

Configure Geneve Interfaces in Secure FTDv

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Configure Performance Tier License for FTDv](#)

[Configure the VTEP Source Interface](#)

[Configure the VNI interface](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure Geneve encapsulation for FTDv data interfaces in AWS.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firepower Management Center configuration deployment
- Secure Firepower Threat Defense Virtual deployed in AWS
- AWS instance EC2 virtualization.

Configuring Geneve encapsulation for Cisco Secure Firepower Threat Defense in AWS, requires FTD version 7.1 or greater.

Performance Tier License of FTDv20 or greater is also required.

You can only configure one Virtual Tunnel Endpoint (VTEP) source interface per FTDv device. The VTEP is defined as a Network Virtualization Endpoint (NVE); Geneve encapsulation for VTEP is the only natively supported NVE at the time.

You can refer to this documentation to [Deploy the Threat Defense Virtual on AWS](#).

Components Used

The information in this document is based on these software and hardware versions:

- Secure Firepower Management Center - 7.3.0
- Secure Firepower Threat Defense - 7.3.0
- AWS c5.2xlarge (4 core/8 GB) instance
- Performance tier license - FTDv50

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

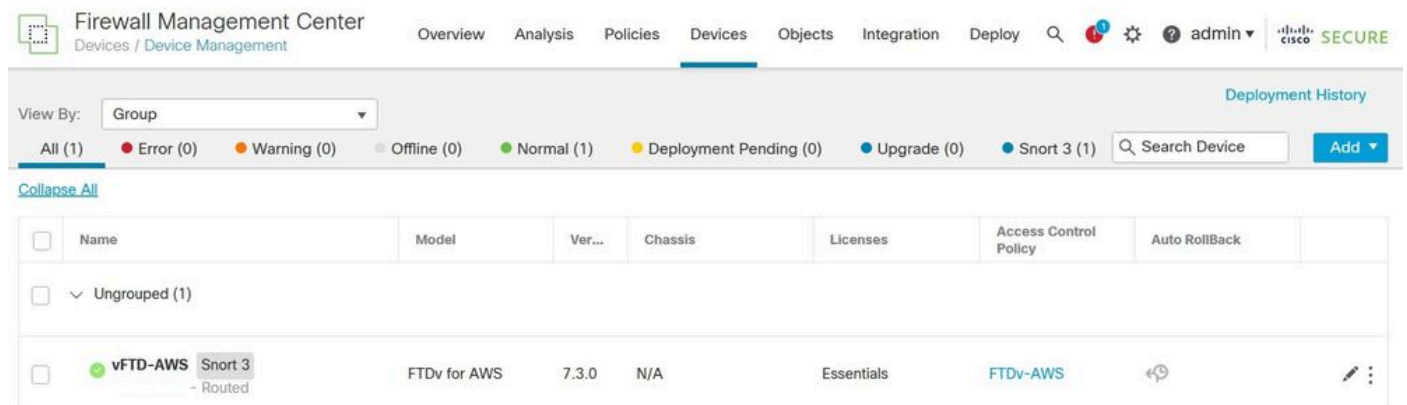
Configure Performance Tier License for FTDv

Use a supported browser to access your FMC GUI:

<#root>

https://FMC_IP_Address

Navigate to **Devices > Device Management**:



Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin | cisco SECURE

View By: Group

Deployment History

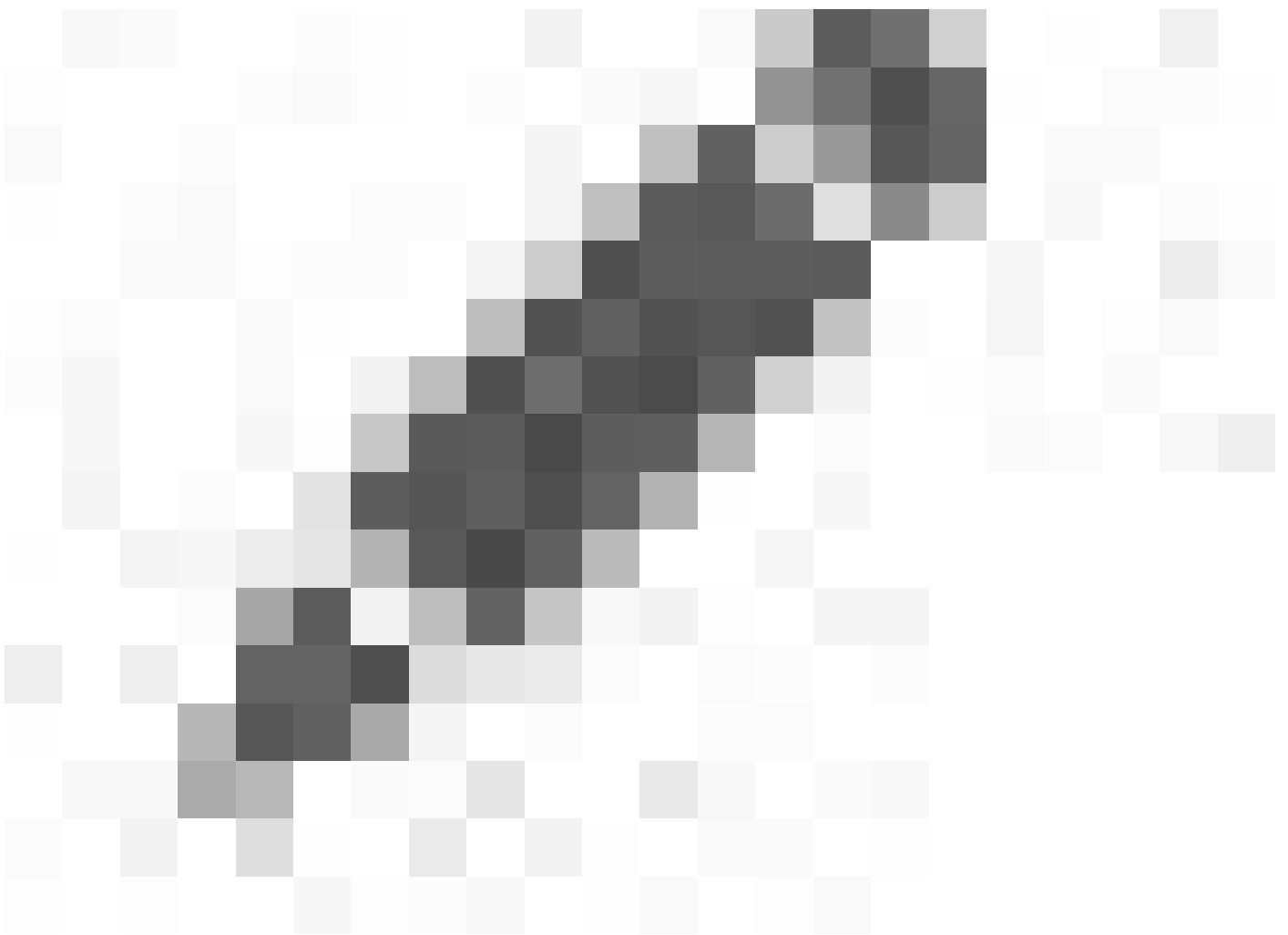
All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (0) Upgrade (0) Snort 3 (1) 🔍 Search Device Add

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Ver...	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	vFTD-AWS <small>Snort 3</small> - Routed	FTDv for AWS	7.3.0	N/A	Essentials	FTDv-AWS	↻	✎ ⋮

Device Management

Select the edit Icon for the FTDv in question:



Edit

Click **Device** tab, then edit configuration in the **License** summary:

vFTD-AWS

Cisco Firepower Threat Defense for AWS

- Device
- Routing
- Interfaces
- Inline Sets
- DHCP
- VTEP

General		License	
Name:	vFTD-AWS	Performance Tier :	FTDv - Variable
Transfer Packets:	Yes	Essentials:	Yes
Mode:	Routed	Export-Controlled Features:	Yes
Compliance Mode:	None	Malware Defense:	No
Performance Profile:	Default	IPS:	No
TLS Crypto Acceleration:	Disabled	Carrier:	No
		URL:	No
Device Configuration:	<input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Download"/>	Secure Client Premier:	No
		Secure Client Advantage:	No
		Secure Client VPN Only:	No

Device License

Select the **FTDv20 (Core 4 / 8 GB)** or greater from the **Performance Tier** drop-down list. For this example, FTDv50 Performance Tier License is selected as shown in this image:

License Types

Performance Tier: Dv50 - Tiered (Core 12 / 24 GB) ▾

Essentials:

FTDv5 - Tiered (Core 4 / 8 GB)

FTDv10 - Tiered (Core 4 / 8 GB)

Export-Controlled Features:

FTDv20 - Tiered (Core 4 / 8 GB)

FTDv30 - Tiered (Core 8 / 16 GB)

Malware Defense:

FTDv50 - Tiered (Core 12 / 24 GB)

IPS:

FTDv100 - Tiered (Core 16 / 32 GB)

FTDv - Variable

Carrier: URL: Secure Client Premier: Secure Client Advantage: Secure Client VPN Only:

If a device already has Secure Client VPN Only they cannot have Secure Client Premier or Secure Client Advantage. If a device has Secure Client Premier or Secure Client Advantage it cannot have Secure Client VPN Only

Cancel

Save

Choose Performance Tier License FTDv20 or Greater

Next, Select **Save** and **Deploy** the configuration to FTDv.

Configure the VTEP Source Interface

Navigate to **Devices > Device Management > Choose edit > VTEP** and select **Enable NVE**:

vFTD-AWS

Cisco Firepower Threat Defense for AWS

You have unsaved changes [Save](#) [Cancel](#)

Device Routing Interfaces Inline Sets DHCP **VTEP**

Enable NVE

[Add VTEP](#)

Encapsulation type	Encapsulation port	NVE number	VTEP Source Interface	Neighbor Address	
No records to display					

Enable VNE

Now, you can Select **Add VTEP**:

Add VTEP



Encapsulation type

GENEVE

Encapsulation port*

6081

(1024 - 65535)

NVE number

1



VTEP Source Interface

Select Interface

[Cancel](#)

[OK](#)

Add VTEP

Enter the value for the **Encapsulation port** within the specified range.



Warning: It is not recommend to change the Geneve port; AWS requires a port of 6081.

Next, you can Select the **VTEP Source Interface**.

