ORACLE

Deploying Cisco Secure Firewall Threat Defense (FTD) with Cisco Firepower Management Center (FMC) on Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance

Version 1.0
Copyright © 2026, Oracle and/or its affiliates
Public

Purpose statement

This solution paper provides guidance for deploying and configuring Cisco Secure Firewall Threat Defense (FTD) with Cisco Secure Firepower Management Center (FMC) on Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA). It addresses the growing enterprise need for advanced network security, threat prevention, and centralized firewall management within Oracle's sovereign cloud infrastructure.

Organizations leveraging Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) can utilize Cisco Secure Firewall to deliver enterprise-grade stateful inspection, intrusion prevention, application visibility, and advanced threat protection while maintaining data sovereignty and regulatory compliance requirements.

This document provides IT architects, network security engineers, and infrastructure teams with step-by-step deployment procedures and configuration guidelines necessary to successfully implement Cisco Secure Firewall Threat Defense (FTD) with Cisco Secure Firepower Management Center (FMC) in Oracle's Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) environments.

Target Audience: Solution architects, network security engineers, infrastructure administrators, and IT professionals responsible for firewall deployment and security policy management on Oracle C3.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.
This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.
This document may include some forward-looking content for illustrative purposes only. Some products and features discussed are indicative of the products and features of a prospective future launch in the United States only or elsewhere. Not all products and features discussed are currently offered for sale in the United States or elsewhere. Products and features of the actual offering may differ from those discussed in this document and may vary from country to country. Any timelines contained in this document are indicative only. Timelines and product features may depend on regulatory approvals or certification for individual products or features in the applicable country or region.

ORACLE

Table of contents

Introduction

Cisco and Oracle Edge Cloud deliver advanced network security through Cisco Secure Firewall Threat Defense (FTD), a comprehensive next-generation firewall platform designed to provide advanced threat protection, deep application visibility, and centralized policy management. This joint solution enables organizations to rapidly and securely deploy enterprise-grade firewall services on Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance environments.

Cisco Secure Firewall Threat Defense Virtual (FTDv) runs the same software used by Cisco's physical firewall appliances, delivering proven security capabilities in a virtualized form factor. When deployed on Oracle Compute Cloud@Customer or Private Cloud Appliance, FTDv can be configured to protect workloads across modern data center environments that dynamically scale, evolve, or shift location over time.

Cisco Firepower Management Center (FMC) provides centralized management for all Cisco Secure Firewall Threat Defense Virtual (FTDv) instances, including policy administration, threat intelligence integration, logging, monitoring, and event correlation.

This solution paper describes the architecture, deployment process, and configuration steps required to implement Cisco Secure Firewall Threat Defense (FTDv) with Cisco Firepower Management Center (FMC) on Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) platforms.

Note: This content is provided for informational purposes and self-supported guidance only. Consultancy or other assistance related to the content is not covered under the Oracle Support contract or associated service requests. If you have questions or additional needs, then please reach out to your Oracle Sales contact directly.

Architecture Overview

The following architecture illustrates the most common and recommended deployment topology for Cisco Secure Firewall Threat Defense Virtual (FTDv) in Routed Firewall Mode on Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA). This design leverages a single Virtual Cloud Network (VCN) with four dedicated subnets: Management, Diagnostic, Inside, and Outside, each mapped to a specific Cisco Secure Firewall Threat Defense Virtual (FTDv) virtual network interface card (VNIC).

The Management subnet (10.0.0.0/24) provides out-of-band administrative access to the Cisco Secure Firewall Threat Defense Virtual (FTDv) CLI via SSH on TCP/22 and serves as the communication channel between Cisco Secure Firewall Threat Defense Virtual (FTDv) and Cisco Secure Firewall Management Center (FMC) over TCP/8305; it carries no production data traffic.

The Diagnostic subnet (10.0.1.0/24) connects to the Cisco Secure Firewall Threat Defense Virtual (FTDv) diagnostic interface and is used exclusively for SNMP polling, syslog export, or NetFlow telemetry.

The Inside subnet (10.52.0.0/24) is attached to GigabitEthernet0/0 (Gig 0/0) and serves as the gateway for internal workloads such as development or application servers, while the Outside subnet (10.53.0.0/24) is attached to GigabitEthernet0/1 (Gig 0/1) and connects to the Internet Gateway or upstream Dynamic Routing Gateway (DRG).

Each traffic-carrying subnet has its own Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) route table configured to direct inter-subnet traffic through the Cisco Secure Firewall Threat Defense Virtual (FTDv) private IP as the next hop, which is critical to ensure symmetric routing and prevent the stateful firewall from dropping half-seen sessions. Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) firewall rules (security lists) are applied at the subnet level to control which traffic is permitted to reach the Cisco Secure Firewall Threat Defense Virtual (FTDv) interfaces, adding an additional layer of defense before packets are inspected by the firewall engine itself.

NOTE: This single-VCN, four-subnet topology represents the most widely deployed architecture for Cisco Secure Firewall Threat Defense Virtual (FTDv) on Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA), and it is the configuration validated and documented in this solution paper. However, this is not the only supported deployment model. Organizations with more complex segmentation requirements may deploy alternative topologies, including multi-VCN architectures where management, inside, and outside interfaces reside in separate VCNs, or designs with multiple subnets per VCN to support additional security zones such as DMZ, partner extranet, or multi-tier application networks. For these advanced scenarios and for the complete set of supported deployment topologies, interface requirements, and platform-specific considerations, refer to the official Cisco documentation: Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.

