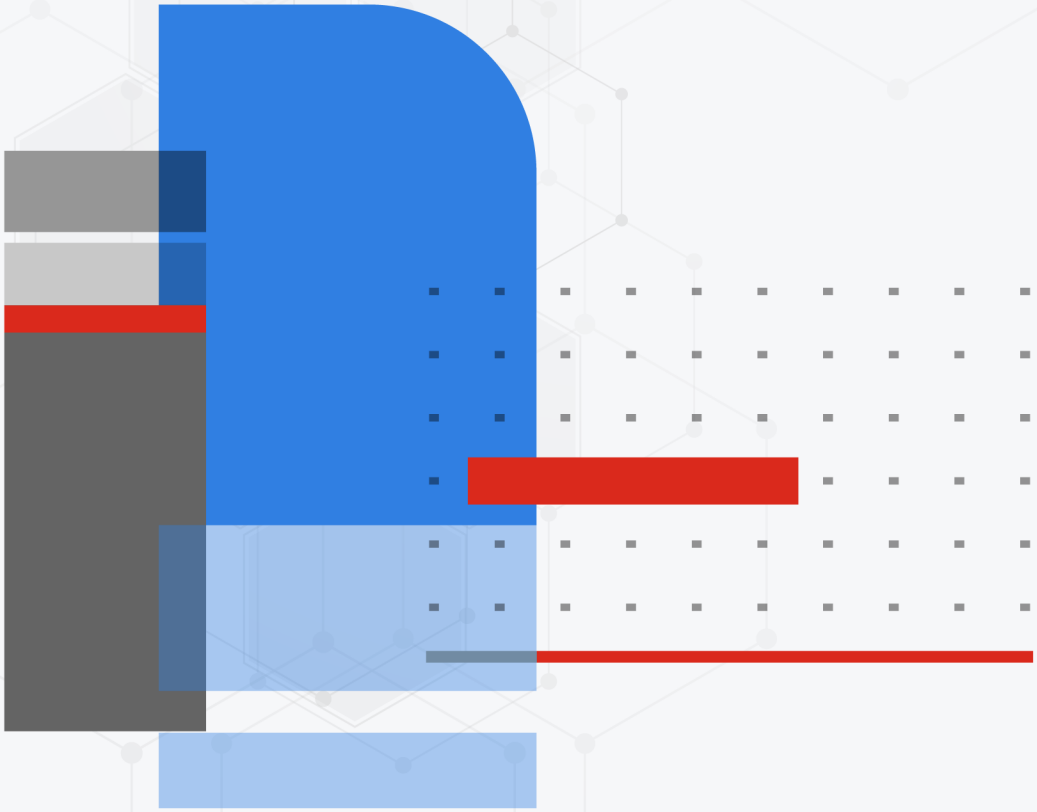
Release Notes

FortiGate CNF 25.3.a



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

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

November 04, 2025
FortiGate CNF 25.3.a Release Notes
77-253a-1220224-20251104

TABLE OF CONTENTS

Change log

Date	Change Description
2025-11-03	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 a 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 IP addresses. FortiGate CNF, powered by FortiGuard Labs IP Reputation Service, can restrict your workloads from accessing unwanted resources.
- **DNS filtering**: Protect your networks with DNS filtering, including FortiGuard category-based filtering, domain filters, and DNS translation.
- **IPS profile**: Utilize Fortinet's Intrusion Prevention System (IPS) to detect network attacks and prevent threats from compromising your network. IPS utilizes signatures, protocol decoders, heuristics (or behavioral monitoring), threat intelligence (such as FortiGuard Labs), and advanced threat detection to prevent exploitation of known and unknown zero-day threats.
- **Geo fencing**: Define security policies to limit the countries that your cloud resources can access.
- **East-west security**: FortiGate CNF instances 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, FQDN, and cloud resource meta data attributes.
- **REST API**: Manage cloud accounts, infrastructure, and FortiGate CNF instances through the FortiGate CNF REST API.

What's new

FortiGate CNF 25.3.a includes the following enhancements:

- Support NAT natively within FortiGate CNF instances to offer cost-effective egress traffic handling.

For more information, see FortiGate CNF New Features.

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 or the Azure Marketplace.
2. Log in to the FortiGate CNF Console.
3. Register FortiGate CNF with FortiCare.
4. Add cloud 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

You can use FortiManager to manage your FortiGate CNF instances.

FortiGate CNF supports the following FortiManager versions:

- 7.2.2 and later

In FortiManager 7.2.10, 7.4.7, 7.6.3, and later, FortiManager does not automatically recognize VM serial numbers, including FortiGate CNF instances.

Additional configuration of FortiManager is required. See Adding VM devices in the FortiManager Administration Guide.

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.
882305	FortiManager does not show cluster members when FortiGate CNF scales up.
882307	FortiManager goes out of sync after FortiGate CNF failover.
1102771	FortiManager probe intermittently fails when adding FortiGate CNF instance.
1106492	*Next* button should be grayed out before you *Save* modified FortiGate CNF instance.
1106552	*Delete* button is active while resolver rule is in *Deleting* state.
1166696	FortiGate CNF in the Thailand region cannot be managed by FortiManager.
1184636	Azure FortiGate CNF instances fail to send logs to FortiAnalyzer. If you are affected by this issue, contact support for assistance.

Special notices

Supported AWS regions

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

- North America
  - Canada (Central)/ca-central-1
  - Northern Californina/us-west-1
  - Ohio/us-east-2
  - Oregon/us-west-2
  - Virginia/us-east-1
- Europe
  - Frankfurt/eu-central-1
  - Ireland/eu-west-1
  - London/eu-west-2
  - Zurich/eu-central-2
- Asia Pacific
  - Hong Kong/ap-east-1
  - Singapore/ap-southeast-1
  - Thailand/ap-southeast-7
  - Tokyo/ap-northeast-1
- Israel
  - Tel Aviv/il-central-1
- South America
  - Sao Paulo/sa-east-1

Supported Azure regions

FortiGate CNF is available for deployment in the following Azure regions:

- North America
  - East US
  - West US
- Europe
  - North Europe

FortiGate version

FortiGate CNF instances initially run FortiOS 7.2.9, but run newer versions when necessary. Instances deployed in the Thailand region initially run FortiOS 7.2.11.

See Editing or viewing a FortiGate CNF instance in the FortiGate CNF Administration Guide.

Egress NAT support

Egress NAT is currently supported only for FortiGate CNF instances on AWS.

In FortiManager, enabling the NAT option for a FortiGate CNF instance policy currently has no effect. Policies with egress NAT enabled can only be configured directly through theFortiGate CNF console, which must be operated in non-FortiManager mode in the current release (25.3.a).

When two policies share the same source, destination, and service, where one enables NAT and the other does not, differentiating them by specifying an IP range in the service will not be effective. The second policy will not take effect.

www.fortinet.com