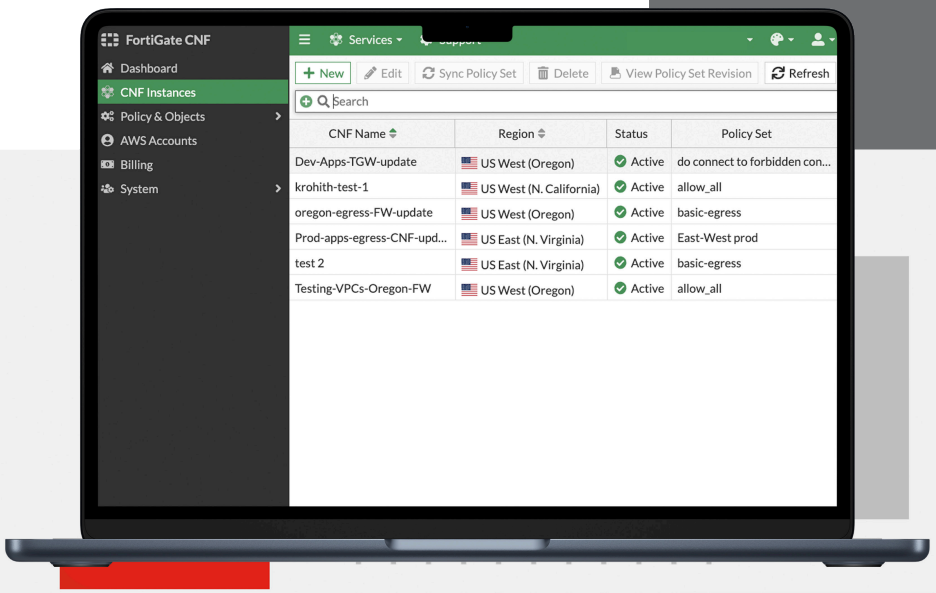
Data Sheet

FortiGate™ CNF Cloud-Native Firewall Service



Highlights

Enterprise-grade Protection: The solution features Geo-IP blocking, advanced filtering, and robust threat protection. It is fully equipped with all the advanced capabilities of the mature FortiOS next-generation firewall, offering comprehensive visibility and enhanced security

Streamlined Security Management: FortiGate CNF provides security for multiple AWS accounts, Azure subscriptions, and networks within a region, streamlining security management and a unified policy to all chosen resources. This approach eliminates the need for deploying and maintaining separate cloud firewalls

Lower Costs: As there is no need to build, deploy, and operate security software infrastructure, costs are reduced. You only pay for the security functionality that is actually used

High Performance with Simplicity

FortiGate Cloud-Native Firewall (CNF) is a SaaS delivered Next Generation Firewall service that simplifies cloud network security while implicitly providing availability and scalability. FortiGate CNF reduces the network security operations workload by eliminating the need to configure, provision, and maintain any firewall software infrastructure while allowing security teams to focus on security policy management. FortiGate CNF offers customers the flexibility to procure on demand or use annual contracts.

Introduction

Managed Cloud Network Security Service

FortiGate CNF (Cloud Network Firewall) is a managed cloud network security service designed to provide customers with next-generation firewall (NGFW) capabilities in a simplified and easy-to-use manner. The service is available for Amazon Web Services (AWS) Virtual Private Clouds (VPCs) and Azure (VNETs). To use CNF, customers simply need to select the cloud networks and resources they want to protect, attach them to a CNF instance they initiate, and define the security policy they want to enforce. CNF will take care of everything else, including managing the infrastructure, scaling, and patching code vulnerabilities.

Customers can define their security policies using a simple and intuitive policy language, which CNF enforces at the network level. The policies can be customized to meet specific needs, including blocking malicious IPs, creating geographical fences around cloud workloads, and enforcing east-west cloud network security using dynamic objects, which eliminates the need to change policies every time a workload moves.

CNF is a regional service, with each CNF instance running in a single region. This deployment makes it highly available and scalable, allowing customers to spin up test CNFs in one region and production CNFs in other regions, or spin up seasonal CNFs in specific regions as needed. The service is especially suitable for customers with highly variable and unpredictable usage and traffic patterns, as it allows them to focus on managing their security policies rather than the infrastructure and maintenance of their network security solution.

