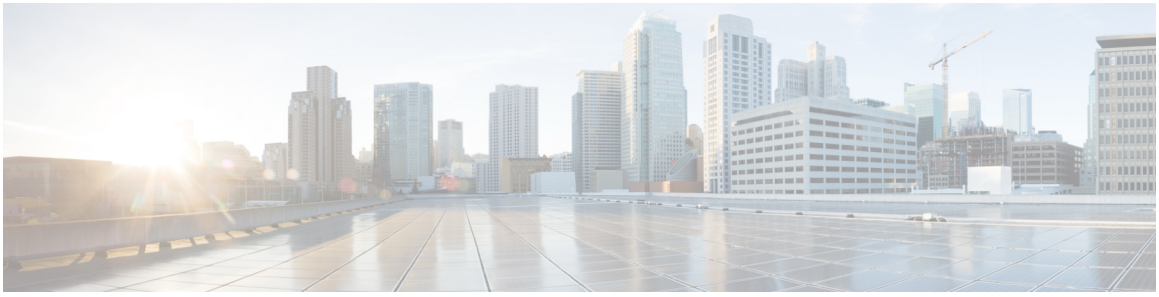
Cisco Secure Firewall ASA to Threat Defense Feature Mapping

First Published: 2023-02-21

Last Modified: 2023-02-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

About This Guide

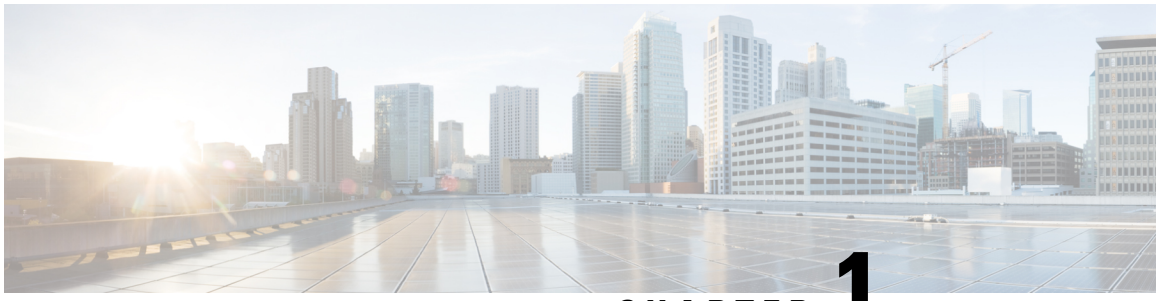
This document lists commonly used ASA features and the equivalent capabilities of the threat defense. For each ASA feature (that correlates to an ASA configuration guide chapter or section), we list the equivalent feature for the threat defense with a UI path for where to configure the feature in the Secure Firewall Management Center or Cisco Defense Orchestrator (CDO) cloud-delivered Firewall Management Center. We also provide management center documentation links, so you can read more about the feature implementation. For each feature, we provide known limitations or differences if present.

The management center is a multi-device manager that lets you apply security policies to multiple devices.

The threat defense includes many useful security features that are not present in the ASA, as well as management features provided by the management center that are not available in ASA management methods. This guide does not list threat defense features that are not available in ASA.

Note The management center supports some ASA features using a CLI tool called FlexConfig.

About This Guide



CHAPTER 1

General Operations Features

Getting Started

Table 1: Getting Started

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
ASA CLI for Configuration	**Limited Threat Defense CLI for Configuration, Full GUI Configuration** See: Getting Started Guides (console access), Command Reference, Device Configuration Guide	The threat defense CLI includes *limited* commands for initial configuration only and some special operations. Configuration needs to be performed in the management center, which has limited device configuration discovery.
ASA CLI for Monitoring	**Threat Defense CLI for Monitoring** UI path: **System** (⚙) > **Health** > **Monitor> Advanced Troubleshooting** > **Threat Defense CLI** See: Getting Started Guides (console access), Command Reference, Using the Threat Defense CLI from the Web Interface	You can use the same **show** commands that are available on the ASA. You can access the CLI at the console, using SSH, or you can use the CLI web tool.
Initial Configuration	**Initial Configuration** See: Getting Started Guides (console access)	Use the CLI or the device manager to set network settings and register with the management center.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Configuration Changes	**Configuration Deployment** UI path: **Deploy** See: Configuration Deployment	You need to deploy any changes from the management center.
Smart Licenses	**Smart Licenses** UI path: **System** > **Licenses** > **Smart Licenses** See: Licenses How To: Register the Management Center with Cisco Smart Account	Licenses are consumed and assigned by the management center.
Transparent or Routed Firewall Mode	**Transparent or Routed Firewall Mode** See: Transparent or Routed Firewall Mode	Like the ASA, you need to change the firewall mode using the CLI before you register the device to the management center.

