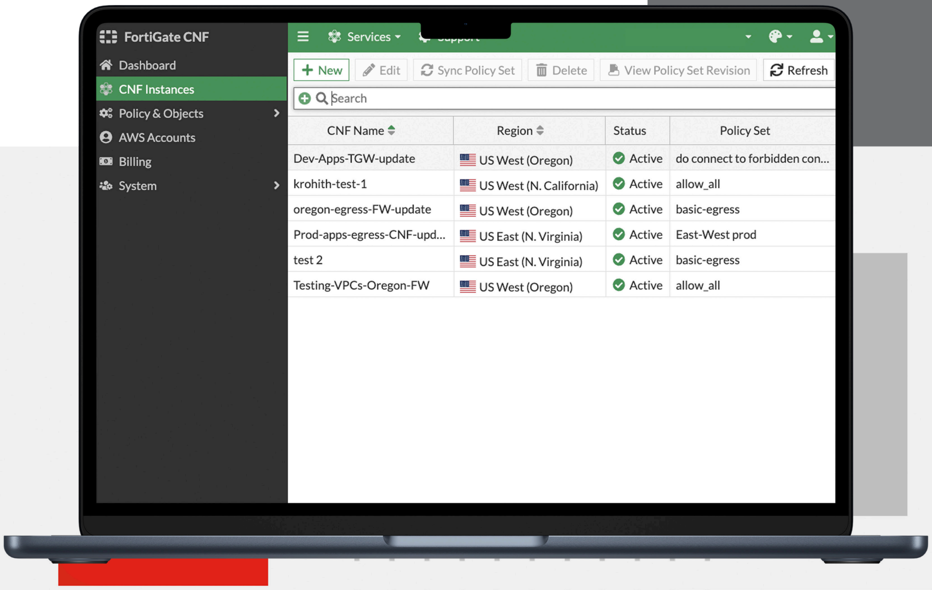
FERTINET

Data Sheet

FortiGate™ CNF Cloud-Native Firewall Service

aws



CNF Name	Region	Status	Policy Set
Dev-Apps-TGW-update	US West (Oregon)	✓ Active	do connect to forbidden con...
krohith-test-1	US West (N. California)	✓ Active	allow_all
oregon-egress-FW-update	US West (Oregon)	✓ Active	basic-egress
Prod-apps-egress-CNF-upd...	US East (N. Virginia)	✓ Active	East-West prod
test 2	US East (N. Virginia)	✓ Active	basic-egress
Testing-VPCs-Oregon-FW	US West (Oregon)	✓ Active	allow_all

Highlights

Enterprise-grade Protection: includes Geo-IP blocking, advanced filtering, and threat protection. Supports the complete set of mature security capabilities of a next-generation firewall, providing deep visibility and advanced protection

Streamlined Security Management: With the ability to aggregate security from all networks in an AWS region into a single CNF, it simplifies security and applies a single policy for all resources chosen. No requirement to build and maintain separate cloud firewalls

Lower Costs: Because there is no security software infrastructure to build, deploy, and operate, costs are reduced, only pay for security processing functionality that is utilized

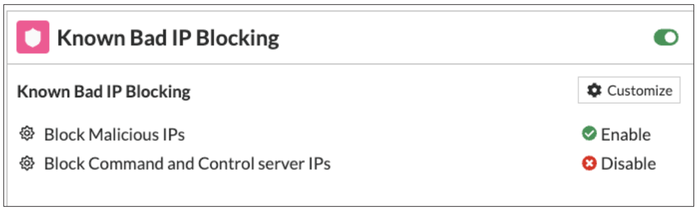
High Performance with Simplicity

FortiGate Cloud-Native Firewall (CNF) is a SaaS 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.

Capabilities

Known Bad IP Filtering

Protect any cloud-based workload from accessing known bad IPs. Whether malicious IPs or known Command and Control servers, FortiGate CNF, powered by FortiGuard Labs IP Reputation Intelligence, can simply and effectively restrict your workloads from accessing unwanted resources.



