficiency.

The centralized FortiManager management solution allows enterprises to apply security policies consistently across hybrid environments—on-premises and on AWS. Complexity in securing elastic workloads, where network address–based policies won't work, is reduced using its dynamic object policies. Cloud-first enterprises can also leverage the lightweight user interface and intuitive wizards in the FortiGate CNF console to easily create, deploy, and manage security policies for their AWS environment.

Organizations that deploy FortiGate CNF also save on infrastructure costs as there is no security software infrastructure to build, deploy, or operate. They also save on training and resourcing costs otherwise necessary to deliver DIY security on AWS.

FortiGate CNF delivers the following benefits:

- Comprehensive network protection
- Streamlined cloud workflows
- Consistent hybrid-cloud security management
- Optimized TCO

The public cloud Infrastructure-as-a-Service (IaaS) market is expected to reach $225 billion by 2025. The size of cloud security—at nearly $20 billion already in 2022—underscores the importance of security to organizations in various phases of their cloud journey.[2]

Comprehensive Security for AWS Begins with FortiGate Cloud-Native Firewall

With today's C-suite focused on the business value of cloud adoption, cloud security is now a business imperative. They need network security options in the cloud that offer enterprise-grade security, simplicity, flexibility, and predictable costs. And increasingly, they need those services to span their hybrid network environments. FortiGate Cloud-Native Firewall delivers on these needs, providing advanced network protection at any scale. With FortiGate CNF, you can maintain a robust security posture and accelerate your cloud journey on AWS without compromising security and compliance.

[1] "Cloud Security Report," Cybersecurity Insiders, accessed November 23, 2022.

[2] Ibid.