New Features in Cloud-delivered Firewall Management Center 2023

November 30, 2023

Table 1: New Features: Version 20231117

Feature	Min. Threat Defense	Details
Administration		
Schedule a Secure Firewall Threat Defense Device Backup in Cloud-delivered Firewall Management Center	Any	Use the cloud-delivered Firewall Management Center to perform scheduled backups of the Secure Firewall Threat Defense devices it manages. See Schedule Remote Device Backups for more information.

October 19, 2023

Table 2: New Features: Version 20230929

Feature	Min. Threat Defense	Details
Platform		
Threat defense Version 7.4.0 support.	7.4.0	You can now manage threat defense devices running Version 7.4.0. Version 7.4.0 is available *only* on the Secure Firewall 4200. You must use a Secure Firewall 4200 for features that require Version 7.4.0. Support for all other platforms resumes in Version 7.4.1.
Secure Firewall 4200.	7.4.0	You can now manage the Secure Firewall 4215, 4225, and 4245 with cloud-delivered Firewall Management Center. These devices support the following new network modules: • 2-port 100G QSFP+ network module (FPR4K-XNM-2X100G) • 4-port 200G QSFP+ network module (FPR4K-XNM-4X200G) See: Cisco Secure Firewall 4215, 4225, and 4245 Hardware Installation Guide
Performance profile support for the Secure Firewall 4200.	7.4.0	The performance profile settings available in the platform settings policy now apply to the Secure Firewall 4200. Previously, this feature was supported only on the Firepower 4100/9300 and on threat defense virtual. See: Configure the Performance Profile
Numbering convention for cloud-delivered Firewall Management system.	Any	The cloud-delivered Firewall Management system is a feature of CDO. For the purposes of troubleshooting, we identify the version number of the cloud-delivered Firewall Management Center on the FMC Services page. See: View Services Page Information.
Platform Migration		
Migrate from Firepower 1000/2100 to Secure Firewall 3100.	Any	You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100. New/modified screens: **Devices** > **Device Management** > **Migrate** Platform restrictions: Migration not supported from the Firepower 1010 or 1010E. See: Migrate the Configuration to a new Model.

Feature	Min. Threat Defense	Details
Migrate devices from Firepower Management Center 1000/2500/4500 to cloud-delivered Firewall Management Center.	Any	

Feature	Min. Threat Defense	Details
		You can migrate devices from Firepower Management Center 1000/2500/4500 to cloud-delivered Firewall Management Center. To migrate devices, you must *temporarily* upgrade the on-prem management center from Version 7.0.3 (7.0.5 recommended) to Version 7.4.0. This temporary upgrade is required because Version 7.0 management centers do not support device migration to the cloud. Additionally, only standalone and high availability threat defense devices running Version 7.0.3+ (7.0.5 recommended) are eligible for migration. Cluster migration is not supported at this time. **Important** Version 7.4.0 is only supported on the 1000/2500/4500 during the migration process. You should minimize the time between management center upgrade and device migration. To summarize the migration process: **1.** Prepare for upgrade and migration. Read, understand, and meet all the prerequisites outlined in the release notes, upgrade guides, and migration guide. Before you upgrade, it is especially important that the on-prem management center is "ready to go," that is, managing only the devices you want to migrate, configuration impact assessed (such as VPN impact), freshly deployed, fully backed up, all appliances in good health, and so on. You should also provision, license, and prepare the cloud tenant. This must include a strategy for security event logging; you cannot retain the on-prem management center for analytics because it will be running an unsupported version. **2.** Upgrade the on-prem management center and all its managed devices to at least Version 7.0.3 (Version 7.0.5 recommended). If you are already running the minimum version, you can skip this step. **3.** Upgrade the on-prem management center to Version 7.4.0. Unzip (but do not untar) the upgrade package before uploading it to the management center. Download from: Special Release. **4.** Onboard the on-prem management center to CDO. **5.** Migrate all devices from the on-prem management center to the cloud-delivered Firewall Management Center as described in the migration guide. When you select devices to migrate, make sure you choose **Delete FTD from On-Prem FMC**. Note that the device is not fully deleted unless you commit the changes or 14 days pass. **6.** Verify migration success. If the migration does not function to your expectations, you have 14 days to switch back or it is committed automatically. However, note that Version 7.4.0 is unsupported for general operations. To return the on-prem management center to a supported version you must remove the re-migrated devices, re image back to Version 7.0.x, restore from backup, and reregister the devices.

