



Administration Guide

FortiGate CNF 24.1.c



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



April 02, 2024

FortiGate CNF 24.1.c Administration Guide

77-241c-1015560-20240402

TABLE OF CONTENTS

Change Log	7
Introduction	8
Features	8
Benefits	8
Cloud support	9
Autoscaling	9
Managed infrastructure	9
AWS Firewall Manager integration	9
Requirements	10
Getting started	11
Subscribing to FortiGate CNF	11
Before you begin	11
Subscribing	12
30-day free trial	15
Switching from free trial to paid subscription	17
Logging in	18
FortiCloud Organization support	18
Adding AWS accounts	20
Adding Azure accounts	20
Protecting workloads with FortiGate CNF	21
Networking	21
Security	21
Using the console	21
Banner	22
Forms	23
Tables	25
Charts	27
Product registration and technical support	28
Onboarding	29
Dashboard	31
License Information	31
Annual Credits Information	31
CPU	31
Bandwidth	32
CNFs per region	32
Protected subnets	33
Memory	34
Service health dashboard	35
CNF instances	37
Deploying a FortiGate CNF instance	37
Creating a new AWS FortiGate CNF instance	38
Creating a new Azure FortiGate CNF instance	39

Creating a new FortiGate CNF instance from a template	39
Adding an endpoint to an AWS instance	40
Adding an endpoint to an Azure instance	41
Configuring policy sets	42
Editing or viewing a FortiGate CNF instance	42
Primary details	43
Endpoints and load balancers	44
Policy sets	45
Instance Version	46
Deleting a CNF instance	46
Viewing a policy set revision	46
Viewing the policy set revision diff	47
Saving a FortiGate CNF instance as template	48
Synchronizing policy sets	49
Configuring Route 53 resolver rules	49
Scheduling FortiGate CNF instance upgrades	52
Rollback	52
Scheduling an upgrade	53
Rolling back an upgrade	53
FortiManager mode	54
Adding a FortiGate CNF instance to FortiManager	54
Management restrictions	55
Managing a FortiGate CNF instance in FortiManager	58
FortiAnalyzer logging	59
Troubleshooting	60
Using packet capture	61
Configuration	62
Policy sets	62
Creating a policy set	63
Editing or viewing a policy set	64
Deleting a policy set	65
Addresses	65
Address objects	65
Address groups	67
Services	67
Services	68
Service groups	68
Internet service database objects	68
Security profiles	69
Editing security profiles	70
CNF templates	72
Viewing template details	72
Deleting a template	72
Creating an instance from a template	72
Configuring DNS filtering on AWS	72
Configuring DNS filtering on Azure	74

Cloud accounts	75
Adding an AWS account	75
Configuring Security Lake	76
Adding an Azure account	77
Service Principal Object ID	78
Billing	79
Summary charts	79
System	80
Audit log	80
Tenant info	80
API keys	80
Appendix A - Deployment scenarios	82
Examples	82
Distributed egress: north-south traffic Example	83
Scenario objective	83
Before deployment of FortiGate CNF	83
After deployment of FortiGate CNF	84
Distributed inter-subnet east-west traffic in one AZ Example	85
Scenario objective	85
Before deployment of FortiGate CNF	85
After deployment of FortiGate CNF	86
Distributed inter-subnet east-west traffic between AZ Example	87
Scenario objective	87
Before deployment of FortiGate CNF	87
After deployment of FortiGate CNF	88
Distributed inter-VPC east-west traffic Example	89
Scenario objective	89
Before deployment of FortiGate CNF	89
After deployment of FortiGate CNF	91
Centralized ingress: inspection before load balancer Example	92
Scenario objective	92
Before deployment of FortiGate CNF	92
After deployment of FortiGate CNF	94
Centralized ingress: inspection after load balancer Example	95
Scenario objective	95
Before deployment of FortiGate CNF	95
After deployment of FortiGate CNF	97
Centralized egress Example	98
Scenario objective	98
Before deployment of FortiGate CNF	99
After deployment of FortiGate CNF	101
Centralized east-west, inter-VPC Example	102
Scenario objective	102
Before deployment of FortiGate CNF	103
After deployment of FortiGate CNF	105
Azure ingress and egress using public IP Example	106

Scenario objective	106
Before deployment of FortiGate CNF	106
After deployment of FortiGate CNF	107
Azure ingress and egress using Load Balancer with public IP Example	108
Scenario objective	108
Before deployment of FortiGate CNF	108
After deployment of FortiGate CNF	109
Appendix B - Using AWS Firewall Manager	110

Change Log

Date	Change Description
2024-03-28	Initial release.
2024-04-02	Updated Audit log on page 80.

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 or Azure 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.
- **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 in order to prevent exploitation of known and unknown zero-day threats.
- **Geo fencing:** Define security policies to limit the countries that can be accessed by your cloud resources.
- **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, FQDNs, and AWS or Azure resource meta data attributes.
- **REST API:** Manage AWS accounts, infrastructure, and FortiGate CNF instances through the FortiGate CNF REST API.

Benefits

FortiGate CNF offers the following benefits:

- [Cloud support on page 9](#)
- [Autoscaling on page 9](#)
- [Managed infrastructure on page 9](#)
- [AWS Firewall Manager integration on page 9](#)

For more information, see the [FortiGate CNF datasheet](#).

Cloud support

FortiGate CNF supports deployments on Amazon Web Services (AWS) and Azure.

- FortiGate CNF instances are hosted in AWS or Azure infrastructure and placed in the same region as your protected workload.
- A single FortiGate CNF instance deployed into AWS can aggregate security for multiple VPCs, availability zones, and AWS accounts in a single region using a shared policy.
- A single FortiGate CNF instance deployed into Azure can aggregate security for multiple virtual networks, availability zones, and Azure accounts in a single region using a shared policy.
- The FortiGate CNF console runs highly available on AWS and allows you to access the FortiGate CNF from anywhere across the globe. The console backend manages and controls your access to FortiGate CNF instances.
- FortiGate CNF supports AWS Firewall Manager and allows you to manage the deployment of FortiGate CNF instances and rollout of security services using Firewall Manager.

Autoscaling

FortiGate CNF instances dynamically scale to support your network security capacity needs so you will never run out of capacity even for the most demanding network security needs.

Instances scale based on throughput, CPU, and memory utilization of each node.

Managed infrastructure

FortiGate CNF is a managed service.

Once subscribed from the AWS marketplace follow the built-in setup wizard to deploy FortiGate CNF instances in minutes.

With predefined policies and security profiles, FortiGate CNF delivers the security you need within minutes without the complexity of setting up an NGFW solution.

With no security infrastructure to build, deploy, or operate, operations are simplified and costs are reduced.

AWS Firewall Manager integration

FortiGate CNF is integrated with [AWS Firewall Manager](#).

All FortiGate CNF administration can be done through the FortiGate CNF console, but you can optionally perform the following actions through the AWS Firewall Manager console:

- Create FortiGate CNF instances.
- Apply policy sets to instances.

If you create an instance in Firewall Manager, you must apply the policy set through Firewall Manager after creating the policy set in the FortiGate CNF console.



You must create and configure policies and policy sets in the FortiGate CNF console. They cannot be configured in AWS Firewall Manager. See [Configuration on page 62](#).



In the *CNF Instances* table, the *Managed by* column indicates whether the instance is created through AWS Firewall Manager or directly in the FortiGate CNF console. If you created the instance through AWS Firewall Manager, then the *Configure Policy Set* tab is disabled and you must use AWS Firewall Manager to apply the policy set.

For more information about managing FortiGate CNF instances with AWS Firewall Manager, see [Using AWS Firewall Manager on page 110](#).

Requirements

To use FortiGate CNF, you must first subscribe to the service through the AWS Marketplace. You only need to subscribe once, and you can create any number of FortiGate CNF instances with one subscription.

Before you begin, you need the following:

- An AWS account. This is the account that is billed for the costs of deployed instances, and it may be different than the AWS accounts you will protect with FortiGate CNF.
- A [FortiCloud](#) account.

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. See [Subscribing to FortiGate CNF on page 11](#).
2. Log in to the FortiGate CNF console. See [Logging in on page 18](#).
3. Register FortiGate CNF with FortiCare. See [Product registration and technical support on page 28](#).
4. Add cloud accounts:
 - [Adding AWS accounts on page 20](#).
 - [Adding Azure accounts on page 20](#).
5. Protect workloads with FortiGate CNF instances. See [Protecting workloads with FortiGate CNF on page 21](#).

For more information about using the console, see [Using the console on page 21](#).



The underlying auto-scaling group of FortiGate devices is managed by FortiGate CNF and is not directly accessible.

Subscribing to FortiGate CNF

To use FortiGate CNF, you must first subscribe to the service through the AWS Marketplace. You only need to subscribe once, and you can create any number of FortiGate CNF instances with one subscription.

Before you begin

Requirements

Before you begin the subscription process, you need the following:

- An AWS account. This is the account that is billed for the costs of deployed instances, and it may be different than the AWS account or accounts where you will deploy your instances.
- A [FortiCloud](#) account.

Subscription options

AWS Marketplace offers the following subscription options for FortiGate CNF:

- *Consumption*: You are charged based on FortiGate CNF usage, with no minimum commitment.
- *Contract*: You are charged for a yearly contract (for increments of a one-year commitment) with a committed amount of credits available for use with in the contract period. The credits will be available to use for FortiGate CNF instances and security traffic processing. If your usage exceeds the available credits, the overage is charged at the consumption rate.
- *30 day free trial*: See [30-day free trial on page 15](#).

Sandbox pricing

Sandbox pricing is available, but it is only supported if you have your own AWS sandbox environment.

Supported VPCs

FortiGate CNF supports up to 50 VPCs for each FortiGate CNF instance.

Billing

Billing is calculated based on six factors:

- *CNF Hours (multi-AZ cluster)*: The length of time that FortiGate CNF instances have been deployed.
- *CNF Hours Support*: Support Entitlement Hours – added to every FortiGate CNF instance hour.
- *Traffic*: The amount of data that has been processed by each FortiGate CNF security function.
- *IPS Traffic*: The amount of data that has been processed by each FortiGate CNF for IPS processing.
- *URL and DNS Filter Traffic*: The amount of data that has been processed by each FortiGate CNF for URL and DNS filtering.
- *External Sandbox Traffic*: The amount of data that has been processed by each FortiGate CNF for sandboxing feature.

There is a separate rate for each of these dimensions in AWS Marketplace. Your total bill is the sum of all dimensions.

For more information about pricing, see the [FortiGate CNF datasheet](#).

For more information about the billing report available in the FortiGate CNF console, see [Billing on page 79](#).

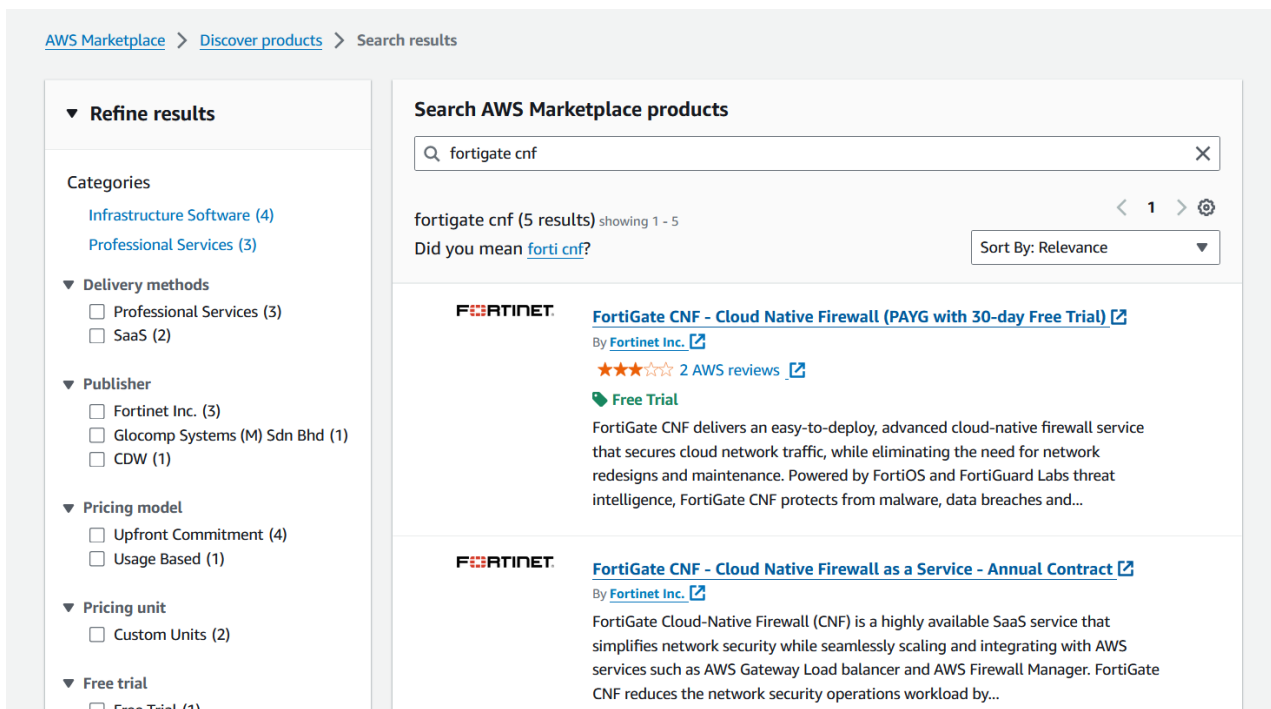
Subscribing



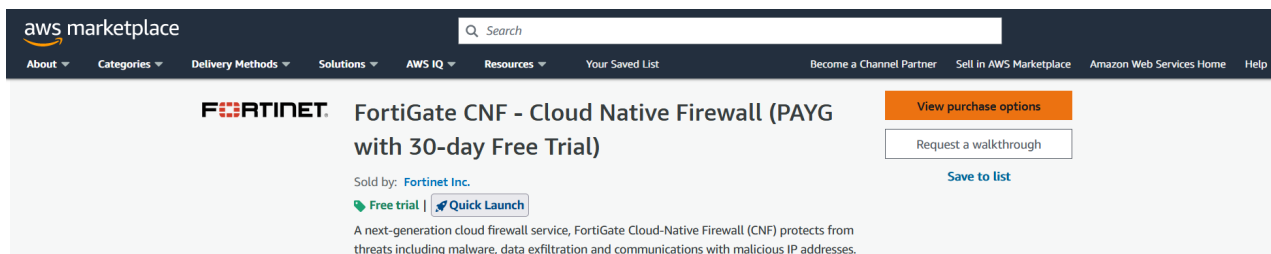
The Safari web browser is not supported.

To subscribe to FortiGate CNF:

1. Log in to AWS and go to the [AWS Marketplace](#).
2. Use the search feature to find FortiGate CNF.

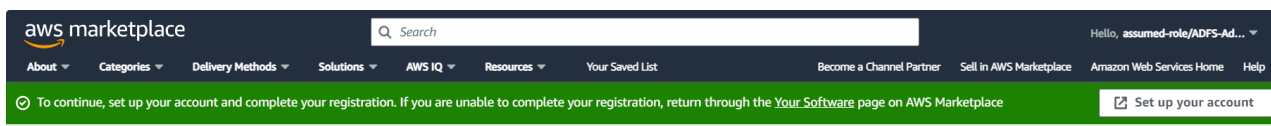


3. In the FortiGate CNF listing, click *View purchase options*.

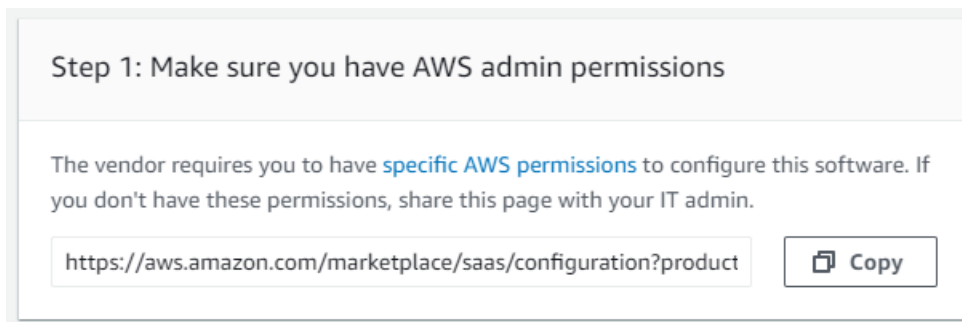


4. Review the pricing information and click *Subscribe*.

5. Click *Set up your account*.



6. Ensure that you have AWS admin permissions.

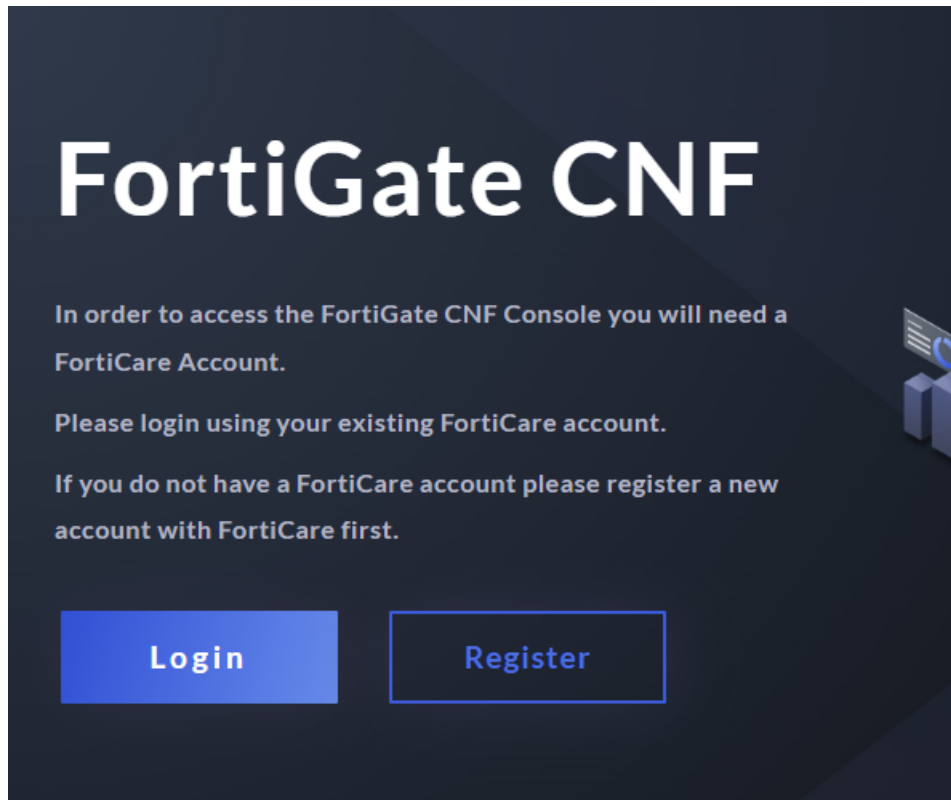


7. Click *Login or create vendor account*.

Step 2: Link a new or existing vendor account [Info](#)

Login or create vendor account

8. Log in to your FortiCloud account, or register for a new account.



FortiGate CNF links your AWS and FortiCloud accounts.

9. Click *Launch Template* to configure your cloud resources.

Step 3: Configure your vendor and AWS Integration [Info](#)

▼ Automatically configure with AWS CloudFormation (recommended)

AWS CloudFormation allows you to automatically launch and configure your resources and their dependencies as a stack. Once the stack's status is **CREATE_COMPLETE**, return here to launch your product.

Fortigate

Launch template [↗](#)

10. In Quick create stack, specify values as needed and click *Create*.

If you will be sending logs to AWS Security Lake, set *SecurityLakeCustomLogSourceName* to your Security Lake custom log source.

The AWS stack is created and configured for use.

Fortigate ⊞ | ✕

Delete Update Stack actions ▾ Create stack ▾

Stack info | **Events** | Resources | Outputs | Parameters | Template | Change sets

Events (20) 🔄

🔍 Search events ⊞

Timestamp	Logical ID	Status	Status reason
2023-09-22 08:35:23 UTC-0700	Fortigate	🟢 CREATE_COMPLETE	-
2023-09-22 08:35:22 UTC-0700	NotificationToFortinetFWaaS	🟢 CREATE_COMPLETE	-
2023-09-22 08:35:22 UTC-0700	NotificationToFortinetFWaaS	🟡 CREATE_IN_PROGRESS	Resource creation Initiated
2023-09-22 08:35:19 UTC-0700	NotificationToFortinetFWaaS	🟡 CREATE_IN_PROGRESS	-
2023-09-22 08:35:18 UTC-0700	LoggingS3Bucket	🟢 CREATE_COMPLETE	-

30-day free trial

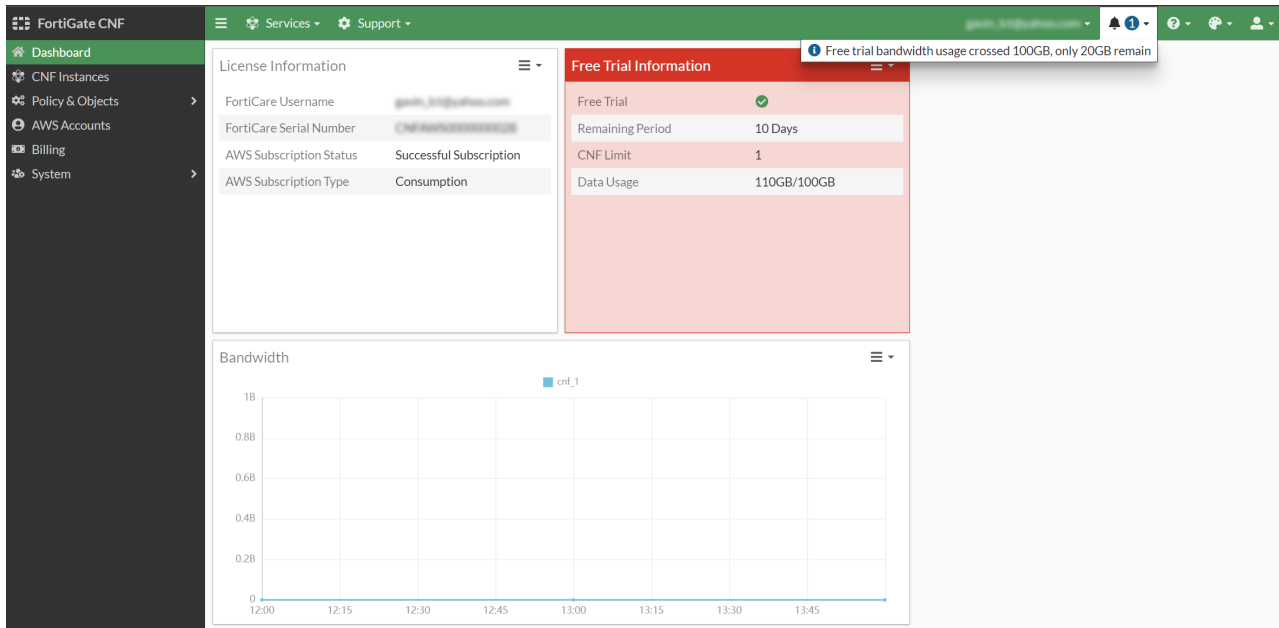
You can subscribe to FortiGate CNF for a free trial.



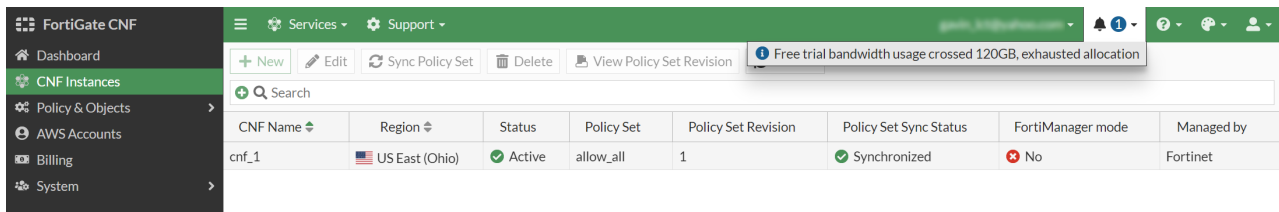
Currently, to switch from a free trial subscription to a paid subscription, you must unsubscribe from the free subscription and then subscribe to a paid subscription. Your free trial configuration can be retained using the *Save as Template* feature. See [Switching from free trial to paid subscription on page 17](#).

The free trial has the following limitations:

- You can create and deploy only one FortiGate instance.
- Once your bandwidth exceed 100 GB of traffic, FortiGate CNF displays alerts on the console and allows a grace of an additional 20 GB.



- After 120 GB bandwidth is exceeded, your FortiGate CNF free trial will be automatically suspended and then deleted.

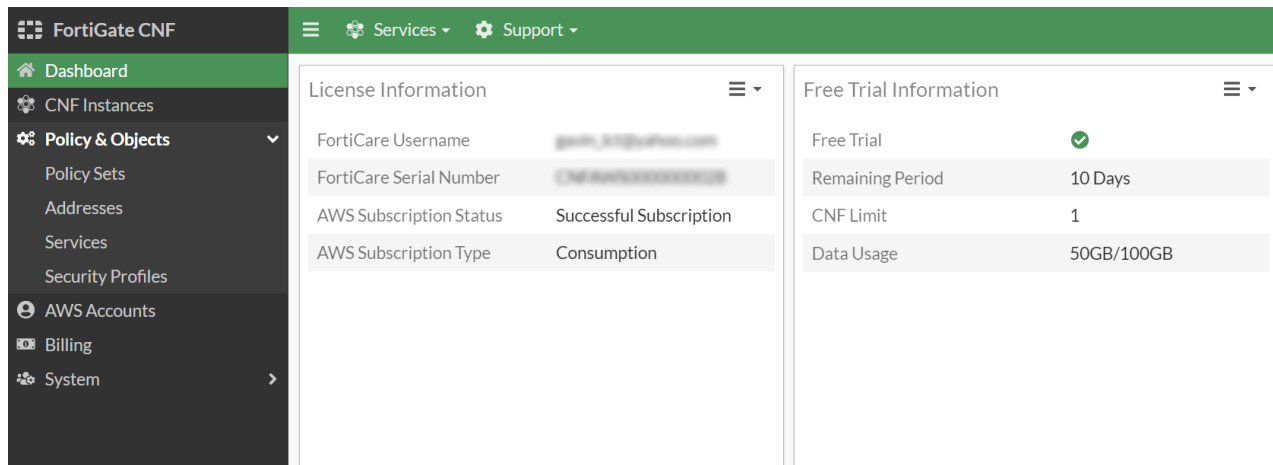


- After 30 days FortiGate CNF will create alerts on the console and allow a grace period of an additional four days.
- After 34 days are complete, your FortiGate CNF free trial will be suspended and then deleted.

To subscribe to the free trial:

1. Log in to AWS and go to the [AWSMarketplace](#).
2. Use the search feature to find *FortiGate CNF - Cloud Native Firewall as a Service free trial*.
3. Continue with the subscription process detailed in [Subscribing to FortiGate CNF in the FortiGate CNF Administration Guide](#).

When you log in to the FortiGate CNF console, the *Free Trial Information* widget is displayed on the dashboard.



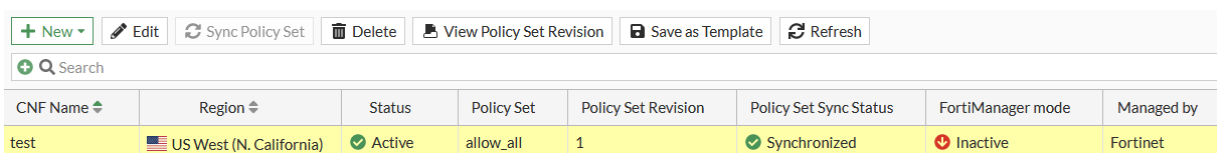
Switching from free trial to paid subscription

The process to backup and restore your existing FortiGate CNF instance configuration when switching from a free trial to a paid subscription is as follows:

1. Backup the configuration of each FortiGate CNF instance.
2. Unsubscribe from the free trial subscription.
3. Subscribe to a paid subscription.
4. Log in to the FortiGate CNF console.
5. Restore the FortiGate CNF instance configurations.

To switch from a free trial to a paid subscription:

1. Backup the configuration of each FortiGate CNF instance:
 - a. In the FortiGate CNF console, in *CNF Instances*, select each instance and click *Save as Template*.



The instance configuration is saved as a template in *Configuration > CNF Templates* and the template is displayed.

2. Unsubscribe from the free trial subscription:
 - a. In the AWS Marketplace console, in the *Manage subscriptions* page, click *Manage* next to the FortiGate CNF free trial subscription, then select *Cancel subscription* from the *Actions* menu.
Your existing CNF instances are deleted.
3. Subscribe to a paid subscription:
 - a. In the AWS Marketplace, subscribe to a paid subscription with the same AWS account. For more information about the subscription process, see [Subscribing to FortiGate CNF on page 11](#).
4. Log in to the FortiGate CNF console.
5. Restore the FortiGate CNF instance configurations:

- a. In the FortiGate CNF console, in *CNF Templates*, select each template and click *Create CNF*.

