New Features and Functionality

This table includes the new and updated features and functionality included in Version 6.2.0.

Table 1: New Features in Version 6.2.0: Migration Enablers

New Feature	Description	Supported Platforms
Migration Tool	Migrating from Cisco ASA-to-Firepower Threat Defense can be a daunting task for customer is with multiple access control lists (ACLs), Network Address Translation policies, and related configuration objects. The migration tool is specifically designed to assist this migration process. The tool allows you to convert ASA configurations (ACL, NAT and related objects) to Firepower Threat Defense configurations, which you can then import into the Firepower Management Center. The migration tool supports the conversion of up to 600,000 total access rule elements per ASA configuration file.	• 64-bit Firepower Management Center Virtual (VMware and KVM)
REST API	Firepower Version 6.2.0 allows REST clients to create and configure interfaces for Firepower Threat Defense devices through the Firepower Management Center REST API. This feature enables the Firepower Management Center to interact with various Cisco products and services as well as those from third-party vendors. Implementation of these APIs is ideal in the following scenarios: • Large enterprises that want to control policy changes in Firepower through other Cisco systems such as Application Centric Infrastructure (ACI) or through their own proprietary orchestration solutions • Managed security service providers that want to adopt software-defined networking, application-centric infrastructure, and network function virtualization solutions **Note** SDN controllers do not have a way to automatically insert Firepower Threat Defense devices in the traffic path.	• Firepower Management Center • 64-bit Firepower Management Center Virtual

New Feature	Description	Supported Platforms
Packet Tracer and Capture	The Packet Tracer and Capture offers the ability to show all the processing steps that a packet takes, the outcomes, and whether the traffic is blocked or allowed. This allows users to initiate and display output of tracing from the Firepower Management Center. The tracing information includes information from SNORT and preprocessors about verdicts and action taken while processing a packet.	• Firepower Threat Defense

Table 2: New Features for Version 6.2.0: Architecture

New Feature	Description	Supported Platforms
Integrated Routing and Bridging (IRB)	Customers often want to have multiple physical interfaces configured to be part of the same VLAN. The IRB feature meets this demand by allowing users to configure bridges in routed mode, and enables the devices to perform L2 switching between interfaces (including subinterfaces).	• Firepower Threat Defense on ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, or ASA 5555-X • Firepower Threat Defense on Firepower 4100 Series • Firepower Threat Defense on Firepower 9300
Interchassis Clustering	Clustering lets you group multiple FXOS chassis Firepower Threat Defense devices together as a single logical device. A cluster provides all the convenience of a single device (management and integration into a network) while achieving the increased throughput and redundancy of multiple devices. Firepower Version 6.2.0 supports clustering across multiple chassis (interchassis clustering), allowing for higher scalability. You can use the Firepower Management Center to automatically discover all nodes of a cluster.	• Firepower Threat Defense on Firepower 4100 Series • Firepower Threat Defense on Firepower 9300 Appliances

New Feature	Description	Supported Platforms
Policy Change Improvement	Deploying policy changes to a Firepower Threat Defense device can result in restarting the SNORT process and the related loss of some packets. As part of a continuing effort to address this issue, Firepower Version 6.2.0 allows you to configure actions separately for fault conditions, such as SNORT Busy/Overload or SNORT Down. This feature allows you to emphasize either continuity or security by checking a checkbox option in the Firepower Management Center.	Firepower Threat Defense (inline mode only)

Table 3: New Features for Version 6.2.0: Platform/Integration

New Feature	Description	Supported Platforms
Firepower Threat Defense on Microsoft Azure	In Firepower Version 6.2.0, Cisco Firepower Threat Defense Virtual is available in the Microsoft Azure Marketplace. This new platform enables you to secure workloads consistently across the data center and public cloud. Managed centrally by an on-premises Firepower Management Center, Firepower Threat Defense Virtual provides advanced threat protection in the Azure environment without forcing customers to return traffic to the data center.	• Firepower Threat Defense virtual
Firepower Threat Grid API Key Integration	This feature streamlines the process of associating a Threat Grid account with your Firepower Management Center.	• Firepower Management Center • 64-bit Firepower Management Center Virtual