High Availability and Scalability

Table 2: High Availability and Scalability

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Multiple Context Mode	**Multi-instance Mode** or **Virtual Routers** UI path: • Firepower 4100/9300 Multi-Instance: **Logical Devices** > **Add** (chassis manager) • Virtual Routers: **Devices** > **Device Management** > **Edit** > **Routing** > **Manage Virtual Routers** See: Using Multi-Instance Capability on the Firepower 4100/9300, Virtual Routers How To: Create a Virtual Router, Assign Interfaces to Virtual Routers, Configure NAT for a Virtual Router, Provide Internet Access with Overlapping Address Spaces, Configure Routing Policy	In many cases, your customers may only need separate routing tables rather than full separation. In this case, you can use virtual routers. For complete configuration separation, use mutli-instance mode on supported platforms. This implementation is different from the ASA multiple context mode, but the functionality is similar.
Active/Standby Failover	**High Availability** UI path: **Devices** > **Device Management** > **Add** > **High Availability** See: High Availability How To: Create a high availability (HA) pair	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Clustering	**Clustering** UI path: • Firepower 4100/9300: **Logical Devices** > **Add** (chassis manager) **Devices** > **Device Management** > **Add** > **Device** (management center) • Threat Defense Virtual for public cloud: **Devices** > **Device Management** > **Add** > **Device** • Secure Firewall 3100: **Devices** > **Device Management** > **Add** > **Cluster** • Threat Defense Virtual for private cloud: **Devices** > **Device Management** > **Add** > **Cluster** See: Deploy a Cluster for Threat Defense on the Secure Firewall 3100, Deploy a Cluster for Threat Defense on the Firepower 4100/9300, Deploy a Cluster for Threat Defense Virtual in a Public Cloud, Deploy a Cluster for Threat Defense Virtual in a Private Cloud How To: Create a Cluster, Modify an Existing Cluster, Add Nodes to an Existing Cluster, Remove a Data Node from a Cluster, Break a Cluster, Delete a Cluster, Break a Node from Clustering, Delete a Data Node from Clustering	Inter-site clustering and distributed site-to-site VPN is not supported.

Interfaces

For the threat defense, interfaces are configured per device. However, for most features, you assign interfaces to security zones and then apply policies to *zones*, not directly to interfaces. Zones, like the security policy itself, are configured as objects that can be shared across multiple devices.

Note The threat defense supports regular firewall interfaces like the ASA, but it also supports a different type of IPS-only interface.

Table 3: Interfaces

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Management Interface	**Management Interface** UI path: **Devices** > **Device Management** > **Edit** > **Devices** > **Management** See: Complete the Threat Defense Initial Configuration	The ASA has a management-only interface that has its own routing table, but operates for the most part like data interfaces. The threat defense has a Management interface separate from the data interfaces. It is used to set up and register the device to the management center. It uses its own IP address and static routing.
Physical Interfaces	**Physical Interfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Interface Overview How To: Configure Interface Settings	
Firepower 1010 Switch Ports	**Firepower 1010 Switch Ports** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure Firepower 1010 Switch Ports	
EtherChannels	**EtherChannels** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure EtherChannel Interfaces	
Loopback Interfaces	**Loopback Interfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure Loopback Interfaces	
VLAN Subinterfaces	**VLAN Subinterfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure VLAN Subinterfaces and 802.1Q Trunking	
VXLAN Interfaces	**VXLAN Interfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure VXLAN Interfaces	
Routed and Transparent Mode Interfaces	**Routed and Transparent Mode Interfaces** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure Routed and Transparent Mode Interfaces	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Advanced Interface Configuration	**Advanced Interface Configuration** UI path: **Devices** > **Device Management** > **Edit** > **Interfaces** See: Configure Advanced Interface Settings	
Traffic Zones	**ECMP** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **ECMP** See: ECMP	