Overall, CNF provides customers with a simplified and easy-to-use network security solution that allows them to define, enforce, and manage their security policies effectively while eliminating the need to invest engineering resources in building their own solution.

Ideal Customer

FortiGate CNF is designed to meet the needs of two types of customers. The first type includes existing Fortinet customers who use FortiManager to manage their fleet of FortiGates on-premises and in the cloud. FortiGate CNF is an ideal solution for these customers, as it provides an easy-to-implement FortiOS NGFW solution that addresses cloud network security use cases that are more difficult to address with existing FortiGate VMs, such as outbound traffic. Moreover, these customers may require a service that manages the availability, scalability, and software updates for their network security for specific cloud workloads.

The second type of customer that CNF targets is those who require a Cloud SaaS network security solution that continuously evolves around two main use cases. Firstly, outbound traffic security, which includes blocking malicious IPs and creating geographical fences around cloud workloads, considering that most of their traffic is encrypted, rendering IPS less important. Secondly, east-west cloud network security, which utilizes dynamic objects, thereby eliminating the need to change policies every time a workload moves. Furthermore, these customers also understand that IPS is less critical since most of their traffic is encrypted.

Capabilities

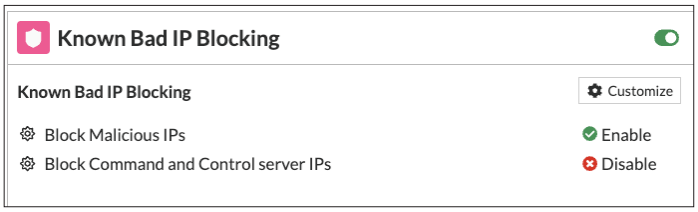
Egress Security

In today's highly connected world, egress traffic from cloud networks has become a major security concern for businesses. The increasing reliance on cloud technology has led to a rise in potential threats such as data exfiltration, malware propagation, botnet formation, and excessively high volumes of egress traffic. To address these risks, organizations need a solution that can effectively secure their cloud networks and ensure the protection of sensitive data.

FortiGate CNF provides a comprehensive egress cloud network security solution to mitigate these risks. The solution enforces a consistent security policy across multiple cloud accounts and networks, thereby reducing the likelihood of security incidents. With its robust security features, FortiGate CNF provides protection against data exfiltration, helps to prevent the spread of malware, stops the formation of botnets, and controls excessive egress traffic volumes.

Known Bad IP Filtering

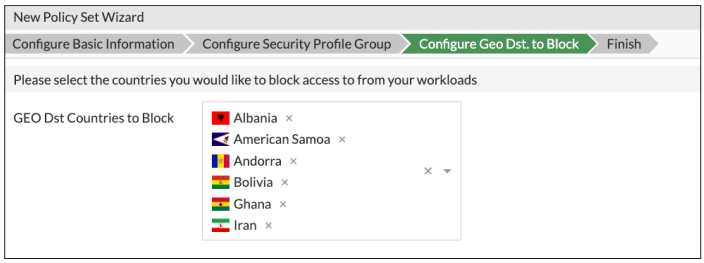
FortiGate CNF, powered by FortiGuard Labs IP Reputation Intelligence, provides an effective solution for protecting cloud-based workloads from accessing known bad IPs. This blocking includes both malicious IPs and known Command and Control servers. The solution makes it simple for organizations to restrict their workloads from accessing unwanted resources, thereby enhancing the security of their cloud networks. With its powerful IP reputation intelligence capabilities, FortiGate CNF ensures that cloud-based workloads remain protected from potential security threats, providing peace of mind for businesses relying on cloud technology.



Capabilities

Geo Fencing

FortiGate CNF offers a simple and effective solution for organizations looking to implement country-level security policies and stay compliant. With the intuitive Geo Policy wizard, implementing these policies is easy, even for organizations that are not experts in network security. The wizard allows for the specific definition of which countries can be accessed by cloud resources, ensuring that security policies are properly enforced.

