FORTINET

Security Considerations for Your AWS Cloud Migration

Cross security off your list with Fortinet's Firewall-as-a-Service

Table of Contents

Digital Transformation Presents Cloud Security Challenges

Global events of the last few years have forced organizations to emphasize scalability, agility, and resiliency as key elements of their digital transformation initiatives. At this point, many companies have migrated some portion of workloads to the cloud to achieve these goals.

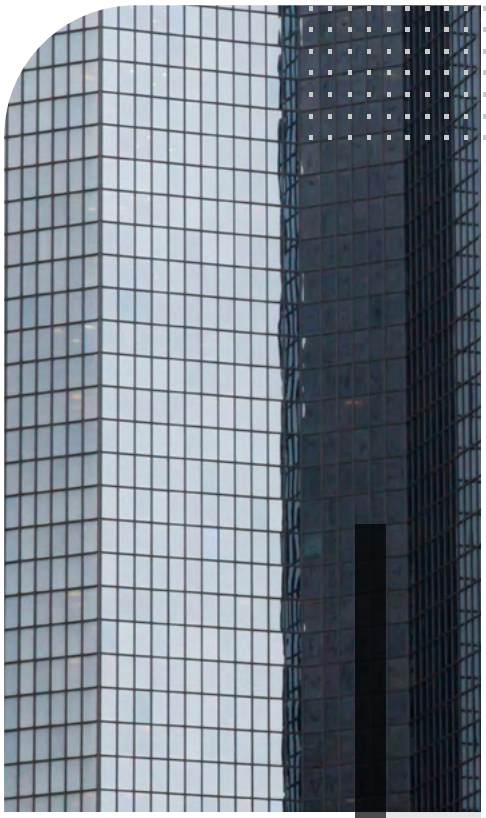
Illustrating this shift is recent research by the Enterprise Strategy Group (ESG), which found that 55 percent of organizations report their application workloads run on cloud Infrastructure-as-a-Service (IaaS) today.[1] That number is projected to increase to 62 percent by the end of 2024.[1] Not only are workloads migrating to cloud infrastructure, but new applications are being natively built on the cloud. Almost half of all organizations follow a cloud-first policy in which new applications are deployed on public cloud services absent a compelling case for on premises.[1]

While digital transformation continues to accelerate cloud adoption, it's evident that security teams are struggling to keep pace, as 88 percent of respondents reported they face challenges securing their IaaS environments.[2]

Some of these challenges might feel familiar to your organization:

- An increase in the threat landscape
- An increase in the amount of IaaS usage at your organization
- Lack of skilled security personnel and skills
- Ineffective security tools

Coupling these difficulties with the fact that the cloud can require fundamentally different security requirements than on premises, it's easy to see why most organizations feel uncertain about their cloud security presence.



1. Enterprise Strategy Group, "Complete Survey Results, 2023 Technology Spending Intentions Survey", November 2022
2. Enterprise Strategy Group, "Complete Survey Results, Network Security Trends in Hybrid Cloud Environments", December 2021

The Reality of Hybrid and Multi-Cloud Security

Digital transformation doesn't mean that organizations are moving everything to the cloud. Only 12 percent of organizations plan to shift everything to the cloud.[3] However, most organizations plan to modernize their data centers and invest in a cloud-like experience on premises. Almost half of all businesses are incorporating this hybrid model today, with another 27 percent planning to over the next 24 months.[4]

When it comes to securing hybrid deployments, a key challenge is the lack of visibility and control, making it tough to identify and respond to security concerns. For multi-cloud deployments, this issue compounds with challenges in maintaining consistent security policies across their environments. Ultimately, this can result in overwhelming complexity, especially for organizations that might lack enough skilled security personnel.

When faced with securing cloud deployments, organizations might first turn to the network security tools offered by their cloud service providers (CSP). This is especially true for organizations that have shifted some security responsibilities to developers. Generally, these offer simple scalability and can be easy to set up.