CNF Name	Region	FortiManager mode	Enable FortiAnalyzer IP	External Logging	Internal Logging
test	US West (N. California)	Inactive	Disabled	None	None

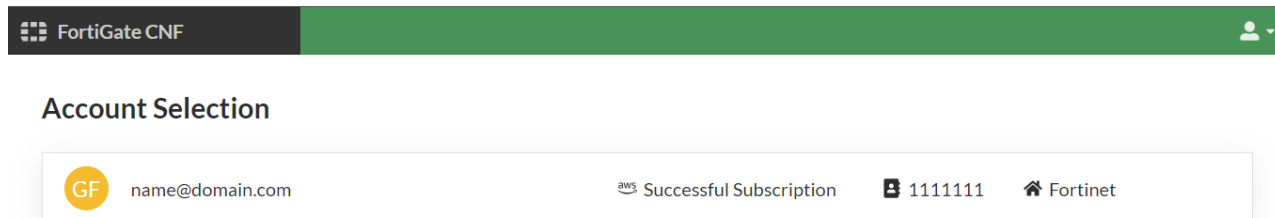
- b. Update the instance as needed and click *OK*.
The new instance is created with the same configuration as the original.

Logging in

After you have completed the subscription process, you can log in to the FortiGate CNF console directly.

To log into FortiGate CNF:

1. Go to <https://fortigatecnf.com/>.
2. Click *Login*. You are redirected to the FortiCloud login page.
3. Log in with your FortiCloud account.
4. Click the appropriate account.




Because a FortiCloud account can grant another user access permissions to its assets, including FortiGateCNF, there may be more than one account listed.

The FortiGate CNF console opens.

FortiCloud Organization support

FortiGate CNF can be connected to FortiCloud Organization to allow multiple users access to FortiGate CNF resources. When logging in, organization users select their account.

Account Selection

▼  Fortinet Cloud Service QA

Fortinet Cloud Service QA team






 | Fortinet | Successful Subscription

▼  SubOU 1






 | Fortinet | Successful Subscription

▼  SubOU 1-1

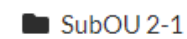




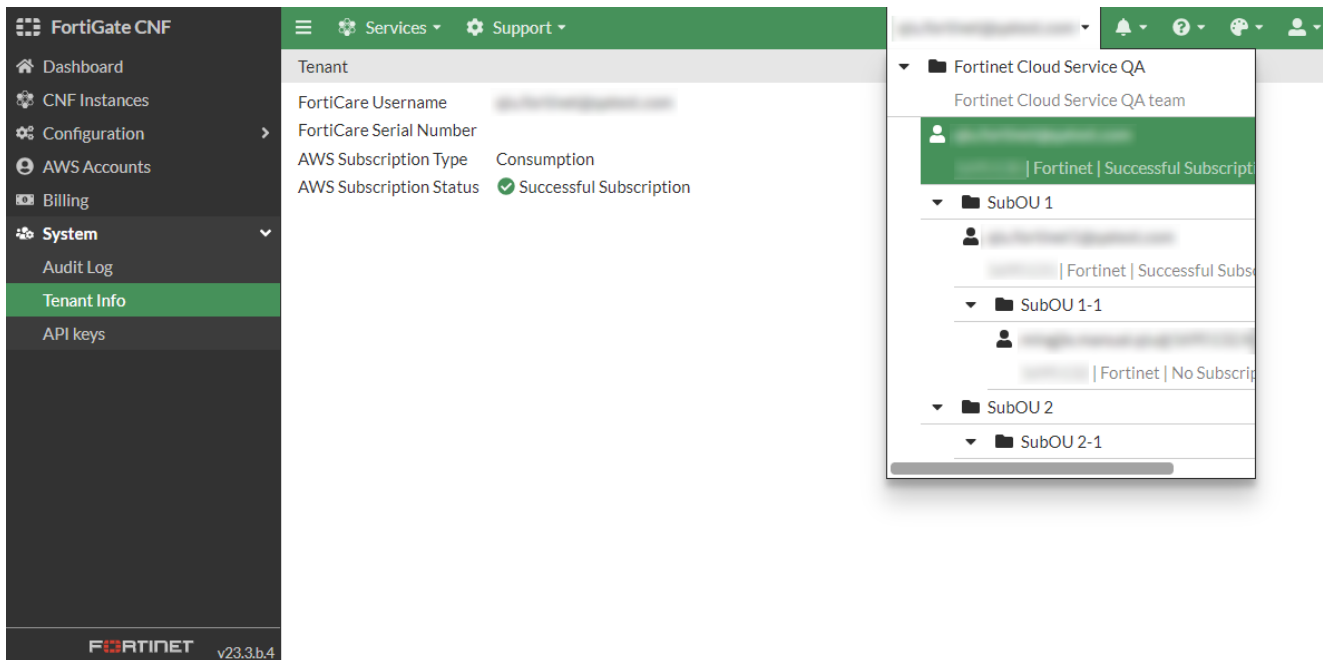
 | Fortinet | No Subscription Found

▼  SubOU 2



 SubOU 2-1

Switch accounts using the account dropdown.



For more information about FortiCloud Organization, see [the FortiCloud Organization Portal documentation](#).

Adding AWS accounts



When you first log in to FortiGate CNF, you are presented with the onboarding wizard, which walks you through the process of adding an AWS account. See [Onboarding on page 29](#).

FortiGate CNF requires access permissions on your AWS account in order to perform various tasks, such as deploying FortiGate CNF endpoints into your VPCs, resolving IP addresses of resources, and sending logs to an S3 bucket.

You must add the AWS account or accounts where your workloads will be running. There are no limits on the number of AWS accounts you may add, and these accounts do not need to have AWS Marketplace subscriptions.

Added accounts do not have to be the same as the billing AWS account.

For more information about adding AWS accounts, see [Cloud accounts on page 75](#).

Adding Azure accounts

FortiGate CNF instances can be deployed to protect workloads in the Azure.

You must add the Azure account or accounts where your workloads will be running. There are no limits on the number of Azure accounts you may add.

For more information about adding Azure accounts, see [Cloud accounts on page 75](#).

Protecting workloads with FortiGate CNF

For each cloud subnet you are protecting, take the following steps.

Networking

Ensure the traffic is routed correctly, as follows:

1. Create and deploy a FortiGate CNF instance. See [Deploying a FortiGate CNF instance on page 37](#).
2. Deploy a load balancer endpoint in your cloud account. Typically the endpoint is put in a subnet by itself. See [Adding an endpoint to an AWS instance on page 40](#).
3. Route traffic to the deployed FortiGate CNF instance. The instance must be in the traffic path of your workload. This requires some routing changes in your cloud infrastructure, and has to be done by you as Fortinet does not have access to your infrastructure. Route traffic to the load balancer endpoint, which sends the traffic to the FortiGate CNF instance to be inspected and returned to the load balancer endpoint. For some deployment examples, see [Deployment scenarios on page 82](#).

Consider FortiGate CNF as a bump-in-the-wire, with the load balancer endpoint as the gate.

Security

Ensure the desired security policies are applied to the deployed FortiGate CNF instance.

1. Create a policy set.
This process is very similar to the policy creation process on FortiGate. *Address*, *Service*, and *Security Profile* objects are used to form policies, which are grouped in an ordered sequence to form a policy set.
2. Apply a policy set to one or more FortiGate CNF instances.
Policy sets can be edited and then updated on deployed instances if needed.

Using the console

This section presents an introduction to the FortiGate CNF console interface.

The following topics are included in this section:

Banner on page 22	The top banner of the FortiGate CNF console is accessible on all pages and provides access to product and account information and functions.
Forms on page 23	Information about forms and form elements in the FortiGate CNF console.
Tables on page 25	Information about table behavior in the FortiGate CNF console.
Charts on page 27	Information about chart functionality in the FortiGate CNF console.

Banner

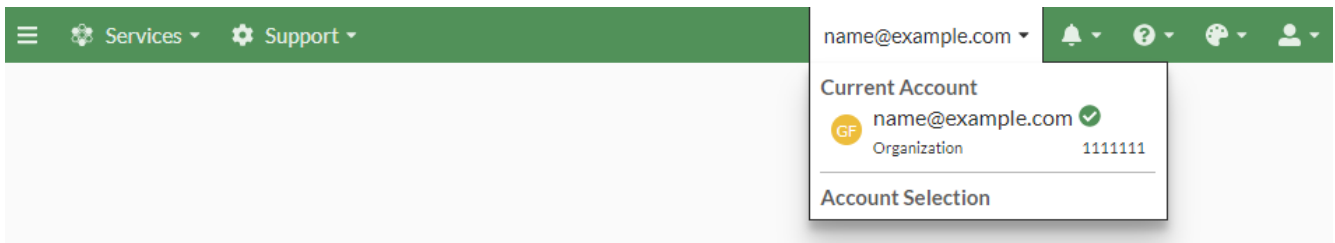


The top banner of the FortiGate CNF console provides access to the following information and functionality:

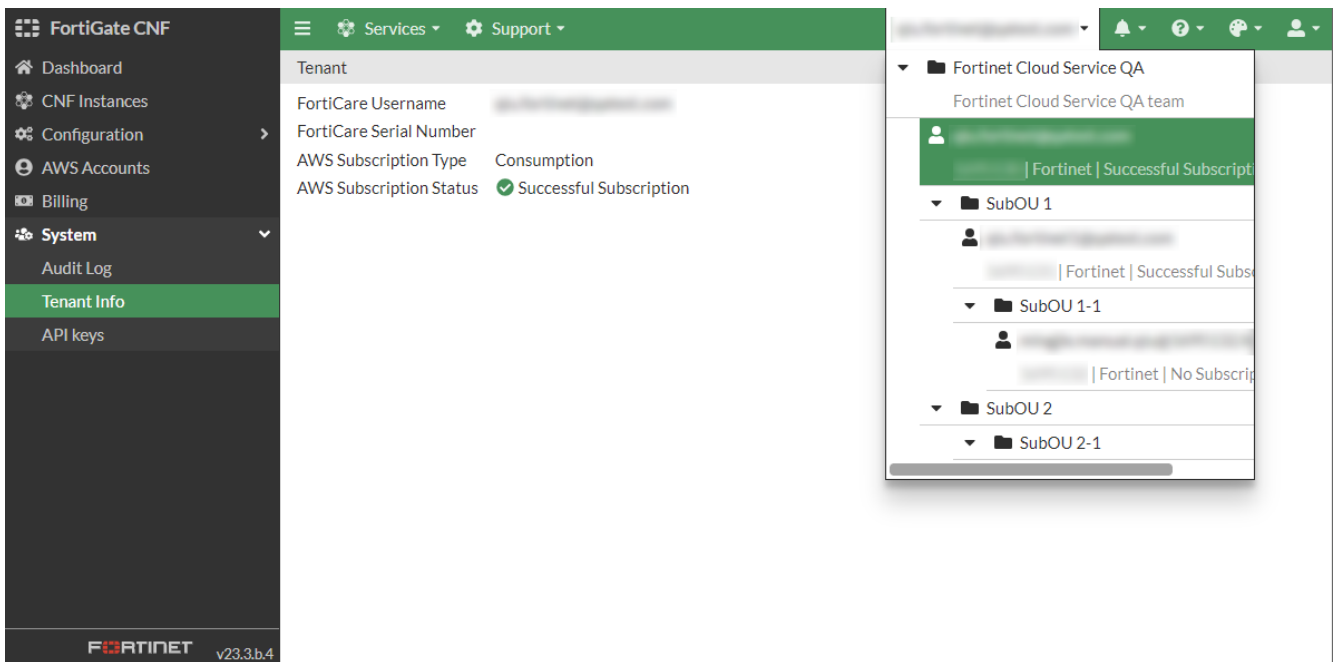
- [User menu on page 22](#)
- System notifications
- [Online help on page 23](#)
- [Theme selection menu on page 23](#)
- [Account menu on page 23](#)

User menu

View the username and account information of the currently logged in user.



If this account is part of an organization, use this menu to switch to another account.

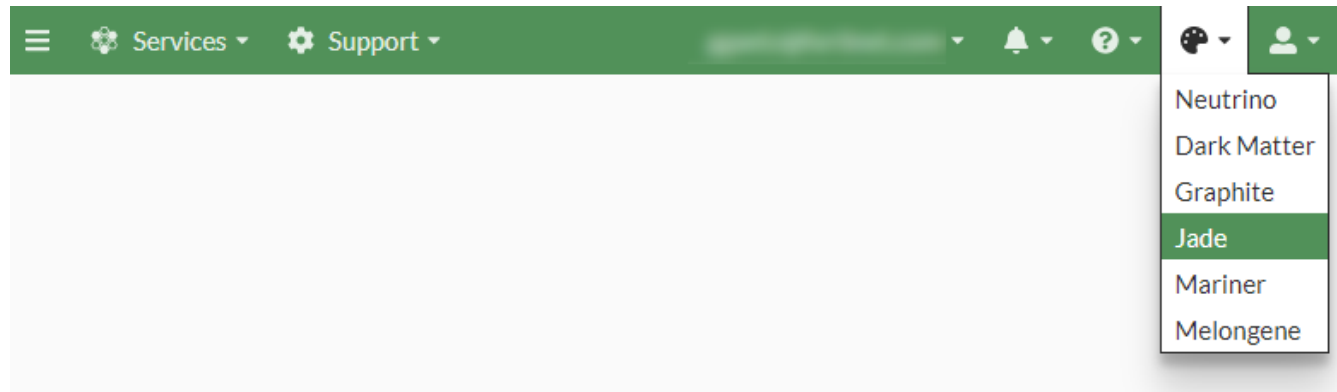


Online help

From any page in the FortiGate CNF console, click *Online Help* to see documentation relevant to the current page.

Theme selection menu

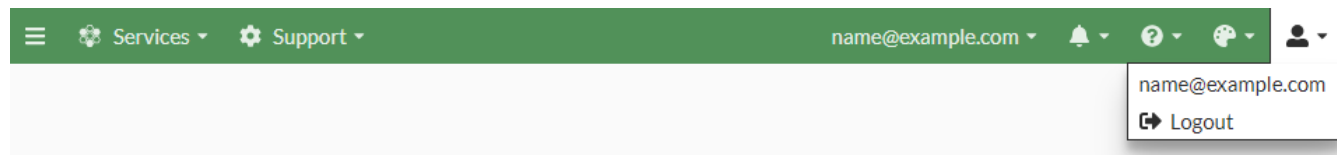
Change the FortiGate CNF console theme.



Account menu

The account menu displays the account username and provides access to the following:

- *Logout*: Log out of FortiGate CNF.

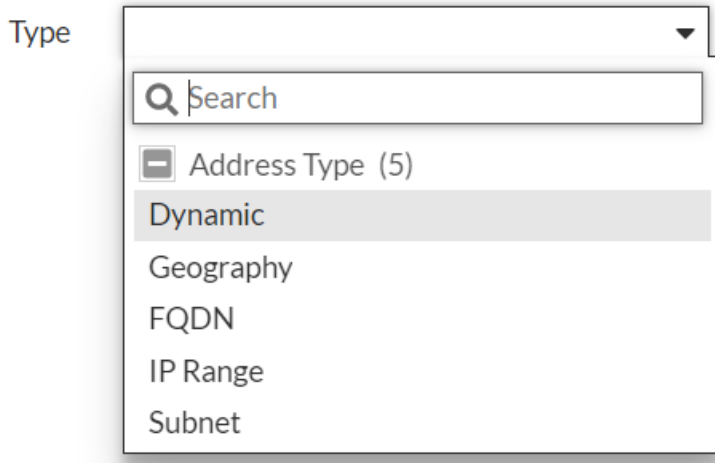


Forms

Forms and form elements in the FortiGate CNF console have the following functionality.

Select fields

Dropdown select fields allow the selection of an item from a list of options.



Search

Form select fields contain a search field at the top of the dropdown.

- Enter search terms in the field and press enter to search.
- Click the X at the end of the field to clear the search.

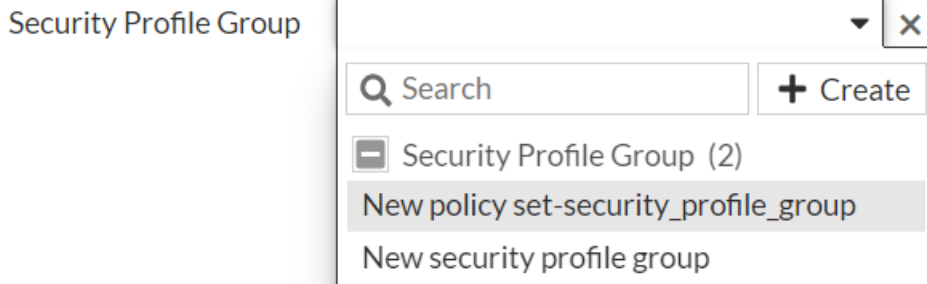
Categories

Some select fields contain items grouped by category. The category title displays the number of items within that category in parentheses.

Expand or hide the items within a category by clicking the category name.

Create

Some select fields include a *Create* button to create a new object of this type. Click *Create* to open the object creation pane without leaving the current form.



Select object fields

Form fields that allow the selection of one or more objects will open an object selection pane. These fields are displayed as a text field with a + icon in the center.

Source

Object selection pane

Click within the field to open the object selection pane.

The screenshot shows two overlapping windows. The background window is titled 'Create New Policy' and contains the following fields:

- Name:
- Source: (with a '+' icon)
- Destination: (with a '+' icon)
- Service: (with a '+' icon)
- Action: ACCEPT DENY (radio buttons)
- Security Profile Group: (with a dropdown arrow and an 'X' icon)

The foreground window is titled 'Select Entries' and contains:

- A search bar with a magnifying glass icon and the text 'Search'.
- A '+ Create' button.
- A list of objects:
 - Source (15)
 - Address (13)
 - all
 - Canada
 - FABRIC_DEVICE
 - FIREWALL_AUTH_PORTAL_ADDRESS
 - gmail.com
 - login.microsoft.com
 - login.microsoftonline.com
 - login.windows.net
 - metadata-server
- Buttons at the bottom: 'Reset', 'OK', 'Cancel', and 'Close'.

In the object selection pane, the following actions are available:

- **Select:** select one or more objects. When clicked, they are added to the form field.
- **Search:** search for objects within the list.
- **Create:** Create a new object of this type. For more information about creating objects, see [Configuration on page 62](#).



Adding and removing items

Click on an item in the object selection pane to add it to the form.

Click the X on an item to remove it from the form.

Tables

Tables can be filtered, sorted, and customized to display particular columns. A common set of functionality is available for all tables.

Name 	Modified At 
allow_all	2022/10/25 11:42:01
Test policy set 2	2022/10/28 12:58:53
Test policy set 3	2022/10/28 15:42:09
Test policy set 6	2022/11/16 10:17:19

4 | Updated: 10:22:48 

Refresh the displayed data

Click the *Refresh* button to refresh the table content.

Filter the displayed data

Filters are used to locate a specific set of information or content in a table. Filtering options vary depending on the information presented in the table.

Applied filters are listed in the *Search* field.

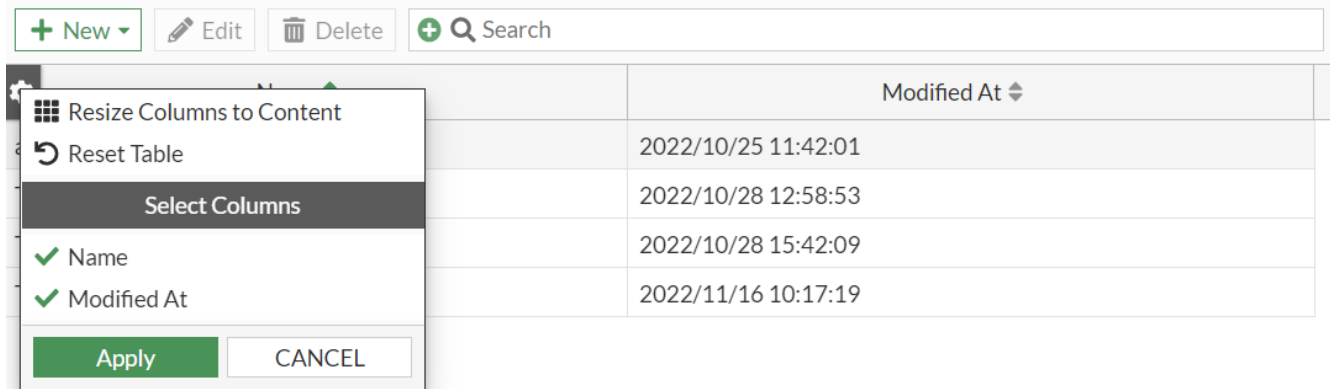
Enter a term in the Search field to filter the report by search term.

Click the green + icon to apply a filter to the report.

Click the X next to an applied filter to remove it.

Configure table display

Hover over the left end of the column headers and click the gear icon to configure the table.



The following configuration options are available:

- *Resize Columns to Content*: Automatically set the width of each column to fit the content.
- *Reset Table*: Reset table display modifications to the default.
- *Select Columns*: Select which columns to display. Displayed columns are marked with a green checkmark.
- *Apply*: Click to apply any changes to the table.
- *Cancel*: Exit the form without saving or applying any changes.

Sort

Sortable columns are noted with a stacked triangle icon next to the column name.

Click on a column header to sort the table by that column in ascending or descending order.

Click the same header again to reverse the sort direction.

Item selection

Click on a row in the table to select it.

Right-click a row to access the context menu for that item.

Double-click a row to open that item. If the item is editable it opens in an editing form.

Table footer

The table footer contains the following information and actions:

- *Count*: The footer displays a count of the number of items displayed in the table.
- *Updated*: Displays the time when the table information was last updated.
- *Refresh*: Click the *Refresh* icon to update the table information.

Charts

Charts are used to display summarized information.

Click on an item in the chart legend to toggle the display of that item.

Product registration and technical support

Before contacting technical support, you must first register your FortiGate CNF serial number with [FortiCare](#).

To find your serial number:

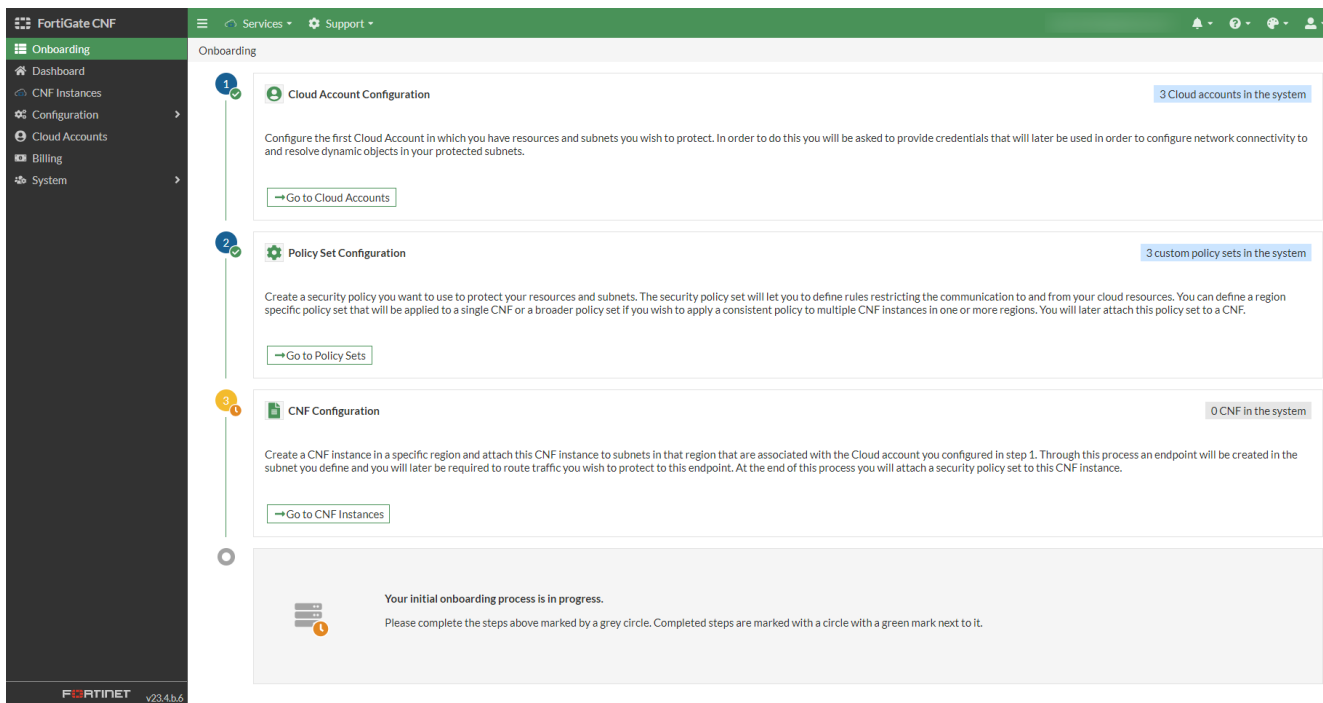
1. In the FortiGate CNF console, go to *System > Tenant Info*.
2. Find the serial number in the *FortiCare Serial Number* field.

Tenant	
FortiCare Username	name@example.com
FortiCare Serial Number	111111111111
AWS Subscription Type	Contract
AWS Subscription Status	✔ Successful Subscription

Onboarding

The onboarding wizard walks you through the initial FortiGate CNF configuration process, from adding your cloud accounts to deploying a configured FortiGate CNF instance.

On your first login, if you have no FortiGate CNF instances configured or running, you are presented with the wizard.



The wizard guides you through the following steps:

1. Add your cloud accounts.

Before any FortiGate CNF instances can be deployed to protect your cloud networks, you must add the cloud accounts that contain the resources you wish to protect. FortiGate CNF requires access permissions to perform various tasks, such as deploying FortiGate CNF endpoints, resolving IP addresses of resources, and sending logs to an AWS S3 bucket or Azure blob storage.

You are guided through each of the steps involved, including configuring the AWS CloudFormation template or Azure ARM template and creating the FortiGate CNF stack.

2. Create your first policy set.

Security policies are grouped into a policy set and provide the rules that control the traffic flow through the FortiGate CNF instance.

The wizard guides you through the steps needed to define your first policy set.

3. Create a FortiGate CNF instance.

The wizard guides you through the steps to create and deploy a FortiGate CNF instance and connect it to your subnets. This creates an endpoint in a subnet in one of the cloud accounts you added in step one.

After each step is completed, and when you have successfully completed the entire process, a success message is displayed.

You can leave and return to the wizard at any time, and you may repeat steps.

Once you have successfully completed the onboarding process, the *Onboarding* menu and page will no longer be available.

Dashboard

The *Dashboard* displays the following widgets:

- [License Information on page 31](#)
- [Annual Credits Information on page 31](#)
- [CPU on page 31](#)
- [Bandwidth on page 32](#)
- [CNFs per region on page 32](#)
- [Protected subnets on page 33](#)
- [Memory on page 34](#)

For FortiGate CNF system status, see [Service health dashboard on page 35](#).

License Information

View information about the FortiGate CNF account. The following information is displayed:

- *FortiCare Username*
- *FortiCare Serial Number*
- *AWS Subscription Status*
- *AWS Subscription Type*

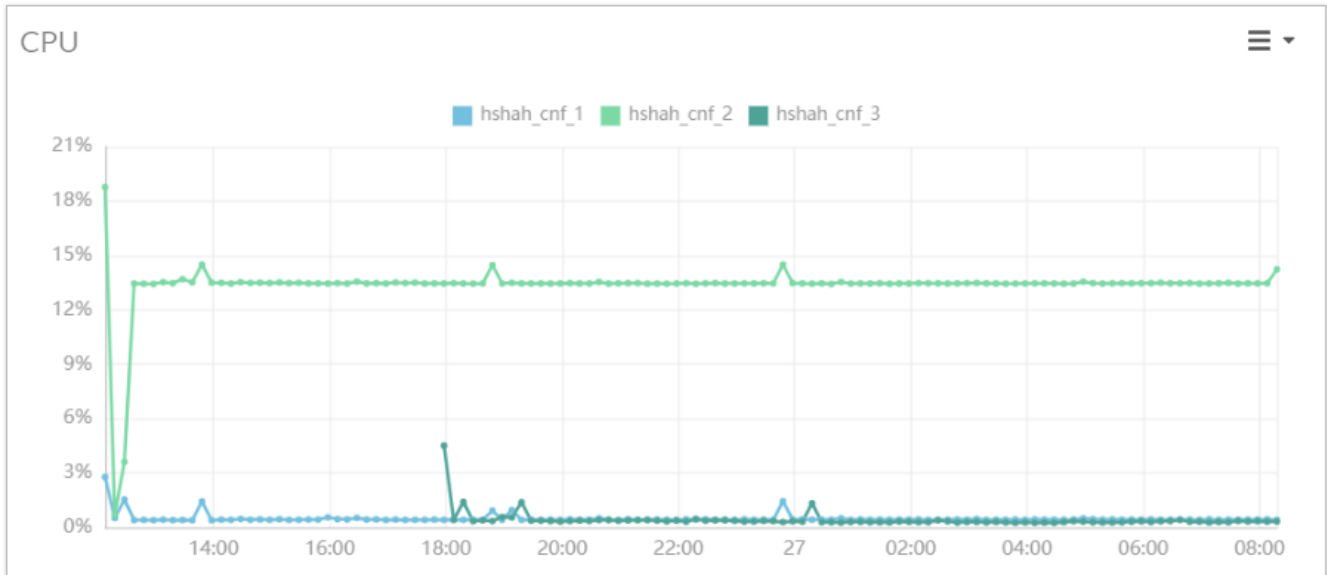
Annual Credits Information

View information about the available credits for your annual subscription.

The widget title displays *Free Trial Information* if you are using a free trial subscription.

