Getting Started with Secure Firewall Threat Defense Virtual in Multicloud Defense

First Published: 2025-07-18

Configure and Deploy a Secure Firewall Threat Defense Virtual Device in Multicloud Defense

Is this Use Case For You?

This use case is intended for:

- Users of Secure Firewall Threat Defense Virtual (FTDv) in Cloud-delivered Firewall Management Center (cdFMC) and Multicloud Defense, Amazon Web Services (AWS), and Azure platforms who are looking to protect their assets over the cloud.
- AWS and Azure cloud service providers.
- Customer administration teams and administrators who are both external and internal to Cisco.

Overview of Secure Firewall Threat Defense Virtual in Multicloud Defense

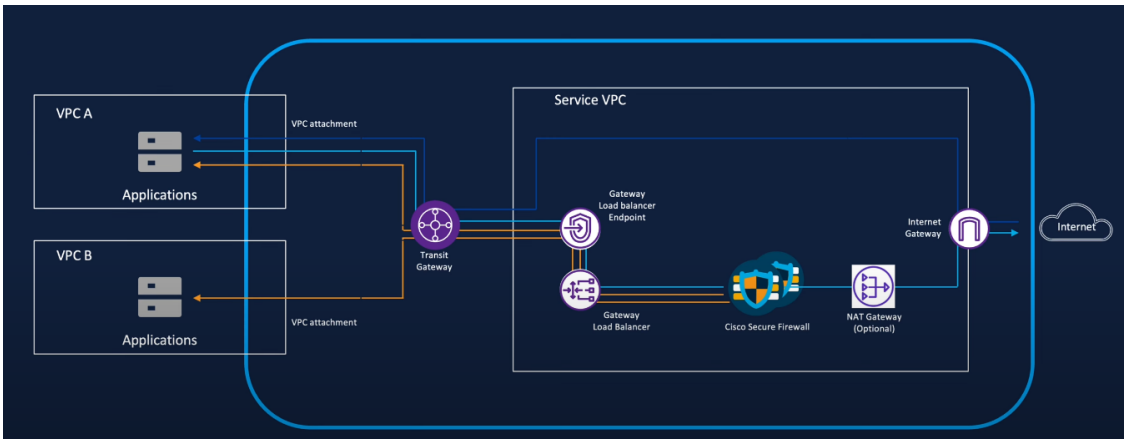
Deploying a virtual firewall or gateway can be a complex, manual process. This requires you to build and configure cloud components such as Secure VPCs, VPC/VNet, subnets, security groups, routes, transit gateways, gateway load balancers, setting up the traffic flow etc. You also need to consider addressing the scaling needs. This can lead to slower deployment time, and increased risk of human errors during configuration. There is an also increased complexity of having multiple service providers in your infrastructure, with different needs for configuration and management. Multicloud Defense helps address these complexities.

Multicloud Defense can fully orchestrate Secure Firewall Threat Defense Virtual device deployments across cloud providers. Multicloud Defense does the orchestration to help automate the creation of all cloud infrastructure VPCs, subnets, load balancers, security groups, with simplification of route tables and setting up of peers. Multicloud Defense enables the automatic onboarding and registering of the FTDv devices to Cloud-delivered Firewall Management Center (cdFMC), from where you can manage policies effectively. Multicloud Defense also addresses auto-scaling needs based on real-time traffic and health of the FTDv devices.

Watch the video on FTDv Orchestration by Multicloud Defense Controller.

Workflow For Configuring a Firewall Threat Defense Virtual on Multicloud Defense

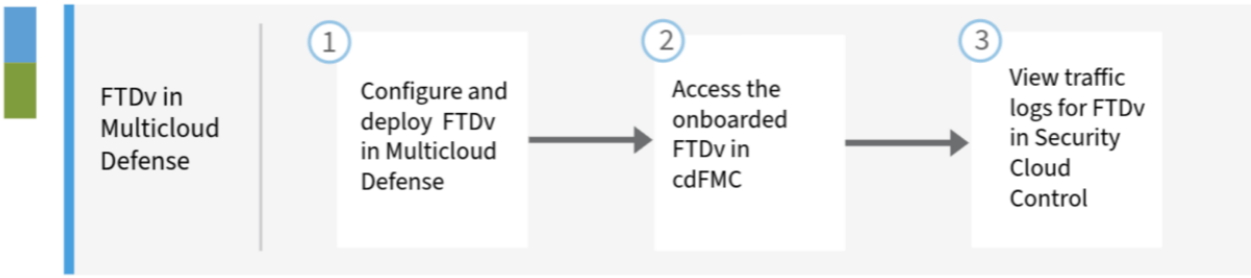
The image here shows the orchestration of an AWS FTDv managed by Cloud-delivered Firewall Management Center in Multicloud Defense, for an Egress/East-West use case.



