

SOLUTION BRIEF

FortiGate VM and Arm Offer High-Performance Security

A scalable, high-performance, and cost-effective security solution

Executive Summary

Fortinet and Arm have partnered to provide a fast, effective security solution for workloads on Amazon Web Services (AWS). Running FortiGate VM next-generation firewalls (NGFWs) on AWS Graviton3-based EC2 instances ensures the best possible experience for end-users, combining performance, cost-effectiveness, agility, and ease of use.

The Challenges

The rapidly increasing pace of digital transformation has driven an increasing number of organizations to move workloads to the cloud in pursuit of greater performance and scalability. However, great potential also carries risk, and the exponential growth of cloud computing makes maintaining a secure environment an imperative. The challenge is protecting your cloud workloads without adversely impacting performance and agility that may hinder your organization's innovation and growth.

Joint Solution

Using FortiGate VM NGFW on AWS Graviton3 delivers a high-performance, agile, cost-effective, and advanced security solution.

AWS Graviton3, the latest generation of Graviton processors for AWS, is an Arm Neoverse 64 core, 55 billion transistor processor designed specifically for high performance workloads on AWS.

FortiGate VM NGFWs provide advanced threat protection and deep visibility across clouds and data centers. They delivers artificial intelligence (AI) -powered threat intelligence, behavioral analysis, and machine learning algorithms to detect emerging threats in real-time. FortiGate VM NGFWs are cloud- and platform-agnostic, allowing you to deploy them in any cloud or virtualized data center, or on-premises. They also provide secure networking with integrated features like software-defined wide area networking (SD-WAN), zero trust enforcement, cloud access security broker, and data loss prevention. FortiGate VMs are an essential component for building your hybrid mesh firewall infrastructure, enabling you to protect applications no matter where they are deployed.

Together, FortiGate VM NGFWs and AWS Graviton3 processors deliver an industry-leading security solution that enables organizations to deliver high-performance secure connectivity, network segmentation, and application security for hybrid-cloud-based deployments. The solution also ensures

Solution Components

- Fortinet: FortiGate VM NGFW
- Arm Neoverse-powered AWS Graviton3 processor

Solution Benefits

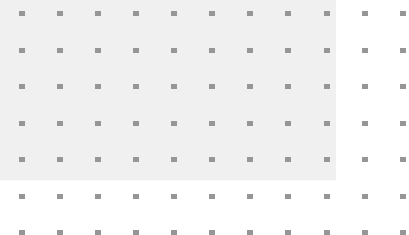
- High Performance: Secure connection to your workloads without performance bottlenecks
- Scalable and agile: Seamless, rapid scaling
- Cost-effective: Flexible consumption models

FortiGate VM running on the AWS Graviton3 processors registers:

176% improved NGFW throughput

Up to 147% improved IPsec throughput

*when compared with a C6in IceLake instance.



centralized, consistent security policy enforcement and application-centric, resilient connectivity through a high-performance virtual private network (VPN) or SD-WAN architectures.

Further, integration with Gateway Load Balancer removes the need for do-it-yourself automation and helps secure your Amazon Virtual Private Cloud (VPC) environments while improving high availability and scaling. With both AWS Graviton3 and FortiGate VM NGFWs tightly integrating with AWS services, auto-scaling and automation on the AWS Cloud are that much easier.

Solution Components



AWS Graviton3 Processor

Arm Neoverse technology gives cloud providers such as AWS, and software developers, the freedom to optimize technology for cloud and edge workloads to improve application performance, lower energy consumption, and reduce total cost of ownership.

Powered by Arm Neoverse, AWS Graviton3 processors provide up to 25% better compute performance, up to 2x higher floating-point performance, and up to 2x faster cryptographic workload performance compared to AWS Graviton2 processors. Additionally, Graviton3 also uses up to 60% less energy for the same performance as comparable EC2 instances, to deliver a sustainable and lower carbon footprint for cloud workloads.



Fortinet FortiGate VM NGFW

FortiGate VM NGFW is at the center of the Fortinet Security Fabric, which integrates a broad range of security tools and services, all supported by the latest AI-driven threat intelligence from FortiGuard Labs. FortiGate VM NGFW, supported by FortiSandBox and FortiGuard Labs delivers protection against advanced zero-day attacks while making it easy to manage security policies wherever your compute occurs.

Joint Use Cases

Use case #1: Building and securing high-traffic cloud-native applications. FortiGate VM NGFW on Graviton3 is ideal for securing applications that generate high traffic volumes or that might need to burst to support changing business needs. The Graviton3's superior performance, especially with cryptographic workloads, makes it ideal for security processing.

Use case #2: Migrating workloads to the cloud and securing them without introducing lag or delay. Cloud computing can increase agility while reducing time to market. However, it can also introduce lag time and hurt application performance. Graviton3 improves performance and helps ensure that migrated applications perform as they should.

Use case #3: Extending security infrastructure to the cloud with hybrid mesh firewalls. FortiGate VM NGFW running on AWS Graviton3 processors enhances these hybrid mesh firewalls with the ability to secure high performance workloads without spinning up additional instances.

About Arm

Arm technology is building the future of computing. The energy-efficient processor designs and software platforms have enabled advanced computing in more than 250 billion chips. Arm technologies securely power products from the sensor to the smartphone and the supercomputer. Together with 1,000+ technology partners, Arm is enabling AI to work everywhere, and in cybersecurity, Arm is delivering the foundation for trust in the digital world – from chip to cloud. The future is being built on Arm.