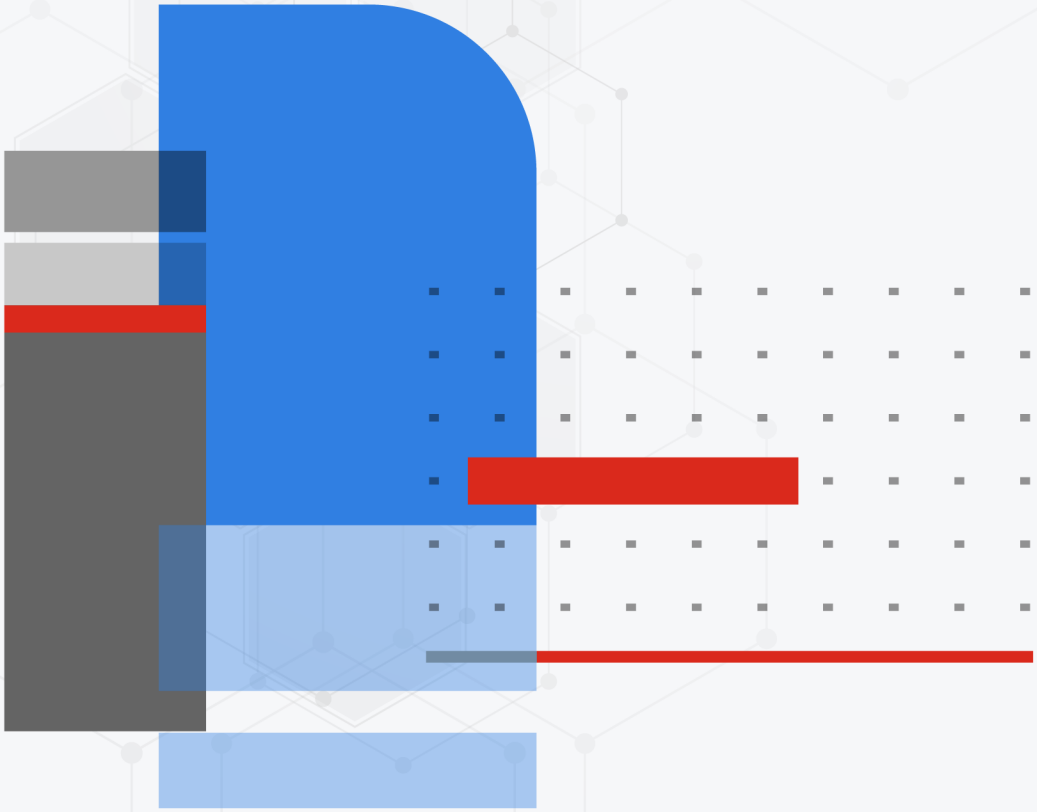
Concept Guide

Cloud Native Firewall 23



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 4, 2023
Cloud Native Firewall 23 Concept Guide
77-231-893394-20230404

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-04-04	Initial release.

What is a cloud native firewall?

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 workloads move to the cloud, networks become more decentralized—and more difficult to secure. Ensuring consistent protection of your cloud resources significantly benefits from a cloud-native solution.

A cloud native firewall (CNF) is a managed cloud network security solution delivered as a service that scales to demand, is highly available within cloud regions and across availability zones, and does not require maintenance by customers. A cloud native firewall allows you to define and assign policies that protect selected networks and cloud compute resources without having to configure, provision, or maintain any firewall software infrastructure.

Benefits

- **Scalability**: Cloud-native firewalls like FortiGate CNF can scale up or down quickly to accommodate changing workload demands.
- **Flexibility**: Cloud-native firewalls are designed to work seamlessly in cloud environments, providing flexibility in terms of deployment and management.
- **Security**: Cloud-native firewalls provide advanced security capabilities to protect workloads against a wide range of threats and vulnerabilities.
- **Egress security**: Cloud-native firewalls like FortiGate CNF provide robust egress security capabilities to help prevent data exfiltration and ensure the confidentiality of cloud data.
- **Visibility**: Cloud-native firewalls provide real-time visibility into cloud network traffic, allowing organizations to identify potential security threats and take proactive measures to mitigate them.
- **Compliance**: Cloud-native firewalls help organizations meet regulatory compliance requirements by providing advanced security and auditing capabilities.
- **Integration**: Cloud-native firewalls can integrate with other security solutions and cloud platforms, enabling organizations to create a comprehensive security ecosystem.
- **Automation**: Cloud-native firewalls like FortiGate CNF can be easily automated, allowing organizations to streamline their security operations and reduce the risk of human error.
- **Performance**: Cloud-native firewalls are optimized for cloud environments, providing high-performance security and networking capabilities that are essential for modern cloud workloads.
- **Cost-effectiveness**: Cloud-native firewalls can be more cost-effective than traditional firewalls, as they are designed to work seamlessly in cloud environments and can be scaled up or down as needed, reducing the need for expensive hardware or software licenses.