Workflow

VPC A and VPC B as shown in the image are the assets that need to be protected. Multicloud Defense creates a Service VPC, a transit gateway and its attachments to VPC A and VPC B, gateway load balancer, gateway load balancer endpoints, and one NAT gateway (optional). Multicloud Defense Controller manages the automatic configuration of these resources, and orchestrates the deployment of all of these resources. There is no need to configure this in your cloud service provider account. All the back-end component configurations are managed seamlessly by the Multicloud Defense Controller. Protected traffic can now flow from your Secure Firewall to the Internet.

This workflow guides your through the configuration of an FTDv in Multicloud Defense:



Number	Step
1.	Configure and deploy an FTDv. For details, refer Configure and Deploy an FTDv in Multicloud Defense.
2.	Access the onboarded FTDv in cdFMC. For details, refer Access the onboarded FTDv in cdFMC.

3.	View traffic logs of the FTDv in Security Cloud Control. For details, refer View Traffic Logs for the FTDv in Security Cloud Control.

Guidelines For Configuring a Firewall Threat Defense Virtual

The prerequisite is that you will need to have a tenant that has been created in Security Cloud Control, with cdFMC enabled. Refer to these guidelines in the relevant guides, when you configure an FTDv.

- For Multicloud Defense related guidelines, refer to Secure Firewall Threat Defense Virtual.
- For cdFMC related guidelines, refer to Guidelines for Managing an FTDv Created in Multicloud Defense.

Configure and Deploy a Firewall Threat Defense Virtual in Multicloud Defense

Procedure

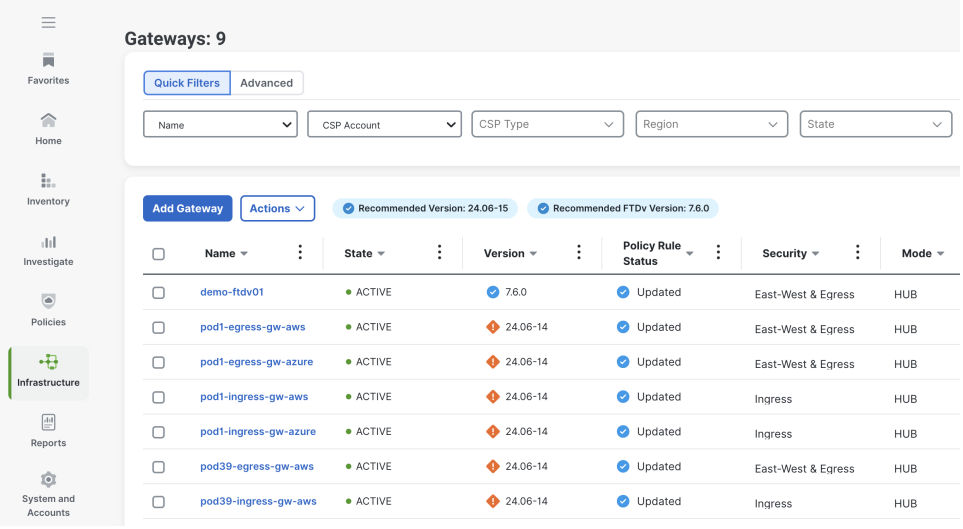
Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Multicloud Defense**.

Step 3 In the upper-right corner, click **Multicloud Defense Controller** to open the controller.

Step 4 In the Multicloud Defense portal, navigate to **Infrastructure** > **Gateways** > **Gateways**.