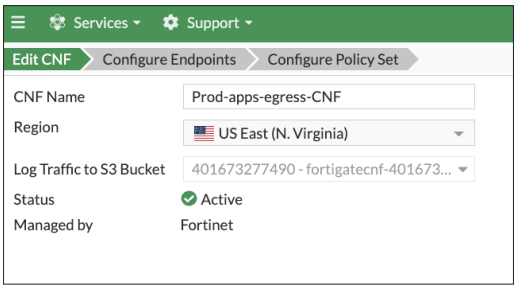


East West Security

For AWS, FortiGate CNF provides comprehensive protection for cloud-based workloads, including dynamic objects such as serverless resources, kubernetes resources, and auto-scaling groups by attaching to customer cloud transit networks and enforcing network security policies, it dynamically scales to meet changing security needs, ensuring capacity for even the most demanding scenarios. The solution integrates with customer transit networks for protection across cloud networks and into them.

Simplified Deployment

FortiGate CNF is quick and easy to set up. Simply subscribe from the AWS marketplace and follow the built-in setup wizard to deploy CNF instances in minutes. The solution comes with predefined policies and default security profiles, so customers can enjoy the security they need without the complexity of setting up other NGFW solutions. For more advanced security functionality, FortiManager unleashes the advanced security functionality from FortiOS in FortiGate CNF. With FortiGate CNF, getting up and running with cloud network security has never been easier.



Capabilities

Dynamic Security

FortiGate CNF allows customers to define security policies using intuitive objects like countries, FQDNs, and Cloud resource metadata attributes. This approach means that customers do not have to constantly update security policies every time their cloud workloads change networks or application resources are redeployed in a CI/CD pipeline. With the ability to define dynamic policies using custom cloud workload metadata, FQDN, and Geo objects, customers can ensure that policies are consistently enforced, no matter where the workloads reside or migrate.

Regulatory Compliance

FortiGate CNF can assist customers in meeting various regulatory compliance requirements, including GDPR, HIPAA, and PCI-DSS. For instance, the solution's ability to restrict access to known bad IPs, protect against data exfiltration and malware propagation, and enforce network security policies can help customers meet GDPR requirements related to data privacy and protection. Additionally, with features like these, FortiGate CNF can assist in meeting HIPAA requirements for the protection of sensitive patient information and PCI-DSS requirements for secure payment card processing and storage. However, it's important to note that the specific regulatory compliance requirements that FortiGate CNF can help meet will depend on the individual customer's needs and the subjective regulations.

FortiGuard Labs Services

FortiGate CNF is powered by FortiGuard Labs, which provides multiple security signatures and IP reputation information to help protect against various cyber threats. As a subscriber of FortiGate CNF, customers will automatically have access to the latest security updates and protections, ensuring their network security remains up-to-date and effective in mitigating potential threats.