Known Bad IP Blocking

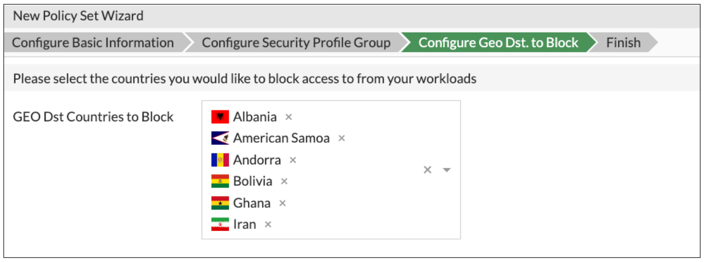
Known Bad IP Blocking

Block Malicious IPs ✓ Enable

Block Command and Control server IPs ✗ Disable

Geo Fencing

Implement simple and effective country-level security policies that help keep your organization in compliance. By utilizing the intuitive Geo Policy wizard, you don't need to deploy complicated network security solutions in order to specifically define which countries can be accessed by your cloud resources.


Configure Basic Information
Configure Security Profile Group
Configure Geo Dst. to Block
Finish

New Policy Set Wizard

Please select the countries you would like to block access to from your workloads

GEO Dst Countries to Block: Albania ×, American Samoa ×, Andorra ×, Bolivia ×, Ghana ×, Iran ×

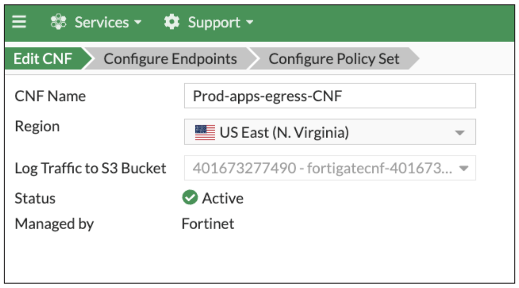
East West Security

In order to effectively secure traffic between cloud workloads, customers often utilize a transit network for security services. FortiGate CNF can attach to customer cloud transit networks and enforce network security policies across cloud networks as well as into cloud networks. FortiGate CNF dynamically scales to support your network security capacity needs so you will never run out of capacity even for the most demanding network security needs.

Capabilities

Simplified Deployment

Once subscribed from the AWS marketplace, follow the built-in setup wizard to deploy CNF instances in minutes. With predefined policies and default security profiles, FortiGate CNF delivers the security you need within minutes without the complexity of setting up other NGFW solutions. More advanced users can easily enable additional security capabilities using FortiManager.



CNF Name: Prod-apps-egress-CNF
Region: US East (N. Virginia)
Log Traffic to S3 Bucket: 401673277490 - fortigatecnf-401673...
Status: Active
Managed by: Fortinet

Dynamic Security

FortiGate CNF offers you the ability to define policies using intuitive and meaningful objects. You can define countries, FQDNs, and any AWS resource meta data attribute as a security policy resource. Utilizing this capability customers do not need to change security policies every time cloud workloads change networks or CI/CD pipelines redeploy application resources. Customers can define dynamic policies using custom clouds workload meta-data, FQDN, and Geo objects and then policies are enforced regardless of where workloads reside or migrate.

Regulatory Compliance

Address regulatory compliance requirements for cloud applications, including PCI DSS 6.6, NIST, and other NGFW requirements.

FortiGuard Labs Services

FortiGuard Labs fuels FortiGate CNF with multiple security signatures and IP reputation information. As an active FortiGate CNF Subscriber you automatically have the latest protections and updates.