Feature	Min. Threat Defense	Details
		See: • Cisco Secure Firewall Threat Defense Release Notes • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Migrate On-Prem Management Center Managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center If you have questions or need assistance at any point in the migration process, contact Cisco TAC.
S2S VPN support in FTD to cloud migration. Migrate threat defense devices with VPN policies from on-prem to cloud-delivered Firewall Management Center.	7.0.3-7.0.x 7.2 or later	Site-to-site VPN configurations on Secure Firewall Threat Defense devices are now migrated along with the rest of the configuration when the device is migrated from the on-prem Firewall Management Center to the cloud-delivered Firewall Management Center. See: Migrate On-Prem Management Center managed Secure Firewall Threat Defense to Cloud-delivered Firewall Management Center
Interfaces		

Feature	Min. Threat Defense	Details
Merged management and diagnostic interfaces.	7.4.0	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later and: • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence** See: Merge the Management and Diagnostic Interfaces
VXLAN VTEP IPv6 support.	7.4.0	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the threat defense virtual cluster control link or for Geneve encapsulation. New/modified screens: • **Devices** > **Device Management** > **Edit Device** > **VTEP** > **Add VTEP** • **Devices** > **Device Management** > **Edit Devices** > **Interfaces** > **Add Interfaces** > **VNI Interface** See: Configure Geneve Interfaces

Feature	Min. Threat Defense	Details
Loopback interface support for BGP and management traffic.	7.4.0	You can now use loopback interfaces for AAA, BGP, DNS, HTTP, ICMP, IPsec flow offload, NetFlow, SNMP, SSH, and syslog. New/modified screens: **Devices** > **Device Management** > Edit device > **Interfaces** > **Add Interfaces** > **Loopback Interface** See: Configure Loopback Interfaces
Loopback and management type interface group objects.	7.4.0	You can create interface group objects with only management-only or loopback interfaces. You can use these groups for management features such as DNS servers, HTTP access, or SSH. Loopback groups are available for any feature that can utilize loopback interfaces. However, it's important to note that DNS does not support management interfaces. New/modified screens: **Objects** > **Object Management** > **Interface** > **Add** > **Interface Group** See: Interface
High Availability/Scalability		
Reduced "false failovers" for threat defense high availability.	7.4.0	Other version restrictions: Not supported with threat defense Version 7.3.x. See: Heartbeat Module Redundancy
SD-WAN		
Policy-based routing using HTTP path monitoring.	7.2.0	Policy-based routing (PBR) can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination. New/modified screens: **Devices** > **Device Management** > Edit device > Edit interface > **Path Monitoring** > **Enable HTTP based Application Monitoring** check box. Platform restrictions: Not supported for clustered devices. See: Configure Path Monitoring Settings
Policy-based routing with user identity and SGTs.	7.4.0	You can now classify network traffic based on users, user groups, and SGTs in PBR policies. Select the identity and SGT objects while defining the extended ACLs for the PBR policies. New/modified screens: **Objects** > **Object Management** > **Access List** > **Extended** > Add/Edit Extended Access List > Add/Edit Extended Access List Entry > **Users** and **Security Group Tag** See: Configure Extended ACL Objects
VPN		