Basic Settings

Table 4: Basic Settings

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
DNS Server	**DNS Server** UI path: • **Objects** > **Object Management** > **DNS Server Group** • **Devices** > **Platform Settings** > **DNS** See: DNS Server Group, Configure DNS, FlexConfig Policies	DNS servers are part of platform settings that can be applied to multiple devices. **Note** The DNS server for the threat defense dedicated Management interface is configured at the CLI using the **configure network dns servers** and **configure network dns searchdomains** commands
ISA 3000 Hardware Bypass	**ISA 3000 Hardware Bypass** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: How to Configure Automatic Hardware Bypass for Power Failure (ISA 3000)	This feature can be configured using FlexConfig.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
ISA 3000 Precision Time Protocol	**ISA 3000 Precision Time Protocol** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: How to Configure Precision Time Protocol (ISA 3000)	This feature can be configured using FlexConfig.
ISA 3000 Dual Power Supply	**ISA 3000 Precision Dual Power Supply** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: FlexConfig Policies	This feature can be configured using FlexConfig.
DHCP Server	**DHCP Server** UI path: • IPv4: **Devices** > **Device Management** > **Edit** > **DHCP** > **DHCP Server** • IPv6: **Devices** > **Device Management** > **Edit** > **Interfaces** > **IPv6** > **DHCP** See: Configure the DHCPv4 Server, Configure the DHCPv6 Stateless Server	
DHCP Relay Agent	**DHCP Relay Agent** UI path: **Devices** > **Device Management** > **Edit** > **DHCP** > **DHCP Relay** See: Configure the DHCP Relay Agent	
DDNS	**DDNS** UI path: **Devices** > **Device Management** > **Edit** > **DHCP** > **DDNS** See: Configure Dynamic DNS	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Digital Certificates	**Certificates, PKI** UI path: • **Objects** > **Object Management** > **PKI** • **Devices** > **Certificates** See: PKI, Certificates How To: • Certificate Authentication for Remote Access (RA) VPN—Creating a Certificate Map for Certificate Authentication in RA VPN, Associating a Certificate Map to a Connection Profile • Create and Install an Identity Certificate on Device for Remote Access VPN Configuration—PKCS12 Cert Enrollment Object, Manual Cert Enrollment Object, Self-signed Cert Enrollment Object, SCEP Cert Enrollment Object, Install Manual Certificate, Install PKCS12, SCEP, or Self-Signed Certificate, Configure Remote Access VPN • Configuring VPN—Renew a certificate using manual re-enrollment, Renew a certificate using Self-signed, SCEP, or EST enrollment	Create reusable certificate objects and then apply them per device.
ARP Inspection and the MAC Address Table	**ARP Inspection and the MAC Address Table** UI path: • **Devices** > **Device Management** > **Edit** > **Interfaces** > **Advanced** > **ARP and MAC** • **Devices** > **Platform Settings** > **ARP Inspection** See: Advanced Interface Settings, Configure ARP Inspection	ARP inspection is part of platform settings that can be applied to multiple devices.
WCCP	**WCCP** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: FlexConfig Policies	This feature can be configured using FlexConfig.

Routing

Routing is configured per-device.

Table 5: Routing

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Data and Management Routing Tables	**Data and Management Routing Tables** See: Reference for Routing How To: Configure Routing Policy	The ASA and the threat defense have different defaults for which traffic defaults to the management routing table vs. the data routing table. **Note** The dedicated Management interface has a separate Linux routing table that you can configure at the CLI.
Static and Default Routes	**Static and Default Routes** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **Static Route** See: Static and Default Routes How To: Configure a Static Route for VTI	
Policy Based Routing	**Policy Based Routing** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **Policy Based Routing** See: Policy Based Routing	
Route Maps	**Route Maps** UI path: **Objects** > **Object Management** > **Route Map** See: Route Map	
Bidirectional Forwarding Detection Routing	**Bidirectional Forwarding Detection Routing** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **BFD** See: Bidirectional Forwarding Detection Routing	
BGP	**BGP** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **BGP** See: BGP How To: Configure BGP routing for VTI	
OSPF	**OSPF** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **OSPF** See: OSPF	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
ISIS	**ISIS** UI path: • **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** • **Devices** > **FlexConfig** See: FlexConfig Policies	This feature can be configured using FlexConfig.
EIGRP	**EIGRP** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **EIGRP** See: EIGRP	
Multicast Routing	**Multicast Routing** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **Multicast Routing** See: Multicast	
RIP	**RIP** UI path: **Devices** > **Device Management** > **Edit** > **Routing** > **RIP** See: RIP	

AAA Servers

On the threat defense, AAA servers can be used for VPN access. For AAA servers and the local database for management access, see System Administration, on page 10.