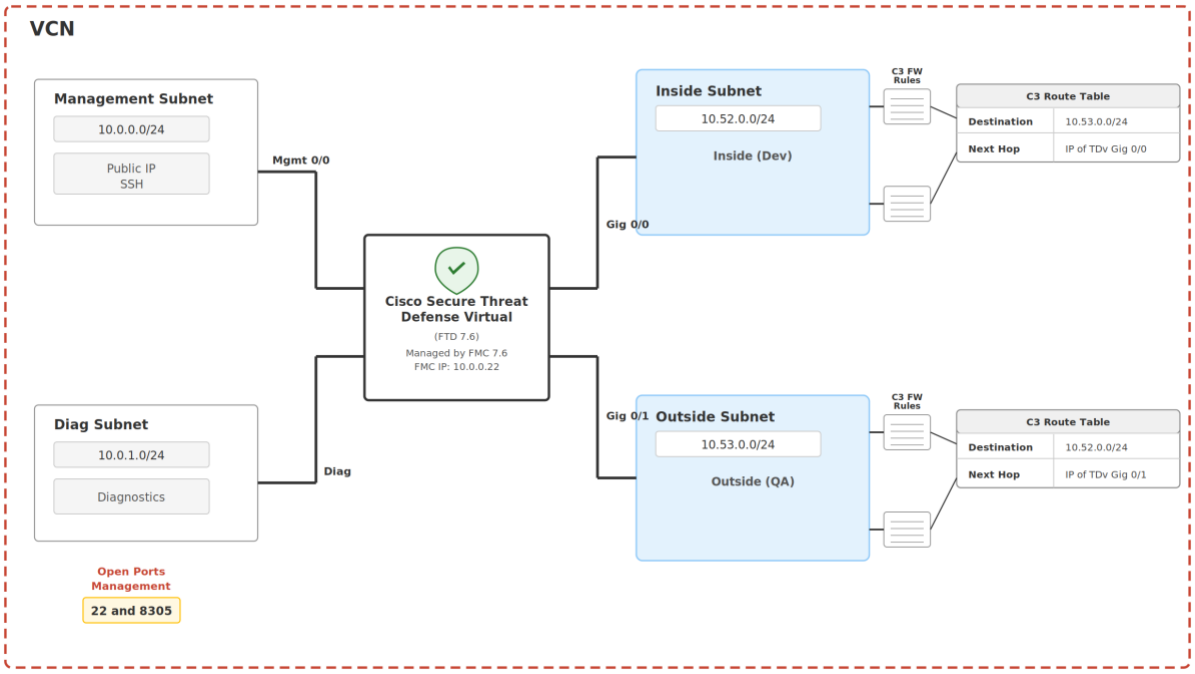

Figure 1: Cisco Secure Firewall Threat Defense Virtual on Compute Cloud@Customer or Private Cloud Appliance (PCA) - Four-Subnet VCN Deployment

Traffic Flow

Traffic between the inside and outside subnets traverses the Cisco Secure Firewall Threat Defense Virtual (FTDv) instance, which enforces stateful inspection, intrusion prevention, and application-aware policies. Each subnet has its own Compute Cloud@Customer or Private Cloud Appliance route table that directs inter-subnet traffic through the Cisco Secure Firewall Threat Defense Virtual (FTDv) as the next hop. The management and diagnostic subnets are isolated from production data traffic.

Four-Subnet Architecture

Management Subnet (10.0.0.0/24): Provides administrative access to the Cisco Secure Firewall Threat Defense Virtual (FTDv) CLI via SSH (TCP/22) and FMC registration (TCP/8305). The FMC instance (10.0.0.22) also resides on this subnet. A public IP is assigned for external administrative access. This is an out-of-band management network, completely isolated from production traffic flows.

Diagnostic Subnet (10.0.1.0/24): Connected to the Cisco Secure Firewall Threat Defense Virtual (FTDv) diagnostic interface. Used for SNMP, syslog, and NetFlow traffic. Cannot carry through traffic.

Inside Subnet (10.52.0.0/24): Connected to the Cisco Secure Firewall Threat Defense Virtual (FTDv) GigabitEthernet0/0 (Gig 0/0) interface. Hosts development and internal workload instances. The Compute Cloud@Customer route table for this subnet directs traffic destined for the outside subnet (10.53.0.0/24) to the Cisco Secure Firewall Threat Defense Virtual (FTDv) Gig 0/0 IP as the next hop.

Outside Subnet (10.53.0.0/24): Connected to the Cisco Secure Firewall Threat Defense Virtual (FTDv) GigabitEthernet0/1 (Gig 0/1) interface. Connects to the DRG, Internet Gateway, or upstream network. The Compute Cloud@Customer route table for this subnet directs return traffic destined for the inside subnet (10.52.0.0/24) to the Cisco Secure Firewall Threat Defense Virtual (FTDv) Gig 0/1 IP as the next hop.