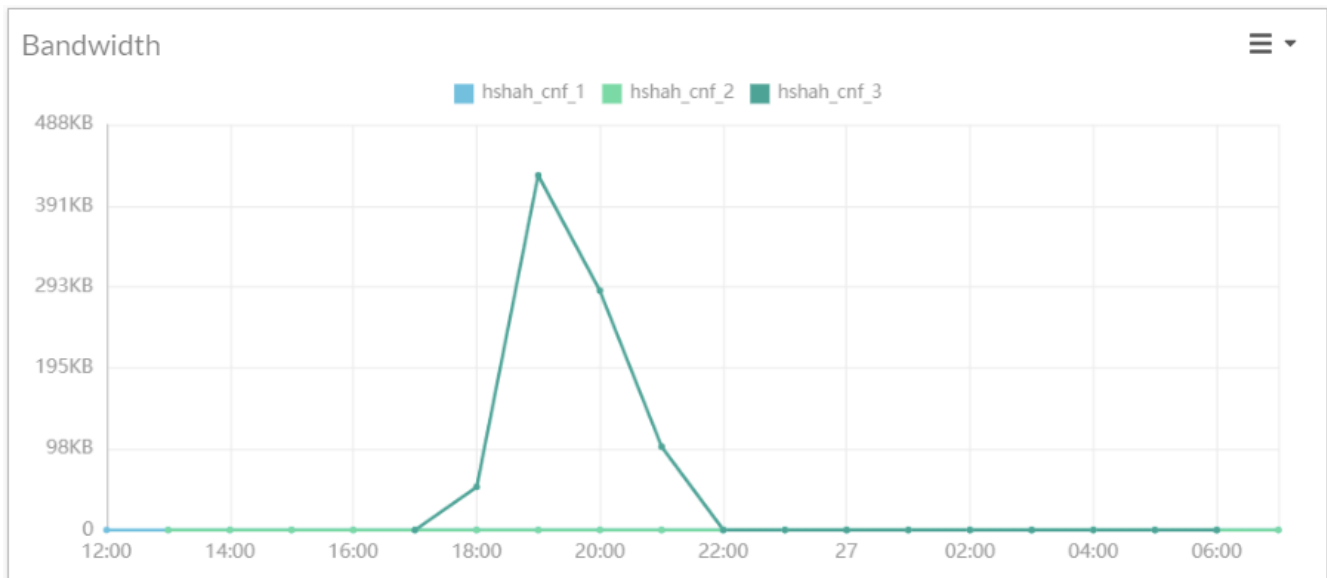
CPU

View the average CPU utilization for each FortiGate CNF instance in the past 24 hours.



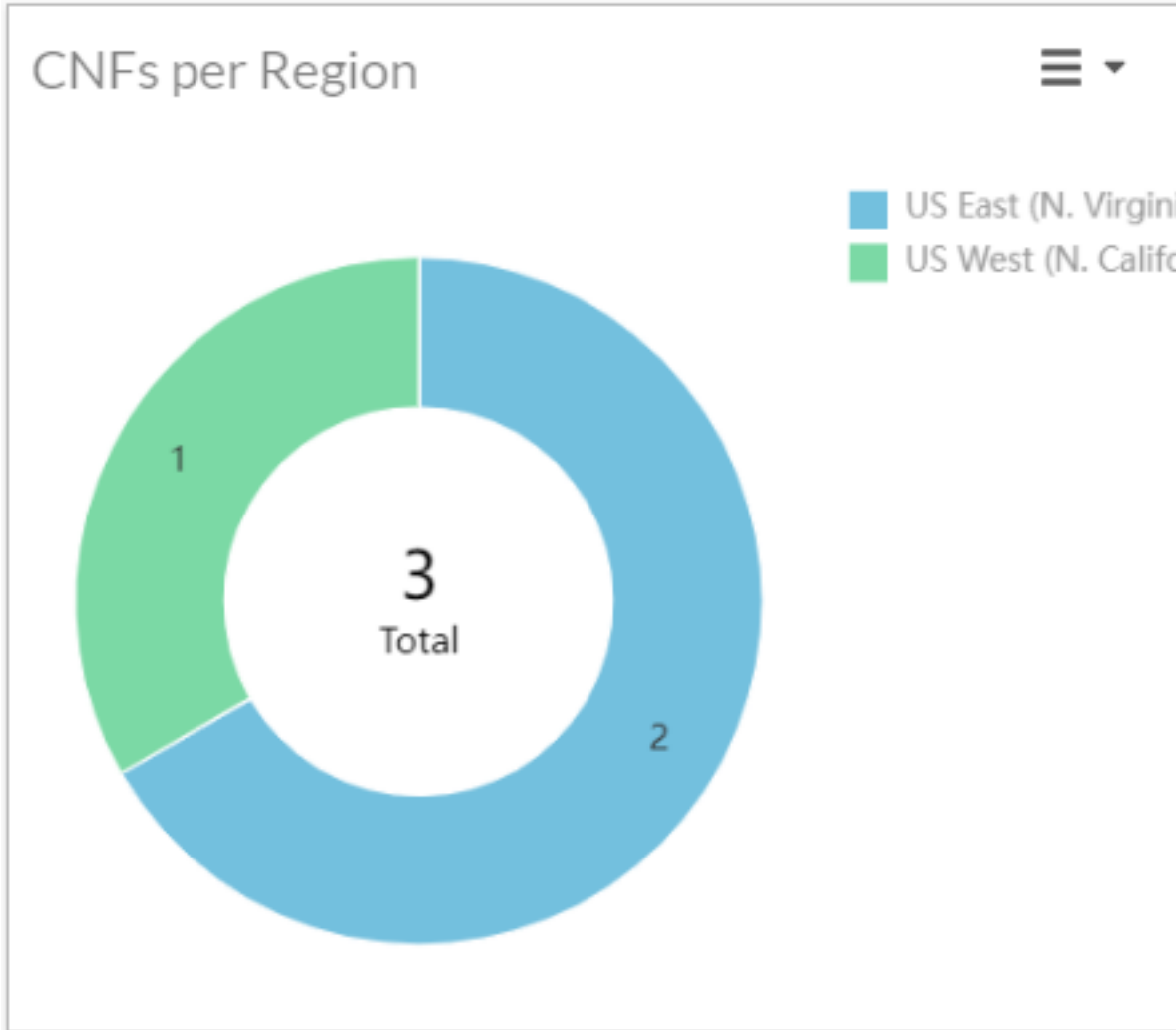
Bandwidth

View bandwidth usage in the past 24 hours.






CNFs per region


View the number of FortiGate CNF instances deployed in each region.



Protected subnets

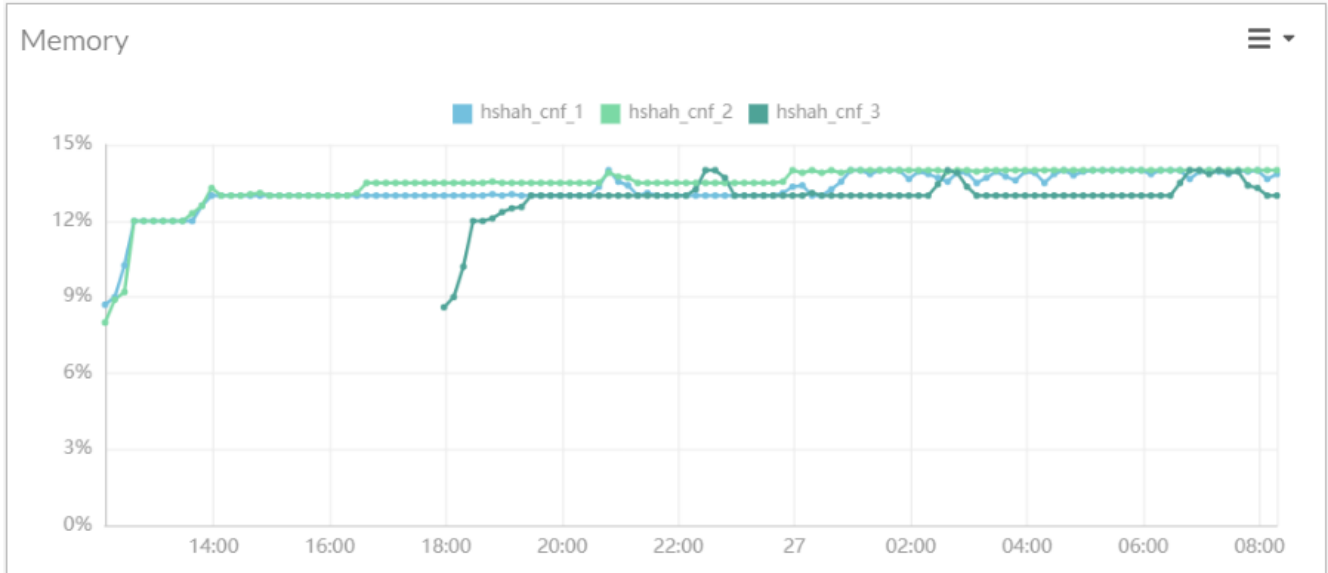
View the number of protected subnets in each availability zone (AZ).

Protected Subnets 	
AZ 	Count 
usw1-az1	1

1 | Updated: 08:28:55 

Memory

View the aggregate memory utilization for each FortiGate CNF instance in the past 24 hours.



Service health dashboard

To view FortiGate CNF system status, go to <https://status.fortigatecnf.com/>.

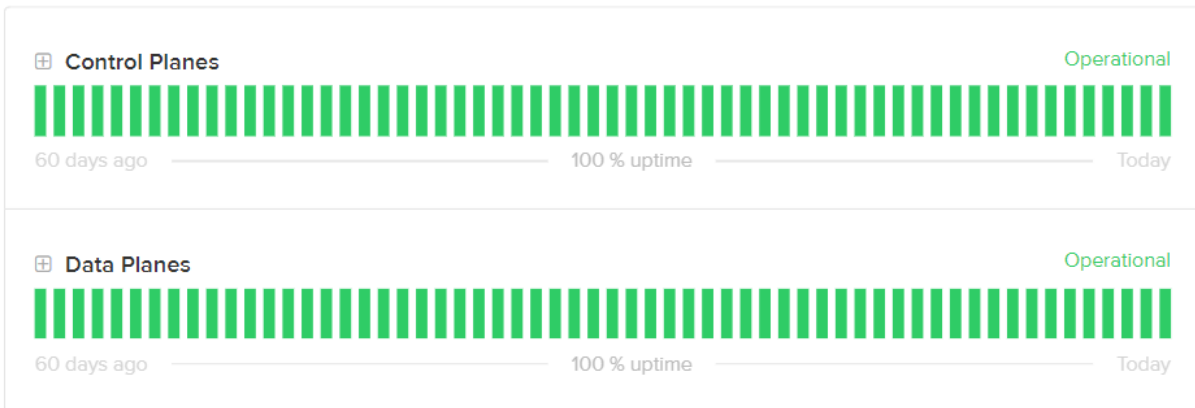


FortiGate
Cloud-Native Firewall

SUBSCRIBE TO UPDATES

All Systems Operational

Uptime over the past 60 days. [View historical uptime.](#)



The service health dashboard displays the following information:

- System health information for each of the control and data planes.
- Notices about upcoming scheduled maintenance.
- Historical information about past incidents.



Click *SUBSCRIBE TO UPDATES* to receive system status updates through any of the following methods:

- Email
- SMS
- Slack
- Atom or RSS feed

CNF instances

The *CNF Instances* page lists the FortiGate CNF instances that have been created.

From this page you can:

- [Create and deploy a new instance.](#)
- [View and edit instance details.](#)
- [Delete an instance.](#)
- [View policy set revisions for an instance.](#)
- [Save an instance as a template.](#)
- [Sync policy sets.](#)
- [Configure Route 53 resolver rules](#)
- [Schedule upgrades.](#)
- [Troubleshoot instances.](#)

Deploying a FortiGate CNF instance

FortiGate CNF instances can be deployed into AWS or Azure. The same general procedure applies to both.

To create and deploy a new FortiGate CNF instance, use the following procedure:

1. Create a new instance.
 - AWS: See [Creating a new AWS FortiGate CNF instance on page 38.](#)
 - Azure: See [Creating a new Azure FortiGate CNF instance on page 39.](#)
 - From a template: See [Creating a new FortiGate CNF instance from a template on page 39.](#)
2. Add endpoints:
 - AWS: See [Adding an endpoint to an AWS instance on page 40.](#)
 - Azure: See [Adding an endpoint to an Azure instance on page 41.](#)



You may create any number of load balancers, allowing for multiple workloads to be protected by the same FortiGate CNF instance. If a different policy set is needed for a load balancer, create a new FortiGate CNF instance with the needed policy set for that load balancer.

3. Configure policy sets. See [Configuring policy sets on page 42.](#)

See [Editing or viewing a FortiGate CNF instance on page 42](#) for more information about instance settings.



For some detailed deployment examples, see [Deployment scenarios on page 82.](#)

Instances are deployed into your cloud infrastructure using gateway load balancer endpoints (in the case of AWS) or load balancers (in the case of Azure).

In the *Configure Endpoints/Load Balancers* page, select an endpoint or load balancer and click *Edit* to view or edit the details. Click *Delete* to remove the endpoint or load balancer from the instance.

Creating a new AWS FortiGate CNF instance

To create a new AWS FortiGate CNF instance:

1. In *CNF Instances*, click *New* and select *AWS*.
2. In *CNF Name*, enter a unique name for this instance.
3. Select the appropriate *Region*. This ideally is in the same region as the workload, but may be different for some configurations, such as east-west traffic.

For more information about possible deployment scenarios, see [Deployment scenarios on page 82](#).

4. Enable or disable *FortiManager mode*. For more information, see [FortiManager mode on page 54](#).



If FortiManager mode is enabled when creating a FortiGate CNF instance, policy management for this instance is disabled in the FortiGate CNF console.

You will be provided with the IP address and login credentials to the FortiGate, which you can use to add the device to FortiManager.

5. Set *Internal Logging* to one of the following options:

- *None*: Disable internal logging.
- *S3 Bucket*: Enable logging to the AWS account S3 bucket, then select the S3 Bucket in *Log Traffic to S3 Bucket*.
- *Security Lake*: Enable logging to AWS Security Lake, then select the destination Security Lake in *Log Traffic to Security Lake*.



FortiGate CNF does not create a Security Lake destination. You must create it and enable access using the CloudFormation template.

In the CloudFormation *Stack Details*, set *SecurityLakeCustomLogSourceName* to your Security Lake custom source.

See [Configuring Security Lake on page 76](#).

6. In *External Logging*, select one of the available options:

- *None*: disable external logging.
- *External Syslog*: Enter the *External Syslog Server IP*.
- *FortiAnalyzer*: Enter the *FortiAnalyzer IP*.

For more information about FortiGate log messages and formats, see [the FortiOS Log Message reference](#).

7. Optionally, add endpoints. For more information about endpoints, see [Adding an endpoint to an AWS instance on page 40](#).
8. Click *OK*.

The *CNF Instances* list displays, with the new instance having a status of *Initializing*. After the instance has initialized, the status changes to *Active* and the instance can be configured with endpoints and policy sets.

In the background, the FortiGate CNF instances and other infrastructure are created. This process takes approximately 10 minutes.

Creating a new Azure FortiGate CNF instance

To create a new Azure FortiGate CNF instance:

1. In *CNF Instances*, click *New* and select *Azure*.
2. In *CNF Name*, Enter a unique name for this instance.
3. Select the region where the instance will be deployed, which is the region containing the workload. East-west configurations in Azure are not supported.

For more information about possible deployment scenarios, see [Deployment scenarios on page 82](#).

4. Enable or disable *FortiManager mode*. For more information, see [FortiManager mode on page 54](#).



If FortiManager mode is enabled when creating a FortiGate CNF instance, policy management for this instance is disabled in the FortiGate CNF console.

You will be provided with the IP address and login credentials to the FortiGate, which you can use to add the device to FortiManager.

5. In *Internal Logging > Blob Storage Logging*, enable or disable logging to Azure blob storage.

6. In *External Logging*, select one of the available options:

- *None*: disable external logging.
- *External Syslog*: Enter the *External Syslog Server IP*.
- *FortiAnalyzer*: Enter the *FortiAnalyzer IP*.

For more information about FortiGate log messages and formats, see [the FortiOS Log Message reference](#).

7. Optionally, add endpoints. For more information about endpoints, see [Adding an endpoint to an Azure instance on page 41](#).
8. Click *OK*.

The *CNF Instances* list displays, with the new instance having a status of *Initializing*. After the instance has initialized, the status changes to *Active* and the instance can be configured with endpoints and policy sets.

In the background, the FortiGate CNF instances and other infrastructure are created. This process takes approximately 10 minutes.

Creating a new FortiGate CNF instance from a template

To create a new FortiGate CNF instance from a template:

1. In *CNF Instances*, click *New* and select *Template*.
2. In *Configuration > CNF Templates*, select a template and click *Create CNF*.
3. Update *CNF Name* with a unique name for this instance.
4. Update other configuration as needed for the instance type.
 - For AWS instances, see [Creating a new AWS FortiGate CNF instance on page 38](#).
 - For Azure instances, see [Creating a new Azure FortiGate CNF instance on page 39](#).
5. Click *OK*.

The *CNF Instances* list displays, with the new instance having a status of *Initializing*. After the instance has initialized, the status changes to *Active* and the instance can be configured with endpoints and policy sets. In the background, the FortiGate CNF instances and other infrastructure are created. This process takes approximately 10 minutes. Any errors are saved to the system audit log.

Adding an endpoint to an AWS instance

An endpoint is added to your VPC to route traffic to and from the FortiGate CNF instance.

To add an endpoint to an AWS instance:

1. In *CNF Instances*, select an instance and click *Edit*.
2. Click *Configure Endpoints*.
3. In the table, click *New*.
4. Enter a name for the endpoint, then select the appropriate AWS account.
5. In *VPC ID*, select the VPC to connect to.
6. In *Subnet*, select a subnet.



AWS subnets must be created and tagged in AWS before they are available in this form. In AWS, create a subnet in this VPC and tag it with *Key* = `fortigatecnf_subnet_type` and *Value* = `endpoint`.

7. Click *Save*. FortiGate CNF creates the endpoint, which may take several minutes. The status of the instance displays as *Active* when this process is complete.



You may create any number of endpoint subnets, allowing for multiple workloads to be protected by the same FortiGate CNF instance. If a different policy set is needed for an endpoint, create a new FortiGate CNF instance with the needed policy set for that endpoint.

Tags created

When an AWS endpoint is added, the following tags are created in the AWS account where the FortiGate CNF instance is deployed:

Tag	Sample value
Region	us-west-2
CNFId	2735
ManagedBy	FortiGate CNF
CNFName	AWS CNF example
Name	beta-c43-s2735-endpoint-subnet-0d1ce21403369975c

Adding an endpoint to an Azure instance

FortiGate CNF instances can protect resources with an Azure public IP: either a VM with a public IP or a load balancer with a public IP.

You must first create and configure the load balancer or VM in the Azure portal.

When you link the FortiGate CNF instance to the given public IP, FortiGate CNF routes traffic in or out of the public IP to the FortiGate CNF instance before sending the traffic to its destination. This does not create any additional resources in your specified resource group.



After linking a load balancer to an Azure FortiGate CNF instance, the following components of the load balancer are no longer editable in the Azure portal:

- Health probes.
- Backend pool instances and network interfaces.

There may be other components that cannot be edited depending on your Azure environment. If possible, configure the load balancer completely before linking to an FortiGate CNF instance.

See [Editing a linked load balancer on page 41](#).



FortiGate CNF does not support Azure *Basic* public IP. The public IP must be created as a *Standard* public IP.

To connect an existing public IP to an Azure instance:

1. In *CNF Instances*, select an instance and click *Edit*.
2. Click *Configure Azure Endpoints*.
3. In the table, click *Link Existing*.
4. Select the *Resource Type* from the following options:
 - *Load Balancer*: Connect to an Azure load balancer with a standard public IP.
 - *Virtual Machine*: Connect to a virtual machine with a standard public IP.
5. In *Account*, select the Azure account that contains the VM or load balancer.
6. Select the *Resource Group* that contains the VM or load balancer.
7. In *Load Balancer* or *Virtual Machine*, select the appropriate resource to link.
8. For a load balancer, select the appropriate *Frontend IP Configurations*.
For a virtual machine, select the appropriate *Network Interface*.
9. Click *OK*. FortiGate CNF connects to the resource, which may take several minutes. The status of the instance displays as *Active* when this process is complete.

Editing a linked load balancer

After linking a load balancer to an Azure FortiGate CNF instance, the following components of the load balancer are no longer editable in the Azure portal:

- Health probes.
- Backend pool instances and network interfaces.

There may be other components that cannot be edited depending on your Azure environment.

If possible, configure the load balancer completely before linking to an FortiGate CNF instance.

If you need to edit any of these components of a linked load balancer after linking to a FortiGate CNF instance, unlink the load balancer, make changes, then relink, as follows:

To edit the components of a linked load balancer:

1. In the FortiGate CNF console, unlink the load balancer from the FortiGate CNF instance:
 - a. In *CNF Instances*, select the instance and click *Edit*.
 - b. Click *Configure Azure Endpoints*.
 - c. In *Endpoints*, select the load balancer and click *Delete*.
2. In the Azure portal, edit the load balancer as needed.
3. In the FortiGate CNF console, link the load balancer to the FortiGate CNF instance. See [Adding an endpoint to an Azure instance on page 41](#).

Configuring policy sets

To configure policy sets:



The default *allow_all* policy set is pre-configured and automatically added to new instances. This policy is for the purpose of troubleshooting traffic routing and should not be used once traffic routing has been completed.

1. In *CNF Instances*, select an instance and click *Edit*.
 2. Click *Configure Policy Set*.
 3. In *Apply Policy Set*, select the policy set to apply and click *Save*. A new revision is created with the new policy set applied.
-



Only one policy set can be applied to an instance at a time.

For information about creating or editing policy sets, see [Policy sets on page 62](#).

Editing or viewing a FortiGate CNF instance


In the *CNF Instances* table, click *Edit* to view or edit the following instance details:

- [Primary details](#)
- [Endpoints \(AWS\) or load balancers \(Azure\)](#)
- [Route 53 resolver rules \(for AWS CNF instances\)](#)
- [Policy sets](#)

- [Instance Version](#)
- [Troubleshooting information](#)

Primary details

The following details are displayed in the *Edit CNF* form.

Item	Description
<i>CNF Name</i>	The unique name of the CNF instance. This field is editable.
<i>Region</i>	The region where this instance is deployed. This field is not editable.
<i>FortiManager mode</i>	Enable to manage this instance with FortiManager. This field is not editable.
<i>Status</i>	<p>The deployment status of the instance.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> • <i>Initializing</i>: The instance is being created and deployed. When an instance is initializing no details may be edited and the instance may not be deleted. • <i>Success</i>: The instance has been deployed. The instance may now be edited or deleted, and endpoints and policy sets may be added. • <i>Deleting</i>: The instance is being deleted. When deletion is complete the instance is removed from the table. • <i>Error</i>: You must delete and begin again. • <i>Policy Set Apply Error</i>: There was an error applying the policy set.
<i>Internal Logging</i>	<p>Set <i>Internal Logging</i> to one of the following options:</p> <ul style="list-style-type: none"> • <i>None</i>: Disable internal logging. • <i>S3 Bucket</i>: Enable logging to the AWS account S3 bucket, then select the S3 Bucket in <i>Log Traffic to S3 Bucket</i>. This option is available if this instance is an AWS CNF instance. • <i>Security Lake</i>: Enable logging to AWS Security Lake, then select the destination Security Lake in <i>Log Traffic to Security Lake</i>. This option is available if this instance is an AWS CNF instance. <hr/> <div style="display: flex; align-items: center;">  <p>FortiGate CNF does not create a Security Lake destination. You must create it and enable access using the CloudFormation template. In the CloudFormation <i>Stack Details</i>, set <i>SecurityLakeCustomLogSourceName</i> to your Security Lake custom source. See Configuring Security Lake on page 76.</p> </div> <hr/> <ul style="list-style-type: none"> • <i>Blob Storage Logging</i>: Enable logging to Azure storage. This option is available if this instance is an Azure CNF instance.
<i>External Logging</i>	The selected external logging destination. Select from <i>None</i> , <i>External Syslog</i> , and <i>FortiAnalyzer</i> . This field is editable.

Item	Description
<i>External Syslog Server IP</i>	The IP address of the syslog server where logs are sent. This field is editable and only displays if <i>External Logging</i> is set to <i>External Syslog</i> .
<i>FortiAnalyzer IP</i>	The IP address of the FortiAnalyzer where logs are sent. This field is editable and only displays if <i>External Logging</i> is set to <i>FortiAnalyzer</i> .
<i>Display Primary FortiGate Information</i>	<p>Enable to display the following connection information:</p> <ul style="list-style-type: none"> • <i>Primary FGT IP</i> • <i>Primary FGT Username</i> • <i>Primary FGT Password</i> <p>This field only displays when <i>FortiManager mode</i> is enabled.</p>

Endpoints and load balancers

FortiGate CNF instances are deployed into your cloud infrastructure using gateway load balancer endpoints (in the case of AWS) or load balancers (in the case of Azure).

In the *Configure Endpoints/Load Balancers* page, select an endpoint or load balancer and click *Edit* to view or edit the details. Click *Delete* to remove the endpoint or load balancer from the instance.

- [Endpoints on page 44](#)
- [Load balancers on page 45](#)

Endpoints

Item	Description
<i>Name</i>	The name of the endpoint. The name must be unique within the CNF instance and does not affect the subnet. This field is only editable if <i>Status</i> is <i>error</i> .
<i>Account</i>	The AWS account in which the VPC has been created. This field is not editable after the endpoint has been created.
<i>VPC ID</i>	The AWS identifier for the VPC. This field is not editable.
<i>Subnet</i>	The subnet within the VPC. This field is not editable.
<i>Select from all subnets</i>	<p>Disable to display only endpoints that have been tagged with <i>Key = fortigatecnf_subnet_type</i> and <i>Value = endpoint</i>.</p> <p>Enable to display all subnets in the selected VPC.</p>
<i>Status</i>	<p>The deployment status of the endpoint.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> • <i>Initializing</i>: The endpoint is being added to the instance. When an endpoint is initializing no details may be edited. • <i>Active</i>: The endpoint has been added and may now be edited or deleted. • <i>Deleting</i>: The endpoint is being deleted. When deletion is complete the endpoint is removed from the table. • <i>Error</i>: You must delete and begin again.

Load balancers

Item	Description
<i>Name</i>	The name of the load balancer. The name must be unique within the CNF instance and does not affect the subnet. This field is editable.
<i>Account</i>	The Azure account containing the resources to be protected. This field is not editable after the load balancer has been created.
<i>Resource Group</i>	The Azure resource group. This field is not editable after the load balancer has been created.
<i>Subnet</i>	The subnet within the VPC. This field is not editable.
<i>Select from all subnets</i>	Disable to display only endpoints that have been tagged with <i>Key</i> = <code>fortigatecnf_subnet_type</code> and <i>Value</i> = <code>endpoint</code> . Enable to display all subnets in the selected VPC.
<i>Status</i>	The deployment status of the endpoint. The possible values are: <ul style="list-style-type: none"> • <i>Initializing</i>: The endpoint is being added to the instance. When an endpoint is initializing no details may be edited. • <i>Active</i>: The endpoint has been added and may now be edited or deleted. • <i>Deleting</i>: The endpoint is being deleted. When deletion is complete the endpoint is removed from the table. • <i>Error</i>: You must delete and begin again.

Policy sets

In the *Configure Policy Sets* page, view and update the applied policy set for the instance.

The following information is displayed in the form.

Item	Description
<i>Current Policy Set</i>	The name of the policy set currently applied to the CNF instance.
<i>Revision ID</i>	The ID of the current CNF instance revision. Changing the applied policy set creates a new revision. Click the <i>View Policy Set Revision</i> eye icon to view more information about the revision. See Viewing a policy set revision on page 46 for more information.
<i>Installation Status</i>	The status of the policy set installation on the instance. The possible values are: <ul style="list-style-type: none"> • <i>Installing</i>: The policy set is being deployed to the instance and a new instance revision is being created. • <i>Installed</i>: The policy set has been installed. A new revision of the instance has been created and deployed.
<i>Sync Status</i>	The synchronization status of the policy set.

Item	Description
	<p>The possible values are:</p> <ul style="list-style-type: none"> • <i>Unsynchronized</i>: Changes have been made in the FortiGate CNF console that have not been applied to this instance. <ul style="list-style-type: none"> • Click the <i>Diff</i> button to view the changes. • Click the <i>Synchronize</i> button to update the policy set on the instance. • <i>Synchronized</i>: The deployed policy set matches the local policy set.
<i>Apply Policy Set</i>	<p>Select the policy set to apply.</p> <p>Click <i>Diff</i> to the a comparison with the currently installed policy set.</p>
<i>Policy Set Revision History</i>	<p>Displays a list of the policy set that has been applied by revision, in descending order beginning with most recent.</p> <p>The following actions are available:</p> <ul style="list-style-type: none"> • <i>View</i>: Select a revision and click <i>View</i> (or double-click the revision row) to see details about the policy set in this revision. See Viewing a policy set revision on page 46 for more information. • <i>Diff</i>: Select two revisions and click <i>Diff</i> to review the changes. See Viewing the policy set revision diff on page 47 for more information.

Instance Version

The *Instance Version* page displays the FortiOS version of the FortiGate CNF instance in the *Current Dataplane FortiOS Version* field.

Deleting a CNF instance

To delete a CNF instance:

In the *CNF Instances* table, select an instance and click *Delete*. In the *Confirmation* dialog, click OK to confirm the deletion.