Table 6: AAA Servers

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
RADIUS for VPN	**RADIUS for VPN** UI path: **Objects** > **Object Management** > **AAA Server** > **RADIUS Server Group** See: Add a RADIUS Server Group	
LDAP for VPN	**LDAP for VPN** UI path: **Integration** > **Other Integrations** > **Realms** See: Create an Active Directory Realm and Realm Directory How To: Configure LDAP attribute map for remote access VPN	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
SAML Single Sign-On for VPN	**SAML Single Sign-On for VPN** UI path: **Objects** > **Object Management** > **AAA Server** > **Single Sign-On Server** See: Add a Single Sign-on Server How To: Add SAML Single Sign-On server object	

System Administration

Table 7: System Administration

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Local Database for Device Management	**Internal User (management center)** UI path: **System** (⚙) > **Users** See: Add an Internal User **Users (threat defense)** See: Add an Internal User at the CLI	The management center and threat defense maintain separate user databases. You can configure management center users for web access and CLI access. To add threat defense users, you need to use the CLI. The threat defense users have SSH access.
RADIUS for Device Management	**RADIUS (management center)** UI path: **System** (⚙) > **Users** > **External Authentication** See: Add a RADIUS External Authentication Object for Management Center **RADIUS (threat defense)** UI path: • **System** (⚙) > **Users** > **External Authentication** • **Devices** > **Platform Settings** > **Edit** > **External Authentication** See: Configure External Authentication for SSH	For threat defense users, you enable the RADIUS authentication object as part of the platform settings.

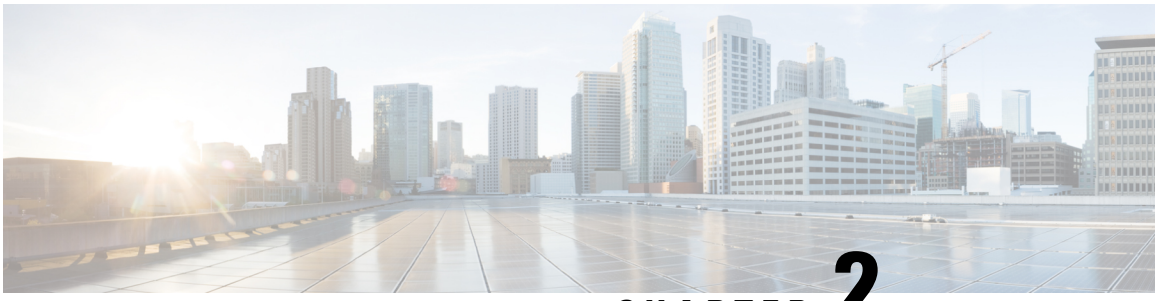
ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
LDAP for Device Management	**LDAP (management center)** UI path: **System** (⚙) > **Users** > **External Authentication** See: Add an LDAP External Authentication Object for Management Center **LDAP (threat defense)** UI path: • **System** (⚙) > **Users** > **External Authentication** • **Devices** > **Platform Settings** > **Edit** > **External Authentication** See: Configure External Authentication for SSH	For threat defense users, you enable the LDAP authentication object as part of the platform settings.
SSH	**Access List (management center)** UI path: **System** (⚙) > **Configuration** > **Access List** See: Access List **Secure Shell (threat defense)** UI path: **Devices** > **Platform Settings** > **Secure Shell** See: Configure Secure Shell	For the management center, SSH is enabled by default. You can limit access in the system configuration. For the threat defense, SSH is enabled by default for the dedicated Management interface. You can limit access using the **configure ssh-access-list** command. For SSH to data interfaces, enable it in platform settings. Platform settings can be applied to multiple devices.
HTTPS	**Access List** UI path: **System** (⚙) > **Configuration** > **Access List** See: Access List	You can control HTTPS access to the management center in the system configuration. The threat defense does not support HTTPS access when managed by the management center.
Upgrade the Software	**Upgrade the Software** UI path: **System** (⚙) > **Updates** See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center How To: Upgrade Secure Firewall Threat Defense	Perform all upgrades using the management center.
Downgrading	**Reverting** UI path: **Devices** > **Device Management** > **More** > **Revert Upgrade** See: Revert the Upgrade	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Backup and Restore	**Backup and Restore** UI path: **System** (⚙) > **Tools** > **Backup/Restore** See: Backup and Restore	
Hot Swap an SSD (Secure Firewall 3100)	**Hot Swap an SSD (Secure Firewall 3100)** See: Hot Swap an SSD on the Secure Firewall 3100	Use the CLI to perform the hot swap.
Debugging Messages	**Debugging Messages** See: debug command in the Command Reference	
Packet Capture	**Packet Capture** UI path: **Devices** > **Packet Capture** See: Use the Capture Trace How To: Collect packet capture for threat defense device	
Packet Tracer	**Packet Tracer** UI path: **Devices** > **Packet Tracer** See: Use the Packet Tracer How To: Collect packet trace to troubleshoot threat defense device	
Ping	**Ping** UI path: **System** (⚙) > **Health** > **Monitor> Advanced Troubleshooting** > **Threat Defense CLI** See: ping command in the Command Reference	
Traceroute	**Traceroute** UI path: **System** (⚙) > **Health** > **Monitor> Advanced Troubleshooting** > **Threat Defense CLI** See: traceroute command in the Command Reference	
Connection monitoring	**Connection monitoring** UI path: **System** (⚙) > **Health** > **Monitor> Advanced Troubleshooting** > **Threat Defense CLI** See: show conn command in the Command Reference	
show asp drop	**ASP Drop** UI path: **System** (⚙) > **Health** > **Policy** See: Health Modules	