C3 Route Table Configuration

Each subnet requires its own route table entry pointing to the Cisco Secure Firewall Threat Defense Virtual (FTDv) interface IP as the next hop. This ensures symmetric routing traffic traverses the firewall in both directions, preventing dropped packets.

Subnet	Route Table Destination	Next Hop
Inside (10.52.0.0/24)	10.53.0.0/24	IP of FTDv Gig 0/0
Outside (10.53.0.0/24)	10.52.0.0/24	IP of FTDv Gig 0/1

Open Ports for Management

- **TCP/22 (SSH):** CLI access to the FTDv management interface.
- **TCP/8305:** FMC-to-FTDv registration and communication channel.

Environment

Component	Detail
Platform	Oracle Compute Cloud@Customer (C3) Or Private Cloud Appliance
Firewall	Cisco Secure Firewall Threat Defense 7.6.2
Manager	Cisco Secure Firewall Management Center 7.6.2
FTD Management IP	10.0.0.20
FMC IP	10.0.0.22
Diagnostic Subnet	10.0.1.0/24
Inside Subnet (Dev)	10.52.0.0/24
Outside Subnet (QA)	10.53.0.0/24

Prerequisites

- A Cisco Account for licensing and image download (create at https://software.cisco.com/).
- License the Firewall Threat Defense Virtual.
  - License entitlements configured for all security services from the Firewall Management Center. Refer to “Licensing” in the Cisco Secure Firewall Management Center Admin Guide for more information about how to manage licenses.
- Virtual Network Interface (VNICs) requirements: Cisco Secure Firewall Threat Defense Virtual (FTDv) requires a minimum of 4 interfaces (management, diagnostic, inside, outside).
  - Management interfaces (2) - One to connect Cisco Secure Firewall Threat Defense Virtual (FTDv) to FMC, one for diagnostics; cannot be used for through traffic.
  - Traffic interfaces (2) - Used to connect Cisco Secure Firewall Threat Defense Virtual (FTDv) to inside hosts and to the external network.

NOTE: Ensure ‘Skip Source/Destination Check’ is enabled on all VNICs of the Cisco Secure Firewall Threat Defense Virtual (FTDv) instance. This is critical for the firewall to forward traffic that does not match its own IP address.

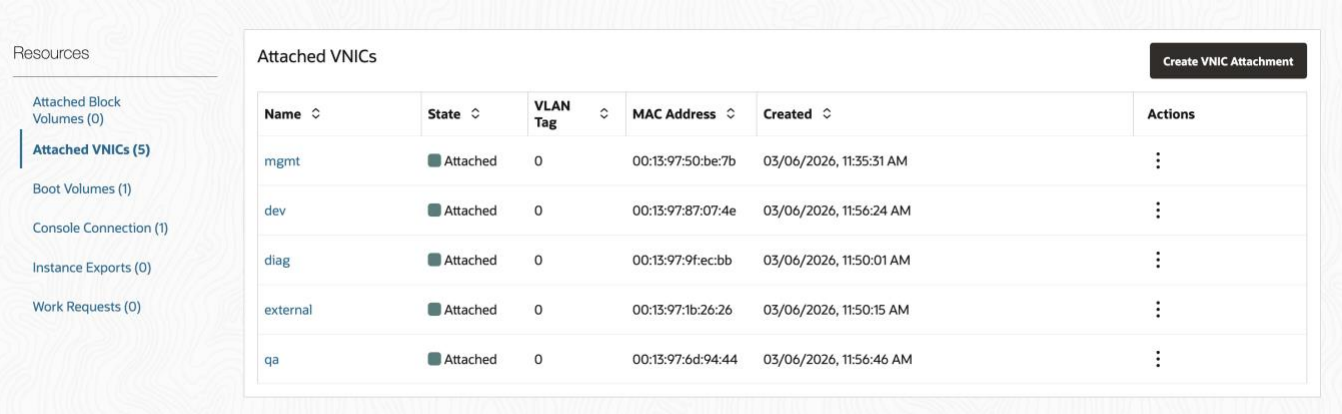

Figure 2: Virtual Interfaces attached to Cisco Secure Firewall Threat Defense Virtual (FTDv) on Compute Cloud@Customer or Private Cloud Appliance (PCA) - Four-Subnet VCN Deployment

NOTE: It is important to note that a minimum of four virtual network interfaces (vNICs) is required for a Cisco Secure Firewall Threat Defense Virtual (FTDv) instance. For production environments, additional vNICs can be configured as needed, depending on the Compute Cloud@Customer or Private Cloud Appliance instance sizing (e.g., OCPUs and memory) and the applicable Cisco FTDv licensing model.

- Communications paths: Public IP for SSH access (TCP/22) and FMC registration (TCP/8305) into Cisco Secure Firewall Threat Defense Virtual (FTDv) management interface.

For Firewall Threat Defense Virtual system requirements, see Cisco Secure Firewall Threat Defense Compatibility Guide.

- Local management via Firewall Device Manager (FDM) is not supported - FMC is required.
- Transparent, inline, and passive modes are not supported.
- Separate routing rules are required for Cisco Secure Firewall Threat Defense Virtual (FTDv) for both static and DHCP configurations.
- When using four subnets in a single VCN, the routes specific to each subnet must be added to the route table associated with that subnet.