The deletion may take several minutes.

Viewing a policy set revision

The *Policy Set Revision* pane displays read-only information about the policy set for a particular revision.



Policy set revisions are revisions of the policy set as applied to an instance. Policy sets, policies, and objects themselves are not versioned.

Policy Set Revision ✕

Test policy set 3 ✔ Installed

Policies Addresses Services Security Profiles

+ 🔍 Search

Name	Source	Destination	Service	Action	Sec. Profile	Status
Test policy set-default-policy	all	all	ALL	✔ ACCEPT	Test policy set-security_profile_group	✔ Enabled

The header displays the policy set name, the policy set revision number, and the policy set installation status.

The information is displayed in the following tabs:

- **Policies:** Displays the list of policies in this policy set. See [Policy sets on page 62](#) for more information about policies and policy sets.
- **Addresses:** Displays the address objects (IP address ranges, FQDNs, Subnets. and address groups) used in the policy set. See [Addresses on page 65](#) for more information.
- **Services:** Displays the service objects used in the policy set. See [Services on page 67](#) for more information.
- **Security Profiles:** Displays the security profiles used in the policy set. See [Security profiles on page 69](#) for more information.

Within each category, double-click on an item to see more details.

Viewing the policy set revision diff

The *Policy Set Diff* displays the changes from one revision to another.

Policy Set Diff ✕

Revision ID 2	Revision ID 1
Policy Set Test policy set	Policy Set allow_all
Installation Status ✔ Installed	Installation Status ✔ Installed
Created At 2022-11-22 13:52:13	Created At 2022-11-22 13:14:41

Name	Change Type	Detail
☰ Ips Sensor 1		
intrusion_prevention-72	Added	👁 View Details
☰ Policy 2		
Test policy set-default-policy	Added	👁 View Details
allow_all	Deleted	👁 View Details

3 | Updated: 05:29:48 🔄

The report displays the changes that have been made to get from the revision on the right to the revision on the left.



If the report is displaying an unsynchronized policy, the report displays the changes that have been made to get from the revision on the left to the revision on the right.

The header section of the pane displays information about the two revisions being compared. If the diff is being displayed for policy set changes that have not been synchronized yet, the policy on the right will only display the policy set name.

Click on *View Details* in an item to view detailed information about the item that has been added or removed. For more information about the CLI output displayed in the detail, see the [FortiOS CLI Reference](#).

Policy Detail

```

Rev {
Pol  "name": "intrusion_prevention-72",
Inst "block-malicious-url": "enable",
Cre  "scan-botnet-connections": "disable"

```

intr

Tes

allo

Saving a FortiGate CNF instance as template

Save a FortiGate CNF instance as a template.

The following configuration is saved:

- The FortiGate CNF instance name is saved as the template name.
- Logging configuration

- Any FortiManager association.
- Attached VPCs and subnets, including the entire configuration of endpoints or load balancers.

The deployed security policy is not included. You will need to deploy a policy set to any instances created from the template.

Any errors are saved to the system audit log.

To save a FortiGate CNF instance as a template:

In *CNF Instances*, select an instance and click *Save as Template*.

The template is saved and displayed.

Synchronizing policy sets

When a policy set is changed locally in the FortiGate CNF console, CNF instances are not automatically synchronized with the updated policy set.

To synchronize a policy set:

In *CNF Instances*, select the instance and click *Sync Policy Set*.

Alternatively, in the instance *Configure Policy Set* form, click *Synchronize*.

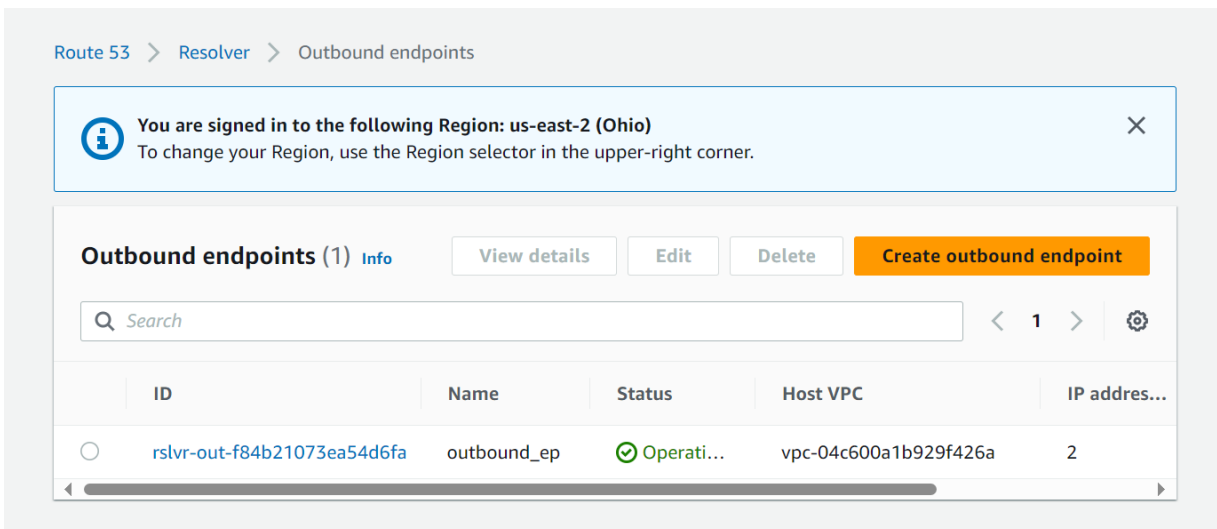
The policy set changes are synchronized to the instance and a new revision is created and deployed.

Configuring Route 53 resolver rules

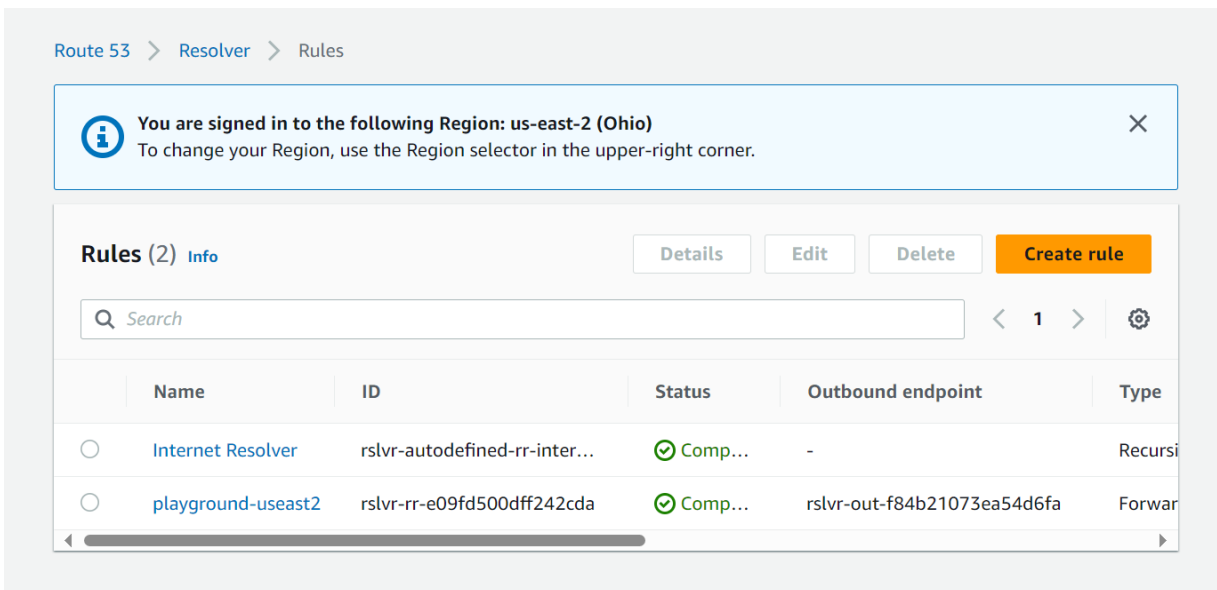
You can share AWS Route 53 DNS forwarding rules with your FortiGate CNF instances. This allows FortiGate CNF to resolve DNS addresses in your environment instead of resolving them independently.

To configure and share Route 53 forwarding rules:

1. In AWS Route 53, configure DNS forwarding rules:
 - a. In AWS Route 53 create an outbound endpoint for DNS requests.



- b. Create a rule forwarding DNS requests through the outbound endpoint to your DNS server.



- c. In AWS Resource Access Manager, share the DNS forwarding rule with the FortiGate CNF instance AWS account.

[Resource Access Manager](#) > Shared by me: Resource shares

Shared by me: Resource shares

Resource shares owned by your account.

Resource shares (2)

1

	Name	ID	Owner	Allow external principals	Status
<input type="radio"/>	MyRuleShare	ac1d6c89-2ea0-41e1-85be-5f1b37c4591a		Yes	✔ Active
<input type="radio"/>	cnf-share	dcf46796-d4b1-4066-99bf-dd5e99239ff6		Yes	✔ Active

Summary

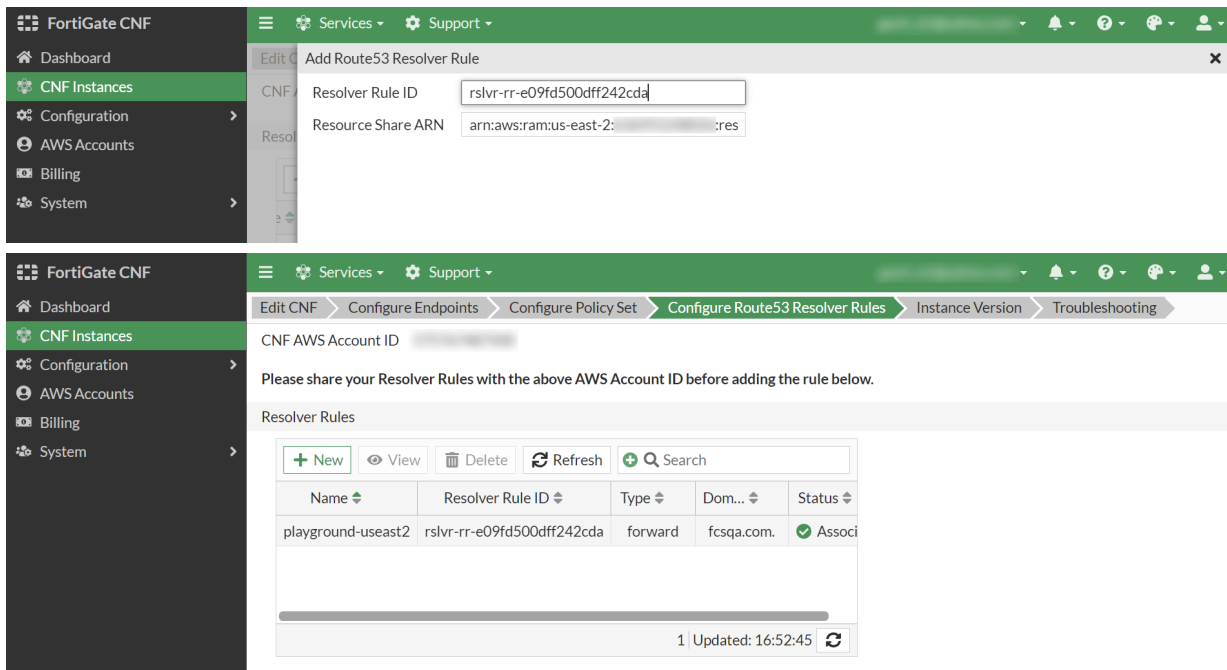
Name cnf-share	Owner [Redacted]	Created on 2023/10/17	Status ✔ Active
ID dcf46796-d4b1-4066-99bf-dd5e99239ff6	ARN arn:aws:ram:us-east-2:[Redacted]:resource-share/dcf46796-d4b1-4066-99bf-dd5e99239ff6	Allow external principals Yes	

Shared resources (1)

1

	Resource ID	Resource type	Status
<input type="checkbox"/>	rslvr-rr-e09fd500dff242cda	route53resolver:ResolverRule	✔ Associated

2. In the FortiGate CNF console, add the forwarding rule to a FortiGate CNF instance.
 - a. In *CNF Instance*, select an instance and click *Edit*.
 - b. In *Configure Route53 Resolver Rules*, click *New*.
 - c. Enter the *Resolver Rule ID* and *Resource Share ARN* of the shared rule, then click *OK*.



The rule is attached to the VPC where the FortiGate CNF instance is deployed. This rule is used for forwarding DNS requests to the specified DNS server.

Scheduling FortiGate CNF instance upgrades

When a new FortiGate CNF instance version is released, an upgrade will be scheduled by Fortinet. You can change the timing of your instance upgrade from within a 30-day window.

When a FortiGate CNF instance version upgrade is planned, your existing instances can use the older (current) version up to the final day of the available upgrade window.



The FortiGate CNF instance will go down for approximately five minutes during the upgrade.

For a regular upgrade, if you do not schedule the upgrade, the system will automatically perform the upgrade at the end of the available upgrade time window.

Rollback

If the upgrade of the FortiGate CNF instance is incompatible with your network configuration, you may roll back the upgrade to the previous version.

The rollback feature is available for seven days after an upgrade.

After a rollback, if you do not schedule an upgrade, you will not receive an upgrade notice until the next version is available for upgrade.

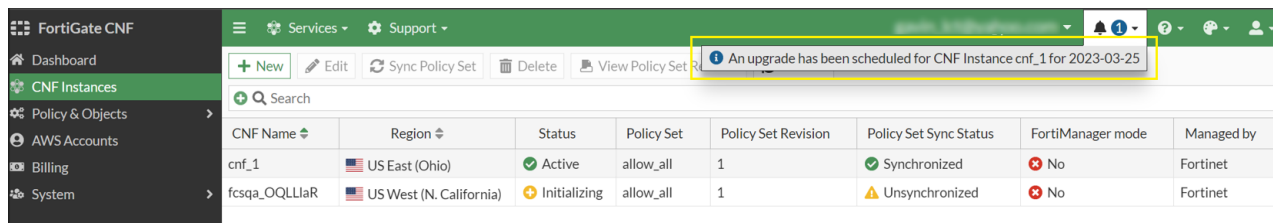
You may perform as many rollbacks and upgrades as you want within the available upgrade window.

Scheduling an upgrade

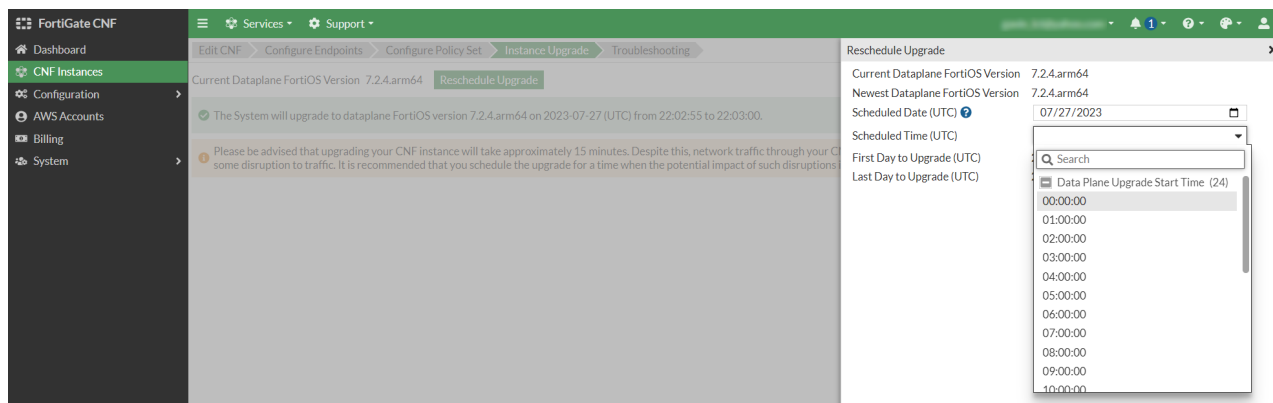
To set the schedule for your CNF instance upgrade:

1. An upgrade schedule is created by Fortinet, with an upgrade start date and end date. The upgrade will be scheduled within this upgrade window. Typically the end date will be 30 days after the start date, although this may vary.

In your FortiGate CNF console, a notification is displayed.



2. In the FortiGate CNF console, go to *CNF Instances*, select the appropriate instance from the list and click *Edit*.
3. Click *Instance Upgrade*. This option is only available when an upgrade has been scheduled by Fortinet. When an upgrade has not been scheduled, *Instance Version* is displayed.
4. Click *Reschedule Upgrade* and select the new upgrade date and time. The new time cannot be later than the last time to upgrade in the available upgrade window.



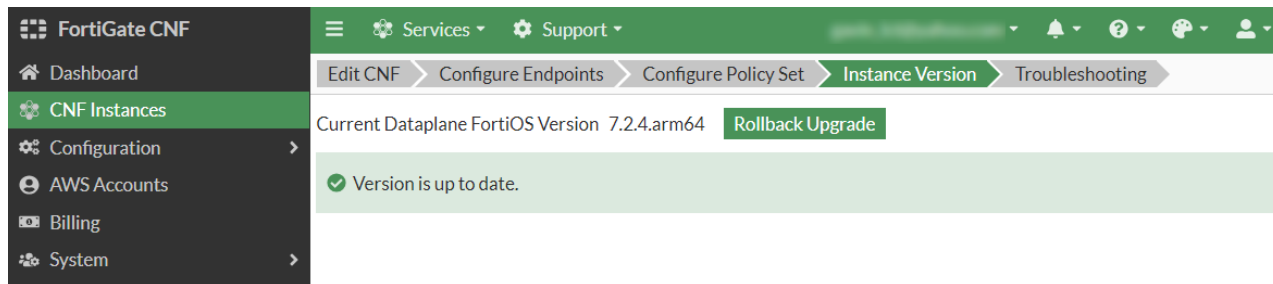
The upgrade is set to the new date.

FortiGate CNF sends two reminder emails leading up to the scheduled upgrade: 24 hours and one hour prior to the scheduled upgrade start time.

Rolling back an upgrade

To roll back an upgrade:

1. Within seven days after an upgrade, in the FortiGate CNF console, go to *CNF Instances*.
2. Select the appropriate instance from the list and click *Edit*.
3. Click *Instance Version*.



4. Click *Rollback Upgrade*.

The instance is rolled back to the previous version.

After a successful rollback of an upgrade, FortiGate CNF sends a notification email that includes a reminder of the rescheduled upgrade.

FortiManager mode

Create a FortiGate CNF instance in FortiManager mode to enable management of the instance from FortiManager.

When FortiManager mode is enabled, policies can only be deployed to this instance through FortiManager.



FortiManager 7.2.2 or later is required.

- [Adding a FortiGate CNF instance to FortiManager on page 54](#)
- [Managing a FortiGate CNF instance in FortiManager on page 58](#)

Adding a FortiGate CNF instance to FortiManager

FortiManager can be used to install and monitor security features on FortiGate CNF instances.



FortiManager 7.2.2 or later is required.

To add a FortiGate CNF instance to FortiManager:

1. In FortiGate CNF, in the *Display Primary FortiGate Information* field in the *Edit CNF* form, find the FortiGate connection details.
2. In FortiManager, go to *Device & Groups > Add Device*.
3. Click *Discover Device*.
4. Enter the *IP Address* of the FortiGate CNF instance.
5. Enable *Use Legacy Device Login* and enter the *User Name* and *Password*, then click *Next*.
6. Update or enter any required details and click *Next*.

7. Click *Finish*. The FortiGate CNF instance is added to FortiManager. There may be a short delay before the device is available.
8. Import the *FG-traffic* policy package from the FortiGate CNF instance into FortiManager.



Use either *Import each VDOM step by step* or *Automatically import one VDOM at a time* to import *FG-traffic*. You do not need to import *root*.

Use this policy package in FortiManager to install policies to the FortiGate CNF instance.

FortiGate CNF clusters are treated differently than the normal FortiGate auto-scale cluster on AWS. Hover over the information icon next to the cluster name to see more information about the cluster.

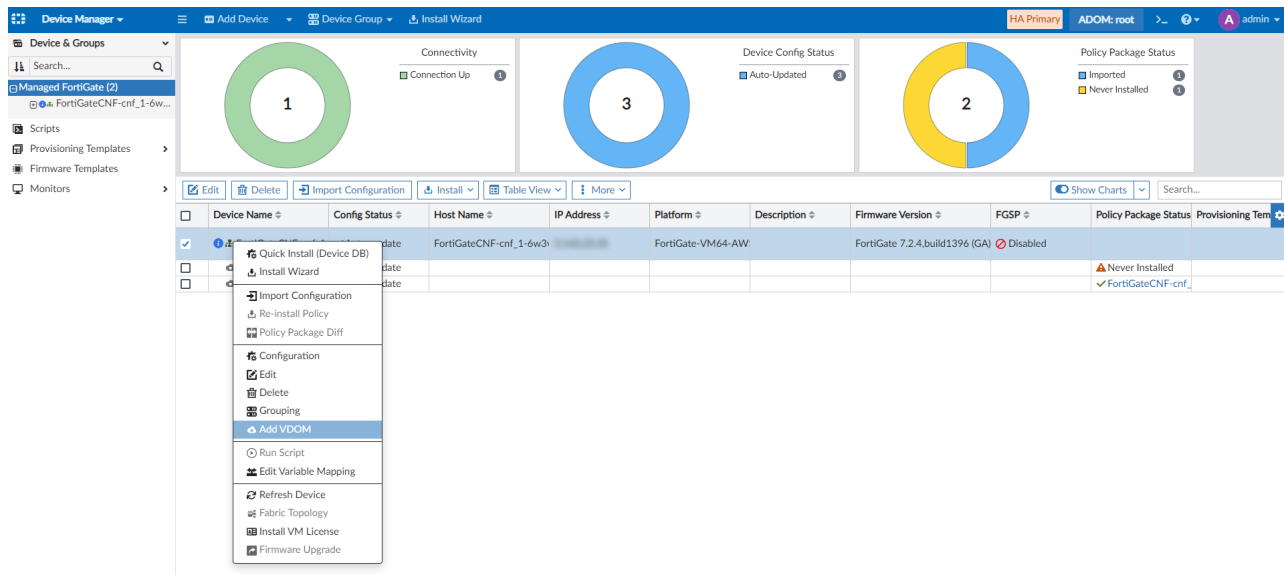


Device Name	Config Status	Host Name	IP Address	Platform	Description	Firmware Version	FGSP	Policy Package Status	Provisioning Tem
FortiGateCNF-cnfr-1	Synchronized	FortiGateCNF-cnfr-1-6w3		FortiGate-VM64-AW		FortiGate 7.2.4.build1396 (GA)	Disabled	Never Installed	
								Never Installed	
								FortiGateCNF-cnfr	

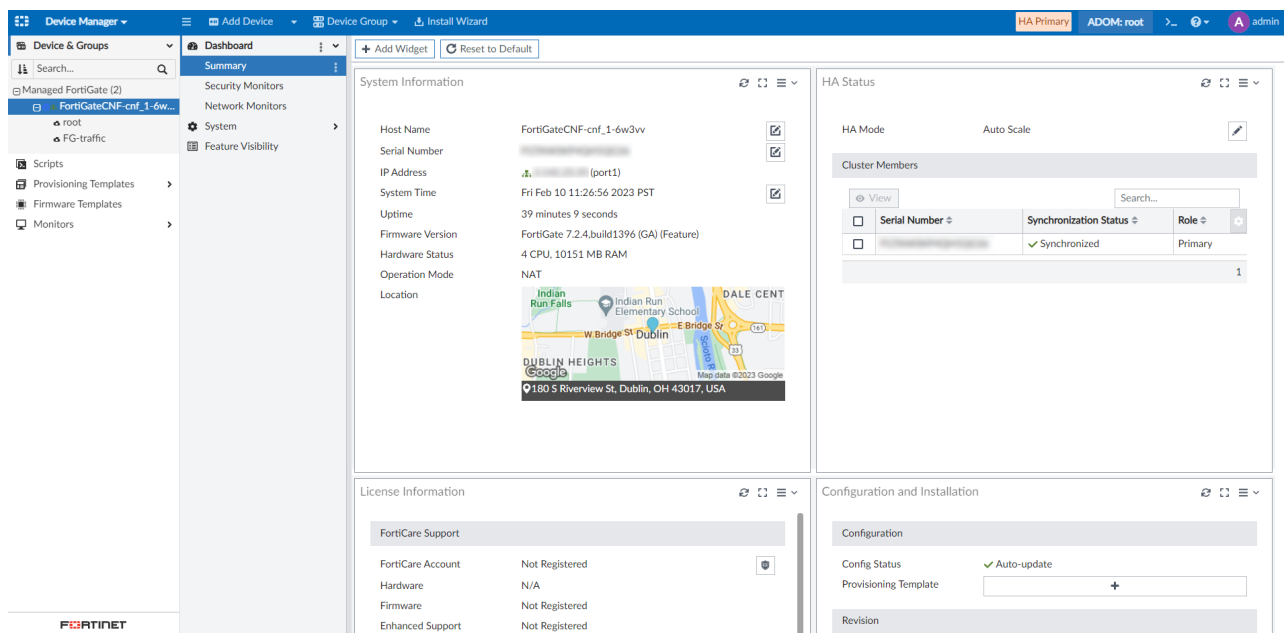
Management restrictions

FortiGate CNF is a Fortinet-managed service and there are limited configurations that are permitted from FortiManager. The following management operations are restricted:

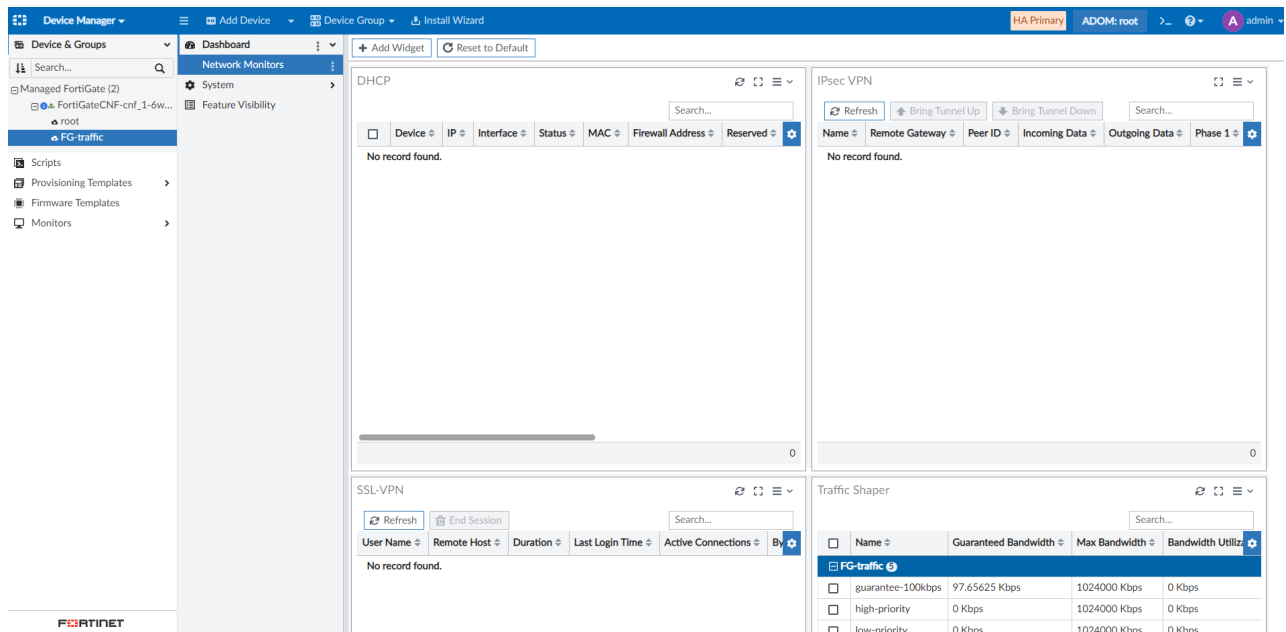
- VDOM creation not permitted and the option is greyed out.



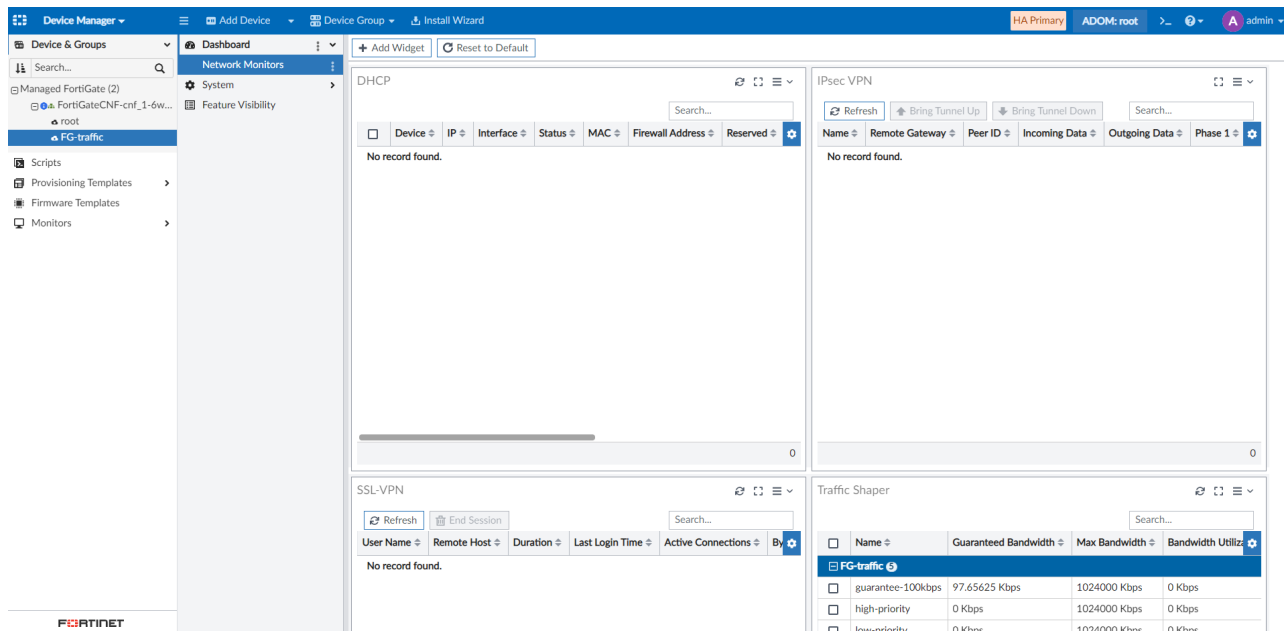
- Changes in CLI configuration are not permitted and if tried there is an error.