Monitoring

Table 8: Monitoring

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Logging	**Syslog** UI path: • ASA-style syslogs: **Devices** > **Platform Settings** > **Syslog** • Alerts for file and malware, connection, Security Intelligence, and intrusion events: **Policies** > **Access Control** > **Edit** > **Logging** • Alerts for access control rules, intrusion rules, and other advanced services: **Policies** > **Actions** > **Alerts** See: Configure Syslog, About Sending Syslog Messages for Security Events, Creating a Syslog Alert Response	The threat defense supports the same syslog capability as the ASA. But it also supports logging and alerts generated by the next-generation IPS support that only the threat defense supports. Syslog settings are part of platform settings that can be applied to multiple devices.
SNMP	**SNMP** UI path: **Devices** > **Platform Settings** > **SNMP** See: Configure SNMP	SNMP settings are part of platform settings that can be applied to multiple devices.
Cisco Success Network	**Cisco Success Network** UI path: **Integration** > **SecureX** > **Cisco Cloud Support** See: Configure Cisco Success Network Enrollment	
Alarms for the ISA 3000	**Alarms for the ISA 3000** UI path: **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object** See: Alarms for the Cisco ISA 3000	This feature can be configured using FlexConfig.



CHAPTER 2

Firewall Features

The following topics explain how to configure ASA firewall features, or their equivalents, in the Secure Firewall Threat Defense using the Secure Firewall Management Center or cloud-delivered Firewall Management Center. The features are loosely organized based on how they are documented in the *CLI/ASDM Book 2: Cisco Secure Firewall ASA Series Firewall CLI/ASDM Configuration Guide* documents.

Access Control

When you use ASA CLI or ADSM to configure an ASA, you are always configuring a single device at a time.

In comparison, the access control policy in Secure Firewall Management Center is always a shared policy. You create the policy, then you assign it to one or more devices.

Typically, you would create an access control policy for multiple devices. For example, you might assign the same policy to all remote location firewalls (which connect remote sites to the main corporate network). Then, you might have a different policy for the firewalls that reside in your core data center. You can, of course, create separate policies for each device, but that is not an efficient use of a multiple device manager.

Whether a given acess control rule will apply to a device is controled by the interfaces specified in the rule:

- If you specify no interfaces, the rule applies to all devices that are assigned the policy.
- If you specify security zones, which are objects that are a list of specific device interfaces, the rule applies, and is deployed, to only those devices that have interfaces in the specified zones. Security zones do not simply include interface names, but "interface on device" pairs. For example, "inside on device1" could be in a zone that does not contain "inside on device2."

