

Introduction to the Cisco Secure Firewall Threat Defense Virtual

The Cisco Secure Firewall Threat Defense Virtual (Firewall Threat Defense Virtual) brings Cisco's Next Generation Firewall functionality to virtualized environments, enabling consistent security policies to follow workloads across your physical, virtual, and cloud environments, and between clouds.

Today, organizations rely on a mixture of physical and virtual control points to meet their network security needs. They need the flexibility to deploy different physical and virtual firewalls across a wide range of environments while still maintaining consistent policy across branch offices, corporate datacenters, and all points between. From data center consolidation to office relocations, mergers and acquisitions, as well as seasonal peaks in demand on your applications, Cisco’s virtual firewall portfolio helps you simplify security management with the convenience of unified policy and the flexibility to deploy everywhere.

The Cisco Secure Firewall Threat Defense Virtual combines Cisco’s proven network firewall with Snort IPS, URL filtering, and malware defense. It simplifies threat protection with consistent security policies across physical, private, and public cloud environments. Get deep visibility into your network and quickly detect threat origin and activity. Then, stop attacks before they impact your operations.

Secure Firewall Threat Defense Virtual is the popular virtualized solution. Prioritize threats with automated risk rankings and impact flags to focus your resources on events requiring immediate action. License portability provides flexibility to move from your on-premises private cloud to public cloud while maintaining consistent policy and unified management across all of your appliances. Cisco Smart Software Licensing makes it easy to deploy, manage, and track virtual firewall instances.

- Secure Firewall Threat Defense Virtual on Azure Post-installation Tasks, on page 1
- What to do next, on page 2

Secure Firewall Threat Defense Virtual on Azure Post-installation Tasks

Secure Firewall Management Center

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that the Firewall Threat Defense allows, use the Firewall Management Center to configure your devices instead of the integrated Firewall Device Manager. For detailed information, see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center

Important You cannot use both the Firewall Device Manager and the Firewall Management Center to manage the Firewall Threat Defense device. Once the Firewall Device Manager integrated management is enabled, it won't be possible to use the Firewall Management Center to manage the Firewall Threat Defense device, unless you disable the local management and re-configure the management to use the Firewall Management Center. On the other hand, when you register the Firewall Threat Defense device to the Firewall Management Center, the Firewall Device Manager onboard management service is disabled.

Caution Currently, Cisco does not have an option to migrate your Firewall Device Manager configuration to the Firewall Management Center and vice-versa. Take this into consideration when you choose what type of management you configure for the Firewall Threat Defense device.

Secure Firewall Device Manager

The Firewall Device Manager is a web interface included on most Firewall Threat Defense devices. It lets you configure the basic features of the software that are most commonly used for small networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network with many devices. For detailed information, see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Device Manager

Note See the *Cisco Secure Firewall Threat Defense Compatibility Guide* for list of devices that support the Firewall Device Manager.

What to do next

Click on the cloud provider chapter as per your requirement. The table below contains a list of links to some of the important sections in the guide.

Cloud Provider	Section

AWS	• Configure AWS Environment
	• Deploy the Firewall Threat Defense Virtual
	• Integrate Amazon GuardDuty with Secure Firewall Threat Defense
	• Auto Scale Solution for the Threat Defense Virtual on AWS
	  • Auto Scale Solution with NLB
	  • Customize and Deploy the NLB Infrastructure Template on the Amazon CloudFormation Console
	  • Deploy the Auto Scale Solution with NLB
	  • Auto Scale Solution with GWLB
	  • Customize and Deploy the GWLB Infrastructure Template on the Amazon CloudFormation Console
	  • Deploy the Auto Scale Solution with GWLB

Azure	• Deploy the Firewall Threat Defense Virtual from the Azure Marketplace Using the Solution Template • Deploy the Firewall Threat Defense Virtual from Azure Using a VHD and Resource Template
GCP	• Configure GCP Environment • Deploy the Firewall Threat Defense Virtual
OCI	• Configure OCI Environment • Deploy the Threat Defense Virtual on OCI
Alibaba Cloud	• Configuring Policies and Device Settings • Configuring Alibaba Environment • Deploy the Threat Defense Virtual
VMware	• Deploy the Firewall Threat Defense Virtual to vSphere vCenter • Deploy the Firewall Threat Defense Virtual to a vSphere ESXi Host • Complete the Firewall Threat Defense Virtual Setup Using the CLI
KVM	• Prepare the Day 0 Configuration File • Deploy the Firewall Threat Defense Virtual

Cloud Provider	Section
Cisco HyperFlex	• Deploy the Firewall Threat Defense Virtual • Complete the Firewall Threat Defense Virtual Setup using CLI
Nutanix	• Upload the Firewall Threat Defense Virtual QCOW2 File to Nutanix • Prepare the Day 0 Configuration File • Deploy the Firewall Threat Defense Virtual • Complete the Firewall Threat Defense Virtual Setup
OpenStack	• Upload the Firewall Threat Defense Virtual Image to OpenStack • Create the Network Infrastructure for OpenStack and Firewall Threat Defense Virtual • Deploy the Firewall Threat Defense Virtual