New Feature	Description	Supported Platforms
ISE and SGT tags without Identity	Before Firepower Version 6.2.0, you had to create a realm and identity policy to perform user control based on ISE Security Group Tag (SGT) data, even if you did not want to configure passive authentication using ISE. In Firepower Version 6.2.0, you no longer need to create a realm or identity policy to perform user control based on ISE Security Group Tag (SGT) data.	• Firepower Management Center • Firepower Management Center Virtual • 7000 and 8000 Series • NGIPSv • ASA with FirePOWER Services • Firepower Threat Defense • Firepower Threat Defense Virtual
TS Agent (VDI Identity Support)	To design policies that enforce rules based on the user's identity, you must be able to identify the user correctly. This is a problem in a shared environment, where multiple users are using the same IP address, identifying which user certain traffic applies to becomes difficult. Firepower now provides the ability to better identify individual users in shared environments, such as Citrix's Virtual Desktop Infrastructure (VDI), to accurately enforce user-based policy rules on the firewall. Rather than just associating a user with an IP address, Firepower now associates the user with both the IP address and a port range combination through the use of a new agent deployed on the Windows Terminal Server. The Cisco Terminal Services Agent (TS Agent) intercepts every log in to the terminal server and assigns a port range to every user that logs in. Using RESTful APIs it communicates this information (user, IP address and port range) to the Firepower Management Center, which in turn communicates it to the individual Firepower Threat Defense devices. Now, when **User 1** logs in, Firepower Threat Defense devices not only see the IP address, but also know the port range assigned to the user. Based on the IP address and the port range, Firepower Threat Defense devices properly map the traffic to **User 1**. When **User 2** logs in, a new port range is assigned which enables the Firepower Threat Defense devices to map the appropriate traffic to that user while applying any specific policy rules to that user and their traffic.	• Firepower Management Center • Firepower Management Center Virtual

Table 4: New Features for Version 6.2.0: Firepower Threat Defense and Threat

New Feature	Description	Supported Platforms
Site-to-Site VPN	The site-to-site VPN with public key infrastructure (PKI) support is an addition to the current capability of site-to-site VPN with preshared keys. The Firepower Device Manager (FDM) also allows you to configure site-to-site VPN with pre shared keys.	• Firepower Threat Defense managed by Firepower Management Center • Firepower Threat Defense Virtual
PKI Support for Firepower Management Center	PKI is required to create certificate-based trusted identities for devices establishing site-to-site VPN tunnels. This feature allows you to associate PKI certificate data with devices on the Firepower Management Center.	• Firepower Threat Defense • Firepower Threat Defense Virtual
User-based Indications of Compromise (IOCs)	This feature allows you to generate user-based IOCs from intrusion events or view the associations of users and IOCs. You can also enable and disable eventing of a given IOC per user (against false positives). With this feature, you can correlate IOCs and events to both hosts and users and give them more visibility and alerting options on a per-user basis.	• Firepower Management Center • 64-bit Firepower Management Center Virtual • 7000 and 8000 Series • NGIPSv • ASA with FirePOWER Services • Firepower Threat Defense managed by Firepower Management Center • Firepower Threat Defense Virtual

New Feature	Description	Supported Platforms
URL Lookups	This feature allows you to perform a bulk lookup of URLs (up to 250 URLs at a time) to obtain information such as reputation, category, and matching policy. You can also export the results as a file of comma-separated values. The feature reduces the manual work necessary to determine if your organization is protected against a malicious URL or if you should add a custom rule for a specific IOC. You can use this feature to reduce the number of custom rules, which in turn reduces the chance of performance degradation due to extensive custom rule lists.	• Firepower Management Center Virtual • 64-bit Firepower Management Center Virtual

New Feature	Description	Supported Platforms

FlexConfig	The FlexConfig feature allows you use the Firepower Management Center to deploy ASA CLI template-based functionality to Firepower Threat Defense devices. This feature allows you to enable some of the most valuable ASA functions that are not currently available on Firepower Threat Defense devices. This functionality is structured as templates and objects that work together in a policy. The default templates are officially supported by Cisco TAC.
	