VTEP Source Interface

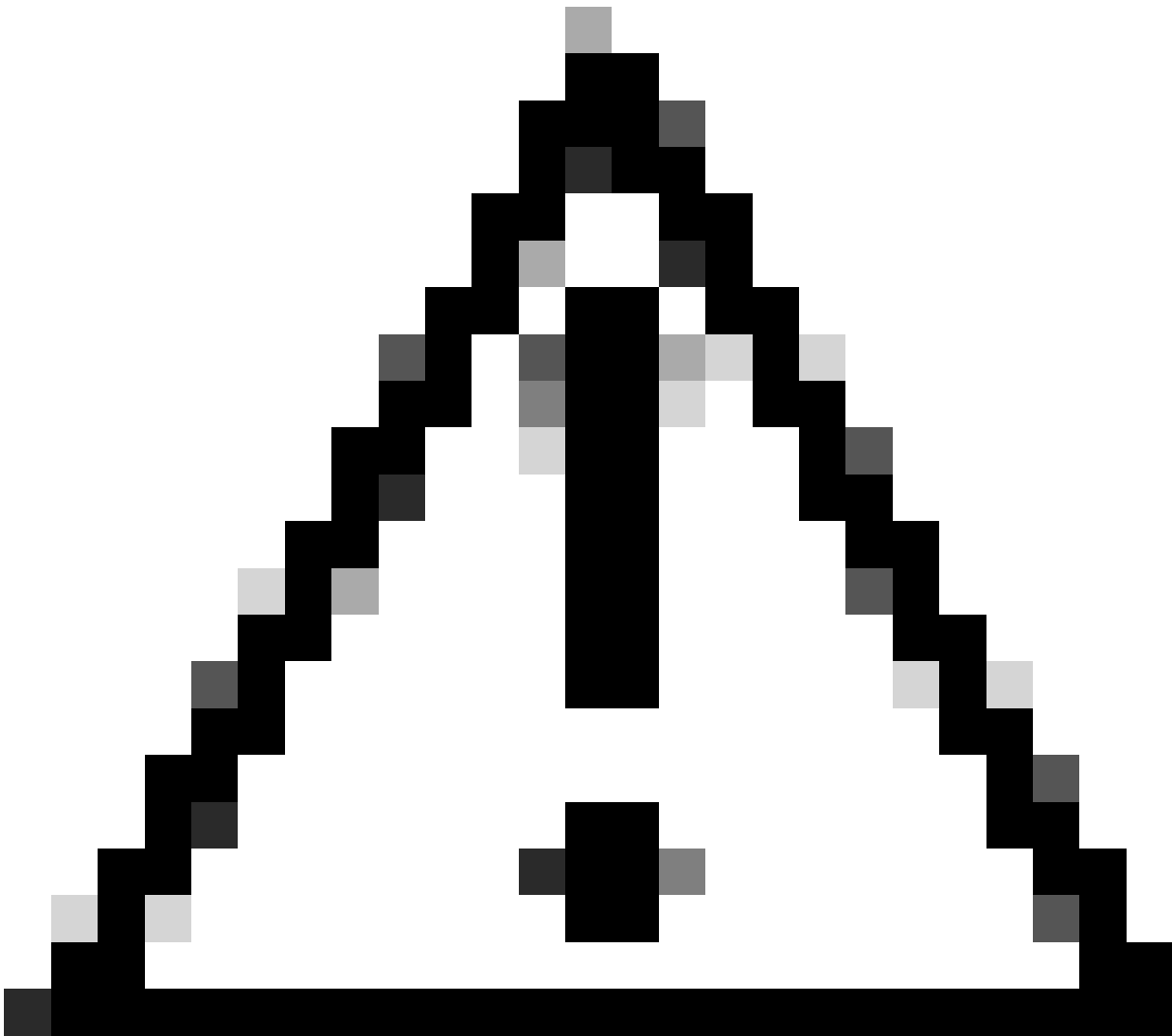
Outside



Outside Interface as VTEP Source Interface

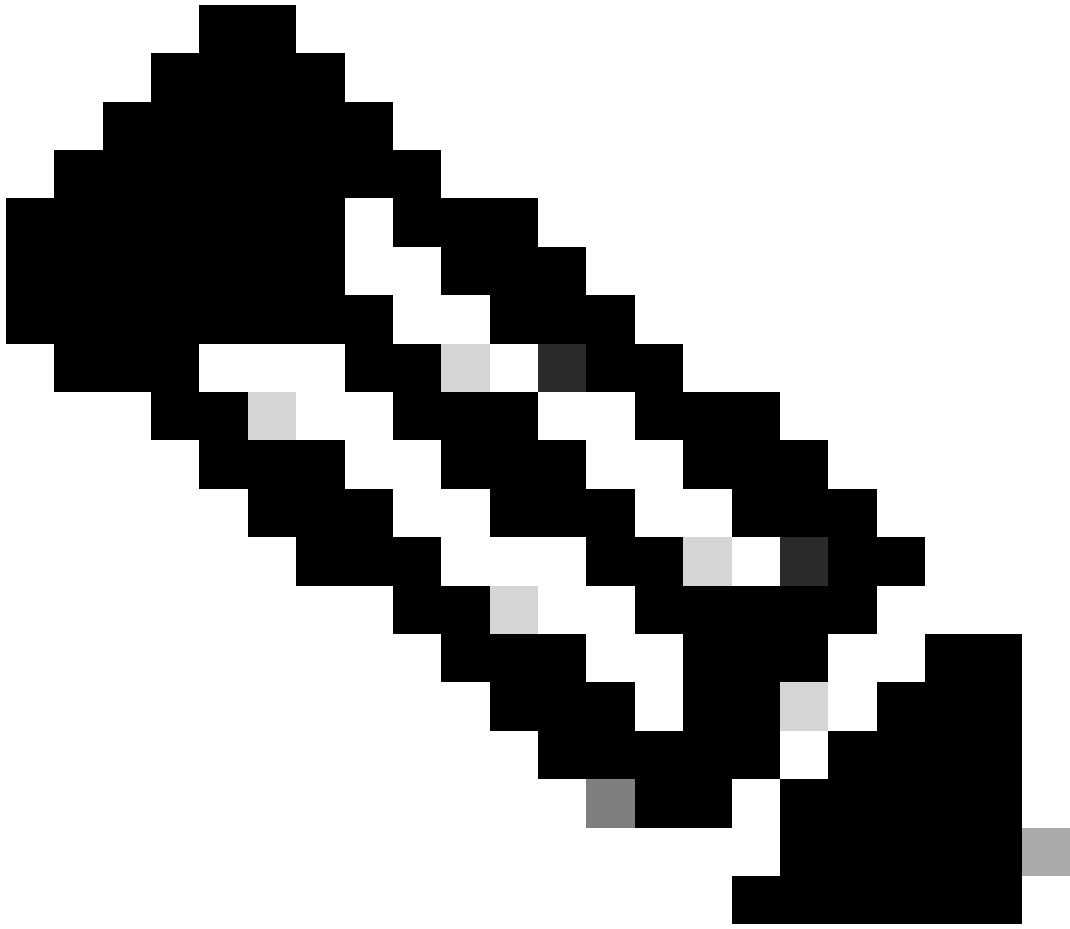


Note: Select from the list of available physical interfaces present on the device. In case the interface Name is not displayed in the list, you can validate if the desired interface is **Enabled** and has a **Name** configured.



Caution: FMC automatically raises the MTU to 1806 bytes of the selected interface in case MTU is lower than 1806 bytes.

Next, Click **OK**.



Note: FMC shows Jumbo Frame is enabled:

Jumbo Frame Changed

Jumbo Frame is enabled on the device.
Please reboot the device after next
deployment to reflect the changes.

OK

Jumbo Frame Changed

Select **Ok** and **Save**.

Configure the VNI interface

Add a Virtual Network Interface(VNI) interface, associate it with the VTEP source interface, and configure basic interface parameters.

Navigate to **Interfaces Tab** and click **Add Interfaces**.

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration Deploy

vFTD-AWS Save Cancel

Cisco Firepower Threat Defense for AWS

Device Routing **Interfaces** Inline Sets DHCP VTEP

Search by name Sync Device **Add Interfaces**

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stan...	IP Address	Path Monit...	Virtual Router	
Diagnostic0/0	diagnostic	Physical				Disabled	Global	
TenGigabitEthernet0/0	Outside	Physical				Disabled	Global	
TenGigabitEthernet0/1	Inside	Physical				Disabled	Global	