Intended audience

This guide is written primarily for users of public cloud services, such as Amazon Web Services (AWS), who are interested in protecting their cloud networks and have an understanding of public cloud networking and security concepts.

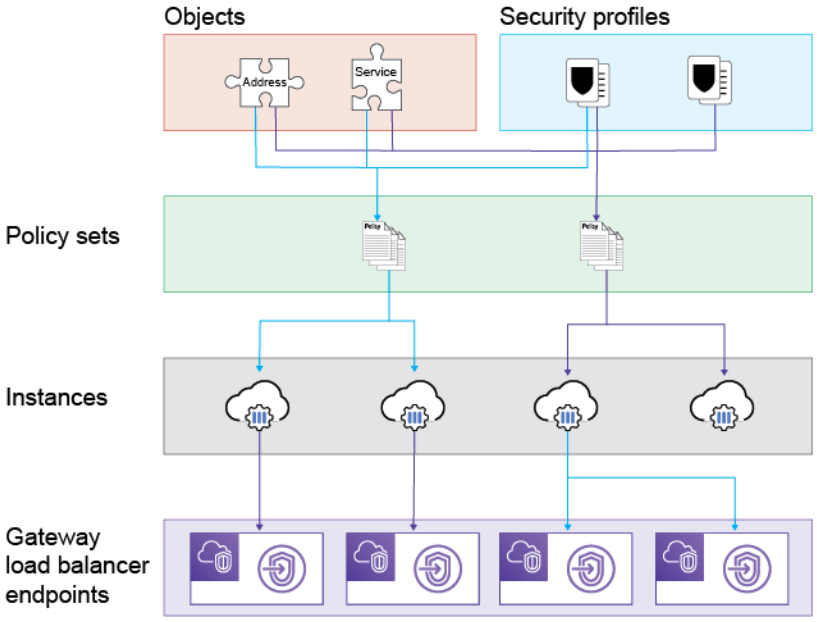
For cloud native firewall security policy implementation, you should also have working knowledge of FortiOS policy configuration.

About this guide

This guide provides an introductory overview of public cloud firewall concepts and introduces Fortinet's FortiGate Cloud Native Firewall (CNF) solution. Industry standard terminologies are used, with introductions to Fortinet specific terms, concepts, and technologies. You can move on to the FortiGate CNF Architecture Guide when you are familiar with the concepts and terminology and to the FortiGate CNF Deployment Guide when you are ready to explore cloud deployment options.

Cloud native firewall concepts

This chapter introduces the essential concepts of cloud native firewalls:



Objects

An object is a piece of information that is used in a firewall policy, much like a variable. Objects may be re-used in multiple policies.

The two primary types of cloud native firewall objects are addresses and services.

Addresses and address groups

Addresses define sources and destinations of network traffic. The address may refer to a specific address, address range, subnet, FQDN, or be defined as dynamic.

Address objects may be collected into address groups.

Services and service groups

Service objects refer to services such as SSH or DNS.

Like addresses, service objects may be collected into service groups.

Security profiles

Security profiles collect pre-configured intrusion prevention, URL filtering, anti-virus, or other profiles into a re-usable group that defines what actions to take with matching traffic.

Security profiles are predefined in the FortiGate CNF console but can be customized in the console or using FortiManager.

Policies and policy sets

Policies are rules that govern how traffic is handled by the firewall. Policies use address and service objects to build matching rules and security profiles to define what action is to be taken.

Policy sets are groups of rules. A single policy set is deployed to a firewall instance, but policy sets may be re-used across multiple firewall instances.

Each CNF instance uses a single policy set at a time, but a single policy set can be used by multiple FortiGate CNF instances. Objects can also be used across multiple policy sets.

CNF Instances

An instance is a logical cloud native firewall unit dedicated to protect a specific set of cloud networks, with the following features:

- Runs in a single region.
- Protects across multiple availability zones.
- Uses a single policy set at a time.
- Connects to one or more VPCs.
- A single instance can protect resources in multiple AWS accounts.

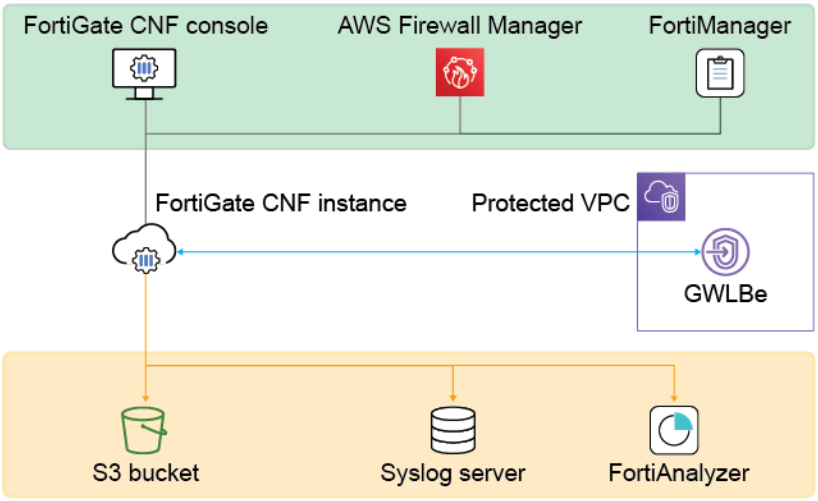
Gateway load blancer endpoints

The gateway load balancer endpoint (GWLBe) is a virtual interface that privately connects the customer's protected VPC with the FortiGate CNF instance. Traffic is routed through this endpoint to and from the FortiGate CNF instance.