	The targeted features unlocked by FlexConfig potentially include:
	• Non-Inspection Templates:
	  • Routing (EIGRP, PBR, and IS-IS)
	  • Netflow (NSEL) export
	  • MPF connection limits, timeouts (including DCD), and Normalizer settings
	  • Platform sysopt commands
	  • Proxy ARP Neighbor Discovery (**sysopt noproxyarp** *interface*)
	  • IPv6 Prefix Delegation
	  • IPV6
	  • WCCP
	  • VXLAN
	• Application Layer Inspection Templates:
	  • ALGs default configuration
	  • GTPv1/v2 support
	  • Diameter inspection
	  • LISP inspection
	  • SCTP support and inspection
	  • SIP
	  • SS7 inspection
		• Firepower Threat Defense
		• Firepower Threat Defense Virtual

• Changed Functionality, on page 8

Changed Functionality

The following are a few of the changes in Version 6.2.0:

- Version 6.2.0 introduces new functionality related to latency-based performance settings in access control policies. In Version 6.2.0 and later, by default, new access control policies obtain latency-based performance settings from the latest intrusion rule update. You can choose to overwrite these settings with custom settings. For more information, see "Latency-Based Performance Setting Configuration" in the Firepower Management Center Configuration Guide.

  When you update to Version 6.2.0, the system determines whether existing access control policies use default or custom latency-based performance settings and continues as appropriate under the following conditions:

  - If existing policies use default settings, the system sets the **Apply Settings From** option to **Installed Rule Update**. When you deploy the access control policy, the system obtains the latency-based performance settings from the latest intrusion rule update and uses them in that policy.
  - If existing policies do not use default settings, the system sets the **Apply Settings From** option to **Custom** and retains the pre-upgrade settings.

- Version 6.2.0 does not support international characters in URLS for URL objects or inline values in access control policy rules. (CSCux24338)
- Private keys are no longer mandatory when importing certificates. (CSCvb13045)
- Generated troubleshoot now includes captive portal information. (CSCvb26174)
- If you create an access control policy or NAT policy referencing an object or object group that contains an invalid characters in the name, the system now generates an **Unsupported object names are used in the policy for devices** error message and does not save the policy. (CSCvb29308)
- The ASA-to-FTD migration process failed if the ASA configuration file included an access list entry (ACE) with an interface object configured as source network, destination network, or both. Now, the migration tool converts this ASA configuration as a disabled FTD rule. (CSCvb49745)
- Upgrading to Version 6.2.0 from Version 6.1.0.3 or a subsequent 6.1.0.x patch removes the Intelligent Application Bypass (IAB) **All applications including unidentified application** option from the user interface. You must install the Version 6.2.0.1 patch or a subsequent 6.2.0.x patch to restore this option.

  If this option is enabled when you upgrade, and your access control policy does not contain IAB bypassable application and filter configurations, the user interface has the following unexpected behaviors:

  - IAB is enabled, but the **All applications including unidentified applications** option is no longer present.
  - The IAB configuration page displays **1 Applications/Filters**, incorrectly indicating that you have configured one application or filter.
  - The Selected Applications and Filters window in the applications and filters editor displays one of the following, depending on which appliance you are using: *deleted* (Firepower Management Center, ASA with FirePOWER Services and *Any Application* (ASA FirePOWER module managed by ASDM).

We recommend deleting *deleted* or *Any Application* from the Selected Applications and Filters window. Installing Version 6.2.0.1 or a subsequent 6.2.0.x version restores the missing option.