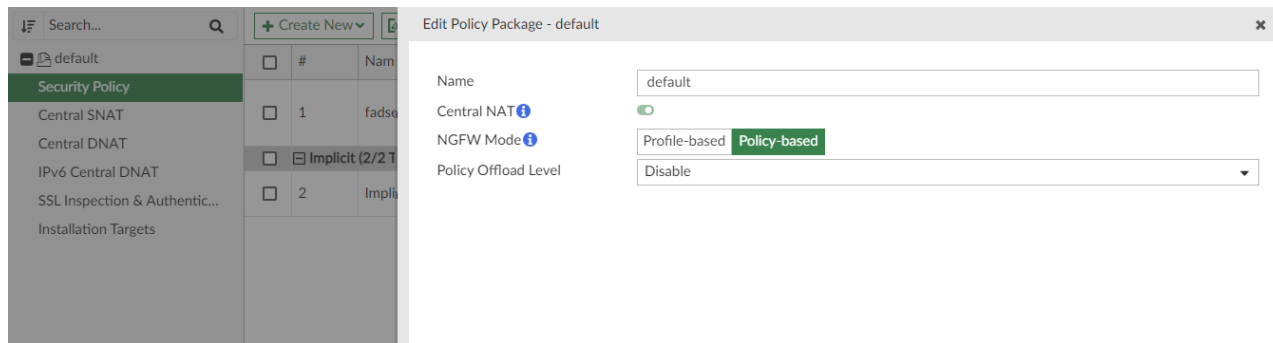
- Changes to networking components of the FortiGate are restricted and if tried there is an error.



- CLI access to the FortiGate CNF instance is not allowed from FortiManager.



- FortiGate CNF only supports *profile-based* NGFW mode policy packages. While FortiManager allows the selection of *policy-based* NGFW mode, this setting causes policy installation to fail.



In FortiManager, in *Device Manager*, the imported FortiGate CNF may display a message "Firmware Upgrade License Not Found". You may safely ignore this message.

For more information about adding devices to FortiManager, see [Adding online devices using Discover mode](#) in the FortiManager Administration Guide.

Managing a FortiGate CNF instance in FortiManager

After you have added a FortiGate CNF instance to FortiManager, you can use the following FortiManager features for this FortiGate CNF instance:

- View the dashboard
- Create and install policies
- Manage certificates



The following FortiManager features are not available:

- Interfaces
- System
- Users
- CLI

For information about managing FortiGate devices in FortiManager, see the [FortiManager Administration Guide](#).

Also see [FortiManager supports FortiGate Cloud-Native Firewall as device type](#) in the FortiManager New Features documentation.

Managing certificates

Certificates must be managed in the *FG-traffic* VDOM for any FortiGate CNF instances managed in FortiManager.

To view and import certificates in FortiManager:

1. In FortiManager, go to Device Manager and select the FortiGate CNF instance.
2. Click *Feature Visibility* and enable *System > Certificates*.
3. Click the *FG-traffic* VDOM, then click *System > Certificates*.

The list of available certificates displays. Use *Import* to import certificates for use on this FortiGate CNF instance. For more information about managing certificates in FortiManager, see [Certificates in the FortiManager Administration Guide](#).

FortiAnalyzer logging

FortiGate CNF instance logs can be sent to FortiAnalyzer for analysis.

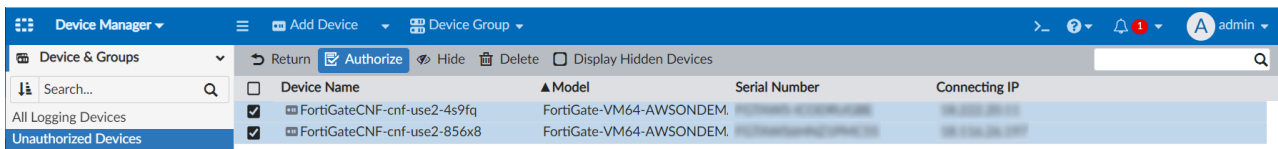
To send logs to FortiAnalyzer:

1. In the FortiGate CNF console, create a new instance with *Log Type* set to *FortiAnalyzer* and the *FortiAnalyzer IP* entered.

The screenshot shows the configuration page for a FortiGate CNF instance named 'cnf_1'. The 'Logging Options' section is expanded, showing the following settings:

- Internal S3 Logging:
- Log Traffic to S3 Bucket: 636955248026 - fortigatecnf-636955...
- External Logging: None External Syslog FortiAnalyzer
- FortiAnalyzer IP: 32.48.29.3

2. In FortiAnalyzer, go to *Device Manager > Unauthorized Devices*.
3. Select the FortiGate CNF instances and click *Authorize*.



4. Click *OK*.

The screenshot shows the 'Authorize Device' dialog box in FortiAnalyzer. It contains a table with the following data:

Device Name	Assign New Device Name
FortiGateCNF-cnf-use2-4s9fq	FortiGateCNF-cnf-use2-4s9fq
FortiGateCNF-cnf-use2-856x8	FortiGateCNF-cnf-use2-856x8

At the bottom right of the dialog, there are two buttons: 'OK' and 'Cancel'.

FortiAnalyzer adds the FortiGate CNF instance and begins receiving logs.

Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)
FortiGateCNF-cnf-use2-4s9fq		FortiGate-VM64-AWSONDEMAND	Real Time	0
root		vdom	Real Time	0
FortiGateCNF-cnf-use2-856x8		FortiGate-VM64-AWSONDEMAND	Real Time	0
root		vdom	Real Time	0

If the FortiGate CNF instance is authorized but logs are not received, FortiAnalyzer displays an error.

Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage
FortiGateCNF-cnf-use2-4s9fq		FortiGate-VM64-AWSON	Real Time	N/A	(0%)
FortiGateCNF-cnf-use2-856x8		FortiGate-VM64-AWSON	Real Time	N/A	(0%)

Troubleshooting

FortiManager
 Status: Disabled | Connectivity: Disconnected

Policy Counters

Sequence ID	Policy Name	Status	Bytes
1	subnet_block	Enabled	690.144 KB
2	dynamic_allow	Enabled	1.092 KB

2 | Updated: 10:26:06

Resolved IP Address

dy_addr1

IP Address
10.1.81.102
10.1.81.101

3 | Updated: 10:24:14

Packet Capture [Start Packet Capture]

- 8.828717 -- 192.168.6.174:None -> 10.1.81.52:None: icmp: type-#5
- 8.832318 -- 10.1.81.52:None -> 10.1.82.149:None: icmp: type-#8
- 9.840750 -- 192.168.6.174:None -> 10.1.81.52:None: icmp: type-#5
- 9.844357 -- 10.1.81.52:None -> 10.1.82.149:None: icmp: type-#8
- 10.864737 -- 192.168.6.174:None -> 10.1.81.52:None: icmp: type-#5

Buttons: Reset, Save, Back, Next, Finalize, Exit

To troubleshoot a deployed FortiGate CNF instance:

1. In the FortiGate CNF console, go to *CNF Instances*, then select an instance and click *Edit*.
2. Click *Troubleshooting*.
3. In the *Troubleshooting* dashboard, the following actions are available:
 - View FortiManager status.
 - View policy counters since the most recent policy push.
 - View all resolved IP addresses.
 - Run packet capture.

Using packet capture

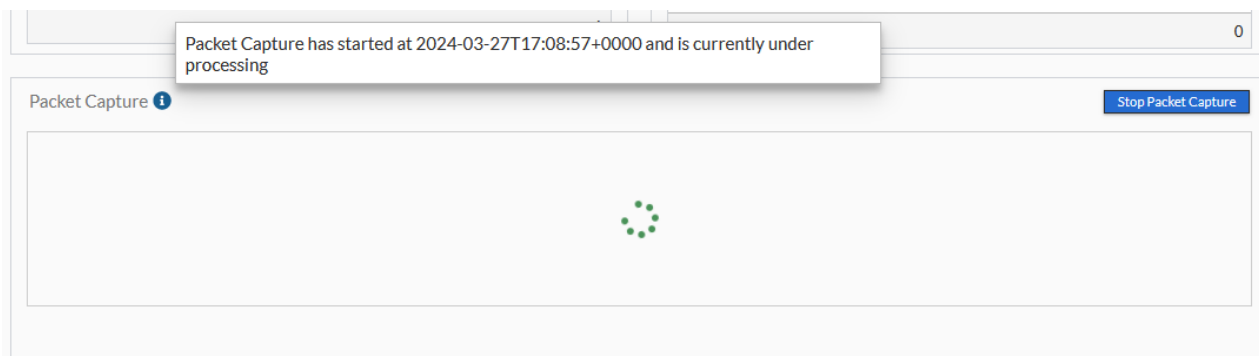
When troubleshooting your network configuration, use the packet capture tool to see the headers of the packets passing in and out of the FortiGate CNF instance.

To use packet capture:

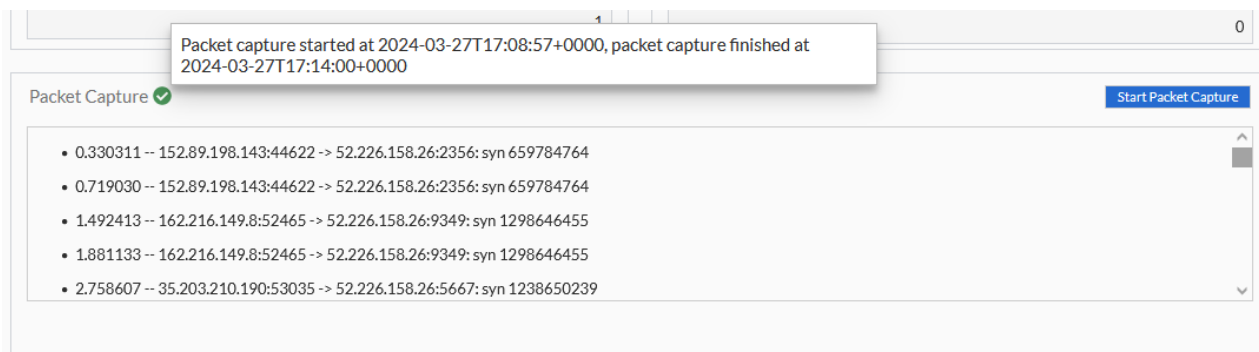
1. In the FortiGate CNF console, go to *CNF Instances*, select an instance, and click *Edit*.
2. Click *Troubleshooting*.
3. In *Packet Capture*, click *Start Packet Capture*.

Packet capture starts. Packet capture will run for five minutes or until you click *Stop Packet Capture*.

When packet capture is running, the displayed icon is an "i". The status message details the start time and indicates that the process is running.



When packet capture is completed, the displayed icon is a checkmark. The status message details the start and end time.



Configuration

This section contains topics on configuring policy sets and related objects:

- [Policy sets on page 62](#)
- [Addresses on page 65](#)
- [Services on page 67](#)
- [Security profiles on page 69](#)
- [CNF templates on page 72](#)

Policy sets

Creating FortiGate CNF policies is similar to FortiGate, but with a more limited set of policy and security profile options.

An ordered group of policies forms a policy set. A single policy set is then applied to a FortiGate CNF instance, rather than individual policies.

The same policy set may be installed on multiple instances.

A policy set can only be installed to CNF instances in the specified *Cloud Platform*. The possible values are as follows:

- *ALL*: This policy set can be deployed to AWS or Azure instances. *All* policy sets may not take advantage of platform-specific features.
- *AWS*: This policy set can only be deployed to AWS CNF instances.
- *Azure*: This policy set can only be deployed to Azure CNF instances.



FortiGate CNF comes with a preconfigured *allow_all* policy set that cannot be edited or deleted.



The *allow_all* policy set should only be used during the initial testing stage to help test routing. It should not be used for production since it does not provide any security protection.

The *Policy Sets* page lists the existing policy sets.

From this page you can:

- [Create a new policy set.](#)
- [Edit a policy set.](#)
- [Delete a policy set.](#)

For more detailed information about FortiGate policies, see [Policies in the FortiGate Administration Guide](#).

Creating a policy set

FortiGate CNF provides two options for creating policy sets:

- [Create New > Policy Set by Wizard](#): For most workloads in AWS, the inbound and outbound policies are very simple. The wizard creates these policies with only a couple of clicks. Once the policy set is created, you can edit the created objects, if needed. For more information about editing the various types of policy objects, see [Configuration on page 62](#).
- [Create New > Policy Set](#): Create *Address*, *Service*, and *Security Profile* objects individually and assemble them to form a policy.

For more information about policy set settings, see [Editing or viewing a policy set on page 64](#).

To create a new policy set by wizard:

1. In *Policy Sets*, click *Create New* and select *Policy Set by Wizard*.
2. Enter a name for the policy and select the Wizard Type:
 - *Outbound Basic* : Creates an outbound policy that prevents the workload from contacting malicious IP addresses such as command-and-control centers.
 - *Outbound Geo Policy*: Creates an outbound policy identical to the *Outbound Basic* type and an inbound policy that blocks incoming traffic from certain geographic locations.
3. Enable or disable logging.
4. Select the *Cloud Platform* from the following options:
 - *ALL*: This policy set can be deployed to AWS or Azure instances.
 - *AWS*: This policy set can only be deployed to AWS CNF instances.
 - *Azure*: This policy set can only be deployed to Azure CNF instances.
This setting cannot be changed.
5. Click *Next*.
6. Select the security profiles to enable, then click *Next*.
For more information, see [Security profiles on page 69](#).
7. If *Geographical Boundaries* was selected, select the countries to block, then click *Next*.
8. Click *Finalize*. The policy set is created and can now be installed on one or more FortiGate CNF instances.

To create a new policy set:

1. In *Policy Sets*, click *Create New* and select *Policy Set*.
2. Enter a *Name* for the policy set.
3. Select the *Cloud Platform* from the following options:
 - *ALL*: This policy set can be deployed to AWS or Azure instances.
 - *AWS*: This policy set can only be deployed to AWS CNF instances.
 - *Azure*: This policy set can only be deployed to Azure CNF instances.
This setting cannot be changed.
4. Click *OK*. The new empty policy set is created.
5. Add policies as needed.
For more information about policy settings, see [Editing or viewing a policy set on page 64](#).

Editing or viewing a policy set

In the *Policy Sets* table, select a policy set and click *Edit* to view or edit the following policy set details:

- [Policy Set](#)
- [Policies](#)
- [CNF Associations](#)

For more detailed information about FortiGate policies, see [Policies](#) in the FortiGate Administration Guide.

Policy Set

The following details are displayed in the *Policy Set* form.

Item	Description
<i>Name</i>	The unique name of the policy set. This field is editable.
<i>Cloud Platform</i>	Displays the cloud platform for this policy set. This field is not editable.

Policies

In the *Policies* page, select a policy and click *Edit* to view or edit the policy details. Click *Delete* to remove the policy from the policy set. Click *New* to add a new policy.

The following details are displayed in the *Policies* form. All fields are editable.

Item	Description
<i>Name</i>	The unique name of the policy.
<i>Source</i>	The source addresses, address groups, or internet service. For more information, see Addresses on page 65 and Internet service database objects on page 68 .
<i>Destination</i>	The destination addresses or address groups. For more information, see Addresses on page 65 and Internet service database objects on page 68 .
<i>Service</i>	The service or service group this policy applies to. For more information, see Services on page 67 .
<i>Action</i>	The action taken when traffic matches this policy, either <i>ACCEPT</i> or <i>DENY</i> .
<i>Security Profiles</i>	The security profiles applied to this policy. For more information, see Security profiles on page 69 .
<i>Log Allowed Traffic</i>	Enable or disable logging of allowed traffic. The available logging options are: <ul style="list-style-type: none"> • <i>Security Event</i> • <i>All Sessions</i>
<i>Generate Logs When Session Start</i>	Enable or disable generation of logs when a session starts.
<i>Enable This Policy</i>	Enable or disable this policy.

CNF Associations

The *CNF Associations* table displays a read-only list of the FortiGate CNF instances where this policy set is installed.

Deleting a policy set

To delete a policy set:

1. In the *Policy Sets* table, select a policy set and click *Delete*.
2. Click *OK* to confirm the deletion.

Addresses

Define address objects for re-use in multiple policies.

Go to *Configuration > Addresses* to view the list of configured address objects.

You can create the following objects from this page:

- [Addresses](#)
- [Address groups](#)



FortiGate CNF comes with several address objects pre-configured. The pre-configured objects are not editable but can be cloned into new objects.



FortiGate CNF only supports IPv4 addresses. IPv6 addresses are not supported.

Address objects

Address objects have the following options:

Item	Description
<i>Name</i>	The unique name of the object.
<i>Type</i>	Select the address type: <ul style="list-style-type: none"> • <i>Dynamic</i>: Select available cloud resources. • <i>Geography</i>: Select countries. • <i>FQDN</i>: Enter a fully-qualified domain name. • <i>IP Range</i>: Enter an IP addresses range. • <i>Subnet</i>: Specify an IP address subnet.

Item	Description
<i>Dynamic options</i>	
<i>Cloud Platform</i>	Select AWS or Azure.
<i>AWS/Azure Account ID</i>	Select the account ID.
<i>AWS Region</i>	Select the region. This option is only available if <i>Cloud Platform</i> is AWS.
<i>SDN Address Type</i>	Select the software defined network address type: <ul style="list-style-type: none"> • <i>Private</i> • <i>Public</i> • <i>All</i>
<i>Filter</i>	<p>Enter one or more filters as selection criteria.</p> <p>The available filters vary based on the resources in the selected cloud platform, account, and region, as well as other factors such as the FortiOS version. The following lists of filters are provided as an example of available filters.</p> <p>For AWS, this includes:</p> <ul style="list-style-type: none"> • EC2 instance characteristics, including: <ul style="list-style-type: none"> • Architecture • Availability zone • Image ID • Instance ID • Instance type • Private DNS name • Public DNS name • Subnet • Security group • VPC • Endpoint ID • Endpoint service name • Tags <p>For AWS addresses, most filters are only available if there are active EC2 instances deployed in the VPC.</p> <p>For Azure, this may include:</p> <ul style="list-style-type: none"> • VM • Size • Location • Security group • Vnet • Subnet • Subscription • Load balancer

Item	Description
	<ul style="list-style-type: none"> • Application gateway • Tag <p>For Azure addresses, most filters are only available if there are active instances deployed.</p> <p>For both AWS and Azure, Kubernetes-related filters are available if Kubernetes resources are deployed in the selected account and region.</p>
<i>Geography options</i>	
<i>Country/Region</i>	Select the country or countries.
<i>FQDN options</i>	
<i>FQDN</i>	Enter a fully-qualified domain name.
<i>IP Range options</i>	
<i>IP Range</i>	Enter the IPv4 range (in format $x.x.x.x-x.x.x.x$).
<i>Subnet options</i>	
<i>IP/Netmask</i>	Enter the IPv4 subnet and netmask (in format $x.x.x.x/xx$).

Address groups

Address groups collect address objects into a group for reuse. They have the following options:

Item	Description
<i>Name</i>	The unique name of the object.
<i>Cloud Platform</i>	Select <i>AWS</i> or <i>Azure</i> or <i>ALL</i> .
<i>Members</i>	Select the addresses to include in this group.

Services

Define service objects for re-use in multiple policies.

Go to *Configuration > Services* to view the list of configured service objects.

You can create the following objects from this page:

- [Services](#)
- [Service groups](#)



FortiGate CNF comes with several service objects preconfigured. The preconfigured objects are not editable but can be cloned into new objects.

Services

Services have the following options:

Item	Description
<i>Name</i>	The unique name of the object.
<i>Category</i>	Select the service category. This selection is a convenience for grouping and does not affect the available options.
<i>Protocol Type</i>	Select the service protocol type: <ul style="list-style-type: none"> • <i>TCP/UDP/SCTP</i> • <i>ICMP</i> • <i>IP</i>
<i>TCP/UDP/SCTP options</i>	
<i>Address</i>	Select <i>IP Range</i> or <i>FQDN</i> and enter the appropriate value.
<i>Destination Port</i>	Select the port type and enter the range values.
<i>Specify Source Ports</i>	Enable or disable source ports. If enabled, enter source ports for each destination port entry.
<i>ICMP options</i>	
<i>Type</i>	Enter the service type.
<i>Code</i>	Enter the service code.
<i>IP options</i>	
<i>Protocol Number</i>	Enter the IP protocol number.

Service groups

Service groups collect services into a group for re-use. They have the following options:

Item	Description
<i>Name</i>	The unique name of the object.
<i>Members</i>	Select the services to include in this group.

Internet service database objects

The Internet Service Database (ISDB) is a comprehensive public IP address database that combines IP address range, IP owner, service port number, and IP security credibility. The data comes from the FortiGuard service system. Information is regularly added to this database, for example, geographic location, IP reputation, popularity & DNS, and so on.

You can use the contents of this database as criteria for inclusion or exclusion in a policy as you would other object types, such as addresses.

To use an ISDB object in a security policy:

1. Create or edit a security policy.
2. In *Source* or *Destination*, click + to open the *Select Entries* pane.
3. Click *Internet Service* and select an ISDB object.



If *Destination* is set to an ISDB object, *Service* is disabled.

4. Configure the rest of the policy and click *OK*.

Security profiles

Security profiles collect pre-configured intrusion detection profiles into a re-usable group. After a security profile is created it can be further customized.

Go to *Configuration > Security Profiles* to view the list of configured security profiles.

Security profiles have the following basic options:

Item	Description
<i>Name</i>	Enter a unique name for the security profile.
<i>DNS Filter</i>	Enable or disable DNS filters.
<i>Known Bad IP Blocking</i>	Enable or disable filters to block or monitor known bad addresses.
<i>Intrusion Prevention</i>	Enable or disable intrusion prevention system (IPS).

The security profile is created with a default set of options.

Editing security profiles

To edit a security profile:

1. Select a security profile from the list and click *Edit*.
2. Click *Customize* in the appropriate filter profile.

DNS filter options



In order for DNS filtering to work, you must first configure your cloud environment.


- [Configuring DNS filtering on AWS on page 72.](#)
- [Configuring DNS filtering on Azure on page 74.](#)

Item	Description
<i>Redirect Botnet C&C to Block Portal</i>	Enable or disable botnet redirection.
<i>FortiGuard Category Based Filters</i>	Enable or disable category filters. For each filter category, select the action: <ul style="list-style-type: none"> • <i>Allow</i> • <i>Redirect to Block Portal</i> • <i>Monitor</i>
<i>Domain Filters</i>	Enable or disable domain filters, then add or edit filters and configure the following options.
<i>Domain</i>	Enter the domain to filter.
<i>Type</i>	Select the type of matching for the entered domain.
<i>Action</i>	Select the action: <ul style="list-style-type: none"> • <i>Allow</i> • <i>Redirect to Block Portal</i> • <i>Monitor</i>
<i>Status</i>	Enable or disable this domain filter.
<i>DNS Translation</i>	Enable or disable DNS translation filters, then add or edit filters and configure the following options.
<i>Address Type</i>	Only IPv4 addresses are supported. This is not configurable.
<i>Destination</i>	Enter the destination IP address.
<i>Net Mask</i>	Enter the net mask.
<i>Source</i>	Enter the source IP address.
<i>Status</i>	Enable or disable this domain filter.

Known Bad IP Blocking options

Item	Description
<i>Block Malicious URLs</i>	<p>Enable or disable blocking of malicious URLs.</p> <p>Select the action:</p> <ul style="list-style-type: none"> • <i>Enable</i> • <i>Disable</i>
<i>Block Command and Control server IPs</i>	<p>Block known command and control server IPs.</p> <p>Select the action:</p> <ul style="list-style-type: none"> • <i>Enable</i> • <i>Disable</i> • <i>Monitor</i>

Intrusion Prevention options

Item	Description
<i>IPS Profile</i>	<p>Select the preset IPS profile to use. The profiles cannot be further configured.</p> <ul style="list-style-type: none"> • <i>all_default</i>: Filters all predefined signatures, and sets action to the signature's default action. • <i>all_default_pass</i>: Filters all predefined signatures, and sets action to pass/monitor. • <i>default</i>: Filters all predefined signatures with severity of Critical/High/Medium. Sets action to signature's default action. • <i>high_security</i>: Filters all predefined signatures with severity of Critical/High/Medium, and sets action to Block. For Low severity signatures, sets action to signature's default action. • <i>protect_client</i>: Protects against client-side vulnerabilities by filtering on Target=Client. Sets action to signature's default action. • <i>protect_email_server</i>: Protects against email server-side vulnerabilities by filtering on Target=Server and Protocol=IMAP, POP3 or SMTP. Sets action to signature's default action. • <i>protect_http_server</i>: Protects against HTTP server-side vulnerabilities by filtering on Target=Server and Protocol=HTTP. Sets action to signature's default action. • <i>sniffer-profile</i>: Filters all predefined signatures with severity of Critical/High/Medium. Sets action to signature's default action. <p>For more information about signatures and the default actions for each, see the FortiGuard Threat Encyclopedia.</p> <hr/> <div style="display: flex; align-items: center;">  <p>FortiGate CNF does not include <i>block-malicious-url</i> as part of the <i>high_security</i> sensor. We recommend enabling <i>Known Bad IP Blocking</i> in the security profile to enable blocking known and bad IPs.</p> </div>

CNF templates

View and manage saved FortiGate CNF templates.

This page lists the saved templates.

From this page you can:

- [View template details.](#)
- [Delete templates.](#)
- [Create a new FortiGate CNF instance from a template.](#)

Viewing template details

In *Configuration > CNF Templates*, select a template and click *View*.

From this view, click *Cancel* to close the page or *Create CNF* to create a new FortiGate CNF instance. See [Creating an instance from a template on page 72](#).



FortiGate CNF templates are not editable.

Deleting a template

To delete a saved FortiGate CNF template:

1. In *Configuration > CNF Templates*, select a template and click *Delete*.
2. Click *OK* to confirm the deletion.

Creating an instance from a template

To create a FortiGate CNF instance from a template:

1. In *Configuration > CNF Templates*, select a template and click *Create CNF*.
2. Name the new FortiGate CNF instance.
3. Update other configuration as needed.
4. Click *OK*.

Any errors are saved to the system audit log.

Configuring DNS filtering on AWS

In order for DNS filtering to work properly in FortiGate CNF instance policies, the AWS environment must be configured.

By default, compute resources within a VPC use AWS's internal DNS servers. The DNS traffic will stay inside the VPC and not be routed to the deployed FortiGate CNF instance. VPC configurations must be changed to route those DNS requests to an external DNS server to be scanned by the FortiGate CNF instance.

To configure DNS requests:

1. In the AWS VPC, create a new DHCP option set using any external DNS.

The screenshot shows the AWS console page for a DHCP option set. The breadcrumb trail is 'VPC > Your VPCs > vpc-08086c663b39e2a2b > Edit DHCP option set'. The main heading is 'Edit DHCP option set' with an 'Info' link. Below this is a section titled 'DHCP settings' with the subtitle 'The DHCP option set to associate with the VPC.' The 'VPC ID' is 'vpc-08086c663b39e2a2b'. The 'DHCP option set' dropdown menu is open, showing a search bar and a list of options: 'No DHCP option set', 'dopt-0ff012a02bd280880', and 'dopt-075bc7dcf6b12827d (test-dns)'. The 'test-dns' option is highlighted. A blue callout box on the right side of the dropdown menu contains the text: 'ved to 'Edit VPC settings' choose 'Actions' > 'Edit V'.

dopt-075bc7dcf6b12827d / test-dns Delete DHCP option set			
Details Info			
DHCP option set ID dopt-075bc7dcf6b12827d	Domain name -	Domain name servers 1.1.1.1	NTP servers -
NetBIOS name servers -	NetBIOS node type -	Owner 636955248026	

2. Update the DHCP option set in the desired VPC to use the new DHCP option set.

The screenshot shows the 'Edit DHCP option set' page in the AWS console. The breadcrumb trail is 'VPC > Your VPCs > vpc-08086c663b39e2a2b > Edit DHCP option set'. The main heading is 'Edit DHCP option set' with an 'Info' link. Below this is a section titled 'DHCP settings' with the subtitle 'The DHCP option set to associate with the VPC.' The 'VPC ID' is 'vpc-08086c663b39e2a2b'. The 'DHCP option set' dropdown menu is open, showing a search bar and a list of options: 'No DHCP option set', 'dopt-0ff012a02bd280880', and 'dopt-075bc7dcf6b12827d (test-dns)'. The 'test-dns' option is highlighted. A blue callout box on the right side of the dropdown menu contains the text: 'ved to 'Edit VPC settings' choose 'Actions' > 'Edit V'.