Feature	Min. Threat Defense	Details
IPsec flow offload on the VTI loopback interface for the Secure Firewall 4200.	7.4.0	On the Secure Firewall 4200, qualifying IPsec connections through the VTI loopback interface are offloaded by default. Previously, this feature was supported for physical interfaces on the Secure Firewall 3100. You can change the configuration using FlexConfig and the **flow-offload-ipsec** command. Other requirements: FPGA firmware 6.2+ See: IPSec Flow Offload
Crypto debugging enhancements for the Secure Firewall 4200.	7.4.0	We made the following enhancements to crypto debugging: • The crypto archive is now available in text and binary formats. • Additional SSL counters are available for debugging. • Remove stuck encrypt rules from the ASP table without rebooting the device. New/modified CLI commands: **show counters** See: Troubleshooting Using Crypto Archives
VPN: Remote Access		
Customize Secure Client messages, icons, images, and connect/disconnect scripts.	7.2.0	You can now customize Secure Client and deploy these customizations to the VPN headend. The following are the supported Secure Client customizations: • GUI text and messages • Icons and images • Scripts • Binaries • Customized Installer Transforms • Localized Installer Transforms Threat defense distributes these customizations to the endpoint when an end user connects from the Secure Client. New/modified screens: • **Objects** > **Object Management** > **VPN** > **Secure Client Customization** • **Devices** > **Remote Access** > Edit VPN policy > **Advanced** > **Secure Client Customization** See: Customize Secure Client
VPN: Site to Site		

Feature	Min. Threat Defense	Details
Easily exempt site-to-site VPN traffic from NAT translation.	Any	We now make it easier to exempt site-to-site VPN traffic from NAT translation. New/modified screens: • Enable NAT exemptions for an endpoint: **Devices** > **VPN** > **Site To Site** > **Add/Edit Site to Site VPN** > **Add/Edit Endpoint** > **Exempt VPN traffic from network address translation** • View NAT exempt rules for devices that do not have a NAT policy: **Devices** > **NAT** > **NAT Exemptions** • View NAT exempt rules for a single device: **Devices** > **NAT** > **Threat Defense NAT Policy** > **NAT Exemptions** See: NAT Exemption
Easily view IKE and IPsec session details for VPN nodes.	Any	You can view the IKE and IPsec session details of VPN nodes in a user-friendly format in the Site-to-Site VPN dashboard. New/modified screens: **Overview** > **Site to Site VPN** > Under the Tunnel Status widget, hover over a topology, click **View**, and then click the **CLI Details** tab. See: Monitoring the Site-to-Site VPNs
Access Control: Threat Detection and Application Identification		
Sensitive data detection and masking.	7.4.0 with Snort 3	**Upgrade impact. New rules in default policies take effect.** Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage and generates events only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events, using built-in patterns. Disabling data masking is not supported. See: Custom Rules in Snort 3

Feature	Min. Threat Defense	Details
Clientless zero-trust access.	7.4.0 with Snort 3	We introduced Zero Trust Access that allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy. The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications. New/modified screens: • **Policies** > **Zero Trust Application** • **Analysis** > **Connections** > **Events** • **Overview** > **Dashboard** > **Zero Trust** New/modified CLI commands: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** See: Zero Trust Access.
Routing		
Configure graceful restart for BGP on IPv6 networks.	7.3.0	You can now configure BGP graceful restart for IPv6 networks on managed devices version 7.3 and later. New/modified screens: **Devices** > **Device Management** > Edit device > **Routing** > **BGP** > **IPv6** > **Neighbor** > Add/Edit Neighbor. See: Configure BGP Neighbor Settings
Virtual routing with dynamic VTI.	7.4.0	You can now configure a virtual router with a dynamic VTI for a route-based site-to-site VPN. New/modified screens: **Devices** > **Device Management** > Edit Device > **Routing** > **Virtual Router Properties** > Dynamic VTI interfaces under **Available Interfaces** Platform restrictions: Supported only on native mode standalone or high availability devices. Not supported for container instances or clustered devices. See: About Virtual Routers and Dynamic VTI
Access Control: Threat Detection and Application Identification		