Supported Features on C3

- Deployment in the OCI Virtual Cloud Network (VCN)
- Routed mode (default)
- Licensing - BYOL (Bring Your Own License) only
- IPv6 (dual-stack with VCN IPv4 and IPv6 configuration)
- Firewall Management Center (FMC) management

Performance Tiers for FTDv Smart Licensing

The FTDv supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements:

Performance Tier	Device Specs (Core/RAM)	Rate Limit	RA VPN Sessions

FTDv5, 100 Mbps	4 core / 8 GB	100 Mbps	50
FTDv10, 1 Gbps	4 core / 8 GB	1 Gbps	250
FTDv20, 3 Gbps	4 core / 8 GB	3 Gbps	250
FTDv30, 5 Gbps	8 core / 16 GB	5 Gbps	250
FTDv50, 10 Gbps	12 core / 24 GB	10 Gbps	750
FTDv100, 16 Gbps	16 core / 32 GB	16 Gbps	10,000

End-to-end Deployment Procedure

The following workflow describes the complete deployment process for Cisco Secure Firewall Threat Defense Virtual on Compute Cloud@Customer or Private Cloud Appliance (PCA):

Phase 1 - Configure the C3 Environment

- Create or configure the Virtual Cloud Network (VCN) with the required CIDR block.
- Create the Network Security Group (NSG) with rules allowing SSH (TCP/22) and FMC registration (TCP/8305).
- Create the Internet Gateway (if external access is required).
- Create all four subnets: Management, Diagnostic, Inside, and Outside.
- Configure route tables for each subnet with appropriate next-hop entries pointing to FTDv interfaces.

Phase 2 - Deploy the FTDv Instance

- Download the Cisco Secure Firewall (.qcow2) image from Cisco official website. Reach out to your Cisco sales team.
- Launch the compute instance, selecting the appropriate Flex shape based on your licensing and network bandwidth requirements.
- Provide the Day-0 configuration during instance launch, including management IP, FMC IP, and registration key.

  NOTE: If you prefer, Under Initialization Script, click the Paste Cloud-Init Script radio button to provide the day0 configuration for your Firewall Threat Defense Virtual. The day0 configuration is applied during the firstboot of the Firewall Threat Defense Virtual. The following example shows a sample day0 configuration you can copy and paste in the Cloud-Init Script field, example:

```
{
"Hostname": "ftdv-oci",
"AdminPassword": "myPassword@123456",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"IPv6Mode": "dhcp",
"ManageLocally":"No",
"FmcIp": "1.2.3.4",
"FmcRegKey":"cisco123reg",
"FmcNatId": "cisco123nat"
}
```

  - FmcRegKey—This is a one-time-use registration key used to register registering the device to a Firewall Management Center. The registration key is any user-defined alphanumeric value up to 37 characters in length.
  - FmcNatId—This is a unique one-time-use string (user-defined). If the device and the Firewall Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.
- Attach the additional VNICs (diagnostic, inside, outside) to the FTDv instance after launch.

Phase 3 - Connect and Register

- Connect to the FTDv instance via SSH using the public IP on the management subnet.
- Verify network configuration and interface status from the FTD CLI.
- Register the FTDv with FMC for centralized management and policy deployment.

Login to the FTD CLI

Once the Cisco Secure Firewall Threat Defense Virtual (FTDv) instance has been successfully deployed on Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA), the first operational step is to establish a command-line session with the firewall. There are two methods available for initial access:

- The preferred method is to connect via SSH using the public IP address assigned to the management VNIC during instance creation. This requires the SSH private key that corresponds to the public key provided during the Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) instance launch wizard.
- The second method, which is useful when the management network is not yet reachable or when troubleshooting connectivity issues, is to use the serial console available through the Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) compute instance details page (Compute → Instances → Instance Details → Console Connection).

To connect via SSH, use the following command from a terminal or SSH client:

```
ssh -i <private-key> admin@<management-public-ip>
```

Replace <private-key> with the path to your SSH private key file and <management-public-ip> with the public IP address assigned to the management VNIC. The default administrative username is admin. On the very first login, the FTDv will present the Cisco End User License Agreement (EULA), which must be accepted before proceeding. You will then be prompted to set a new admin password. This password is used for all subsequent CLI and SSH access to the device. Once the password has been set, the system will complete its initial boot configuration and present the FTDv CLI prompt, confirming that the Cisco Firepower eXtensible Operating System (FX-OS) and the Threat Defense application are running. At this point, the device is ready for network verification and manager registration.

NOTE: If you are connecting through a bastion host or jump server on the management subnet, ensure that the Network Security Group (NSG) associated with the management subnet permits inbound SSH traffic on TCP/22 from the bastion host's private IP. Additionally, if the serial console is used, the console connection must be created beforehand from the Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) console, and the SSH key pair used for the console connection is separate from the key pair used for the instance itself.