3. Setup the routing as you would for egress inspection.

4. If there are any existing resources in this VPC, restart them so that the DNS cache will reset and pickup the new DNS server.

Configuring DNS filtering on Azure

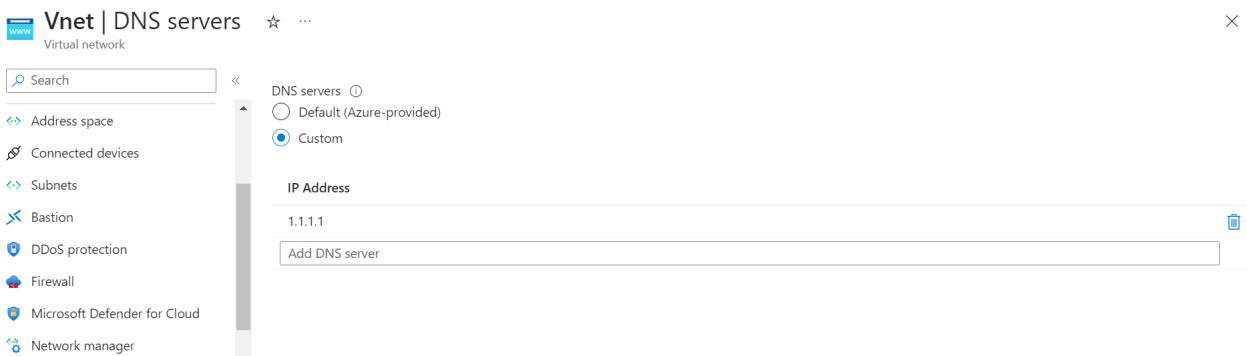
In order for DNS filtering to work properly in FortiGate CNF instance policies, the Azure environment must be configured.

By default, compute resources within a resource group use Azure internal DNS servers. The DNS traffic will stay inside the Azure network and will not be routed to the deployed FortiGate CNF instance. DNS configurations must be changed to route those DNS requests to an external DNS server to be scanned by the FortiGate CNF instance.

To configure DNS requests:

1. In the Azure resource group, create a new virtual network.
2. In the new virtual network, edit *DNS servers*.
3. Set *DNS servers* to *Custom* and enter the IP addresses of the external DNS servers.

[Home](#) > [Resource groups](#) > [46327461_467528266](#) > [Vnet](#)



4. Click **Save**.

Cloud accounts

On the *Cloud Accounts* page, manage your connected AWS and Azure accounts. These accounts are where your workloads reside.

You may connect more than one account.

From this page, you can:

- [Add a new account.](#)
- [View details of an account.](#)
- [Delete an account.](#)

To add a new cloud account:

For AWS, see [Adding an AWS account on page 75](#).

For Azure, see [Adding an Azure account on page 77](#).

To view the details of a cloud account:

On the *Cloud Accounts* page, select an account in the table and click *View*.

To delete a cloud account:

On the *Cloud Accounts* page, select an account in the table and click *Delete*.

Adding an AWS account



AWS accounts cannot be edited after they are fully added (the *Status* is *Success*), but the custom name can be changed.



To send logs to AWS Security Lake, Security Lake must be configured before adding the AWS account. See [Configuring Security Lake on page 76](#).

To add a new AWS account:

1. In the AWS console, log into this AWS account. The following CloudFormation steps will be performed in your AWS console.
2. In FortiGate CNF, in the *Cloud Accounts* page, click *New* and select *AWS*.
3. In *AWS Account Name*, enter a name for this account to be displayed in select lists.
4. In *AWS Account ID*, enter the AWS account number.

5. Click *Launch CloudFormation Template*.



Enter the AWS account number without dashes.

6. Update the AWS CloudFormation template fields as needed and click *Create Stack*.

To review the template, click *Download CloudFormation Template*.

The template does the following:

- Creates an S3 bucket for storing the FortiGate CNF logs, with write permissions for FortiGate CNF.
- Allows FortiGate CNF read-only access to your VPCs.
- Grants access to your AWS Security Lake, if applicable. See [Configuring Security Lake on page 76](#).

7. After the CloudFormation setup has completed successfully, return to the FortiGate CNF *AWS Accounts* page and verify that the account has been added and displays a *Success* message in the *Status* field.
-



The instructions displayed on the AWS account edit page are out of date and will be fixed in the March release.

- 2.a: "The custom Source must be created in US West (Oregon)" restriction is removed. The custom source can be created in any supported region.
 - 2.b: *OCSF Event Class* should be *Network Activity* instead of *Security Finding*.
-

8. Set the logging S3 bucket region.

9. If needed, set the Security Lake S3 bucket location and enable access to Security Lake

Configuring Security Lake

When creating FortiGate CNF instances in AWS, you can specify your existing AWS Security Lake as a log output destination.

FortiGate CNF does not create a Security Lake destination. You must create it and enable access using the CloudFormation template.



FortiGate CNF supports AWS Security Lake custom sources created in any FortiGate CNF supported regions.

To connect FortiGate CNF to Security Lake:

1. In AWS Security Lake, create a custom data source using *AWS Account ID* from *AWS Accounts* in the FortiGate CNF console.

In *OCSF Event class*, select *Network Activity*.

In *External ID*, enter a custom number string.

[Security Lake](#) > Create custom source

Create custom data source

To create a custom data source, provide the source details and enter the AWS Account ID which is authorized to write data to your data lake.

Custom source details

Data source name
Provide a globally unique name for the data source.

OCSF Event class

Region
You can only create a custom data source in your current Region.

US West (Oregon)

Account details
Enter the AWS account ID and external ID of the custom source that will write logs and events to the data lake.

AWS account ID

External ID

Service access View permission details

Security Lake requires permission to invoke AWS Glue on your behalf. [Learn more](#)

Create and use a new service role
 Use an existing service role

Service role name

AmazonSecurityLakeCustomDataGlueCrawler-

Cancel Create

- When running the CloudFormation template, in *Stack Details*, set `SecurityLakeCustomLogSourceName` to *Data source name* from your Security Lake custom source.

Adding an Azure account



Azure accounts cannot be edited after they are fully added (the *Status* is *Success*), but the custom name can be changed.

To add a new Azure account:

1. Configure Azure:
 - a. In the Azure console, log in to your Azure subscription.
 - b. Create or reuse a managed identity and assign *User Access Administrator* and *Contributor* roles for the Azure subscription. Additionally, assign the Entra ID role *Application Administrator* to this managed identity.
This managed identity is used to deploy an ARM Template to onboard the Azure account into FortiGate CNF. Please note that the storage account (for FortiGate CNF logs) will be created in the same resource group as the managed identity.
2. In the FortiGate CNF console, go to *Cloud Accounts*.
3. Click *New*, then select *Azure*.
4. In *Azure Account Name*, enter a name for the account.
5. Enter the *Azure Directory ID* and the *Azure Subscription ID*.
6. Click *Launch ARM Template*.
The Azure portal opens.
7. Enter the *Managed Identity Name* and *Resource Group*.
8. Click *Review + Create*, then click *Create*.
The deployment script runs.
To review the template, click *Download ARM Template*.
The template does the following:
 - Creates a storage account for storing the FortiGate CNF logs, with write permissions for FortiGate CNF.
 - Allows FortiGate CNF access to your networks.
9. Click *Outputs*, then copy the value from *spObjectId*.
10. In the FortiGate CNF console, in *Service Principal Object ID*, enter the *spObjectId* value. See [Service Principal Object ID on page 78](#).
11. Click *Update*.
The Azure account is added to the *Cloud Accounts* list with status *Success*.

Service Principal Object ID

The *Service Principal Object ID* is used by FortiGate CNF to access your Azure environment.

A FortiGate CNF Azure app registration is used for all customer environment-related operations. This app registration requires access to your Azure environment for operations such as linking load balancers and dynamic address objects.

The ARM Template creates a Service Principal in your Azure environment to provide the FortiGate CNF app registration the access required to perform these operations.

Billing

The billing report displays the AWS costs per month, region, CNF instance, and type for your FortiGate CNF instances.

You will be charged by AWS directly to your AWS account. The billing information here serves as a detailed breakdown of your cost, and is provided for information only. It may not exactly match your AWS bill.

Click *Download as .csv* to download the report in CSV format.

Summary charts

The summary charts display totals from the report table.

- *Region*: View costs broken down by region.
- *CNF*: View costs broken down by CNF instance.
- *Type*: View costs broken down by AWS cost type (*Compute* or *Traffic*).

System

View FortiGate CNF system information.

Audit log

System > Audit Log displays FortiGate CNF system events, such as creating a new instance or deleting a policy.

The audit log is different than the FortiGate logs, which display information about traffic on a deployed FortiGate CNF instance.

Audit logs are saved for 365 days.

If you need an export of your audit log, contact Fortinet Support through [the FortiCare portal](#).

Tenant info

View information about the FortiGate CNF account. The following information is displayed:

- *FortiCare Username*
- *FortiCare Serial Number*
- *AWS Subscription Type*
- *AWS Subscription Status*

API keys

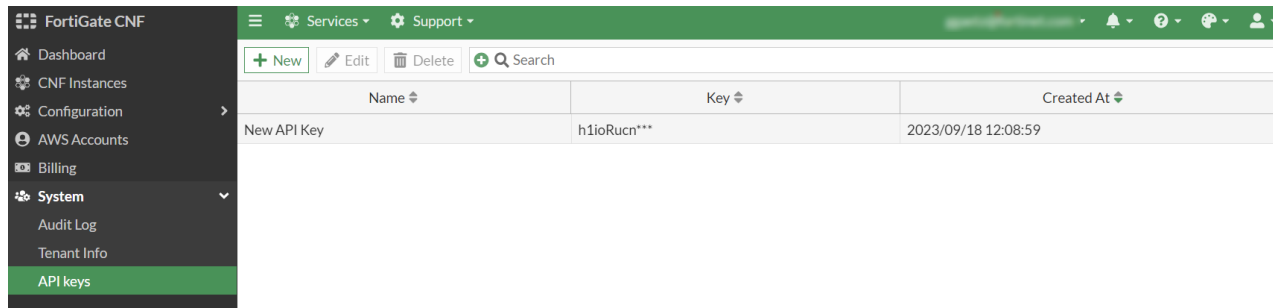
Create and manage the API keys that allow access to the FortiGate CNF REST API.

The FortiGate CNF REST API allows you access to the following features:

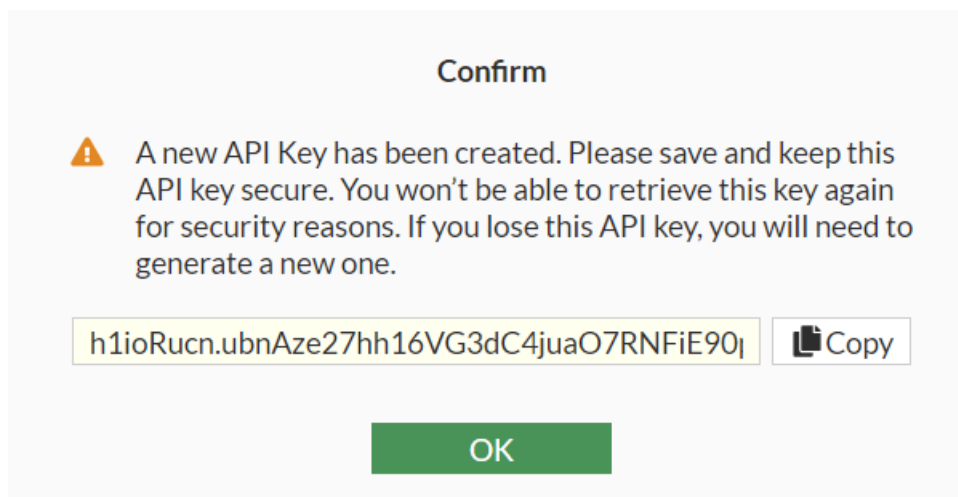
- **AWS Accounts:** Add, remove, and modify your connected AWS accounts.
- **AWS infrastructure:** View details about VPCs in your connected AWS accounts.
- **FortiGate CNF instances:** View, create, modify, and delete FortiGate CNF instances, as well as manage instance upgrades.
- **Gateway load balancer endpoints:** View, create, modify, and delete gateway load balancer endpoints and add them to your FortiGate CNF instances.
- **Policy sets:** View your policy sets.
- **Utility:** Get the supported regions list.

To use the REST API:

1. In the FortiGate CNF console, in the System submenu, click API keys.



2. Click *New*.
3. Enter a name for the key and click *OK*.
4. Copy the key to your clipboard and click *OK*.



API keys do not expire. To invalidate or disable an API key, you must delete it.



The key cannot be accessed again to copy, so you must copy it at this step. If you did not copy it or you lose the key, delete it and create a new one.

5. Include this key in the 'X-API-Key' header when making API requests.

For example:

```
curl -k -X 'POST' 'https://fortigatecnf.com/fortigatecnf/api/v1/aws-account/?action=download_cloudformation'
  -H 'accept: application/json'
  -H 'Content-Type: application/json'
  -H 'X-API-Key: rSczzboi.2kaSXdrqkQ5eUhuRr73TifBQL1Y8Q7Xi'
  -d '{"aws_account_id": "444444444444", "aws_account_name": "ADFS-Admin/example@example.com}"'
```

For more information about the available APIs, see the [FortiGate CNF API documentation on the Fortinet Developer Network \(FNDN\)](#).

Appendix A - Deployment scenarios

Traffic must be correctly routed through a FortiGate CNF instance in order to be inspected. The routing depends on your cloud workload architecture, with a virtually unlimited number of possibilities.

This section presents some typical deployment scenarios in AWS, with instructions on routing traffic to the FortiGate CNF instance. Follow the scenario that matches your architecture, or use the principles presented as a basis for a customized approach.

Broadly, AWS defines two types of security architecture in the context of FortiGate CNF:

- *Distributed*: Each VPC is protected by a FortiGate CNF instance.
- *Centralized*: Multiple VPCs are protected by a single FortiGate CNF instance. If you have workloads in multiple VPCs that require protection, this model may be a cleaner way to provide security than protecting each VPC separately in a distributed model. In the centralized model, all traffic is routed through a dedicated VPC called *Inspection VPC*. The GWLB will be deployed in this VPC to send traffic to the FortiGate CNF instance. You will need to create this inspection VPC and typically a transit gateway is needed.

The primary consideration in planning your deployment is how to route traffic to the FortiGate CNF instance, rather than the architecture of your application.

In each of these scenarios, we will present the following two diagrams:

- *Before deployment of FortiGate CNF*: this topology shows the infrastructure before a FortiGate CNF instance is deployed.
- *After deployment of FortiGate CNF*: this topology shows the changes you will implement to add the FortiGate CNF instance, with changes highlighted.

Examples

The following scenario examples are available:

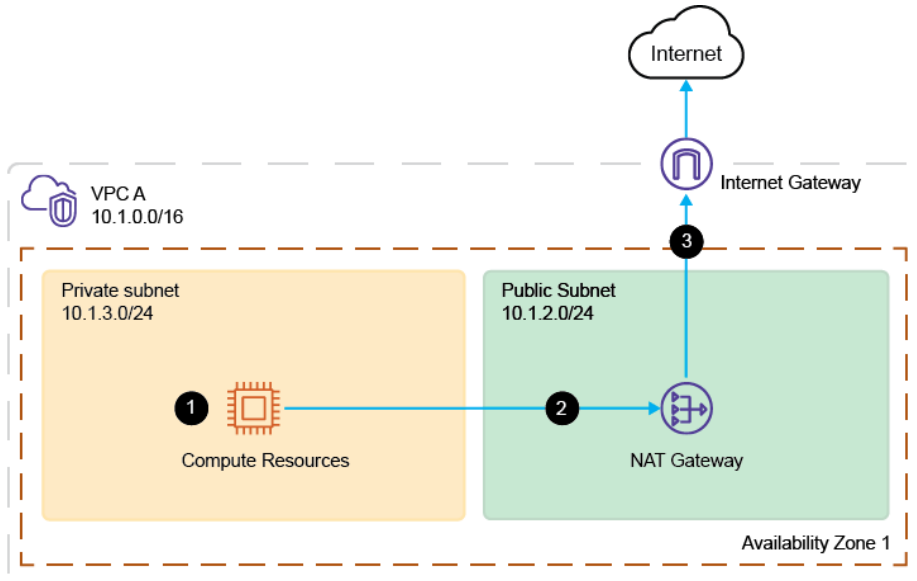
- AWS examples:
 - [Distributed egress: north-south traffic Example on page 83](#)
 - [Distributed inter-subnet east-west traffic in one AZ Example on page 85](#)
 - [Distributed inter-subnet east-west traffic between AZ Example on page 87](#)
 - [Distributed inter-VPC east-west traffic Example on page 89](#)
 - [Centralized ingress: inspection before load balancer Example on page 92](#)
 - [Centralized ingress: inspection after load balancer Example on page 95](#)
 - [Centralized egress Example on page 98](#)
 - [Centralized east-west, inter-VPC Example on page 102](#)
- Azure examples:
 - [Azure ingress and egress using public IP Example on page 106](#)
 - [Azure ingress and egress using Load Balancer with public IP Example on page 108](#)

Distributed egress: north-south traffic - Example

Scenario objective

The FortiGate CNF instance inspects all traffic outbound to the internet.

Before deployment of FortiGate CNF



The *Before deployment of FortiGate CNF* traffic flow is as follows:

1. Workload resources are situated in `Private Subnet (10.1.3.0/24)`.
2. Outbound traffic goes from `Private Subnet` to the `NAT Gateway` located in `Public Subnet (10.1.2.0/24)`.
3. Traffic then passes out through the `Internet Gateway`.

Routing tables

The routing tables are defined as follows.

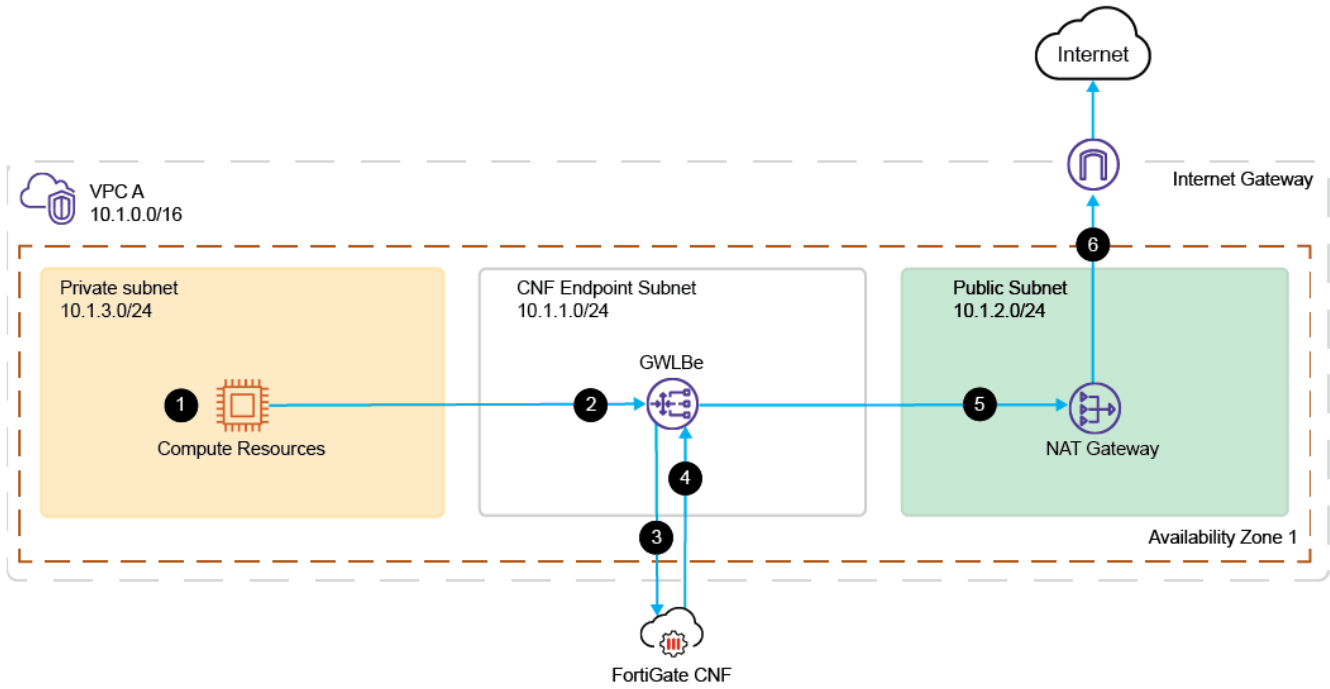
Public Subnet route table

Destination	Target
0.0.0.0/0	Internet Gateway

Private Subnet route table

Destination	Target
10.1.0.0/16	Local

After deployment of FortiGate CNF



The *after* topology traffic flow is as follows:

1. Workload resources are situated in `Private Subnet` (10.1.3.0/24).
2. Outbound traffic goes from `Private Subnet` to the `GWLBe` located in `CNF Endpoint Subnet` (10.1.1.0/24).
3. Traffic is sent to the `FortiGate CNF` instance for inspection.
4. `FortiGate CNF` sends traffic back to the `GWLBe`.
5. The `GWLBe` forwards the traffic to the `NAT Gateway` located in `Public Subnet` (10.1.2.0/24).
6. Traffic then passes out through the `Internet Gateway`.

To deploy the FortiGate CNF instance in this scenario:

1. In AWS, add a subnet `CNF Endpoint Subnet` (10.1.1.0/24) and the associated route table:

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT Gateway

2. In `FortiGate CNF`, deploy a `GWLBe` to this subnet.

- In AWS, add a route to the `Public Subnet` route table to route all traffic to the GWLBe.

Destination	Target
10.1.0.0/16	GWLBe
0.0.0.0/0	Internet Gateway

- In AWS, add a route to the `Private Subnet` route table to route all traffic to the GWLBe.

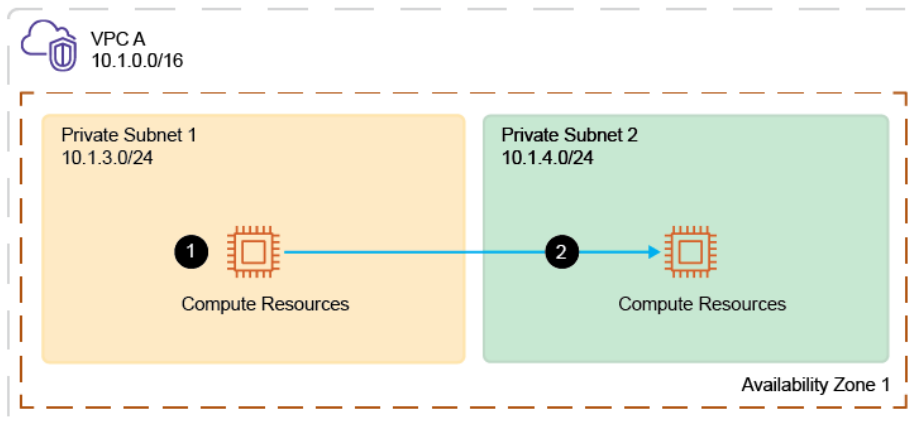
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	GWLBe

Distributed inter-subnet east-west traffic in one AZ - Example

Scenario objective

Traffic between two subnets in the same availability zone (AZ) in one VPC is inspected by a FortiGate CNF instance.

Before deployment of FortiGate CNF



Traffic in this scenario is east-west within the same availability zone (AZ) in a region. All routes are local routes.

The *Before deployment of FortiGate CNF* traffic flow is as follows:

- Traffic originates from compute resources located in `Private Subnet 1` (10.1.3.0/24).
- Traffic goes to compute resources located in `Private Subnet 2` (10.1.4.0/24).

Routing tables

The routing tables are defined as follows.

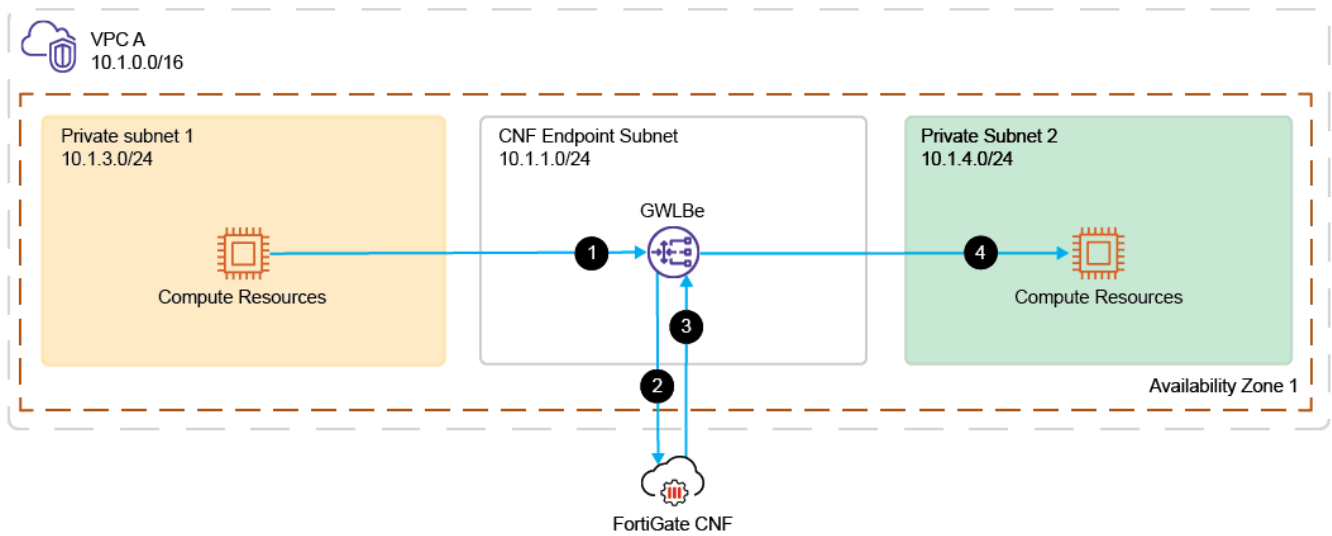
Private Subnet 1 route table

Destination	Target
10.1.0.0/16	Local

Private Subnet 2 route table

Destination	Target
10.1.0.0/16	Local

After deployment of FortiGate CNF



The *After deployment of FortiGate CNF* topology traffic flow is as follows:

1. Traffic goes from Private Subnet 1 (10.1.3.0/24) to the GWLBe located in CNF Endpoint Subnet (10.1.1.0/24).
2. Traffic is sent to the FortiGate CNF instance for inspection.
3. FortiGate CNF sends traffic back to the GWLBe.
4. The GWLBe forwards the traffic to Private Subnet 2 (10.1.4.0/24).

To deploy the FortiGate CNF instance in this scenario:

1. In AWS, add a subnet CNF Endpoint Subnet (10.1.1.0/24) and the associated route table.

Destination	Target
10.1.0.0/16	Local

2. In FortiGate CNF, deploy a GWLBe to this subnet.

- In AWS, add a route to the `Private Subnet 1` route table to route all traffic going to `Private Subnet 2` to the GWLBe.

Destination	Target
10.1.0.0/16	Local
10.1.4.0/24	GWLBe

- In AWS, add a route to the `Private Subnet 2` route table to route all traffic going to `Private Subnet 1` to the GWLBe.

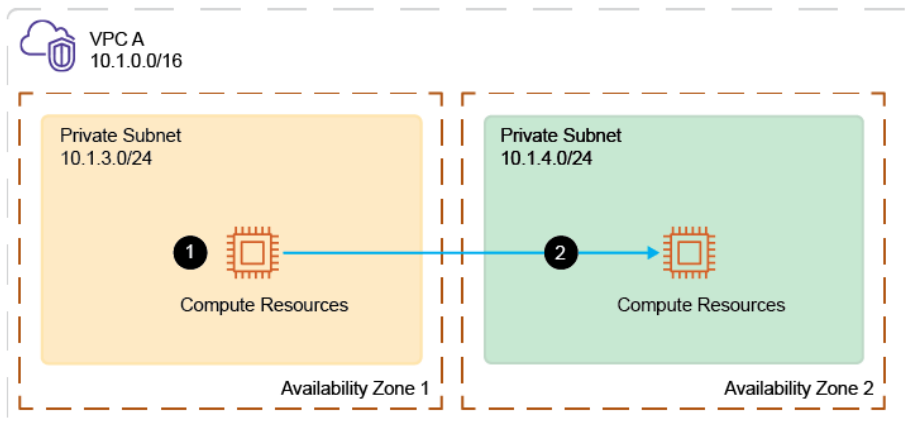
Destination	Target
10.1.0.0/16	Local
10.1.3.0/24	GWLBe

Distributed inter-subnet east-west traffic between AZ - Example

Scenario objective

Traffic between two availability zones (AZ) in one VPC is inspected by a FortiGate CNF instance.

Before deployment of FortiGate CNF



The traffic in this scenario is east-west between two availability zones (AZ) in the same AWS region. All routes are local routes.

The *Before deployment of FortiGate CNF* traffic flow is as follows:

- Traffic originates from compute resources located in `Private Subnet` in `Availability Zone 1` (10.1.3.0/24).
- Traffic goes to compute resources located in `Private Subnet` in `Availability Zone 2` (10.1.4.0/24).

Routing tables

The routing tables are defined as follows.