The following table shows the main access control features for the ASA, and where you would configure them, or their equivalents, on a Secure Firewall Threat Defense device.

Table 9: Access Control Features

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Objects for Access Control.	**Objects** UI path: **Objects** > **Object Management**. See: Object Management. How To: Configure Dynamic Objects	You also can create network and port (service) objects when editing the access control policy. Also supported are security group tags and time ranges. Not supported (or needed) are network-service and local user groups. Additional objects you can use in access control rules: application filters, geolocation, interface security zones, URL, and VLAN tag. These objects apply to features not available on the ASA.
Access Control Lists (ACL) for non-access control groups/rules.	**Access Control Lists (ACL)** UI path: Standard and Extended ACLs: **Objects** > **Object Management**. Ethertype ACLs: **Devices** > **FlexConfig**. See: Object Management and FlexConfig Policies. How To: • Configuring Traffic Filtering for Remote Access (RA) VPN Connections—Creating an Extended Access List for Filtering Traffic on an RA VPN Connection, Adding an Extended Access List to a Group Policy for Filtering Traffic on an RA VPN Connection	You create objects for standard or extended ACLs, then use those objects when configuring routing or other features that require ACLs.
Access Control Rules—basic (network, port, protocol, ICMP).	**Access Control Rules** UI path: **Policies** > **Access Control**. See: Access Control Rules. How To: • Set up your device—Add an Access Control Rule–A Feature Walkthrough, Create an access control policy • Configure a VTI tunnel—Configure an access control rule to allow encrypted traffic over VTI • The New Access Control Policy UI–A Feature Walkthrough—Accessing the New AC Policy UI, The New AC Policy UI–Rules Table, The New AC Policy UI–Rule Creation, The New AC Policy UI–Rule Editing	The access control policy supports basic 5-tuple and VLAN access control rules. In addition, you can use geolocation objects to target IP addresses associated with particular geographical locations. You can also use prefilter policies to control tunneled traffic (such as GRE) and other 5-tuple traffic. Prefilter rules are processed before access control rules and are not available on the ASA. See **Policies** > **Prefilter**.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Access Control Rules—user-based control	**Access Control Rules** UI path: To configure the rules for obtaining user name and group mappings, go to **Policies** > **Identity**. You can then select user names and groups in access control rules; **Policies** > **Access Control**. See: Access Control Rules and User Identity Policies. How To: Configure an Access Control Policy Rule for a Dynamic Object	There are more options for obtaining user/group membership compared to the ASA.
Access Control Rules—security group and Trustsec	**Access Control Rules** UI path: To set up Identity Services Engine, go to **Integration** > **Other Integrations** > **Identity Sources**. You can then select security group tags in access control rules; **Policies** > **Access Control**. See: Access Control Rules and User Control with ISE/ISE-PIC.	You can also use Identity Services Engine to gather username/user group information for user-based control.
(Not available on ASA.) Access Control Rules—layer 7 application control.	**Access Control Rules** UI path: **Policies** > **Access Control**. See: Access Control Rules.	You can write access control rules for applications that otherwise use the same protocol and port, enabling you to differentiate between different types of HTTP/HTTPS traffic, for example. Application filtering can help you apply more granular control than what is available on the ASA.
Access Control Rules—URL Filering.	**Access Control Rules** UI path: **Policies** > **Access Control**. See: URL Filtering.	Requires a URL filtering license for controlling access based on URL category and reputation. You can also use the Security Intelligence policy defined within an access control policy to do early filtering based on URL or network object. The DNS policy can do the same thing for DNS lookup requests.
ICMP access rules for to-the-device traffic (**icmp permit/deny** and **ipv6 icmp permit/deny** commands.)	**ICMP access rules** UI path: **Devices** > **Platform Settings**, **ICMP Access** page. . See: Platform Settings.	Like the access control policy, the platform settings policy is shared and you can apply the policy to multiple devices.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Cisco Umbrella	**Cisco Umbrella** UI path: **Integration** > **Other Integrations** > **Cloud Services** **Policies** > **DNS** **Devices** > **VPN: Site-to-Site** > **SASE Topology**. See: DNS Policies and Site-to-Site VPNs for Secure Firewall Threat Defense.	You can create Umbrella DNS policies and Umbrella SASE VPN topologies.

Network Address Translation

Like the access control policy, the Network Address Translation (NAT) policy is shared. You create the NAT policy, then you assign it to one or more devices. The FlexConfig policy is also shared.