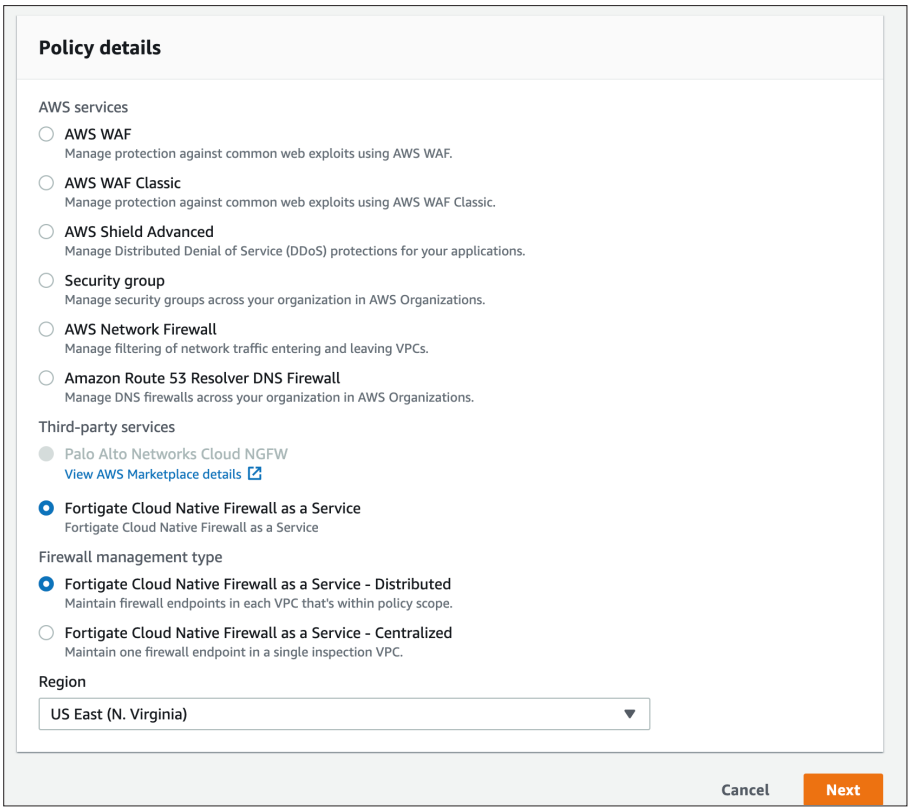
Security Processing Pricing Mechanism

The pricing for the data security processing performed by FortiGate CNF is calculated based on each security function. All traffic passing through the CNF instance is considered traffic processing, while separate charges apply for security functions such as intrusion prevention, URL filtering, and others that are matched by policies. This approach ensures that customers only pay for the security services they actually use and eliminates the need for pre-provisioning of any security capabilities.

Capabilities

AWS Firewall Manager Integration

FortiGate CNF attachment to protected VPCs and policy rollouts can be automated using the AWS Firewall Manager service (FMS). Customers who are using AWS FMS to automate security endpoint and security policy rollouts can utilize this service to extend the FortiGate CNF protection to more VPCs as well as deploy security policies to FortiGate CNF instances.



Fortinet FortiManager and FortiAnalyzer Integration

FortiGate CNF seamlessly integrates with the Fortinet Security Fabric, enabling customers to maintain their network security with the advanced tools and capabilities they are accustomed to. With FortiManager integration, customers can access the latest network security functionalities, including IPS, AV, SSL Man-in-the-middle termination, DLP, sandbox, and more services, all of which are available in FortiGate CNF, with the exception of VPN and NAT. FortiManager also allows for consistent policies across various FortiGate form factors and locations, as well as centralized policy migration across deployments. Furthermore, customers can leverage the benefits of FortiAnalyzer for analytics and network security operations by sending FortiGate CNF logs to their FortiAnalyzer..

Advanced Network Security

FortiGate CNF can be managed by FortiManager, providing a unified solution for customers using either FortiGate hardware appliances on premises or migrating security policies from FortiGate VM instances in the cloud. This solution allows for a seamless transition and the ability to utilize the latest security capabilities offered by FortiOS, no matter the deployment method.

Technical Features

Network Security

- NGFW
- IPS
- Bad IP Filtering
- DNS Filtering
- Geo IP Policies

Authentication

- Active and passive authentication
- Site publishing and SSO
- LDAP, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

Management and Reporting

- Web user interface
- FortiManager Integration
- AWS Firewall Manager Integration
- S3 Logging

Other

- Auto setup and default configuration settings
- Setup wizards for common network security
- Premium Enterprise Support

Deployment Option

- AWS Multi-VPC Egress Security
- AWS Transit-VPC E/W and Ingress
- Azure Load balancer ingress/egress
- Azure public IP ingress/egress

Cloud Integrations

- AWS Gateway Load Balancer
- AWS Firewall Manager
- AWS VPC
- AWS Marketplace
- AWS Meta Data Service
- AWS Route 53
- Azure GWLB
- Azure External Load Balancer
- Amazon Security Lake

FortiGuard Security Services

- Intrusion Prevention
- DNS Security
- Botnet Protection
- Sandbox and AV
- Geo IP and IP Reputation
- File upload scanning with AV and sandbox

Security Processing Credits

- 1GB of Traffic Processing = 1 Credit
- 1GB or URL Filtering = 1 Credit
- 1GB of IPS Processing = 1 Credit
- 1GB of Cloud/On Prem Sandbox = 4 Credits
- 1 Hour of running CNF Instance = 96 Credits

FortiOS Everywhere

Available in

Appliance

Virtual

SaaS

Cloud

Container

FortiOS, Fortinet's Advanced Operating System

FortiOS powers FortiGate CNF and enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks.

Ordering Information

FortiGate CNF is available for purchase on the Amazon Web Services marketplace as a PAYG subscription or an annual contract. The following lists marketplace pricing.

Units	Price
CNF Instances per hour including support	$3.00 / unit
1GB Traffic Processing	$0.031 / unit
1GB Advanced Security Processing	$0.031 / unit
One Million FortiGate CNF Consumption Credits	$30,000 / year

* Not available in AWS GovCloud or AWS China.

