

Manage Multicloud Defense-Onboarded Secure Firewall Threat Defense Virtual Devices

- Overview of Multicloud Defense-Onboarded Firewall Threat Defense Virtual Devices, on page 1
- Onboard and Configure a Secure Firewall Threat Defense Virtual Device in Multicloud Defense, on page 3

Overview of Multicloud Defense-Onboarded Firewall Threat Defense Virtual Devices

You can orchestrate your Secure Firewall Threat Defense virtual (FTDv) device in your cloud service provider manually and then register your device to Cloud-Delivered Firewall Management Center (Cloud-Delivered Firewall Management Center) for management of it. A lot of manual steps are involved in this method such as VPC creation, security groups creation, peer connection and routing in your cloud service provider, which can be cumbersome.

With Multicloud Defense available as part of Security Cloud Control, you can now easily orchestrate, deploy, and register an FTDv device using Multicloud Defense while retaining your FTDv as a gateway. Multicloud Defense communicates with Security Cloud Control for FTDv registration and orchestrates the initial setting up of the FTDv. For more details on deploying an FTDv using Multicloud Defense, see Secure Firewall Threat Defense.

HTTPS configuration under Platform Settings policy is managed by Multicloud Defense. Any other configurations related to Platform Settings need to be done in Firewall Management Center only. Multicloud Defense also adds one mandatory NAT rule under NAT policy. Additional NAT rules can be configured in the Firewall Management Center. You can create and assign access policies, rules, and objects in Cloud-Delivered Firewall Management Center For more details, see Access Control Policies.

Guidelines for Managing an FTDv Created in Multicloud Defense

Consider the following guidelines in the context of Cloud-Delivered Firewall Management Center, when creating gateways for FTDv using Multicloud Defense:

- FTDv registration and configuration can be done only in Multicloud Defense. This information is view-only and cannot be edited in Cloud-Delivered Firewall Management Center. You cannot edit any of the **Devices**, **Interface**, **Inline Sets**, **Routing**, **DHCP** and **VTEP** configuration details in the user interface of Cloud-Delivered Firewall Management Center, because all device-specific configurations are done in Multicloud Defense.

- HTTPS configuration under Platform Settings policy is managed by Multicloud Defense and any changes to it can impact devices or the FTDv gateway. You need to be cautious while changing any configurations in **Platform Settings** as the policy overall is a shared policy.
- Mandatory NAT rule is managed by Multicloud Defense and any changes to the mandatory rule can impact devices or the FTDv gateway.
- Configure NAT rules to translate incoming traffic from the external network to the internal network on the specified port and IP address. Multicloud Defense automatically opens the required port on the load balancer provided by the cloud service. This configuration ensures accurate translation and forwarding of inbound traffic, while the load balancer manages port access.
- Multicloud Defense devices are added under a logical device group for each gateway.
- You can use existing policies that you have in Cloud-Delivered Firewall Management Center or even create new policies from the Multicloud Defense application.
- You can configure or modify an existing policy from Cloud-Delivered Firewall Management Center.
- To add additional policies such as QoS policy or any other policy configuration for Multicloud Defense-related FTDv in Cloud-Delivered Firewall Management Center, the policies must be assigned at the device group level, so that it is applied to all devices in the group. This helps in addressing shared policies and the application of the policy to all devices that are added to the group in future. Note that policies are not applied at the single FTDv device level, but across the group.
- Don't remove an FTDv from Security Cloud Control. Contact your administrator to make any changes, if any, in Multicloud Defense.
- Don't move an FTDv across groups at any point in time or unassign an FTDv from groups in Cloud-Delivered Firewall Management Center.
- Don’t rename the device groups created by Multicloud Defense in Cloud-Delivered Firewall Management Center, because it can hamper the working of the devices.
- Don’t edit or delete the security zones or objects because they are managed in Multicloud Defense and can hamper the working of the devices. You can identify this when you access Platform Settings policies. If the policy is deployed to a device orchestrated by Multicloud Defense, you are notified with a message. For identification, Cloud-Delivered Firewall Management Center uses an additional field with the naming convention `mcdmanaged`. You can identify the security zones by the naming convention used – `ciscomcd-VNI`, `ciscomcd-inside`, or `ciscomcd-outside`.
- Licensing of the FTDv is according to the FTDv plan that you chose, that is, either Bring Your Own License (BYOL) or Software-as-a-Service (SaaS). You can use the existing license that you use for FTDv.
- We recommend that you upgrade the FTDv versions only in the Multicloud Defense application.
- This feature is supported for FTDv version 7.6 and above. You can upgrade or downgrade the FTDv in Multicloud Defense. This is done by creating a new instance. The upgrade or downgrade enables easy scaling up or scaling down of the instances too.
- Your FTDv is listed in Security Cloud Control Firewall Management and Cloud-Delivered Firewall Management Center. You can manage your policies in Cloud-Delivered Firewall Management Center.
- When you trigger a deployment on these FTDvs, you should select together all the FTDvs that belong to same gateway, otherwise the configuration will be out of sync among FTDvs and this can lead to inconsistent traffic behavior.

- Features such as Site-to-Site VPN and Remote Access VPN are not currently supported.
- Multicloud Defense can register FTDv devices with Cloud-Delivered Firewall Management Center by using the supported registration flow for the deployment. For Multicloud Defense-managed FTDv devices, registration can be device-initiated or Cloud-Delivered Firewall Management Center-triggered. In the Cloud-Delivered Firewall Management Center-triggered flow, Cloud-Delivered Firewall Management Center initiates the registration connection to the FTDv by using the registration information that Multicloud Defense provides through Security Cloud Control Firewall Management.

  This support applies only to FTDv devices that are deployed and managed by Multicloud Defense. It does not change the onboarding flow for manually onboarded FTD or FTDv devices in Cloud-Delivered Firewall Management Center.

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

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the Security Cloud Control platform menu, choose **Products > Multicloud Defense.**

Step 3 Register your FTDv in Multicloud Defense and onboard your cloud security provider, either AWS or Azure. For more details, see the Cisco Multicloud Defense User Guide.

Step 4 Create a Service VPC or VNet in Multicloud Defense. For more details, see Create a VPC or VNet.

Step 5 Configure your gateway in Multicloud Defense. For more details, see Add a Gateway with an FTDv.

Step 6 Configure your policy in Cloud-Delivered Firewall Management Center. For more details, see Access Control Policies.

What to do next

You can view your FTDv in Multicloud Defense, Security Cloud Control platform, and Firewall Management Center in your Cloud-Delivered Firewall Management Center account.