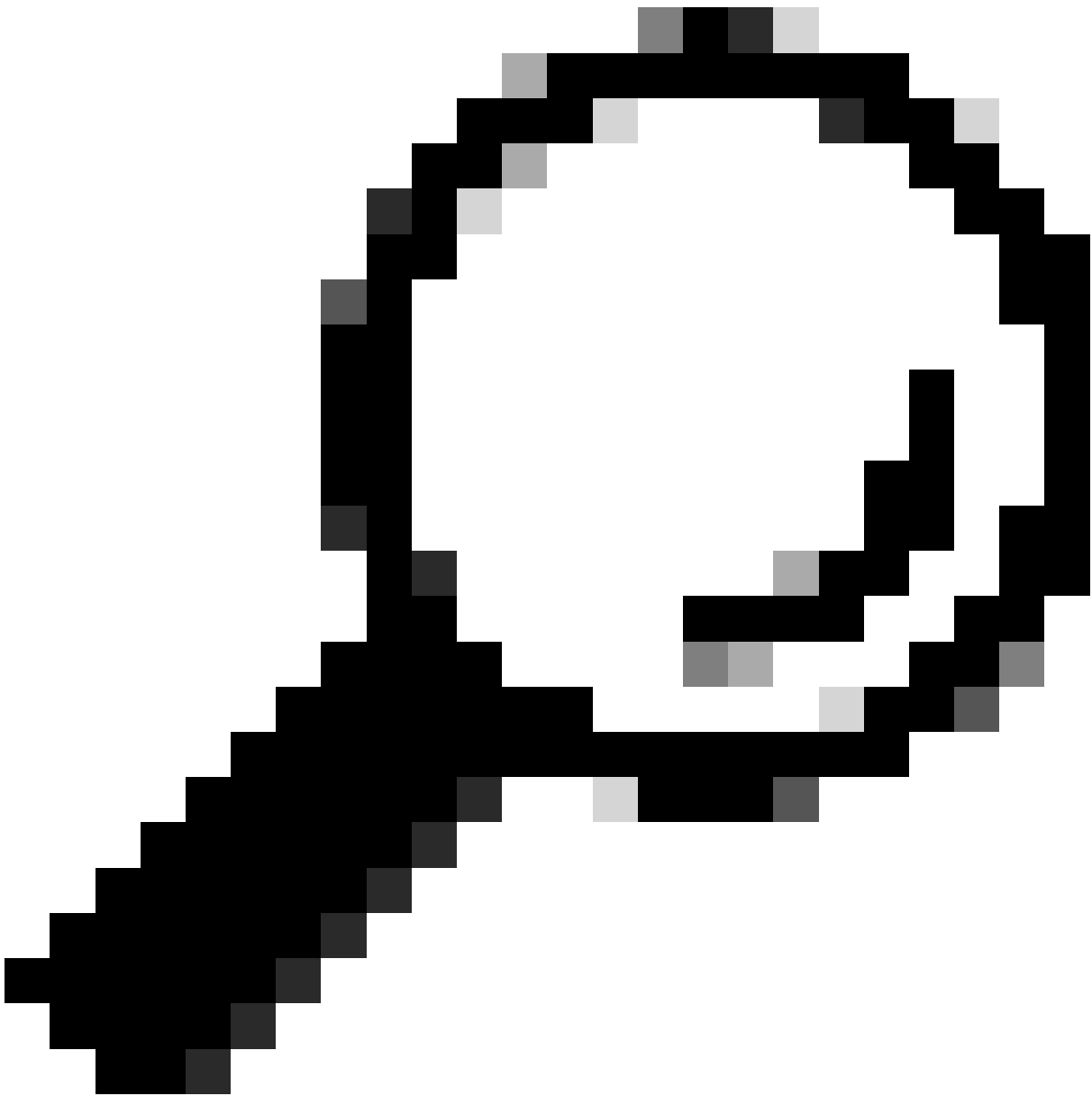
Add Interfaces

Choose **VNI Interface**.

The screenshot shows a network configuration interface. At the top, there are two buttons: 'Sync Device' and 'Add Interfaces'. The 'Add Interfaces' button is open, showing a dropdown menu with the following options: 'Sub Interface', 'Redundant Interface', 'Bridge Group Interface', 'Virtual Tunnel Interface', 'Loopback Interface', and 'VNI Interface'. The 'VNI Interface' option is highlighted in blue. Below the dropdown menu, there is a table with columns for 'Status', 'Type', and 'Action'. The first row shows 'Disabled', 'Global', and a pencil icon. The second row shows 'Disabled', 'Global', and a pencil icon. The third row shows 'Disabled', 'Global', and a pencil icon.