Figure 3: Cisco Secure Firewall Threat Defense Virtual on C3 - Four-Subnet VCN Deployment

Verify network configuration

Before proceeding with FMC registration, it is essential to verify that Cisco Secure Firewall Threat Defense Virtual (FTDv) management interface has received the correct IP address and that the default gateway is reachable. This step confirms that the management VNIC was properly configured during instance launch and that the underlying Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA) networking infrastructure (VCN, subnet, route table, and security lists) is functioning correctly. From Cisco Secure Firewall Threat Defense Virtual (FTDv) CLI, run the following command:

```
show network
```

This command displays the complete management interface configuration, including the assigned IPv4 address, subnet mask, default gateway, DNS server settings, and the management interface status. Verify the following:

- The Management IP matches the private IP assigned to the management VNIC (e.g., 10.0.0.20).
- The Default Gateway is set to the management subnet's gateway (typically the first usable address in the CIDR block, e.g., 10.0.0.1).
- The DNS Server is configured and reachable (required for license activation, threat intelligence updates, and hostname resolution).
- The Management Interface status shows as up/up.

To further validate connectivity, test reachability to the default gateway and to the FMC IP address:

```
ping system 10.0.0.1 ping system 10.0.0.22
```

If the ping to the FMC fails, verify that the Network Security Group for the management subnet allows ICMP traffic and that the FMC instance is running and accessible on the same subnet. Also confirm that the management subnet's route table has a route entry for the subnet CIDR block or a default route that covers the FMC's IP range.

Register the Cisco FTDv with Cisco FMC

Once management network connectivity has been verified, the next step is to register the Cisco Secure Firewall Threat Defense Virtual (FTDv) with Cisco Secure Firewall Management Center (FMC). This registration establishes a secure, encrypted communication channel between the two devices over TCP/8305, which FMC uses to push policies, retrieve events, deploy configurations, and collect health and diagnostic data from the FTDv.

From the Cisco Secure Firewall Threat Defense Virtual (FTDv) CLI, execute the following command to configure the FMC as the management station:

```
configure manager add 10.0.0.22 <registration-key>
```

Replace 10.0.0.22 with the actual IP address of your FMC instance and <registration-key> with a shared secret string that you will also provide on the FMC side when completing the device registration. This key is a one-time-use pre-shared secret used only during the initial registration handshake; it does not need to persist after the devices have successfully paired.

After executing the command, verify the registration status by running:

```
show managers
```

The output will display the FMC IP address, the registration status, and the connection state. Initially, the status will show as Pending while the Cisco Secure Firewall Threat Defense Virtual (FTDv) waits for the FMC to initiate the registration from its side. Once both sides complete the handshake, the status will transition to Completed.

NOTE: The registration process requires that TCP/8305 is open bidirectionally between the Cisco Secure Firewall Threat Defense Virtual (FTDv) management IP and the FMC IP. Ensure that the Network Security Group (NSG) or security list associated with the management subnet includes an ingress rule permitting TCP/8305 from the FMC's private IP to the Cisco Secure Firewall Threat Defense Virtual (FTDv), and an egress rule permitting TCP/8305 from the FTDv to the FMC. If this port is blocked, the registration will remain in a Pending state indefinitely and the two devices will not be able to communicate. Additionally, if the FTDv and FMC reside on different subnets or VCNs, verify that the appropriate route table entries and peering connections are in place to allow traffic between them.

Login to FMC

With the FTDv prepared and waiting for registration, the next step is to log in to the Cisco Secure Firewall Management Center (FMC) web interface. Open a web browser and navigate to: `https://<FMC-IP>`

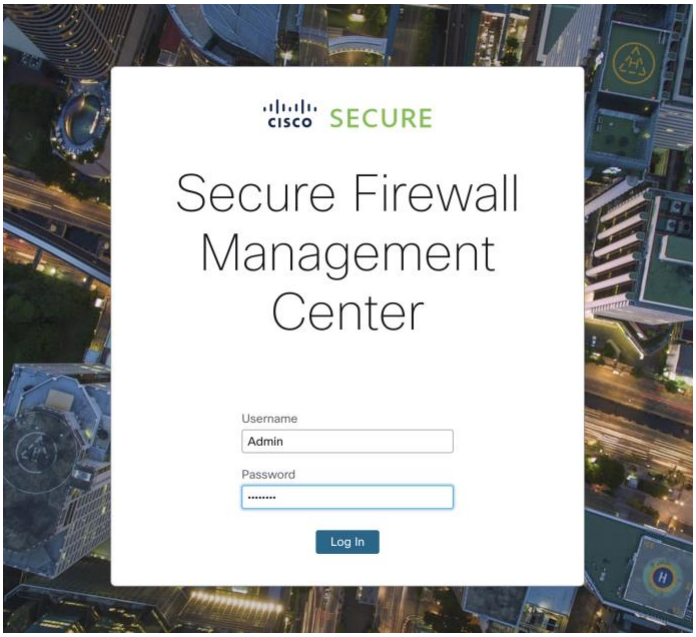

Figure 4: Cisco Secure Firewall Management Center (FMC) on Compute Cloud@Customer or Private Cloud Appliance

Replace `<FMC-IP>` with the private or public IP address of the FMC instance (e.g., https://10.0.0.22). If accessing the FMC from outside the management subnet, you will need to either connect through a bastion host, a VPN connection, or use a public IP assigned to the FMC management VNIC with appropriate NSG rules permitting HTTPS (TCP/443) from your source IP.