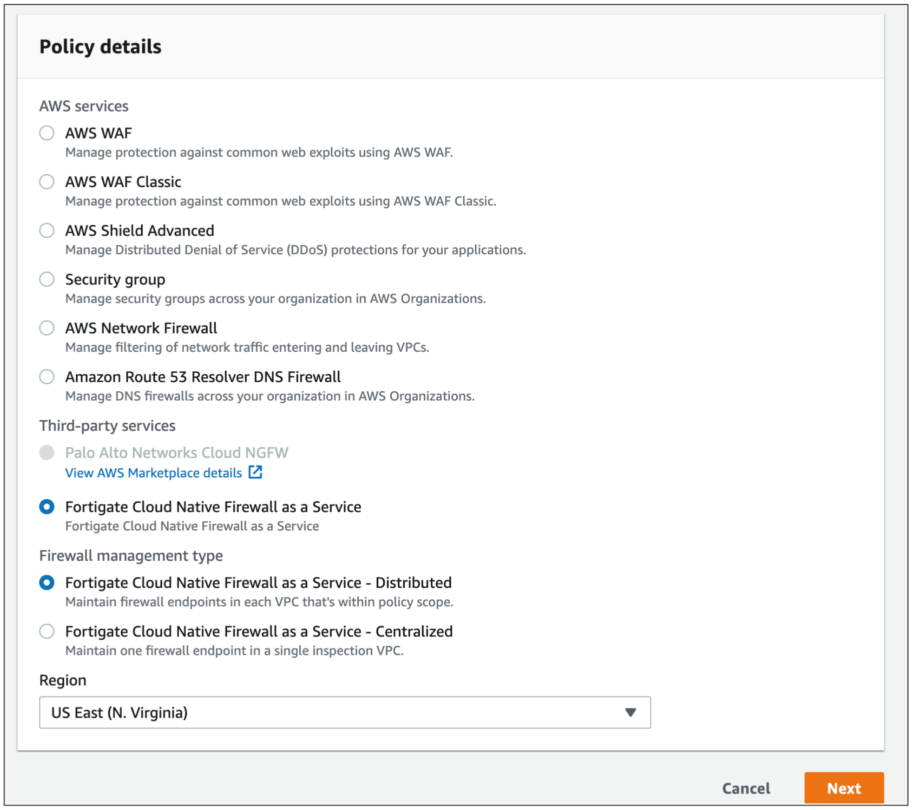
Data Security Processing Unit (DSPU)

DSPU, Data Security Processing Unit, is a charging unit for Traffic Inspection. It is a product of the number of security processing functions utilized and the number of Gigabytes (GB) of traffic volume that is inspected. The security processing functions can be one or any combination of L4 firewall, IPS, Content Inspection, and Encryption/Decryption. The charge per DSPU unit is the same regardless of the type of security processing function used.

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.



Policy details

AWS services

○ AWS WAF
Manage protection against common web exploits using AWS WAF.

○ AWS WAF Classic
Manage protection against common web exploits using AWS WAF Classic.

○ AWS Shield Advanced
Manage Distributed Denial of Service (DDoS) protections for your applications.

○ Security group
Manage security groups across your organization in AWS Organizations.

○ AWS Network Firewall
Manage filtering of network traffic entering and leaving VPCs.

○ Amazon Route 53 Resolver DNS Firewall
Manage DNS firewalls across your organization in AWS Organizations.

Third-party services

○ Palo Alto Networks Cloud NGFW
View AWS Marketplace details

● Fortigate Cloud Native Firewall as a Service
Fortigate Cloud Native Firewall as a Service

Firewall management type

● Fortigate Cloud Native Firewall as a Service - Distributed
Maintain firewall endpoints in each VPC that's within policy scope.

○ Fortigate Cloud Native Firewall as a Service - Centralized
Maintain one firewall endpoint in a single inspection VPC.

Region

US East (N. Virginia) ▼

Advanced Network Security

For customers who are managing network security using FortiManager, and wish to migrate policies from other FortiGate form factors or are looking to utilize the latest in the FortiOS security processing capabilities, FortiGate CNF can be managed by FortiManager.

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

- Multi-VPC Egress Security
- Transit-VPC East West and Ingress

Cloud Integrations

- AWS Gateway Load Balancer
- AWS Firewall Manager
- AWS VPC
- AWS Marketplace
- AWS Meta Data Service

FortiGuard Security Services

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

Data Security Processing Units

- 1GB of NGFW Processing = 1DSPU
- 1GB of IPS Processing = 1DSPU
- 1GB of Sandbox inspection = 1DSPU
- 1GB of encryption/decryption = 1DSPU

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

Available through the Amazon Web Services or via annual contracts. FortiGate CNF Cloud-Native Firewall Service is available for purchase in all regions*. The following lists marketplace pricing.

Units	Price
CNF Instances per hour	$2.70 / unit
Total data Processing protected by FortiGate CNF (GB)	$0.31 / unit
CNF Instance per year	$21,000
100K DSPU Processing	$2,750

* Not available in AWS GovCloud or AWS China.

Supported 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

Fortinet CSR 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

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

December 13, 2022