Add VNI Interface

Specify the interface **Name**, **Description**, and **VNI ID** (between 1 and 10000).



Tip: This ID is only an internal interface identifier.

Check **Enable Proxy**.

This option enables single-arm proxy, and allows traffic to exit the same interface it entered (U-turn traffic).



Warning: If you later edit the interface, you cannot disable single-arm proxy. To do that, you need to delete the existing interface and create a new VNI interface. This option is only available for a Geneve VTEP.

Select **NVE Mapped to VTEP Interface**. This associates this interface with the VTEP source interface.

Add VNI Interface



General

IPv4

IPv6

Advanced

Name:

VNI-Outside

Enabled

Description:

Security Zone:

Outside

Priority:

0

(0 - 65535)

VNI ID*:

1

(1 - 10000)

VNI Segment ID:

(1 - 16777215)

Enable Proxy:

Multicast Group IP

Address:

NVE Mapped to
VTEP Interface:

NVE Number:

1

Cancel

OK

Add NVI Interface

Click **OK** and **Save**. You can see VNI interface is created as shown in this image:

vFTD-AWS Save Cancel

Cisco Firepower Threat Defense for AWS

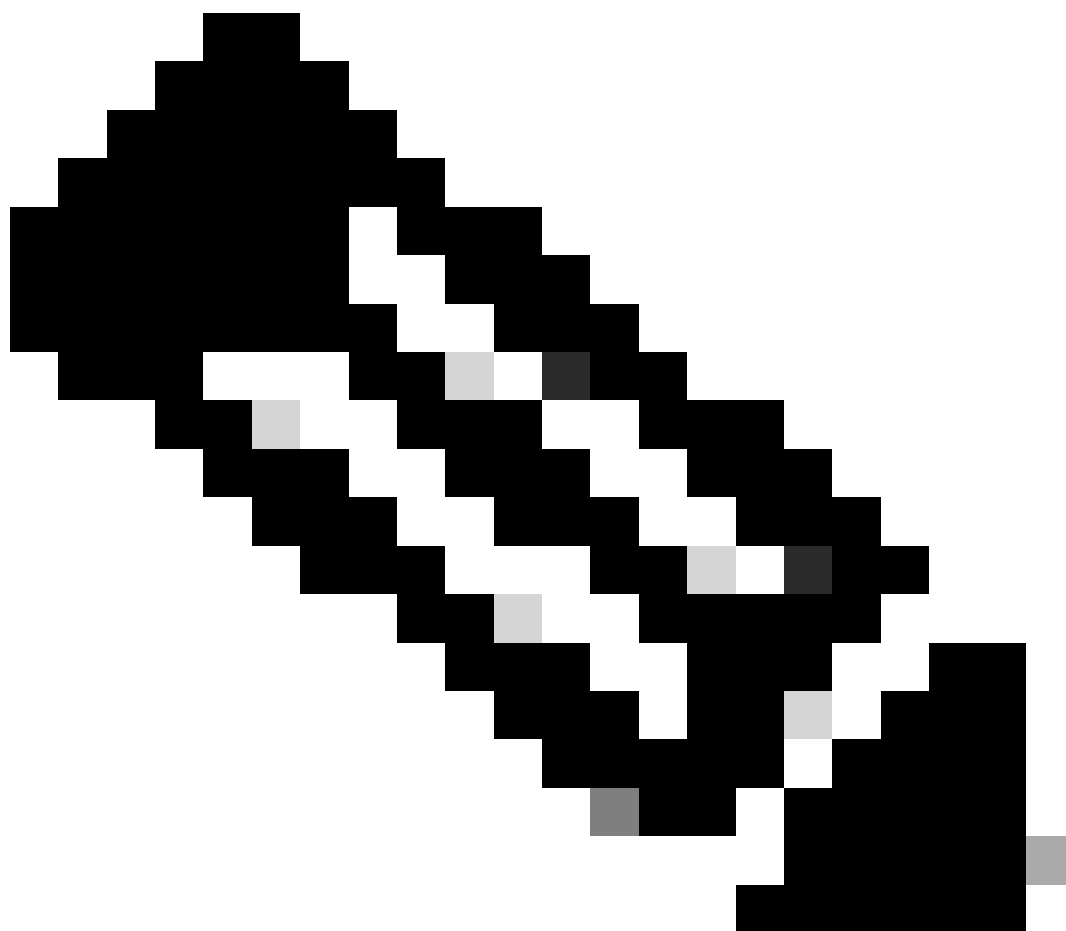
Device Routing **Interfaces** Inline Sets DHCP VTEP