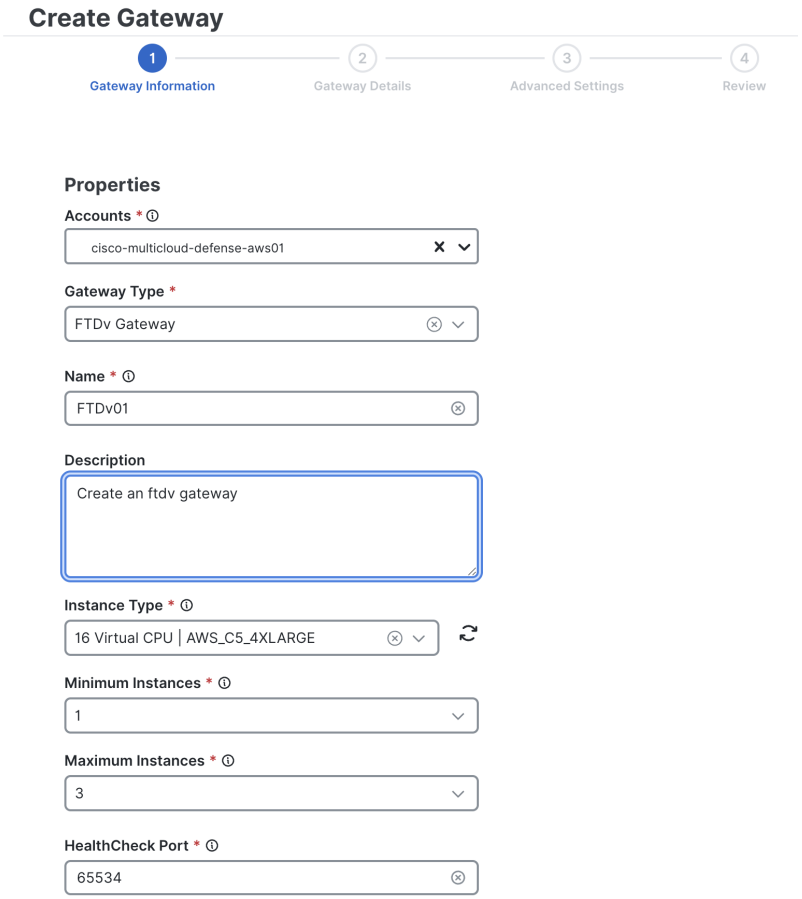
Step 5 Click **Add Gateway**.



Step 6 Provide details for the following fields:

- **Accounts**: For example, cisco-multicloud-defense-aws01
- **Gateway Type**: Choose FTDv Gateway.

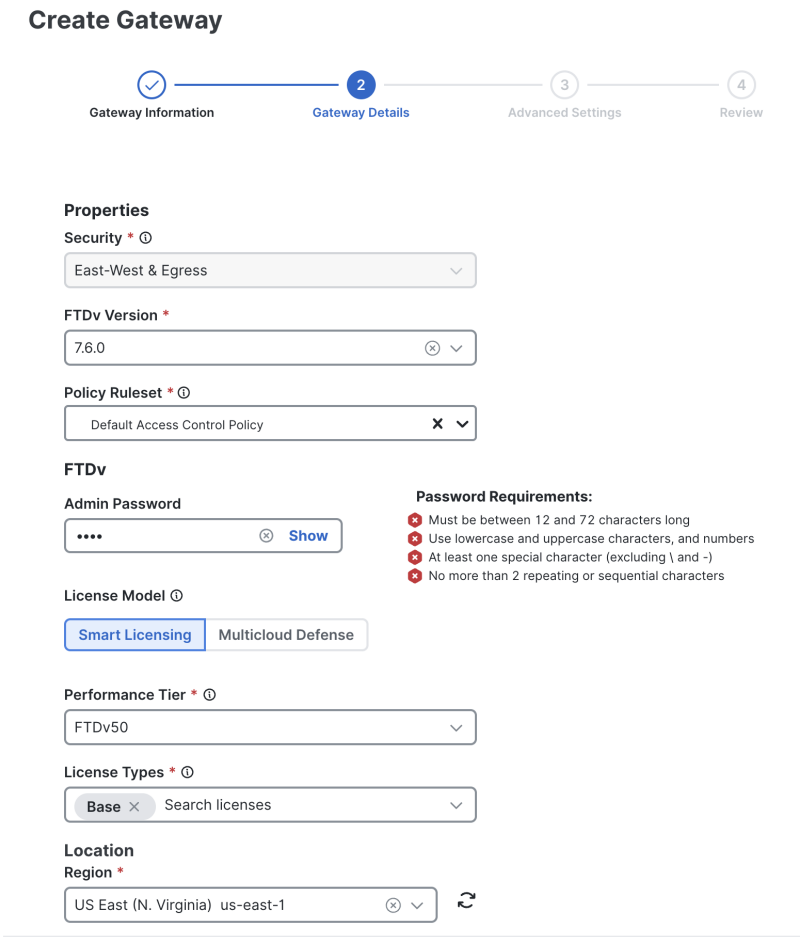
- **Name**: In this example, we provide "FTDv01" as the name.
- **Description**: Enter a description.
- **Instance Type**: Choose an instance from the drop-down list, for example, 16 Virtual CPU AWS_C5_4XLARGE.
- **Minimum Instances**: Choose a value from the drop-down list, for example, 1.
- **Maximum Instances**: Choose a value from the drop-down list, for example, 3.
- **Healthcheck Port**: Choose a value from the drop-down list, for example, 65534