Feature	Min. Threat Defense	Details
Encrypted visibility engine enhancements.	7.4.0 with Snort 3	Encrypted Visibility Engine (EVE) can now: • Block malicious communications in encrypted traffic based on threat score. • Determine client applications based on EVE-detected processes. • Reassemble fragmented Client Hello packets for detection purposes. New/modified screens: Use the access control policy's advanced settings to enable EVE and configure these settings. See: Encrypted Visibility Engine
Exempt specific networks and ports from bypassing or throttling elephant flows.	7.4.0 with Snort 3	You can now exempt specific networks and ports from bypassing or throttling elephant flows. New/modified screens: • When you configure elephant flow detection in the access control policy's advanced settings, if you enable the **Elephant Flow Remediation** option, you can now click **Add Rule** and specify traffic that you want to exempt from bypass or throttling. • When the system detects an elephant flow that is exempted from bypass or throttling, it generates a mid-flow connection event with the reason **Elephant Flow Exempted**. Platform restrictions: Not supported on the Firepower 2100 series. See: Elephant Flow Detection
Improved JavaScript inspection.	7.4.0 with Snort 3	We improved JavaScript inspection, which is done by normalizing the JavaScript and matching rules against the normalized content. See: HTTP Inspect Inspector and Cisco Secure Firewall Management Center Snort 3 Configuration Guide
Access Control: Identity		
Cisco Secure Dynamic Attributes Connector on the management center.	Any	You can now configure the Cisco Secure Dynamic Attributes Connector on the management center. Previously, it was only available as a standalone application. See: Cisco Secure Dynamic Attributes Connector
Event Logging and Analysis		
Configure threat defense devices as NetFlow exporters from the management center web interface.	Any	NetFlow is a Cisco application that provides statistics on packets flows. You can now use the management center web interface to configure threat defense devices as NetFlow exporters. If you have an existing NetFlow FlexConfig and redo your configurations in the web interface, you cannot deploy until you remove the deprecated FlexConfigs. New/modified screens: **Devices** > **Platform Settings** > **Threat Defense Settings Policy** > **NetFlow** See: Configure NetFlow
Health Monitoring		

Feature	Min. Threat Defense	Details
New asp drop metrics.	7.4.0	You can add over 600 new asp (accelerated security path) drop metrics to a new or existing device health dashboard. Make sure you choose the **ASP Drops** metric group. New/modified screens: **System** (⚙) > **Health** > **Monitor** > **Device** See: show asp drop Command Usage
Administration		
Support for IPv6 URLs when checking certificate revocation.	7.4.0	Previously, threat defense supported only IPv4 OCSP URLs. Now, threat defense supports both IPv4 and IPv6 OCSP URLs. See: Certificate Enrollment Object Revocation Options
Store threat defense backup files in a secure remote location.	Any	When you back up a device, the cloud-delivered Firewall Management Center stores the backup files in its secure cloud storage. See: Backup/Restore
Usability, Performance, and Troubleshooting		
Usability enhancements.	Any	You can now: • Manage Smart Licensing for threat defense clusters from **System** (⚙) > **Smart Licenses**. Previously, you had to use the Device Management page. See: Licenses for Clustering • Download a report of Message Center notifications. In the Message Center, click the new **Download Report** icon, next to the **Show Notifications** slider. See: Managing System Messages. • Download a report of all registered devices. On **Devices** > **Device Management**, click the new **Download Device List Report** link, at the top right of the page. See: Download the Managed Device List. • Easily create custom health monitoring dashboards, and easily edit existing dashboards. See: Correlating Device Metrics
Specify the direction of traffic to be captured with packet capture for the Secure Firewall 4200.	7.4.0	On the Secure Firewall 4200, you can use a new **direction** keyword with the **capture** command. New/modified CLI commands: **capture***capture_name***switchinterface***interface_name* [**direction** { **both** | **egress** | **ingress** }] See: Cisco Secure Firewall Threat Defense Command Reference
Management Center REST API		

Feature	Min. Threat Defense	Details
Cloud-delivered Firewall Management Center REST API.	Feature dependent	For information on changes to the management center REST API, see What's New in the API quick start guide.