Almost **50%** of all businesses are incorporating a hybrid model today, with another **27%** planning to over the next 24 months.[4]

3. Enterprise Strategy Group, "Complete Survey Results, Distributed Cloud Series: Application Infrastructure Modernization Trends", March 2022
4. Enterprise Strategy Group, "Complete Survey Results, Network Security Trends in Hybrid Cloud Environments", December 2021

On the other hand, when faced with the reality that most organizations have or will pursue a hybrid or multi-cloud approach, CSP firewalls run into three limitations:

1. **Limited security:** CSP firewalls operate at Layer 4, with rules based on source and destination IP addresses, ports, and protocols. Organizations familiar with the advanced threat protection offered by physical or virtualized next-generation firewalls (NGFW) may be surprised to find that CSP firewalls often lack intrusion prevention systems (IPS), sandboxing, or advanced malware detection.
2. **Single cloud focus:** CSP firewalls provide control over their cloud environment and do not secure on-premises or multi-cloud deployments. This may be less of an issue for organizations that have standardized on a single cloud provider or have a limited on-premises footprint. But for other organizations, this can contribute to tool sprawl and lead to additional complexity.
3. **Cost:** Pricing models can be complex and expensive. Users often must pay for one or more firewall instances for every virtual cloud network they operate. In addition, they are charged for the time the firewall instances are operational, as well as the amount of traffic processed by those firewall instances.

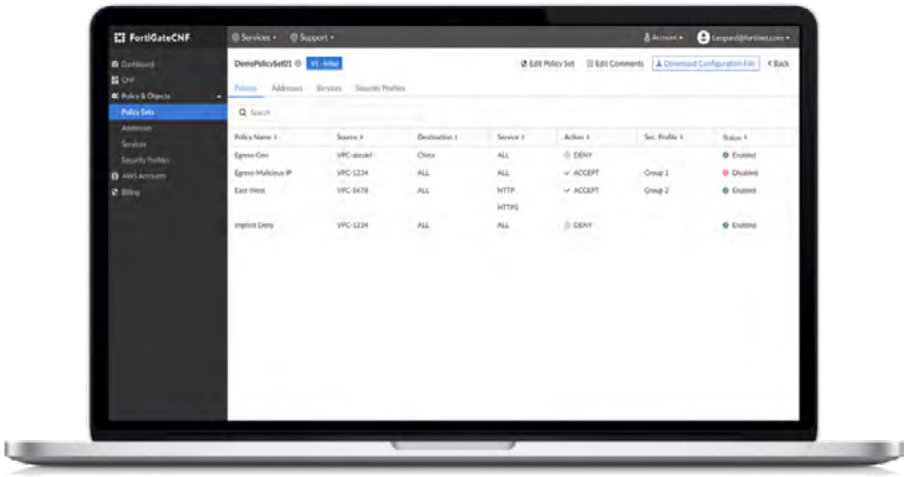
So how does an organization achieve peace-of-mind security across hybrid or multi-cloud networks while overcoming challenges like skill gaps and accelerated cloud adoption?

The answer lies with advanced firewalls that are built from the ground up to natively integrate into the cloud, offering speed, simplicity, and scale.

Mitigating Security Concerns with FortiGate Cloud-Native Firewall

Fortinet is best known for its FortiGate Next Generation Firewalls (NGFWs) that provide deep visibility and security in a variety of form factors, including containers, virtual firewalls, and appliances. Fortinet's new FortiGate Cloud-Native Firewall (CNF) service brings these award-winning NGFW capabilities to the cloud with native integrations with Amazon Web Services (AWS) for rapid deployment, on-demand scaling, and streamlined operations.

As a cloud-native firewall-as-a-service (FWaaS), FortiGate CNF has been designed to help organizations eliminate the burden of managing the underlying scalability and availability of a network security infrastructure on AWS. FortiGate CNF provides advanced network protection at any scale and an optimized cost without any infrastructure management on AWS.



Key benefits of FortiGate CNF

Advanced security

FortiGate CNF offers the same NGFW protection as existing FortiGate products. It provides Layer 7 protection and includes URL and DNS filtering, intrusion prevention, IP reputation, and botnet/command and control protection. The service is supported by FortiGuard Labs global threat intelligence, which leverages artificial intelligence (AI) and machine learning (ML), along with Fortinet's global threat visibility to help block advanced attacks.

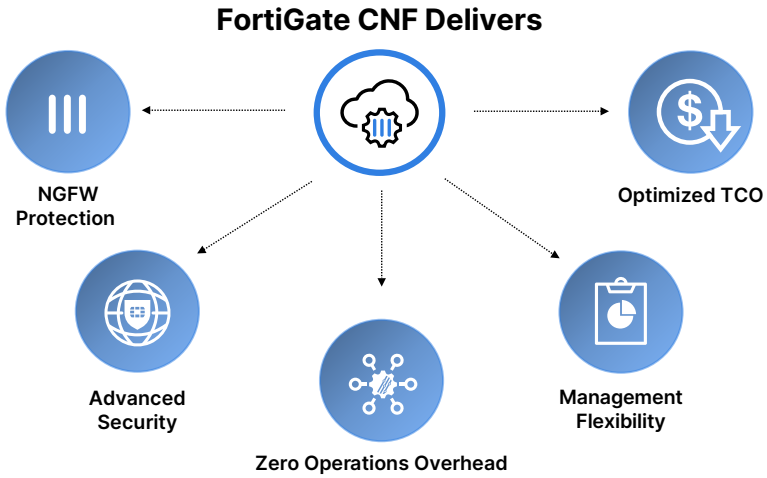
Ease of use

Delivery as Software-as-a-Service (SaaS) on AWS offloads the need for security teams to coordinate provisioning and update activities. Integrations with native AWS services deliver scalability and security across multiple AWS accounts.