Step 7 Provide gateway details in the **Properties** section. The **Security** field is set to **East-West & Egress** by default.

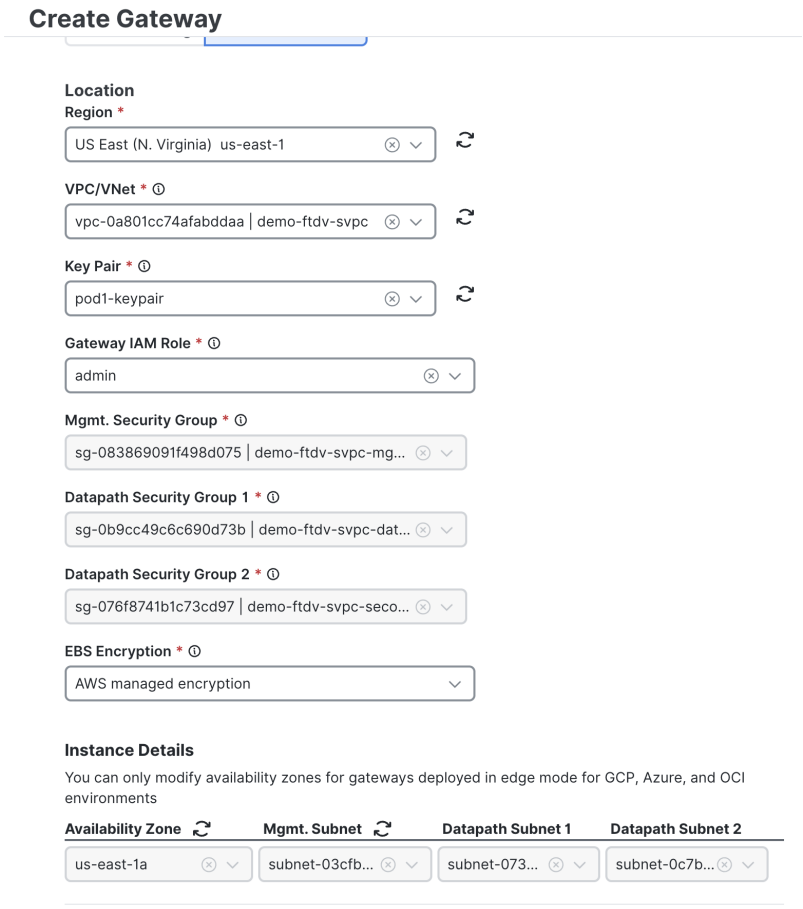
- **FTD Version**: Choose the supported version of 7.6 or above.
- **Policy Ruleset**: Choose an access control policy that you already have created on your cdFMC account or create a new one. For example, Default Access Control Policy.
- **Admin Password**: Enter a password. Ensure the password meets the password requirements.
- **License Model**: Choose Smart Licensing or Multicloud Defense. Smart Licensing is an existing FTDv licensing model, and Multicloud Defense licensing model is an hourly-based licensing model.
- **Performance Tier**: Choose a tier from the drop-down list, for example, FTDv50.

- **License Type**: Choose a license type from the drop-down list, for example, Base. You can choose multiple license types, if required.
- **Region**: Choose a region to deploy the FTDv, from the drop-down list, for example, US East (N.Virginia) us-east-1.