Each CNF instance can connect to multiple GWLBes in order to secure multiple VPCs.

Components

This chapter introduces the components of FortiGate CNF, including management, logging, and automation:



FortiGate CNF console

The FortiGate CNF Console provides you with access to the following functionality:

- Onboard AWS accounts into your FortiGate CNF environment.
- Create and manage FortiGate CNF instances.
- Attach FortiGate CNF instances to protected VPCs in your onboarded AWS accounts.
- Create and deploy network security policy sets.

The FortiGate CNF console also provides an API for AWS Firewall Manager and serves as the interface for AWS Firewall Manager for creation of FortiGate CNF instances, Gateway Load Balancer endpoint (GWLBe) deployments, and deployment of policies to FortiGate CNF instances.

Additionally, the FortiGate CNF console is responsible for the following:

- Controlling the creation, software upgrades, and deletion of FortiGate CNF instances.
- Distributing logs from CNF instances into customer-specific S3 buckets, syslog servers, or FortiAnalyzer.
- Managing entitlement and billing for customers through integration with AWS Marketplace and Fortinet FortiCare.

FortiGate CNF instance

Each FortiGate CNF instance is a customer-dedicated, Fortinet-owned and managed VPC that spans across multiple availability zones in a single region.

Each FortiGate CNF instance is made up of the following components:

- An autoscaling group of FortiOS-based EC2 instances dedicated to the customer.
- An AWS Gateway Load Balancer (GWLB) that resides inside this dedicated VPC that is attached to GWLB endpoints (GWLBe) in the your protected VPCs. These VPCs can be in different AWS accounts in the same region.

The FortiGate CNF instance is responsible for data security processing and address resolution as necessary to protect your attached VPCs.

You can manage CNF instance security policies through the FortiGate CNF console or FortiManager.

You can deploy CNF instances through the FortiGate CNF console or AWS Firewall Manager.

Protected VPC

Protected VPCs contain your managed workloads, applications, and subnets and are assumed to exist prior to the deployment of FortiGate CNF. After deploying a Fortigate CNF instance and attaching it to the specified protected VPC, this VPC will also contain a Fortinet-managed GWLBe.

Management, logging, and automation

The following options are available to you for FortiGate CNF management, logging, and automation.

Fortigate CNF console

The FortiGate CNF console is your primary management interface for FortiGate CNF instance and policy management.

You can fully manage FortiGate CNF instances through the FortiGate CNF Console, including:

- Creating FortiGate CNF instances and attach to VPCs.
- Defining policies, objects, and security profiles.
- Deploying policies.
- Onboarding AWS accounts to be protected by Fortigate CNF.

AWS Firewall Manager

You may use the AWS Firewall manager to create FortiGate CNF instances and attach them to VPCs. You may also use it to push pre-defined policy sets to CNF instances.

Policy sets cannot be defined through the AWS Firewall Manager.

For more information about AWS Firewall Manager, see the AWS Firewall Manager documentation.

FortiManager

You may use FortiManager to create and push policies and policy sets to existing CNF instances. You can also use FortiManager's automation features to automate this process as well.

Logging

The following targets can be defined as log targets for FortiGate CNF instances:

- **S3**: FortiGate CNF can save FortiGate instance logs to an S3 bucket.
- **Syslog**: An external syslog server can be used for logging.
- **FortiAnalyzer**: FortiGate CNF instances can be connected to FortiAnalyzer to take advantage of FortiAnalyzer's advanced log analysis tools.

Conclusion

Fortinet's FortiGate cloud native firewall (CNF) solution simplifies your cloud network security while implicitly providing availability and scalability. This solution reduces your network security operations workload by eliminating the need to configure, provision, or maintain any firewall software infrastructure—allowing your security teams to focus on security policy management.

FortiGate CNF is fully equipped with all the advanced capabilities of the mature FortiOS next generation firewall, offering comprehensive visibility and enhanced security.

To learn more about FortiGate CNF, see the additional resources listed in the Appendix.

Appendix A - More information

Product information

- FortiGate CNF data sheet

Feature documentation

- FortiGate CNF Administration Guide

Related documentation

- FortiOS Administration Guide
- FortiManager Administration Guide
- FortiAnalyzer Administration Guide

External references

- AWS documentation

Concept Guide

Cloud Native Firewall 23