Q Search by name Sync Device Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Diagnostic0/0	diagnostic	Physical				Disabled	Global
TenGigabitEthernet0/0	Outside	Physical				Disabled	Global
TenGigabitEthernet0/1	Inside	Physical				Disabled	Global
vni1	VNI-Outside	VNIinterface	Outside		1.2.3.4/24(Static)	Disabled	Global

VNI Interface is Created

Finally, **Deploy** the interface configuration.



Note: You can configure the routed interface parameters required for your interface at this point. Interface IP address, static or Dynamic routing for VNI interface.

Verify

Connect to FTDv via SSH or console:


```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
admin> enable
Password:
admin#
```

Review Interface details and VNI interface summary:

```
<#root>
```

```
admin# show ip
```

```
System IP Addresses:
Interface      Name      IP address      Subnet mask      Method
Management0/0 diagnostic 10.0.0.61        255.255.255.0    DHCP
vni1           VNI-Outside 1.2.3. 4        255.255.255.0    manual

Current IP Addresses:
Interface      Name      IP address      Subnet mask      Method
Management0/0 diagnostic 10.0.0.61        255.255.255.0    DHCP
vni1           VNI-Outside 1.2.3. 4        255.255.255.0    manual
```

```
admin# show interface VNI summary
```

```
Interface vni1 "VNI-Outside", is up, line protocol is up
  VTEP-NVE 1
  Tag-switching: disabled
  MTU: 1500
  MAC: 0206.104e.ed0f
  proxy mode: single-arm
  IP address 1.2.3. 4, subnet mask 255.255.255.0
  Multicast group not configured
```

You can confirm geneve encapsulation is enabled as shown in this command output:

```
<#root>
```

```
admin#
```

```
show running-config nve
```

```
nve 1
```

```
encapsulation geneve
```

```
source-interface Outside
```

Troubleshoot

Verify both VNI interface and VTEP source interface protocol and status are up/up. As shown next, interface TenGigabitEthernet0/0 and vni1 are up/up:

```
<#root>
```

```
# show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Internal-Control0/0	127.0.1.1	YES	unset	up	up
Internal-Control0/1	unassigned	YES	unset	up	up
Internal-Data0/0	unassigned	YES	unset	down	up
Internal-Data0/0	unassigned	YES	unset	up	up
Internal-Data0/1	169.254.1.1	YES	unset	up	up
Internal-Data0/2	unassigned	YES	unset	up	up
Management0/0	10.0.0.61	YES	DHCP	up	up
TenGigabitEthernet0/0	unassigned	YES	unset	up	up
TenGigabitEthernet0/1	unassigned	YES	unset	up	up
vni1	1.2.3. 4	YES	manual	up	up

Ensure vni interface single-arm and vtep association are present as shown in this output:

```
<#root>
```

```
# show run interface vni 1
```

```
!  
interface vni1  
  proxy single-arm  
  nameif VNI-Outside  
  security-level 0  
  ip address 1.2.3. 4 255.255.255.0  
  vtep-nve 1
```

Review interface counters for VNI interface:

```
<#root>
```

```
# show interface VNI detail
```

Refer to the [Firepower Management Center Configuration Guide](#) for additional information.