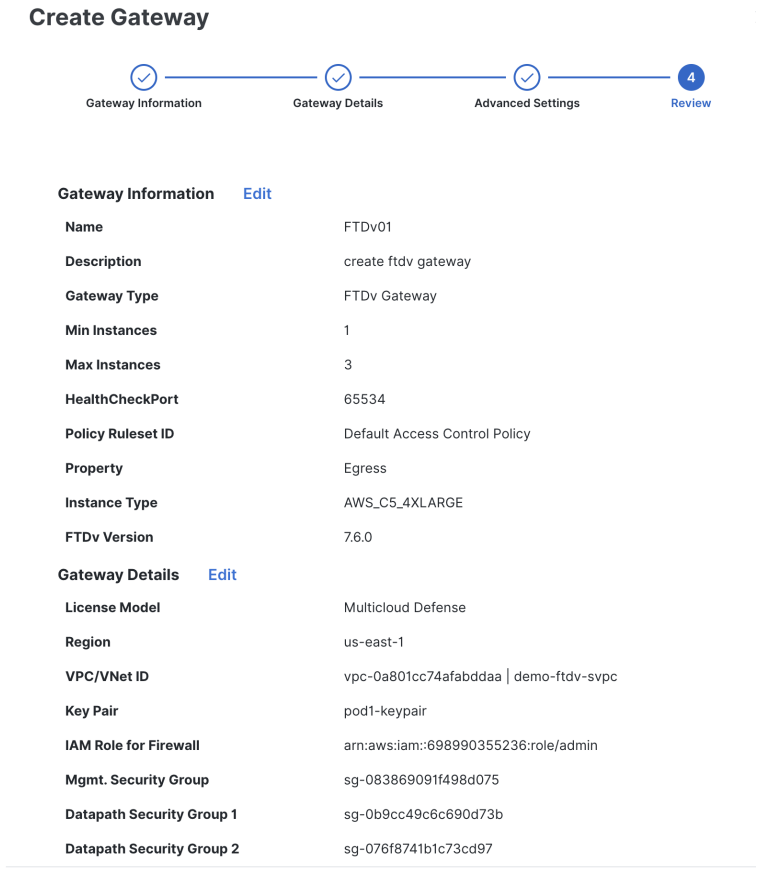
Step 8 Provide additional gateway details in the **Properties** section for:

- **VPC/VNet**: Choose a value from the drop-down list. You can create the VPC or VNet in **Infrastructure** > **Gateways** > **VPCs/VNets**.
- **Key Pair**: Choose a key pair to attach to this instance from the drop-down list, for example, pod1-keypair.
- **Gateway IAM Role**: Choose a role from the drop-down list, for example, admin.
- **Mgmt. Security Group**: Choose a security group from the drop-down list.
- **Datapath Security Group 1**: Choose a security group from the drop-down list.
- **Datapath Security Group 2**: Choose a security group from the drop-down list.
- **EBS Encryption**: Choose an encryption from the drop-down list, for example, AWS managed encryption.
- **Instance Details**. View and verify the instance details that are listed.



Step 9 In the **Advanced Settings** section, use the toggle to enable or disable **Public IP**.

Step 10 Review the information that you provided.



Step 11 Click **Finish**, upon completion of the review.

The gateway is successfully created and starts deploying the FTDv in the AWS account, in the VPC that you provided. It takes approximately 30 minutes for the FTDv to be deployed in the cloud service provider account. Once the FTDv is up and running, the FTDv is onboarded to cdFMC also. The FTDv moves from ENABLING state to ACTIVE PENDING state and then to ACTIVE state.

Access Firewall Threat Defense Virtual Device in Cloud-Delivered Firewall Management Center

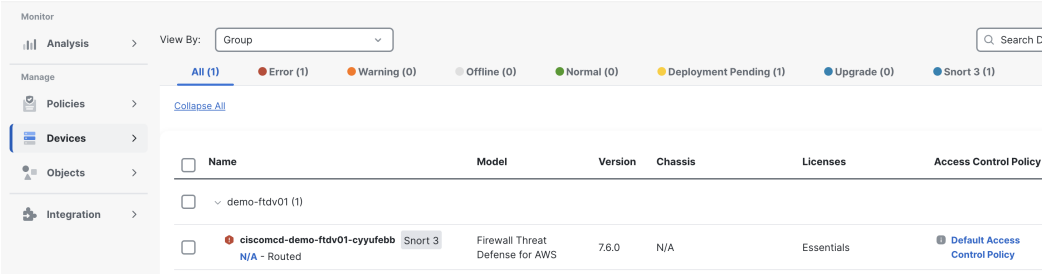
Once an FTDv device is active, Multicloud Defense will start onboarding the FTDv device to the cdFMC that is associated with your tenant.