Table 3: Deprecated Features: Version 20230929

Feature	Deprecated in Threat Defense	Details
Deprecated: NetFlow with FlexConfig.	Any	You can now configure threat defense devices as NetFlow exporters from the management center web interface. If you do this, you cannot deploy until you remove any deprecated FlexConfigs. See: Configure NetFlow
Deprecated: `high unmanaged disk usage` alerts.	7.0.6 7.2.4 7.4.0	The Disk Usage health module no longer alerts with `high unmanaged disk usage`. You may continue to see these alerts until you either deploy health policies to managed devices (stops the display of alerts), or upgrade the devices to Version 7.0.6, 7.2.4, or 7.4 (stops the sending of alerts). For information on the remaining Disk Usage alerts, see Disk Usage and Drain of Events Health Monitor Alerts.

August 3, 2023

Table 4: New Features: August 3, 2023

Feature	Description
Updates to Firewall Migration Tool	Cisco Defense Orchestrator now hosts an updated version of the Firewall Migration Tool. You can now merge multiple contexts in your Secure Firewall ASA devices to a routed-mode instance and migrate them to threat defense devices managed by the cloud-delivered Firewall Management Center. In addition, the migration tool now leverages the virtual routing and forwarding (VRF) functionality to replicate the segregated traffic flow observed in a multi-context ASA environment, which will be part of the new merged configuration. See Migrating Secure Firewall ASA Managed by CDO in *Migrating Firewalls with the Firewall Migration Tool in Cisco Defense Orchestrator* guide for more information.

July 20, 2023

Table 5: New Features: July 20, 2023

Feature	Description
EasyDeploy for Virtual Threat Defense Devices Managed by GCP	You can now create a virtual threat defense device and deploy it to a Google Cloud Platform (GCP) project simultaneously. The EasyDeploy method combines the steps required to create a new virtual device and then associating the device with the cloud environment, streamlining the procedure and minimizing the amount of time required for setup. Note that you **must** have cloud-delivered Firewall Management Center enabled for these onboarding flows. See Deploy a Threat Defense Device to Google Cloud Platform for more information. Minimum threat defense: • 7.0.3 and later 7.0.x versions • 7.2 and later versions

June 8, 2023

Table 6: New Features: June 8, 2023

Feature	Description
EasyDeploy for Secure Firewall Threat Defense with AWS or Azure	You can now create and deploy a Secure Firewall Threat Defense device with either an AWS or Azure environment simultaneously. Onboard the device with CDO and manage the environment in cloud-delivered Firewall Management Center. See Deploy a Threat Defense Device with AWS and Deploy a Threat Defense Device with an Azure VNet respectively for more information. Minimum threat defense: • 7.0.3 and later 7.0.x versions • 7.2 and later versions

May 25, 2023

Table 7: New Features: May 25, 2023

Feature	Description
Threat defense Version 7.3.1 support.	You can now manage threat defense devices running Version 7.3.1.

Feature	Description
Firepower 1010E.	You can now manage the Firepower 1010E, which does not support power over Ethernet (PoE), with cloud-delivered Firewall Management Center. Minimum threat defense: 7.2.3

March 9, 2023

This release introduces stability, hardening, and performance enhancements.

February 16, 2023

This release introduces stability, hardening, and performance enhancements.

January 18, 2023

Table 8: New Features: January 18, 2023

Feature	Description
Remote Access VPN	
Monitor remote access VPN sessions in CDO.	You can now use CDO to monitor RA VPN sessions on threat defense devices managed by the cloud-delivered Firewall Management Center. You can see a a list of active and historical sessions, as well as the details of the device and user associated with each session. Supported threat defense versions: • 7.0.3 and later 7.0.x versions • 7.2 and later versions For more information, see Monitor Remote Access VPN Sessions in the configuration guide.

January 18, 2023