Flexibility

FortiGate CNF helps organizations take charge of their security in three main ways:

1. Applicability for the three main cloud network security use cases by delivering outbound, inbound, and east-west traffic inspection.
2. Three management options are available. First, via the FortiGate CNF console for both service and policy management; second, through AWS Firewall Manager to automate service management with cloud workflows; and third, through FortiManager for consistent security policy management across on-premises and AWS environments.
3. Pricing is available in either annual or on-demand options. In the on-demand model, users pay only for the specific hours of operation and amount of traffic that is scanned by each inspection engine.

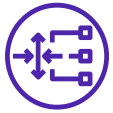


Accelerating a Secure Cloud Journey on AWS

FortiGate CNF integrations with AWS services allow security teams to function at DevSecOps speed and scale. Let's take a closer look at how FortiGate CNF can bring consistent security to your cloud environment.

Integration with Gateway Load Balancer eliminates the need to own deployment automation, provides high availability and fault tolerance, and offers on-demand scaling while securing your Amazon Virtual Private Cloud (Amazon VPC) environments. Integration with AWS Firewall Manager eases security management and automates security rollout. As mentioned earlier, security teams can opt to use the FortiGate CNF console for security policy management and use AWS Firewall Manager to automate service management with cloud workflows.

Gateway Load Balancer



For scaling, resiliency and availability

AWS Firewall Manager

For provisioning CNF and simplifying security policy management workflow

FortiGate CNF inspects and protects outbound, inbound, and east-west network traffic from workloads in Amazon VPCs and streamlines workflows to deliver robust protection.

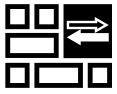
Outbound Traffic Inspection

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 Protection



Inspect and control traffic between AWS VPCs and prevent lateral spread of threats

In addition, FortiGate CNF is available on AWS Marketplace via on-demand or annual contracts to simplify procurement and consumption, while increasing security operations agility.

What about Virtualized Firewalls?

Fortinet has long offered virtual instances of its FortiGate NGFWs. A key difference is that FortiGate VM is deployed as IaaS on Amazon Elastic Cloud Compute (Amazon EC2) instances. As such, with FortiGate VM, it is up to the organization to handle the design, deployment, and management of that underlying IaaS infrastructure.

On the other hand, FortiGate VM can be tailored to fit unique deployments and VPC traffic flows. It can be deployed with common Infrastructure-as-Code (IaC) tools, such as AWS CloudFormation and Terraform, to resemble a cloud-native deployment experience. In addition to NGFW, FortiGate VM can also offer IPsec VPN and SD-WAN capabilities.

For organizations prioritizing speed and simplicity, however, the FortiGate CNF SaaS delivery model allows you to apply Fortinet's proven network security protection in minutes. Simply route traffic to FortiGate CNF endpoints and create security policies. Infrastructure, high availability, automatic updates, and scaling are handled by the FortiGate CNF service, thus simplifying your network security operations. Best of all, a single FortiGate CNF brings security to an entire AWS Region, delivering unmatched scalability to cloud security.

For comprehensive hybrid cloud network security capabilities and flexibility, FortiGate CNF can be managed by FortiManager. This provides a unified solution for organizations using either FortiGate hardware appliances on premises or those that are migrating security policies from FortiGate VM instances in the cloud. This allows for a seamless transition and the ability to utilize the latest security capabilities offered by FortiOS, the foundation of the Fortinet Security Fabric, converging and consolidating many security and networking technologies and use cases into a simplified, single policy and management framework, no matter the deployment method.

Security for the Future

Nearly all companies struggle with skills gaps and maintaining efficiency. Security teams across all company types also must support different use cases and stakeholders. Cybersecurity is now a business imperative with executive oversight. All these factors highlight the need for network security options in the cloud that offer enterprise-grade security, simplicity, and flexibility.

FortiGate CNF delivers on these needs, providing advanced network protection at any scale.

Discover new possibilities for cloud-native firewall protection today by checking out FortiGate CNF options in AWS Marketplace.

March 2023