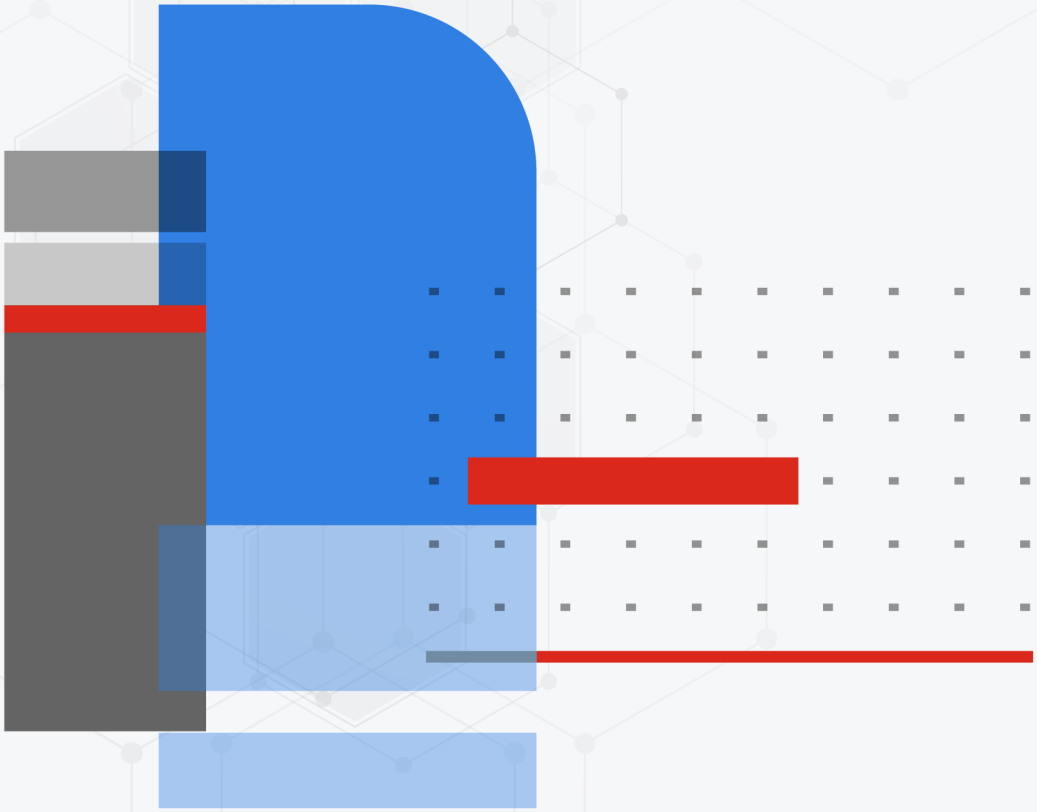
Release Notes

FortiGate CNF 23.2



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 28, 2023
FortiGate CNF 23.2 Release Notes
77-232-889177-20230428

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-04-28	Initial release.

Introduction

FortiGate Cloud-Native Firewall (CNF) is software-as-a-service that simplifies cloud network security while 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 you the flexibility to procure on demand or use annual contracts.

Features

- **Enterprise-grade protection**:includes geo-IP blocking, advanced filtering, and threat protection.
- **Streamlined security management**: Aggregate security from all networks in an AWS region into a single FortiGate CNF and apply a single policy for all resources.
- **Known bad IP filtering**: Protect your cloud-based workload from accessing known bad IPs. FortiGate CNF, powered by FortiGuard Labs IP Reputation Service, can restrict your workloads from accessing unwanted resources.
- **Geo fencing**: Define security policies to limit the countries that can be accessed by your cloud resources.
- **East-west security**: FortiGate CNF can attach to your cloud transit networks to enforce network security policies across cloud networks as well as into cloud networks.
- **Dynamic security**: Define policies using countries, FQDNs, and AWS resource meta data attributes.

What's new

The following new features have been added in FortiGate CNF 23.2:

- Save FortiGate CNF instances as templates and use templates to create new instances.

For more information, see the FortiGate CNF New Features guide.

Getting started

Following is a summary of the steps required to get started with FortiGate CNF.

1. Subscribe to FortiGate CNF through the AWS Marketplace.
2. Log in to the FortiGate CNF Console.
3. Register FortiGate CNF with FortiCare.
4. Add the AWS accounts.
5. Protect workloads with FortiGate CNF instances.

For detailed information about FortiGate CNF, see theFortiGate CNF Administration Guide.

For examples of common deployment scenarios, see Deployment scenarios in the FortiGate CNF Administration Guide.

Compatibility

FortiManager supported versions

FortiGate CNF instances can be managed through FortiManager. The following FortiManager versions are supported:

- 7.2.2 and later

Web browser support

FortiGate CNF Console supports the following web browsers:

- Microsoft Edge 107 and later
- Mozilla Firefox version 107 and later
- Google Chrome version 107 and later

Other web browsers may function correctly, but are not supported.

Known issues

The following issues have been identified in FortiGate CNF.

For inquiries about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
861355	Auto-generated resources are not deleted when the policy set is deleted.
881640	Domain filter / redirect to block portal seeing intermittent issue with CNF/FortiGate 7.2.4.
882305	FortiManager does not show cluster members when FortiGate CNF scales up.
882307	FortiManager goes out of sync after FortiGate CNF failover.
882321	FortiManager goes out of sync after FortiManager manual failover.

Resolved issues

The following issues have been resolved in FortiGate CNF.

For inquiries about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
898170	FortiGate CNF failed to recognize default VPC subnet.
859237	FortiGate CNF theme change not persistent.
894147	Customer may see *CSRF Failed: Referer checking failed* when trying to setup their FortiGate CNF account for the first time.

Special notices

Supported AWS regions

FortiGate CNF is only available for deployment in the following AWS regions:

- US
  - Virginia/us-east-1
  - Ohio/us-east-2
  - Northern Californina/us-west-1
  - Oregon/us-west-2
- Ireland/eu-west-1
- London/eu-west-2
- Frankfurt/eu-central-1
- Tokyo/ap-northeast-1

Fortigate version

FortiGate CNF instances initially run FortiOS 7.2.4, but will run newer versions when necessary.

www.fortinet.com