Supported AWS Regions

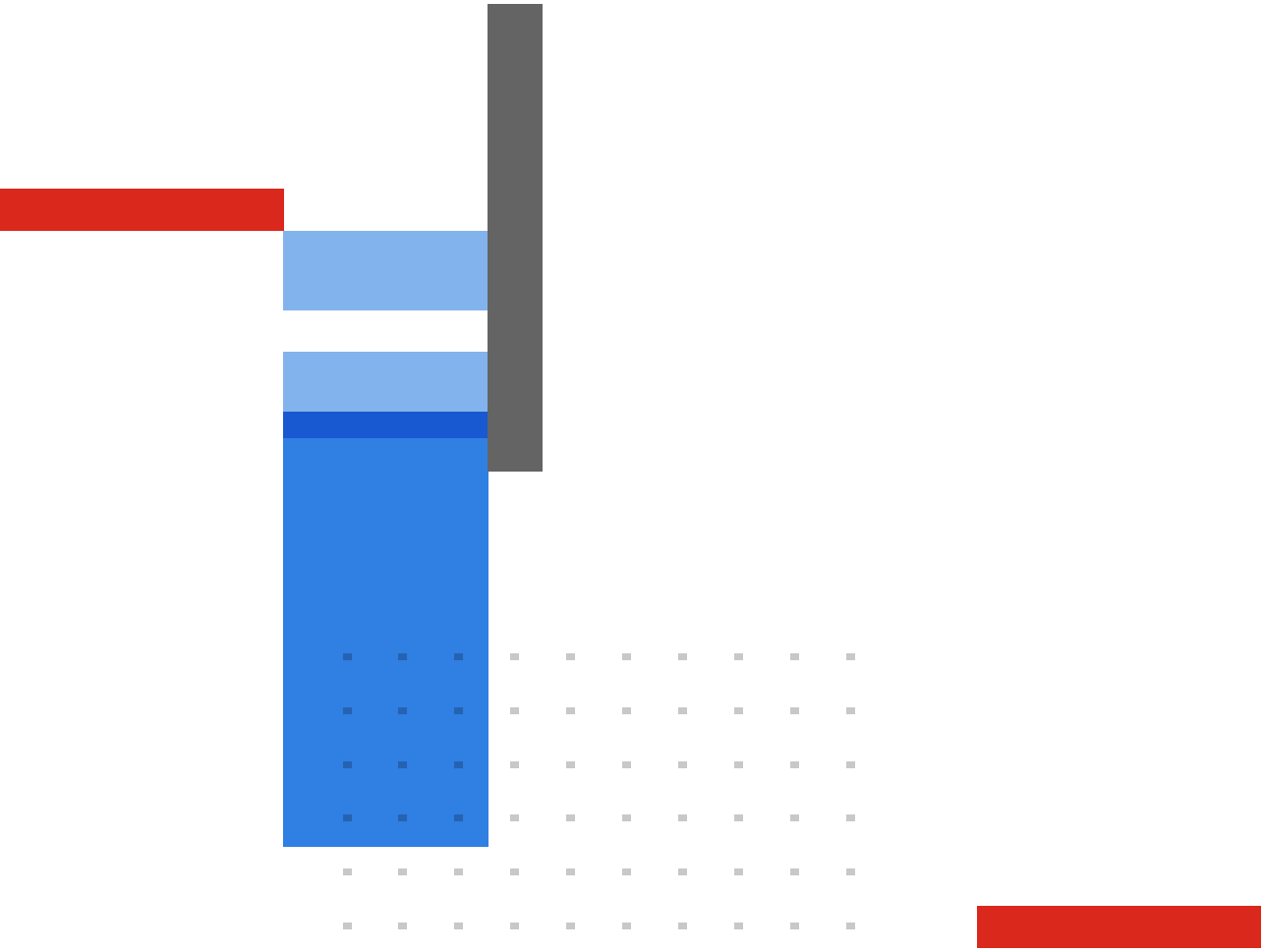
Name	SKU
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Tokyo)	ap-northeast-1
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Singapore)	ap-southeast-1
Europe (Zurich)	eu-central-2
Israel (Tel Aviv)	il-central-1
South America (Sao Paolo)	sa-east-1
Canada (Central)	ca-central-1

Supported Azure Regions

Name	SKU
North Europe (Europe)	northeurope
East US (US)	eastus
West US (US)	westus

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



www.fortinet.com

April 18, 2024

FGCNF-DAT-R08-20240418