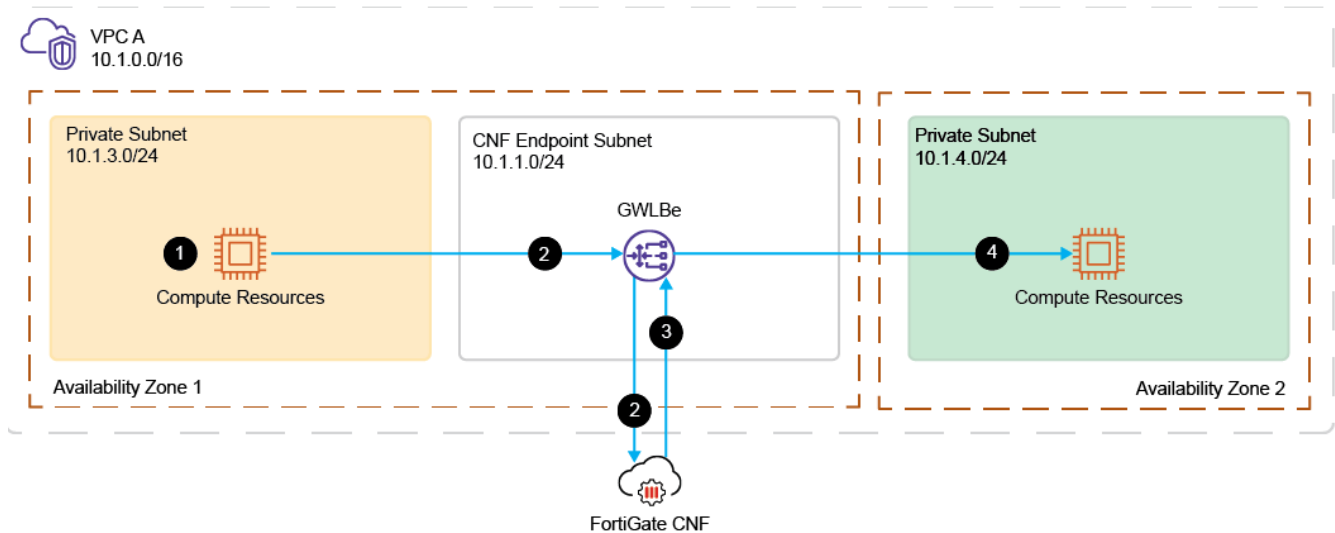
Private Subnet (Availability Zone 1) route table

Destination	Target
10.1.0.0/16	Local

Private Subnet (Availability Zone 2) route table

Destination	Target
10.1.0.0/16	Local

After deployment of FortiGate CNF



The After deployment of FortiGate CNF topology traffic flow is as follows:

1. Traffic goes from Private Subnet in Availability Zone 1 (10.1.3.0/24) to the GWLBe located in CNF Endpoint Subnet in Availability Zone 1 (10.1.1.0/24).
2. Traffic is sent to the FortiGate CNF instance for inspection.
3. FortiGate CNF sends traffic back to the GWLBe.
4. The GWLBe forwards the traffic to Private Subnet in Availability Zone 2 (10.1.4.0/24).

To deploy the FortiGate CNF instance in this scenario:

1. In AWS, add a subnet `CNF Endpoint Subnet` in one of the AZs along with the associated route table.

Destination	Target
10.1.0.0/16	Local

2. In FortiGate CNF, deploy a GWLBe to this subnet.
3. In AWS, add a route to the `Private Subnet in Availability Zone 1` route table to route all traffic going to `Private Subnet in Availability Zone 2` to the GWLBe.

Destination	Target
10.1.0.0/16	Local
10.1.4.0/24	GWLBe

4. In AWS, add a route to the `Private Subnet in Availability Zone 2` route table to route all traffic to `Private Subnet in Availability Zone 1` to the GWLBe.

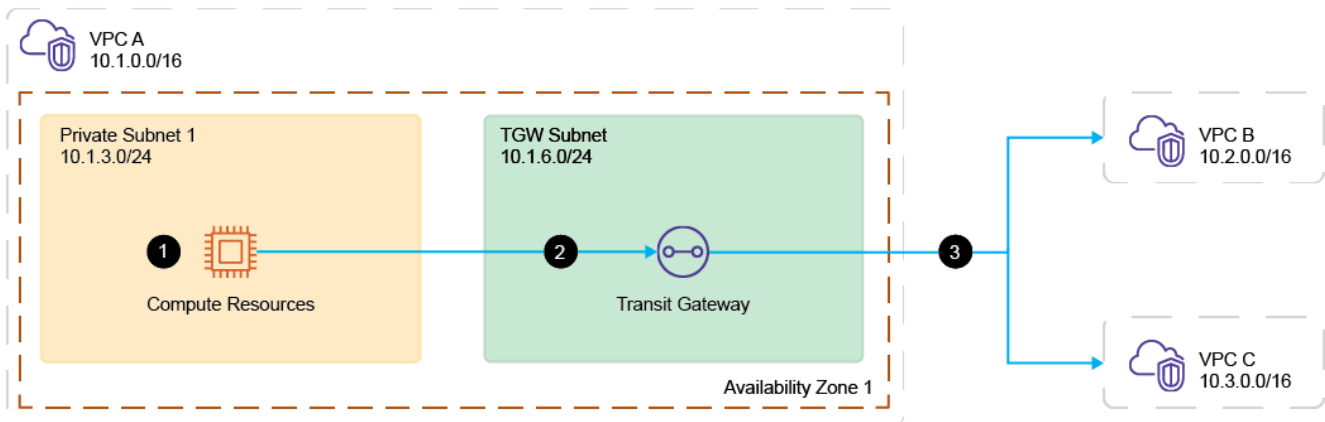
Destination	Target
10.1.0.0/16	Local
10.1.3.0/24	GWLBe

Distributed inter-VPC east-west traffic - Example

Scenario objective

Traffic between multiple VPCs is inspected by a FortiGate CNF instance.

Before deployment of FortiGate CNF



The traffic in this scenario is east-west between two VPCs. A transit gateway attached to the VPC is needed for this to work. The traffic is between `VPC A` and `VPC B`, or `VPC A` and `VPC C`.

The *Before deployment of FortiGate CNF* traffic flow is as follows:

1. Traffic originates from computer resources located in Private Subnet 1 in VPC A (10.1.3.0/24) and goes to AWS Transit Gateway located in TGW Subnet (10.1.6.0/24).
2. AWS Transit Gateway forwards the traffic to VPC B (10.2.0.0/16) or VPC C (10.3.0.0/16).

Routing tables

The routing tables are defined as follows.

Private Subnet route table

Destination	Target
10.1.0.0/16	Local

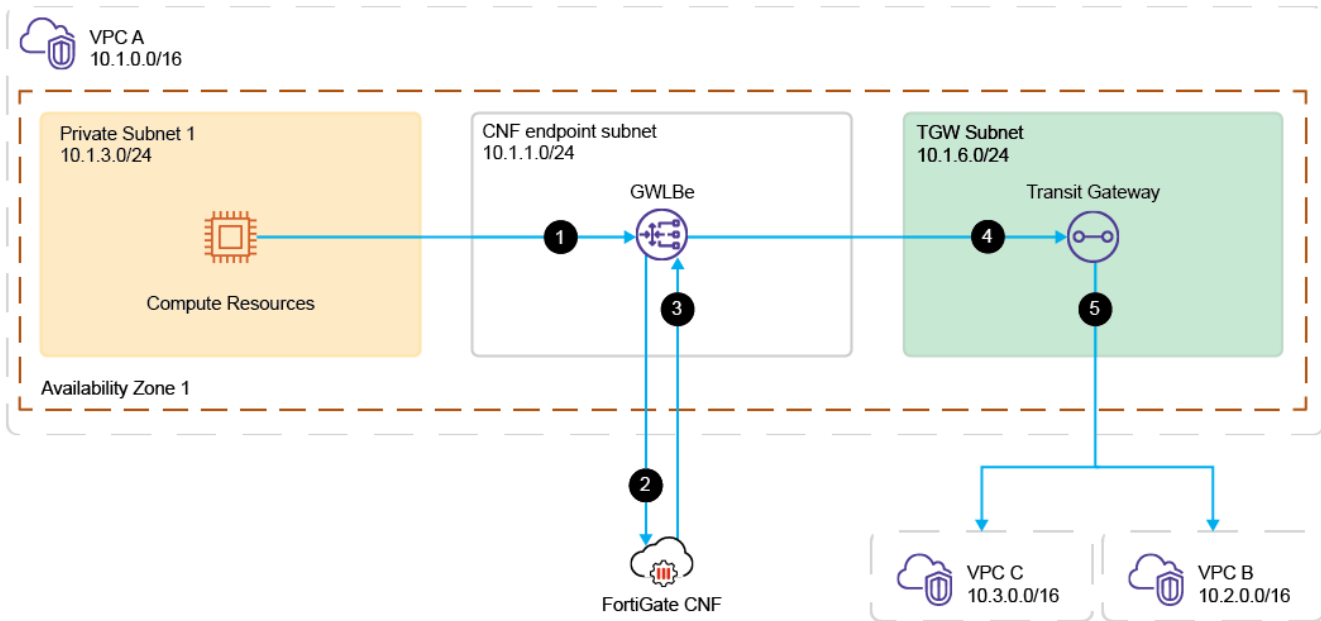
TGW Subnet route table

Destination	Target
10.1.0.0/16	Local

AWS Transit Gateway route table

Destination	Target
10.1.0.0/16	VPC A
10.2.0.0/16	VPC B
10.3.0.0/16	VPC C

After deployment of FortiGate CNF



The After deployment of FortiGate CNF topology traffic flow is as follows:

1. Traffic originates from computer resources located in Private Subnet 1 in VPC A (10.1.3.0/24) and goes to the GWLBe located in CNF Endpoint Subnet (10.1.1.0/24).
2. Traffic is sent to the FortiGate CNF instance for inspection.
3. FortiGate CNF sends traffic back to the GWLBe.
4. Traffic goes to AWS Transit Gateway located in TGW Subnet (10.1.6.0/24).
5. AWS Transit Gateway forwards the traffic to VPC B (10.2.0.0/16) or VPC C (10.3.0.0/16).

To deploy the FortiGate CNF instance in this scenario:

1. In AWS, add a subnet `CNF Endpoint Subnet` in VPC A along with the associated route table.

Destination	Target
10.1.0.0/16	Local
10.0.0.0/8	AWS Transit Gateway

2. In FortiGate CNF, deploy a GWLBe to this subnet.
3. In AWS, add a route to the `Private Subnet 1` route table to route all traffic to 10.0.0.0/8 to the GWLBe.

Destination	Target
10.1.0.0/16	Local
10.0.0.0/8	GWLBe

4. In AWS, add a route to the `TGW subnet` route table to route all traffic to `Private Subnet 1` to the GWLBe.

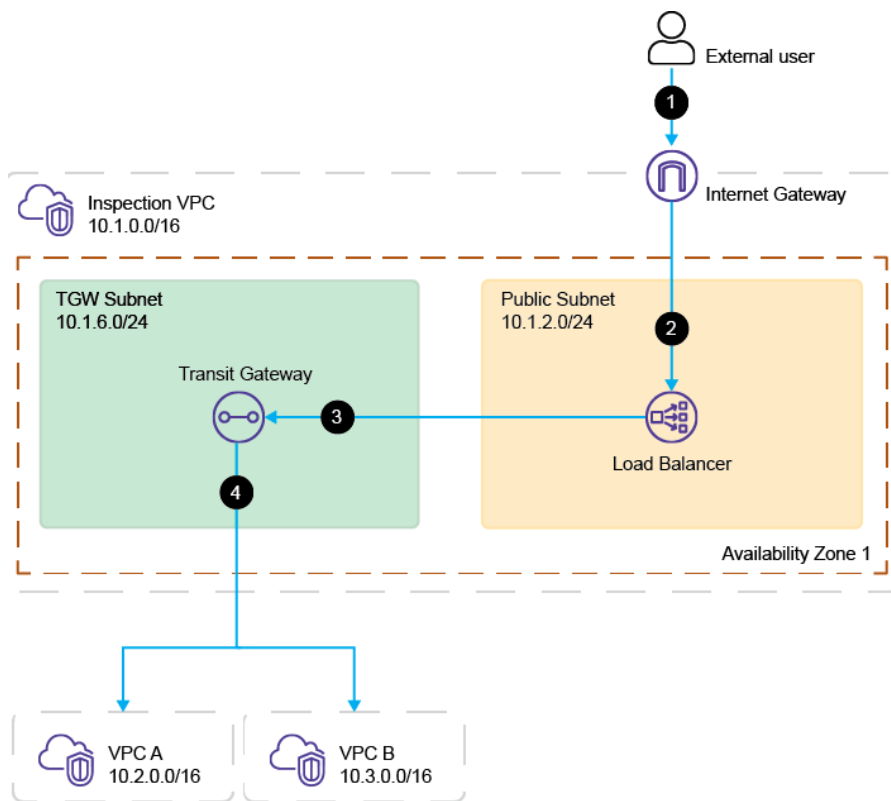
Destination	Target
10.1.0.0/16	Local
10.1.3.0/24	GWLBe

Centralized ingress: inspection before load balancer - Example

Scenario objective

Inbound traffic is inspected by a FortiGate CNF instance before passing to the load balancer.

Before deployment of FortiGate CNF



In this scenario, there is a dedicated VPC called `Inspection VPC` that contains the load balancer. The workloads are in different VPCs (`VPC A` and `VPC B`), and traffic between VPCs is routed through a transit gateway.

The *Before deployment of FortiGate CNF* traffic flow is as follows:

1. Traffic originates from an external user and enters through the `Internet Gateway`.
2. The `Internet Gateway` sends the traffic to the `Load Balancer` located in `Public Subnet (10.1.2.0/24)`.
3. The `Load Balancer` send the traffic to the `AWS Transit Gateway` located in `TGW Subnet (10.1.6.0/24)`.
4. The `AWS Transit Gateway` forwards the traffic to `VPC A (10.2.0.0/16)` or `VPC B (10.3.0.0/16)`.

Routing tables

The routing tables are defined as follows.

Internet Gateway route table

Destination	Target
10.1.0.0/16	Local

Public Subnet route table

Destination	Target
10.1.0.0/16	Local
10.0.0.0/8	AWS Transit Gateway

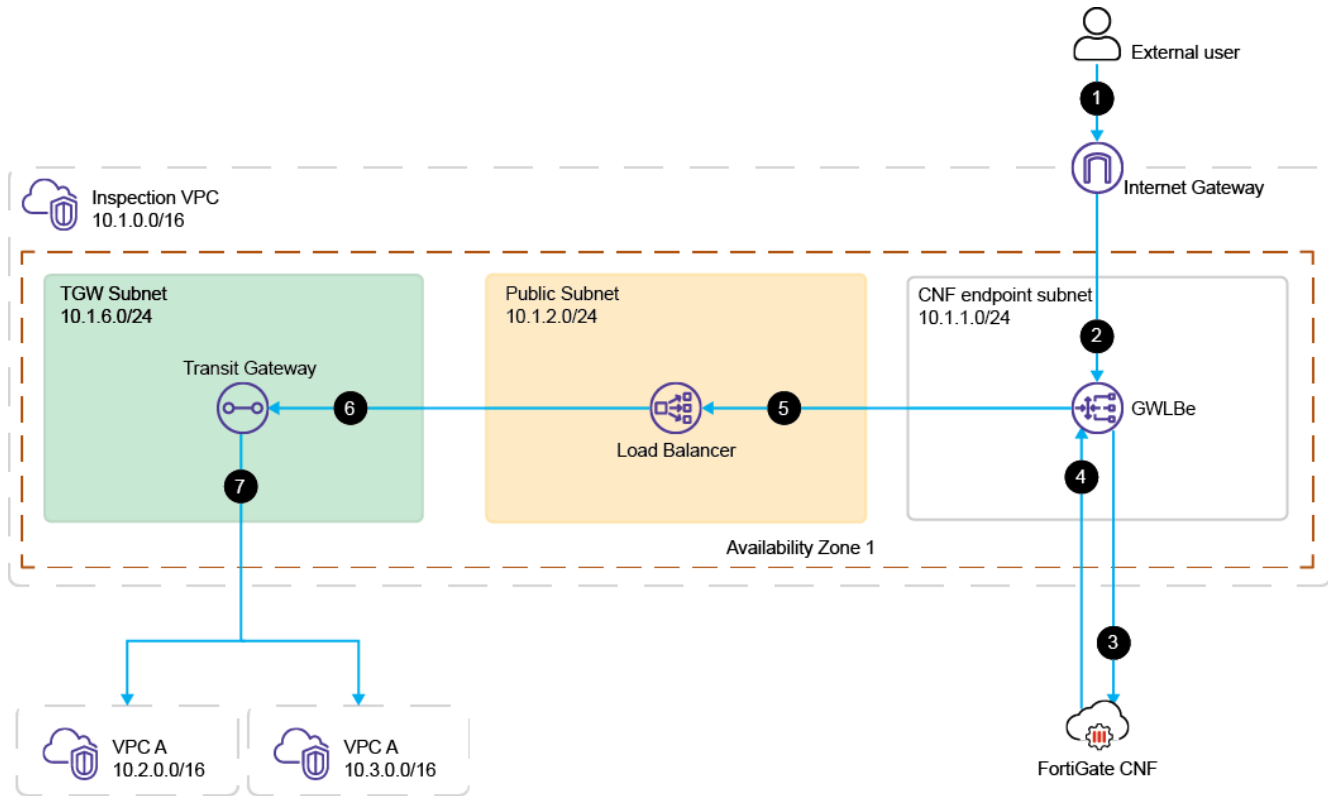
TGW Subnet route table

Destination	Target
10.1.0.0/16	Local

AWS Transit Gateway route table

Destination	Target
10.1.0.0/16	Inspection VPC
10.2.0.0/16	VPC A
10.3.0.0/16	VPC B

After deployment of FortiGate CNF



The After deployment of FortiGate CNF traffic flow is as follows:

1. Traffic originate from an external user and enters through the `Internet Gateway`.
2. The `Internet Gateway` sends the traffic to the `GWLBe` located in `CNF Endpoint Subnet (10.1.1.0/24)`.
3. Traffic is sent to the `FortiGate CNF` instance for inspection.
4. `FortiGate CNF` sends traffic back to the `GWLBe`.
5. `GWLBe` sends traffic to the `Load Balancer` located in `Public Subnet (10.1.2.0/24)`.
6. The `Load Balancer` send the traffic to the `AWS Transit Gateway` located in `TGW Subnet (10.1.6.0/24)`.
7. The `AWS Transit Gateway` forwards the traffic to `VPC A (10.2.0.0/16)` or `VPC B (10.3.0.0/16)`.

To deploy the `FortiGate CNF` instance in this scenario:

1. In AWS, add a subnet `CNF Endpoint Subnet` in `Inspection VPC` along with the associated route table.

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	Internet Gateway

2. In `FortiGate CNF`, deploy a `GWLBe` to this subnet.
3. In AWS, add a route to the `Internet Gateway` route table to route all traffic to `Public Subnet` to the `GWLBe`.

Destination	Target
10.1.0.0/16	Local
10.1.2.0/24	GWLBe

- In AWS, add a route to the `Public Subnet` route table where the load balancer resides to route all traffic to the GWLBe.

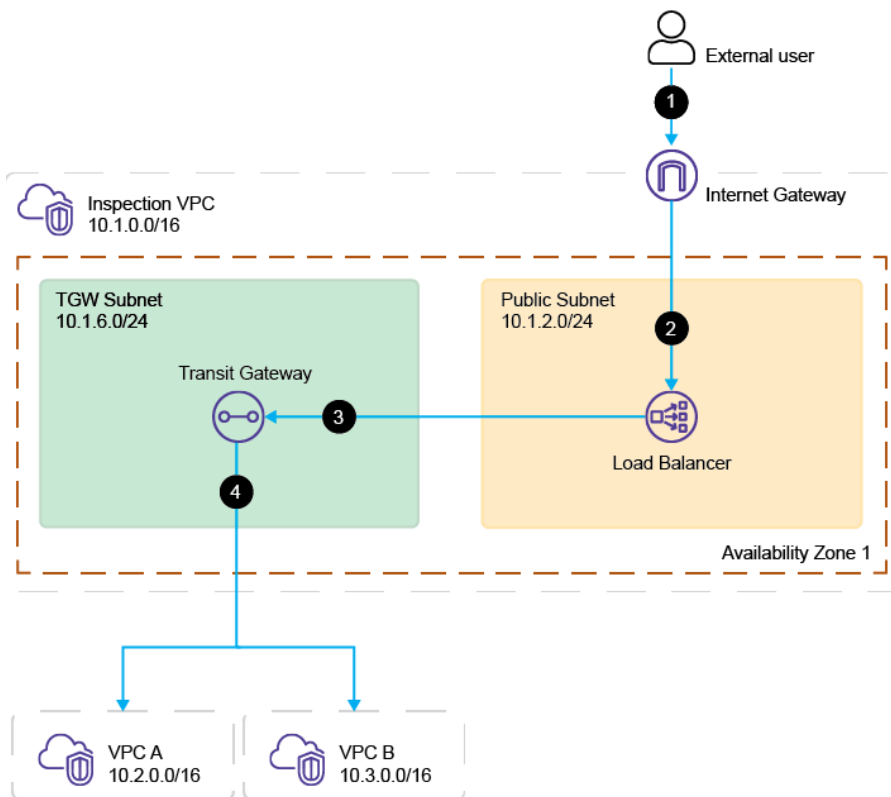
Destination	Target
10.1.0.0/16	Local
10.0.0.0/8	AWS Transit Gateway
0.0.0.0/0	GWLBe

Centralized ingress: inspection after load balancer - Example

Scenario objective

Inbound traffic is inspected by a FortiGate CNF instance after passing through the load balancer.

Before deployment of FortiGate CNF



In this scenario, there is a dedicated VPC called `Inspection VPC` that contains the load balancer. The workloads are in different VPCs (`VPC A` and `VPC B`), and traffic between VPCs is routed through a transit gateway.

The *Before deployment of FortiGate CNF* traffic flow is as follows:

1. Traffic originates from an external user and enters through the `Internet Gateway`.
2. The `Internet Gateway` sends the traffic to the `Load Balancer` located in `Public Subnet (10.1.2.0/24)`.
3. The `Load Balancer` send the traffic to the `AWS Transit Gateway` located in `TGW Subnet (10.1.6.0/24)`.
4. The `AWS Transit Gateway` forwards the traffic to `VPC A (10.2.0.0/16)` or `VPC B (10.3.0.0/16)`.

Routing tables

The routing tables are defined as follows.

Internet Gateway route table

Destination	Target
10.1.0.0/16	Local

Public Subnet route table

Destination	Target
10.1.0.0/16	Local
10.0.0.0/8	AWS Transit Gateway

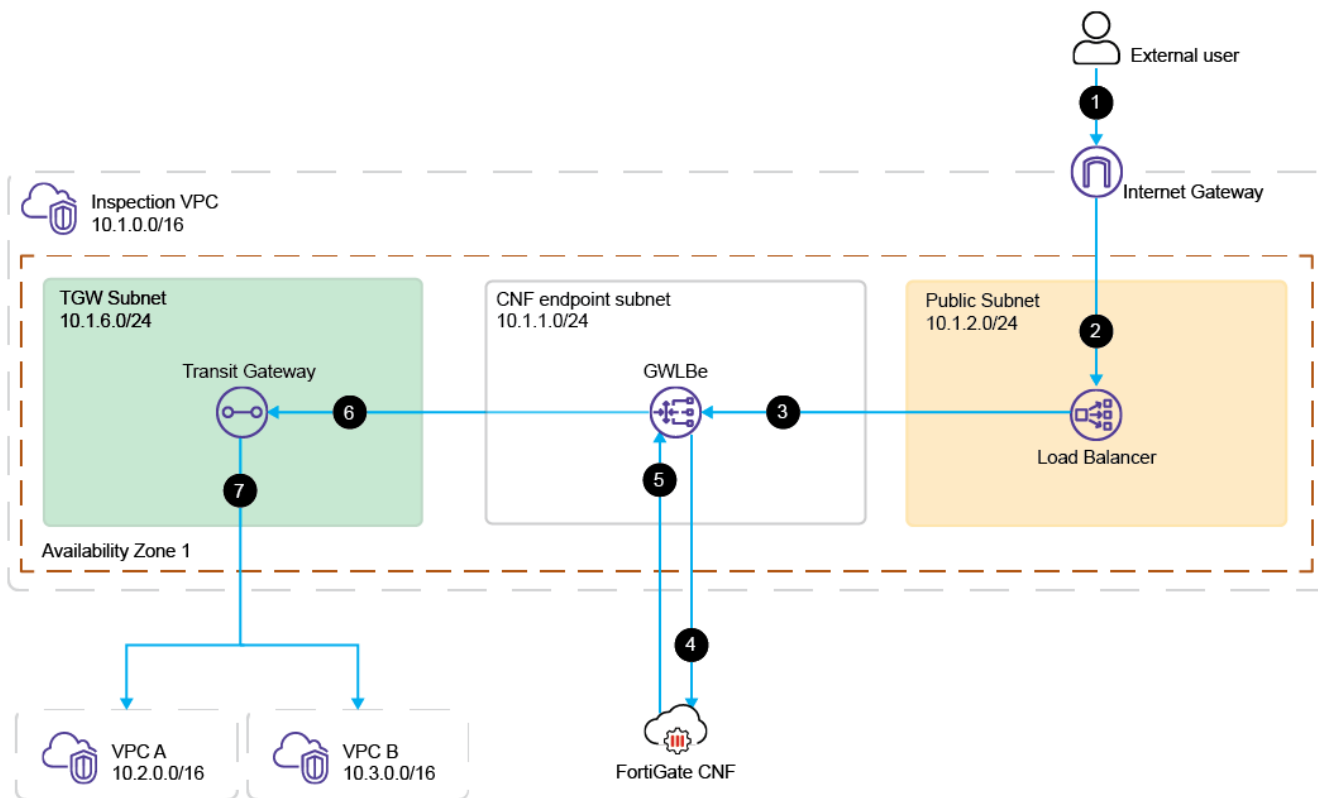
TGW Subnet route table

Destination	Target
10.1.0.0/16	Local

AWS Transit Gateway route table

Destination	Target
10.1.0.0/16	Inspection VPC
10.2.0.0/16	VPC A
10.3.0.0/16	VPC B

After deployment of FortiGate CNF



The After deployment of FortiGate CNF traffic flow is as follows:

1. Traffic originates from an external user and enters through the Internet Gateway.
2. The Internet Gateway sends the traffic to the Load Balancer located in Public Subnet (10.1.2.0/24).
3. The Load Balancer sends the traffic to the GWLBe located in CNF Endpoint Subnet (10.1.1.0/24).
4. GWLBe sends traffic to the FortiGate CNF instance for inspection.
5. FortiGate CNF sends traffic back to the GWLBe.
6. GWLBe sends traffic to the AWS Transit Gateway located in TGW Subnet (10.1.6.0/24).
7. The AWS Transit Gateway forwards the traffic to VPC A (10.2.0.0/16) or VPC B (10.3.0.0/16).

To deploy the FortiGate CNF instance in this scenario:

1. In AWS, add a subnet CNF Endpoint Subnet in Inspection VPC along with the associated route table.

Destination	Target
10.1.0.0/16	Local
10.0.0.0/8	AWS Transit Gateway

2. In FortiGate CNF, deploy a GWLBe to this subnet.
3. In AWS, add a route to the Public Subnet route table where the load balancer resides to route all traffic to 10.0.0.0/8 to the GWLBe.

Destination	Target
10.1.0.0/16	Local
0.0.0.0/8	Internet Gateway
10.0.0.0/8	GWLBe

4. In AWS, add a route to the `Transit Gateway Subnet` route table to route all traffic to the `Load Balancer` located in `Public Subnet` to the `GWLBe`.

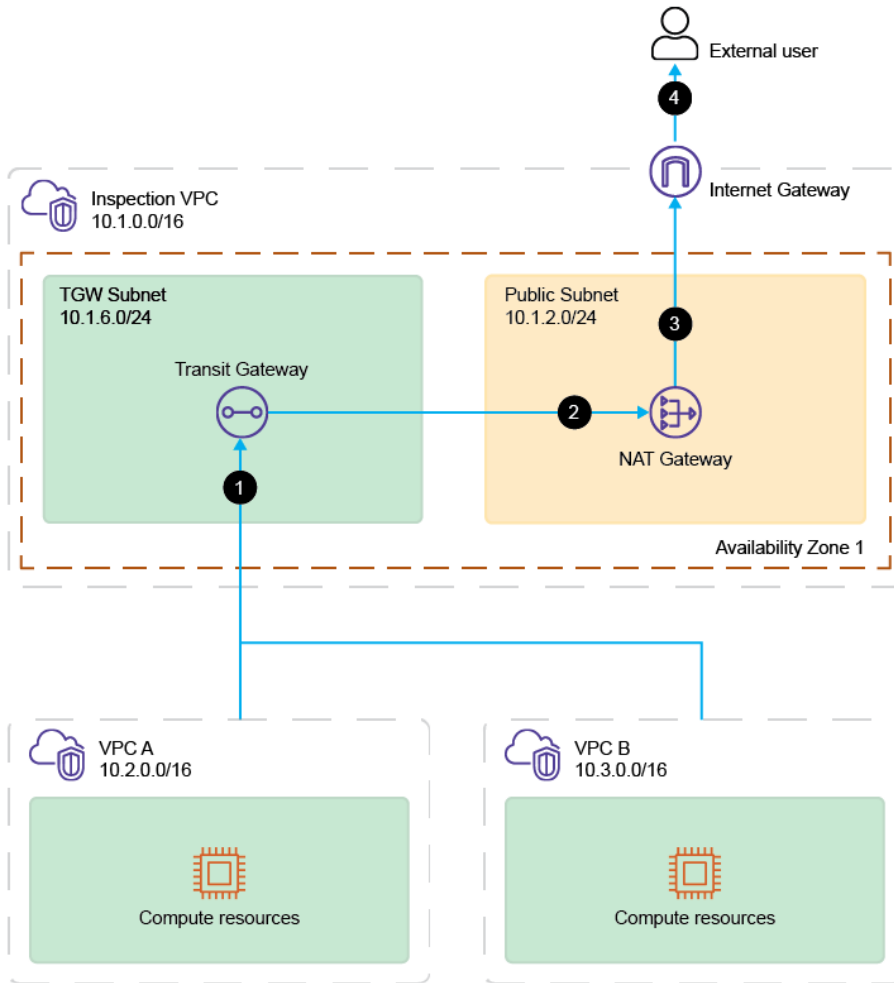
Destination	Target
10.1.0.0/16	Local
10.1.2.0/24	GWLBe

Centralized egress - Example

Scenario objective

Outbound traffic to the internet from a private subnet in `VPC A` or `VPC B` is inspected by a FortiGate CNF instance.