Procedure

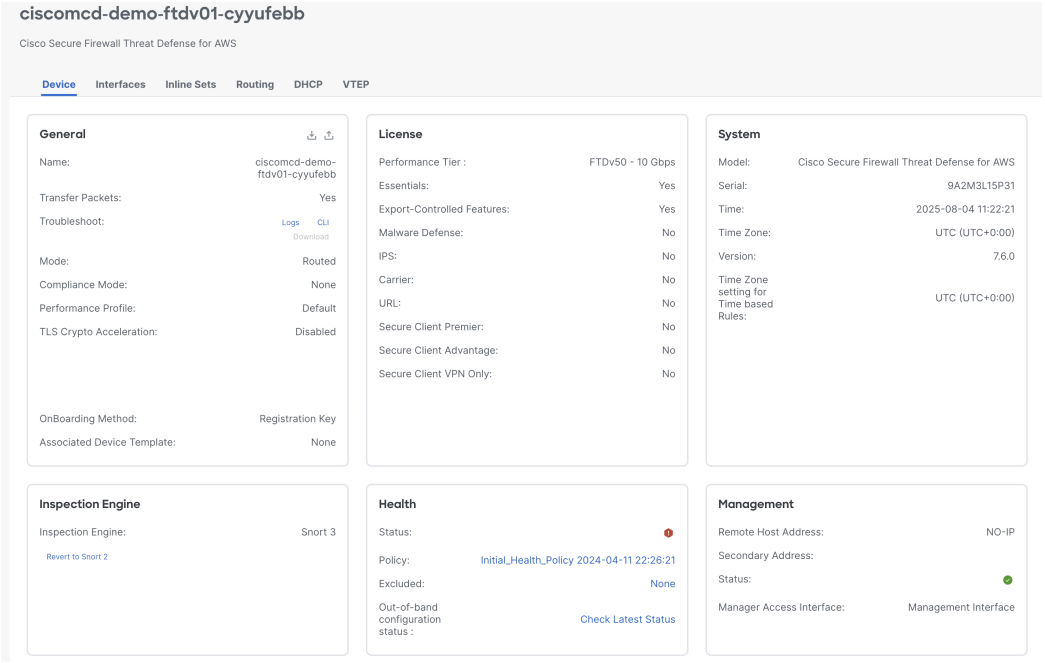
Step 1 From the Security Cloud Control menu, navigate to **Administration > Integrations > Firewall Management Center** and click **Enable Cloud-Delivered FMC**.

Step 2 Navigate to the **Devices > Device Management**.

Step 3 Under the device group, you can view the onboarded FTDv device. The inside interface, outside interface, VNI interface, security zones, and routing are pre-configured for the FTDv device.



You can see that the configurations have been made for networking interfaces, security zone, access control policies, platform settings etc., from the device page. You can view all the details but not edit them.



Once you have attached the policy to the FTDv device in Multicloud Defense, you can perform Policy Management activities such as write rules and policies from within cdFMC.

- Multicloud Defense takes care of the deployment, onboarding of FTDv to the cdFMC, configuring basics such as interface configuration, basic access control policy attachment, and scaling in and scaling out of instances, based on health and traffic.
- Cloud-delivered Firewall Management Center takes care of policy configuration, policy management, and access control rules for policies.
- Security Cloud Control takes care of providing views of logs and events.

View Traffic Logs For Firewall Threat Defense Virtual in Security Cloud Control

In Security Cloud Control, navigate to **Events & Logs > Event Logging**. You can view the traffic logs for the FTDv device.

Troubleshooting For Secure Firewall Threat Defense Virtual on Multicloud Defense

Here are a few aspects to consider, to avoid common issues that can occur:

- Whenever you modify a policy, ensure that it is deployed to all FTDv instances which use the policy.
- Do not manually add or remove instances from a device group.
- Do not edit HTTP-related platform settings.
- For BYOL license, plan for autoscaling scenarios, understand the Performance Tier & License feature, and verify your Smart License account.
- Don’t edit any configurations that are managed by Multicloud Defense directly in your cloud service provider account.
- Don’t stop any FTDv instances from your cloud service provider, since Multicloud Defense will assume that these are faulty instances and will replace them with new instances.

For support, contact Cisco Technical Assistance Center.

Additional Resources For Firewall Threat Defense Virtual in Multicloud Defense

Know more about Firewall Threat Defense Virtual in Multicloud Defense with these additional resources.

- Secure Firewall Threat Defense Virtual
- Create an FTDv Gateway
- Manage Multicloud Defense-Onboarded Secure Firewall Threat Defense Virtual Devices
- Video on FTDv Orchestration by Multicloud Defense Controller