On first login, the FMC may prompt you to complete the initial setup wizard, which includes configuring the management hostname, DNS settings, NTP servers, and accepting the license agreement. Once the setup wizard is complete and you are at the FMC dashboard, the system is ready to receive the FTDv device registration.

NOTE: Ensure that the FMC instance has been fully initialized and that all services are running before attempting to register devices. The FMC boot process can take 15–30 minutes on initial deployment. You can monitor the FMC readiness by checking the system status from the FMC CLI using the expert shell if needed.

Register the firewall device

From the FMC web interface, navigate to **Devices → Device Management** and click the **Add** button, then select **Add Device**. In the registration dialog, provide the following information:

- **Host:** Enter the FTDv management IP address (e.g., 10.0.0.20). This is the private IP assigned to the FTDv management VNIC on the management subnet.
- **Registration Key:** Enter the same shared secret string that was used in the configure manager add command on the FTDv CLI. The key must match exactly on both sides for the registration to succeed.
- **Access Control Policy:** Select an existing Access Control Policy to assign to the device or choose to create a new one. This policy defines the baseline traffic inspection and permit/deny rules that will be deployed to the FTDv.
- **Smart Licensing:** The FTDv will be registered with the Cisco Smart Software Manager through the FMC. Ensure that the FMC has been configured with a valid Smart Account and that the appropriate FTDv license entitlements (Base, Threat, Malware, URL Filtering) are available.

Click **Register** to initiate the pairing process. The FMC will reach out to the FTDv over TCP/8305 using the management IP address and complete the cryptographic handshake using the shared registration key. This process typically takes 2–5 minutes, during which the FMC establishes a secure SSL tunnel with the FTDv and begins pulling the device's initial configuration.

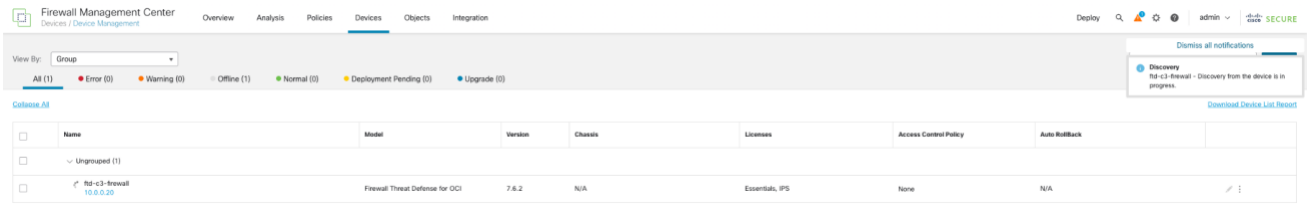

Figure 5: Registering Cisco Secure Firewall Threat Defense Virtual (FTDv) instance with Cisco Secure Firewall Management Center (FMC) on Compute Cloud@Customer or Private Cloud Appliance

Device discovery

After the registration handshake completes successfully, the FMC automatically enters the device discovery phase. During this phase, the FMC retrieves the complete running configuration from the FTDv, including all interface definitions, their current IP addressing and operational status, the platform model and software version, available hardware resources (CPU, memory, disk), existing routing entries, rules if any, and any pre-configured objects or policies.

The discovery process typically takes 3–10 minutes depending on the complexity of the device's configuration and network latency between the FMC and FTDv. During this time, the device status in **Devices → Device Management** will show as **Registering** or **Discovering**.

NOTE: Do not attempt to push policy changes or modify the device until the discovery phase completes and the device icon shows a green health indicator.

Once discovery is complete, the FMC will display the FTDv's full interface inventory (Management0/0, Diagnostic, GigabitEthernet0/0, GigabitEthernet0/1, and any additional interfaces), its software version (e.g., 7.6.2), the platform type

(FTDv for OCI), and the device health status. This information is critical for the next steps: configuring interface zone assignments, IP addressing, routing, and access control policies.

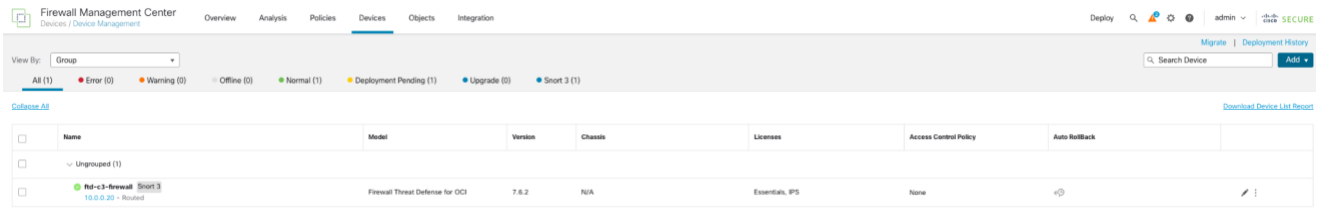

Figure 6: Cisco Secure Firewall Threat Defense Virtual (FTDv) instance connected to Cisco Secure Firewall Management Center (FMC) on Compute Cloud@Customer or Private Cloud Appliance

Verify deployment status

Before and after making any configuration changes, it is important to verify the deployment status of the FTDv from the FMC. Navigate to **Deploy** → **Deployment** in the FMC web interface. This page shows all managed devices and their current deployment state, indicating whether the FTDv's running configuration is in sync with the FMC's intended configuration or whether there are pending changes that need to be pushed.