Before deployment of FortiGate CNF



In this scenario, the workload is located in a private subnet in VPC A or VPC B. The traffic is outbound to internet.

The *Before deployment of FortiGate CNF* traffic flow is as follows:

1. Traffic originates in compute resources located in VPC A (10.2.0.0/16) or VPC B (10.3.0.0/16) and goes to AWS Transit Gateway located in TGW Subnet (10.1.6.0/24) in Inspection VPC (10.1.0.0/16).
2. AWS Transit Gateway sends the traffic to the NAT Gateway located in Public Subnet (10.1.2.0/24).
3. NAT Gateway forwards the traffic on to the Internet Gateway.
4. The Internet Gateway sends the traffic to the external user.

Routing tables

The routing tables are defined as follows.

VPC A Private Subnet route table

Destination	Target
10.2.0.0/16	Local
0.0.0.0/0	AWS Transit Gateway

Public Subnet route table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	Internet Gateway

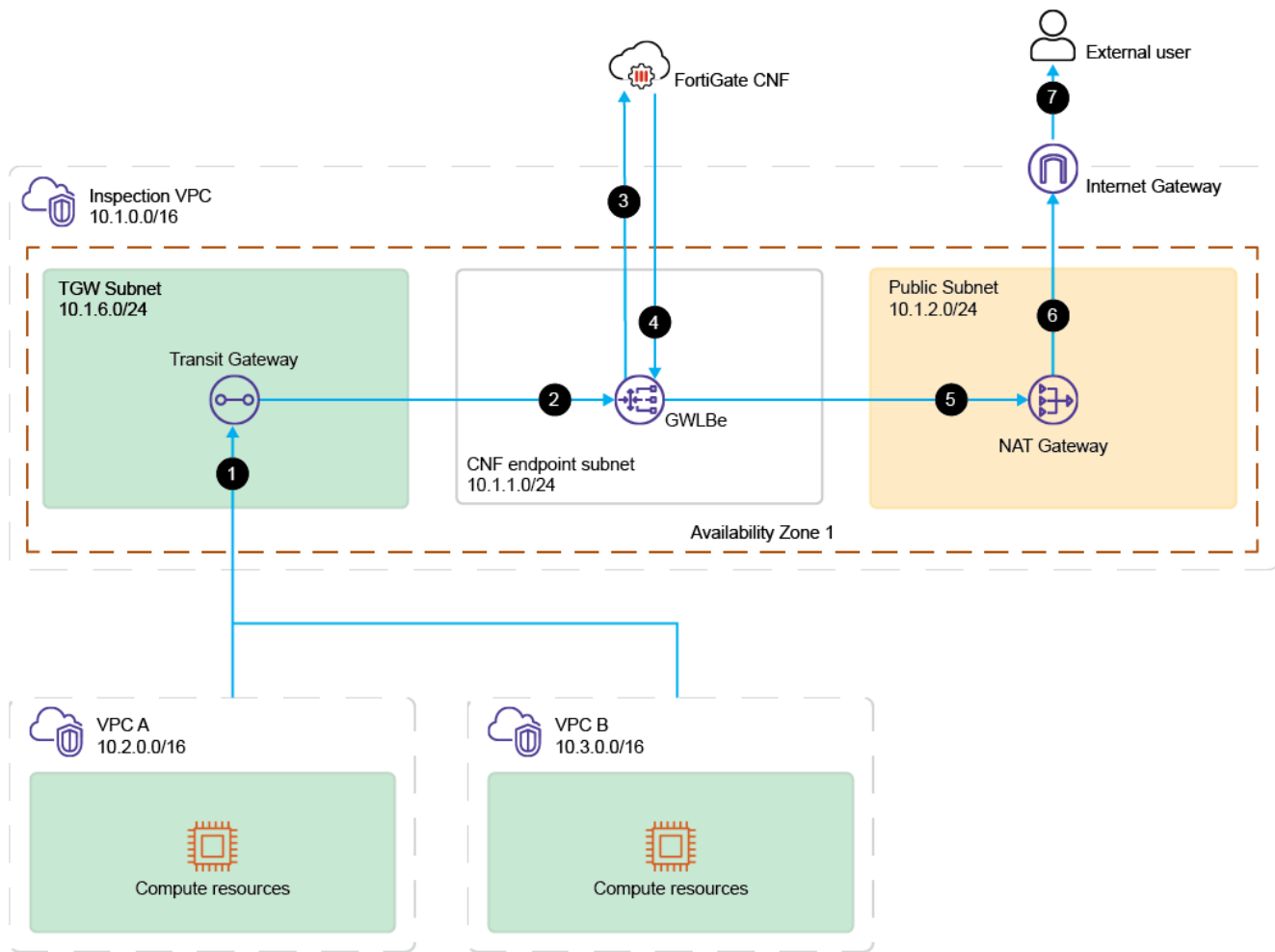
TGW Subnet route table

Destination	Target
10.1.0.0/16	Local

AWS Transit Gateway route table

Destination	Target
0.0.0.0/16	Inspection VPC
10.2.0.0/16	VPC A
10.3.0.0/16	VPC B

After deployment of FortiGate CNF



The After deployment of FortiGate CNF traffic flow is as follows:

1. Traffic originates in compute resources located in VPC A (10.2.0.0/16) or VPC B (10.3.0.0/16) and goes to AWS Transit Gateway located in TGW Subnet (10.1.6.0/24) in Inspection VPC (10.1.0.0/16).
2. AWS Transit Gateway sends the traffic to the GWLBe located in CNF Endpoint Subnet (10.1.1.0/24).
3. Traffic is sent to the FortiGate CNF instance for inspection.
4. FortiGate CNF sends traffic back to the GWLBe.
5. GWLBe sends traffic to the NAT Gateway located in Public Subnet (10.1.2.0/24).
6. NAT Gateway forwards the traffic on to the Internet Gateway.
7. The Internet Gateway send the traffic to the external user.

To deploy the FortiGate CNF instance in this scenario:

1. In AWS, add a subnet `CNF_Endpoint_Subnet` in `Inspection_VPC` along with the associated route table.

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	Internet Gateway
10.0.0.0/8	AWS Transit Gateway

2. In FortiGate CNF, deploy a GWLBe to this subnet.
3. In AWS, add a route to the `Public_Subnet` route table where the NAT gateway resides to route all traffic to 10.0.0.0/8 to the GWLBe.

4.

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	Internet Gateway
10.0.0.0/8	GWLBe

5. In AWS, add a route to the `Transit_Gateway_Subnet` route table to route all traffic to the GWLBe.

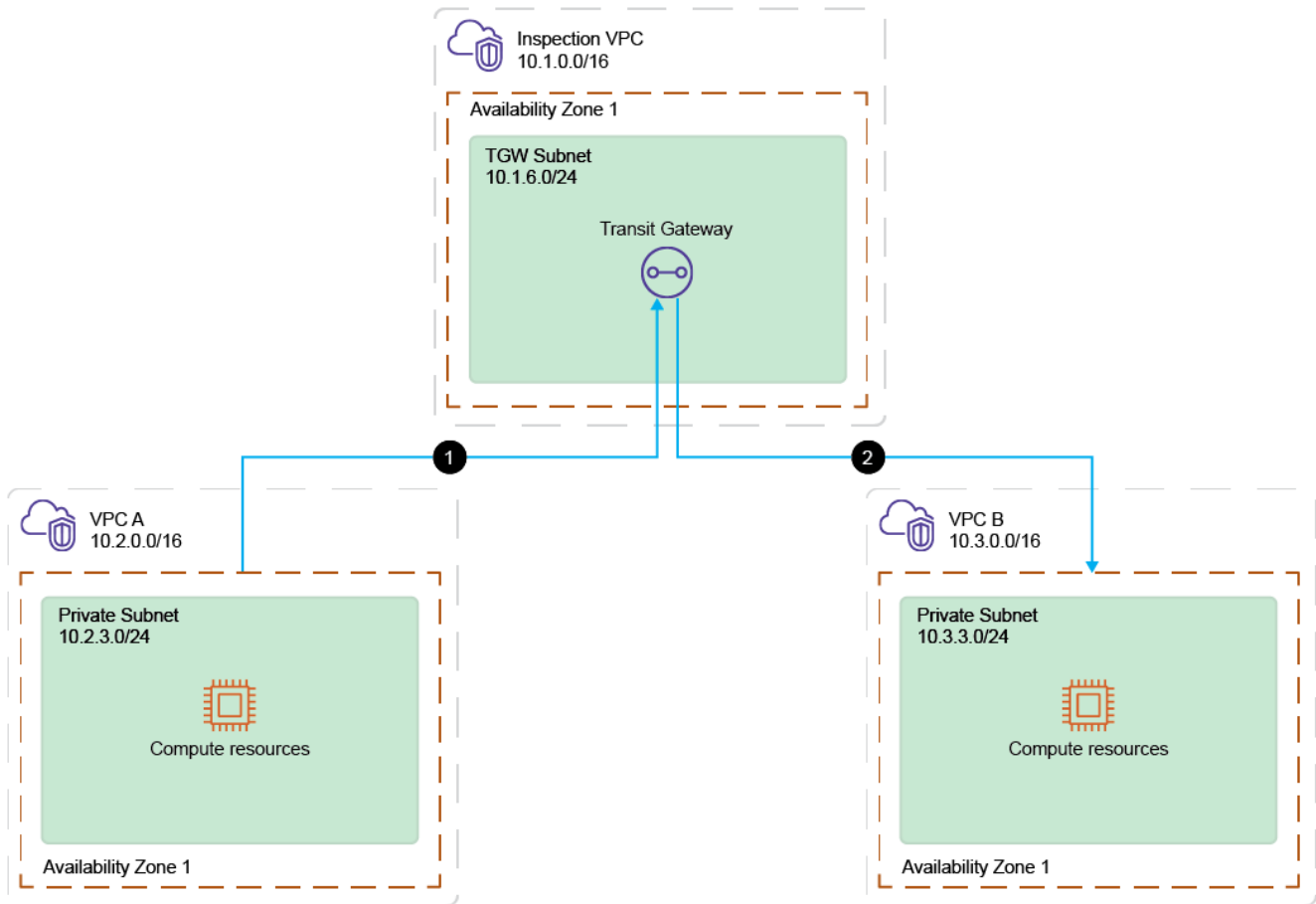
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	GWLBe

Centralized east-west, inter-VPC - Example

Scenario objective

Traffic between two VPCs, `VPC_A` and `VPC_B`, is inspected by a FortiGate CNF instance.

Before deployment of FortiGate CNF



In this scenario, traffic is between two VPCs, VPC A and VPC B, through a transit gateway.

The *Before deployment of FortiGate CNF* traffic flow is as follows:

1. Traffic originates from `Private Subnet (10.2.3.0/24)` in VPC A (`10.2.0.0/16`) and goes to the AWS Transit Gateway located in `TGW Subnet (10.1.6.0/24)` in `Inspection VPC (10.1.0.0/16)`.
2. AWS Transit Gateway sends the traffic to `Private Subnet (10.3.3.0/24)` in VPC B (`10.3.0.0/16`).

Routing tables

The routing tables are defined as follows.

Private Subnet (VPC A) route table

Destination	Target
10.2.0.0/16	Local
0.0.0.0/0	AWS Transit Gateway

Private Subnet AWS Transit Gateway (VPC A) route table

Destination	Target
0.0.0.0/0	Inspection VPC

Private Subnet (VPC B) route table

Destination	Target
10.3.0.0/16	Local
0.0.0.0/0	AWS Transit Gateway

Private Subnet AWS Transit Gateway (VPC B) route table

Destination	Target
0.0.0.0/0	Inspection VPC

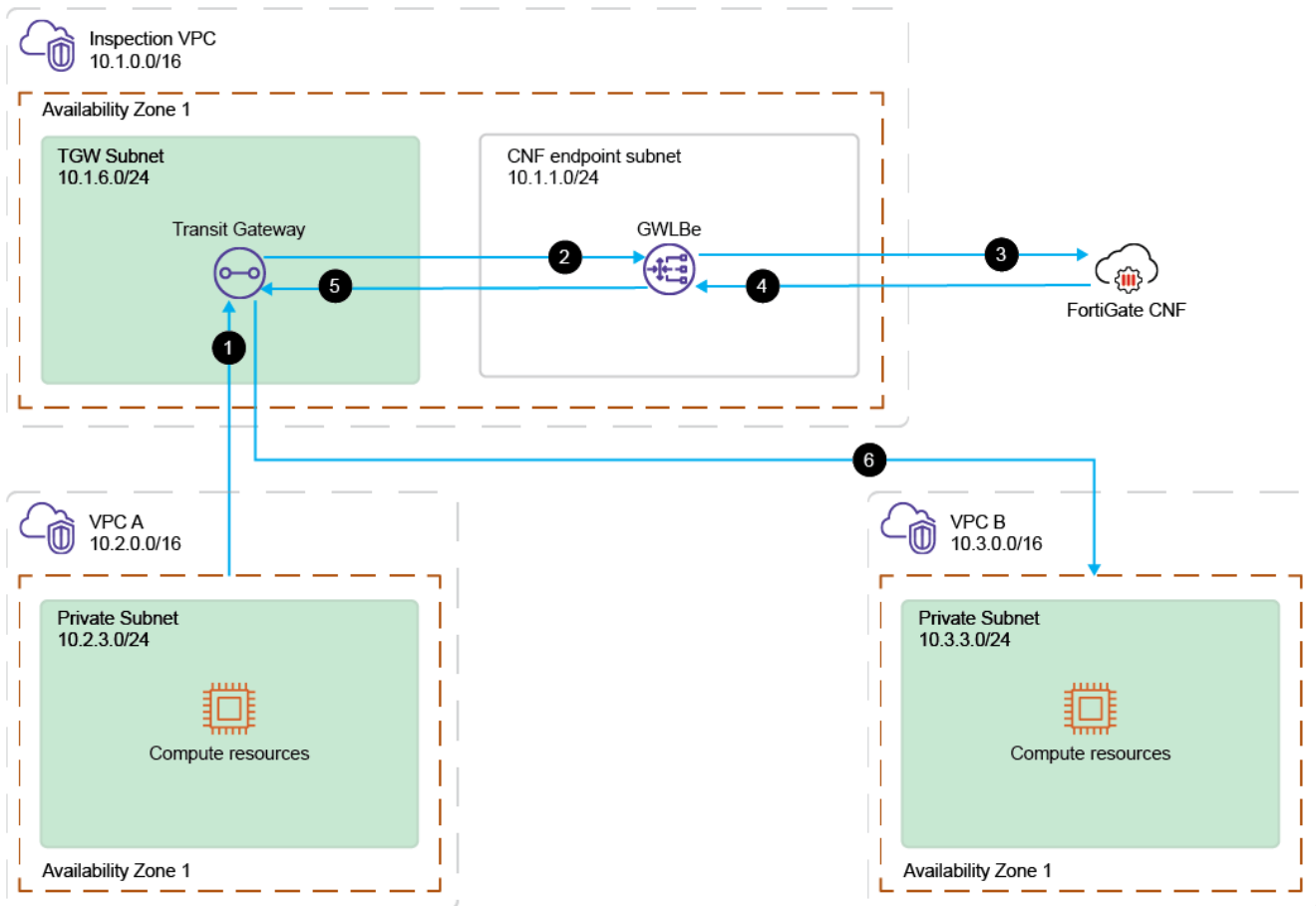
TGW Subnet route table

Destination	Target
10.1.0.0/16	Local

AWS Transit Gateway route table

Destination	Target
10.2.0.0/16	VPC A
10.3.0.0/16	VPC B

After deployment of FortiGate CNF



The After deployment of FortiGate CNF traffic flow is as follows:

1. Traffic originates from Private Subnet (10.2.3.0/24) in VPC A (10.2.0.0/16) and goes to the AWS Transit Gateway located in TGW Subnet (10.1.6.0/24) in Inspection VPC (10.1.0.0/16).
2. AWS Transit Gateway sends the traffic to the GWLBe located in CNF Endpoint Subnet (10.1.1.0/24).
3. Traffic is sent to the FortiGate CNF instance for inspection.
4. FortiGate CNF sends traffic back to the GWLBe.
5. GWLBe sends the traffic to AWS Transit Gateway.
6. AWS Transit Gateway forwards the traffic on to Private Subnet (10.3.3.0/24) in VPC B (10.3.0.0/16).

To deploy the FortiGate CNF instance in this scenario:

1. In AWS, add a subnet `CNF_Endpoint_Subnet` in `Inspection_VPC` along with the associated route table.

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT Gateway
10.0.0.0/8	AWS Transit Gateway

2. In FortiGate CNF, deploy a GWLBe to this subnet.
3. In AWS, add a route to the `Transit_Gateway_Subnet` route table to route all traffic to the GWLBe.

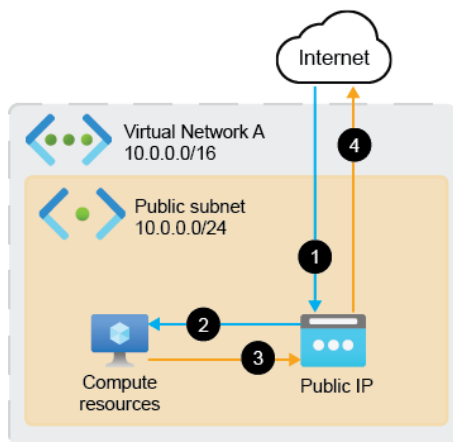
Destination	Target
10.1.0.0/16	Local
0.0.0.0/8	GWLBe

Azure ingress and egress using public IP - Example

Scenario objective

The FortiGate CNF instance inspects all external traffic inbound to compute resources and all traffic outbound from compute resources to the internet.

Before deployment of FortiGate CNF

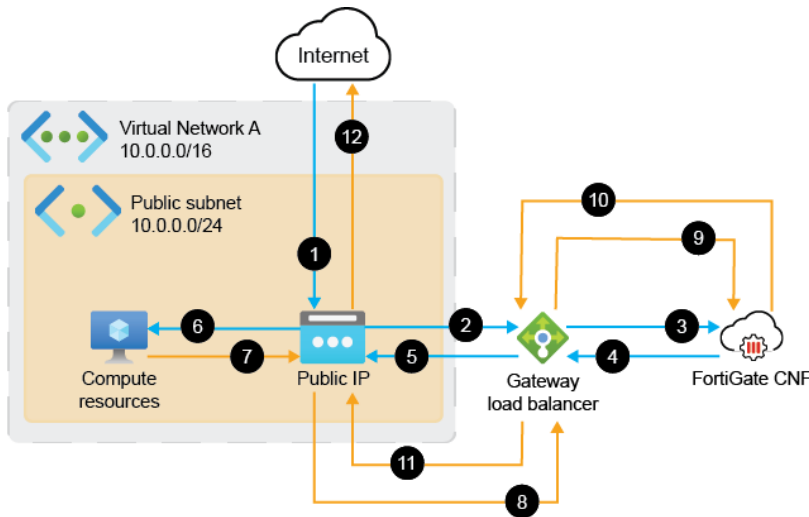


The *Before deployment of FortiGate CNF* traffic flow is as follows:

Workload resources are situated in `Public Subnet` (10.0.0.0/24).

1. Inbound traffic comes from the internet to the `Public IP` located in `Public Subnet (10.0.0.0/24)`.
2. Traffic passes to the workload resources in `Public Subnet (10.0.0.0/24)`.
3. Outbound traffic goes from the workload resources in `Public Subnet` to the `Public IP` located in `Public Subnet (10.0.0.0/24)`.
4. Traffic passes out to the internet.

After deployment of FortiGate CNF



The *after* topology traffic flow is as follows:

1. Inbound traffic comes from the internet to the `Public IP` located in `Public subnet (10.0.0.0/24)`.
2. Traffic is sent to the `Gateway load balancer`.
3. The `Gateway load balancer` forwards the traffic to `FortiGate CNF`.
4. After inspection, `FortiGate CNF` sends the traffic back to the `Gateway load balancer`.
5. The `Gateway load balancer` sends the traffic back to the `Public IP`.
6. The `Public IP` forwards the traffic to the workload resources in `Public Subnet (10.0.0.0/24)`.
7. Outbound traffic goes from the workload resources in `Public Subnet` to the `Public IP`.
8. Traffic is sent to the `Gateway load balancer`.
9. The `Gateway load balancer` forwards the traffic to `FortiGate CNF`.
10. After inspection, `FortiGate CNF` sends the traffic back to the `Gateway load balancer`.
11. The `Gateway load balancer` sends the traffic back to the `Public IP`.
12. Traffic passes out to the internet.

To deploy the FortiGate CNF instance in this scenario:

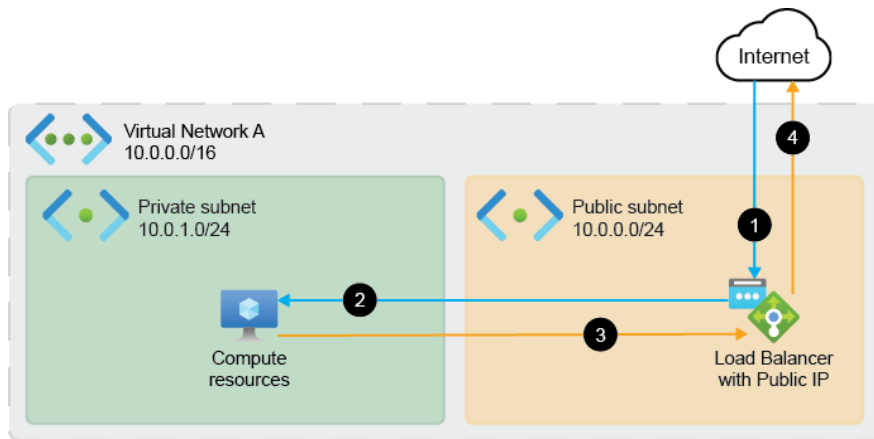
1. In the FortiGate CNF console, in the instance settings, go to *Configure Azure Endpoints*.
2. Click *Link Existing* and connect to the virtual machine `Public IP`.
To edit the load balancer, see [Editing a linked load balancer on page 41](#).

Azure ingress and egress using Load Balancer with public IP - Example

Scenario objective

The FortiGate CNF instance inspects all external traffic inbound to compute resources and all traffic outbound from compute resources to the internet.

Before deployment of FortiGate CNF

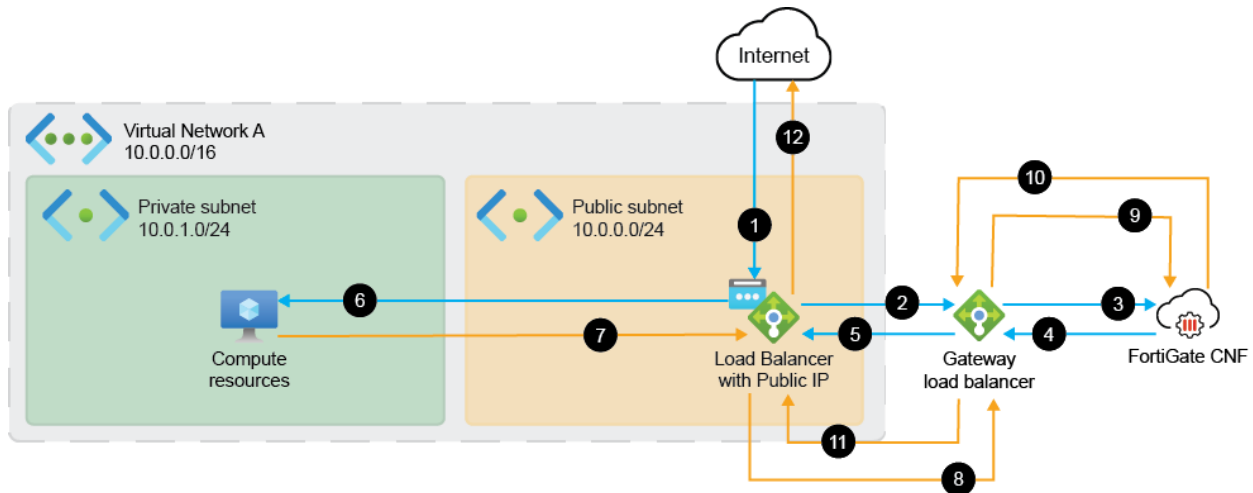


The *Before deployment of FortiGate CNF* traffic flow is as follows:

Workload resources are situated in Private Subnet (10.0.1.0/24) and accessed through Load Balancer with Public IP in Public Subnet (10.0.0.0/24).

1. Inbound traffic comes from the internet to the Load Balancer with Public IP located in Public Subnet (10.0.0.0/24).
2. Traffic passes to the workload resources in Private Subnet (10.0.1.0/24).
3. Outbound traffic goes from the workload resources in Private Subnet to the Load Balancer with Public IP located in Public Subnet (10.0.0.0/24).
4. Traffic passes out to the internet.

After deployment of FortiGate CNF



The *after* topology traffic flow is as follows:

1. Inbound traffic comes from the internet to the Load Balancer with Public IP located in Public subnet (10.0.0.0/24).
2. Traffic is sent to the Gateway load balancer.
3. The Gateway load balancer forwards the traffic to FortiGate CNF.
4. After inspection, FortiGate CNF sends the traffic back to the Gateway load balancer.
5. The Gateway load balancer sends the traffic back to the Load Balancer with Public IP.
6. The Load Balancer with Public IP forwards the traffic to the workload resources in Private Subnet (10.0.1.0/24).
7. Outbound traffic goes from the workload resources in Private Subnet to the Load Balancer with Public IP.
8. Traffic is sent to the Gateway load balancer.
9. The Gateway load balancer forwards the traffic to FortiGate CNF.
10. After inspection, FortiGate CNF sends the traffic back to the Gateway load balancer.
11. The Gateway load balancer sends the traffic back to the Load Balancer with Public IP.
12. Traffic passes out to the internet.

To deploy the FortiGate CNF instance in this scenario:

1. In the FortiGate CNF console, in the instance settings, go to *Configure Azure Endpoints*.
2. Click *Link Existing* and connect to the Load Balancer.

To edit the load balancer, see [Editing a linked load balancer on page 41](#).

Appendix B - Using AWS Firewall Manager

You can use the AWS Firewall Manager to create and deploy FortiGate CNF instances.



Policies and policy sets must be first created in the FortiGate CNF console before they can be used in AWS Firewall Manager.

See [Configuration on page 62](#).

To use AWS Firewall Manager with FortiGate CNF:

1. Go to the AWS console for the appropriate AWS account.
2. Search for AWS Firewall Manager service.
3. In the *Third party firewall association status* section, ensure that *Fortigate Cloud Native Firewall as a Service* is listed with a *Status of Associated*. If *Status is Disassociated*, select the service and click *Associate*.
4. In the left menu, click *Security Policies* then click *Create Policy* and follow the on screen wizard:
 - a. Under *Third-party services*, select *FortiGate Cloud Native Firewall as a Service*.
 - b. In *Firewall management type*, select one of *Distributed* or *Centralized*.
 - c. Select a region.
5. Enter a policy name.
6. In the *FortiGate Cloud Native Firewall as a Service policy configuration* section, select the appropriate policy set then click *Next*.

To configure a policy, select the policy and click *Configure policy* to open the policy in the FortiGate CNF console.

To update the list of policy sets, click the refresh button.
7. Select the availability zones (AZ) where your traffic will be routed. AWS creates a subnet and adds a GWLBe in that subnet.



This process adds a GWLBe in this AWS account, but any required routes must be configured manually to route traffic to this endpoint.

8. In *Define policy scope*, select the appropriate scope for this policy. If you select *Include all accounts*, download and run the CloudFormation template found in the lower section in each member account. For *Resource type*, enable or disable *VPC* and include or exclude VPCs by tag.
9. Optionally, add tags to the policy.
10. Review the policy configuration, then click *Create policy*.

You are redirected to the policy list page and AWS calls FortiGate CNF APIs to create the resources, such as the FortiGate CNF instance, the gateway load balancer, and GWLBe. This process can take 10–15 min.

Click the policy link to view the details.

In the *Accounts within policy scope* section, click on a specific AWS account to view the resources being created.



While these resources are being created, the *Violation reason* column displays the error message: "the FortigateCNF is not provisioned correctly". This message indicates the resource is not ready yet and is not an actual error.



www.fortinet.com

Copyright© 2024 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 Chief Legal Officer, 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.