After initial device discovery, the deployment status should show the device as **In Sync**, meaning the FMC's view of the device matches the FTDv's active running configuration. As you begin configuring interfaces, zones, routing, and access control policies in subsequent steps, the status will change to **Pending Deployment**, indicating that there are uncommitted changes waiting to be pushed to the device.

To deploy pending changes, select the FTDv device checkbox, click **Deploy**, and confirm the deployment. The FMC will compile the policy package, validate the configuration for errors or conflicts, push the compiled rules to the FTDv over the secure management channel, and report the deployment result. A successful deployment will return the device status to **In Sync** with a green check mark. If a deployment fails, the FMC will display a detailed error log identifying the specific configuration element that caused the failure, allowing you to correct the issue and re-deploy.

NOTE: It is a best practice to verify the deployment status after every configuration change and before moving to the next configuration step. This ensures that each change is applied successfully and prevents the accumulation of multiple uncommitted changes that could be difficult to troubleshoot if a deployment failure occurs.

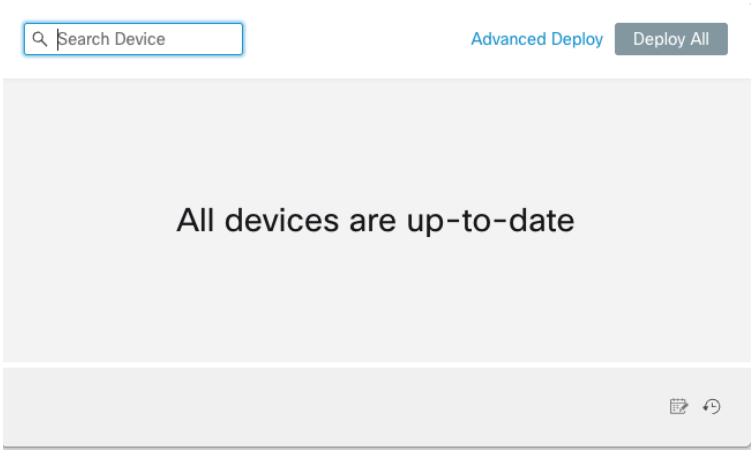

Figure 7: Cisco Secure Firewall Management Center (FMC) Deployment status on Compute Cloud@Customer or Private Cloud Appliance

Run the following command to verify the management network configuration:

```
show network
```

Confirm the management interface has the expected IP address (10.0.0.20) and that the default gateway is reachable.

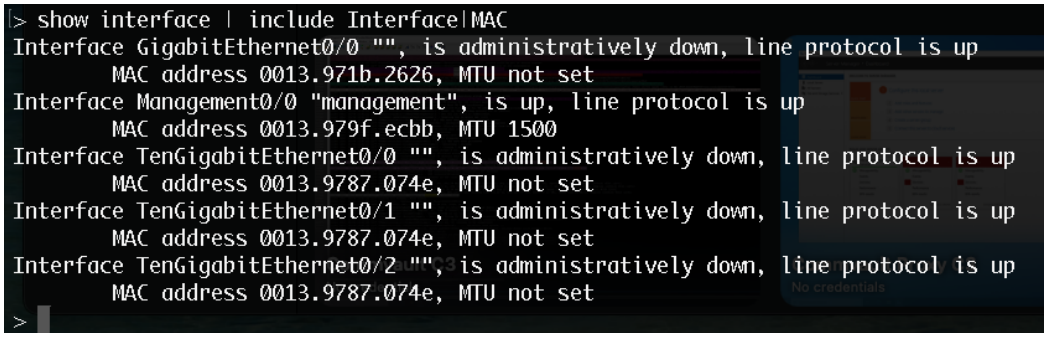

Figure 8: Cisco Secure Firewall Threat Defense Virtual (FTDv) Virtual Interfaces (vNICs)

Interface configuration

Navigate to **Devices → Device Management → Interfaces** to configure each network interface according to the zone mapping defined in the reference architecture.

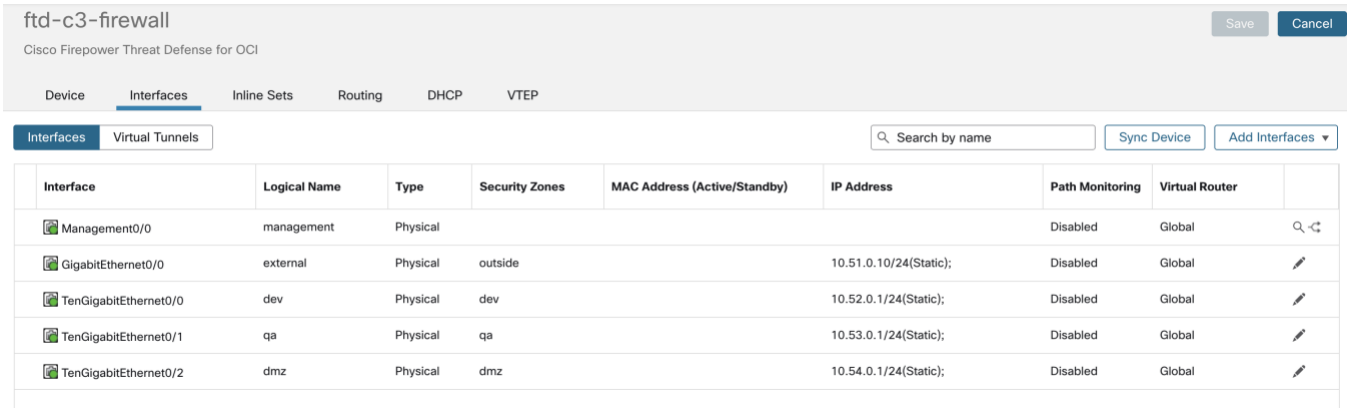

Figure 9: Cisco Secure Firewall Management Center (FMC) Interfaces configuration.

Attach VNICs and configure interfaces

After the FTDv instance is launched with the management VNIC, additional VNICs must be attached for the diagnostic, inside, and outside subnets. Navigate to Compute → Instances → Instance Details → Attached VNICs in the C3 console and attach each VNIC in order.

Note: The FTDv maps interfaces in the order they are attached: VNIC 0 = Management (Mgmt 0/0), VNIC 1 = Diagnostic, VNIC 2 = GigabitEthernet0/0 (Inside), VNIC 3 = GigabitEthernet0/1 (Outside). Verify the mapping using MAC address correlation between the C3 console and the FTD CLI.

VNIC-to-Interface Mapping

VNIC Order	C3 Subnet	FTD Interface	Zone	IP Address
VNIC 0	Management (10.0.0.0/24)	Management0/0 (Mgmt 0/0)	management	10.0.0.20
VNIC 1	Diagnostic (10.0.1.0/24)	Diagnostic (Diag)	diagnostic	DHCP
VNIC 2	Inside (10.52.0.0/24)	GigabitEthernet0/0 (Gig 0/0)	inside	10.52.0.1
VNIC 3	Outside (10.53.0.0/24)	GigabitEthernet0/1 (Gig 0/1)	outside	10.53.0.1

Add route rules for attached VNICs

After attaching the VNICs, configure C3 route rules to direct inter-subnet traffic through the FTDv. Each attached VNIC's subnet requires a route table entry pointing to the FTDv's private IP on that subnet as the next hop.

Inside Subnet Route Table

Destination CIDR	Target Type	Target
10.53.0.0/24	Private IP	FTDv Gig 0/0 private IP (10.52.0.1)

Outside Subnet Route Table

Destination CIDR	Target Type	Target
10.52.0.0/24	Private IP	FTDv Gig 0/1 private IP (10.53.0.1)

NOTE: Ensure 'Skip Source/Destination Check' is enabled on each VNIC attached to the FTDv. Without this, OCI/C3 will drop traffic that does not match the VNIC's assigned IP.

Configuration steps in FMC

Navigate to **Devices** → **Device Management** → **ftd-c3-firewall** → Interfaces and configure each interface:

Configure Inside Interface

Parameter	Value
Interface	GigabitEthernet0/0
Zone	inside
Mode	Routed
IPv4	10.52.0.1/24

Configure Outside Interface

Parameter	Value
Interface	GigabitEthernet0/1
Zone	outside
Mode	Routed
IPv4	10.53.0.1/24

Default route configuration

Navigate to Devices → Routing → Static Route and configure the default gateway:

Parameter	Value
Destination	0.0.0.0/0
Gateway	10.53.0.1 (outside subnet gateway)
Interface	outside

To operationalize and fully secure the deployed Cisco Secure Firewall Threat Defense (FTDv) environment on Oracle Compute Cloud@Customer (C3) or Private Cloud Appliance (PCA), the following post-deployment configurations are recommended:

- **Define Access Control Policies (ACP)**: Use FMC to implement application-aware policies aligned with network segmentation, enforcing least-privilege access across all traffic flows.
- **Enable Advanced Threat Protection**: Activate IPS and Malware/File policies to protect against known and emerging threats.
- **Validate Network Configuration**: Confirm routing, NAT, and (if applicable) high availability configurations to ensure secure and resilient traffic flow.
- **Enable Monitoring and Logging**: Integrate FMC with centralized logging and monitoring tools for visibility, compliance, and incident response.
- **Optimize and Tune Policies**: Continuously refine policies based on traffic patterns and security events to improve effectiveness and reduce false positives.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Copyright © 2026, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Some regulatory certifications or registrations to products or services referenced on this website are held by Cerner Corporation. Cerner Corporation is a wholly-owned subsidiary of Oracle. Cerner Corporation is an ONC-certified health IT developer and a registered medical device manufacturer in the United States and other jurisdictions worldwide.

This document may include some forward-looking content for illustrative purposes only. Some products and features discussed are indicative of the products and features of a prospective future launch in the United States only or elsewhere. Not all products and features discussed are currently offered for sale in the United States or elsewhere. Products and features of the actual offering may differ from those discussed in this document and may vary from country to country. Any timelines contained in this document are indicative only. Timelines and product features may depend on regulatory approvals or certification for individual products or features in the applicable country or region.

Author: Anderson Souza