Whether a given NAT rule is deployed to a device depends on whether you contrain the rule by interfaces, or apply the rule to all interfaces.

- If you specify no interfaces, the rule applies to all devices that are assigned the policy.
- If you specify interface objects, the rule applies, and is deployed, to only those devices that have interfaces in the specified objects.

The following table shows the main network address translation features for the ASA, and where you would configure them, or their equivalents, on a Secure Firewall Threat Defense device.

Table 10: Network Address Translation Features

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Network Address Translation (NAT)—dynamic NAT/PAT, static NAT, identity NAT.	**Network Address Translation (NAT)** UI path: **Devices** > **NAT**. See: Network Address Translation (NAT). How To: • Set up your device—Create a NAT Policy–A Feature Walkthrough • Configure Virtual Routing—Provide Internet Access with Overlapping Address Spaces, Configure NAT for a Virtual Router	You can configure both object and twice NAT. However, they are called auto NAT and manual NAT in Secure Firewall Threat Defense.
Port Address Translation (PAT) with port block allocation.	**Port Address Translation (PAT) with port block allocation**. UI path: To configure the global PAT port block allocation settings (the **xlate block-allocation** command), use **Devices** > **FlexConfig**. Then you can configure the PAT rules using **Devices** > **NAT** See: Network Address Translation (NAT) and FlexConfig Policies.	This feature is used for carrier-grade or large scale PAT.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Per-Session PAT or Multi-Session PAT (the **xlate per-session** command).	**Per-Session PAT or Multi-Session PAT** UI path: **Devices** > **FlexConfig**. See: FlexConfig Policies.	The Secure Firewall Threat Defense default configuration includes the same pre-defined per-session rules as the ASA. Configuration is necessary only if you want non-default behavior.
Mapping Address and Port (MAP)	**Mapping Address and Port (MAP)** UI path: **Devices** > **FlexConfig**. See: FlexConfig Policies.	Mapping Address and Port (MAP) is a carrier-grade feature for translating IPv4 addresses to IPv6.

Application Inspection

Snort is the main inspection engine on a Secure Firewall Threat Defense device. However, ASA inspections continue to run, and they are applied prior to Snort inspection.

Because Snort does a lot of HTTP inspection, the ASA HTTP inspection engine is not supported at all, and you cannot configure it.

Many ASA inspection engines are enabled by default with default settings. In the cases where the ASA inspection engine supports additional configuration, you must use FlexConfig (a shared policy) to configure the settings. If you use the same settings for more than one device, you can create a single FlexConfig policy for your inspection setttings and apply it to all applicable devices.

If you simply need to turn an inspection off (or on), you can use the **configure inspection** command in the device CLI for each device as an alternative to FlexConfig. However, not all possible protocol inspections are available on the command.

The following table lists the various ASA inspection engines, and identifies which are enabled by default on a Secure Firewall Threat Defense device.

Table 11: Application Inspection Features

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Inspection of Basic Internet Protocols	**Inspection** UI path: **Devices** > **FlexConfig**. See: FlexConfig Policies.	Following are the supported inspections. Bold text indicates the inspection is enabled in the default configuration. • DCERPC • **DNS** • **FTP** • **ICMP** • **ICMP Error** • ILS • **IP Options** • IPsec Pass Through • IPv6 • Lisp • **NetBIOS** • PPTP • **RSH** • SMTP/ESMTP • **SNMP** • **SQL*Net** • **Sun RPC** • **TFTP** • WAAS • XDMCP • VXLAN Not supported (done by Snort): HTTP, IM (Instant Messaging), .

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Inspection of Voice and Video Protocols	**Inspection** UI path: **Devices** > **FlexConfig**. See: FlexConfig Policies.	Following are the supported inspections. Bold text indicates the inspection is enabled in the default configuration. • CTIQBE • **H.323 H.225** • **H.323 RAS** • MGCP • **RTSP** • **SIP** • **Skinny** • STUN
Inspection for Mobile Networks.	**Inspection** UI path: **Devices** > **FlexConfig**. See: FlexConfig Policies.	Following are the supported inspections. These inspections require the Carrier license. None of them are enabled by default. • Diameter • GTP/GPRS • M3UA • SCTP • RADIUS Accounting (this inspection does not require the Carrier license)

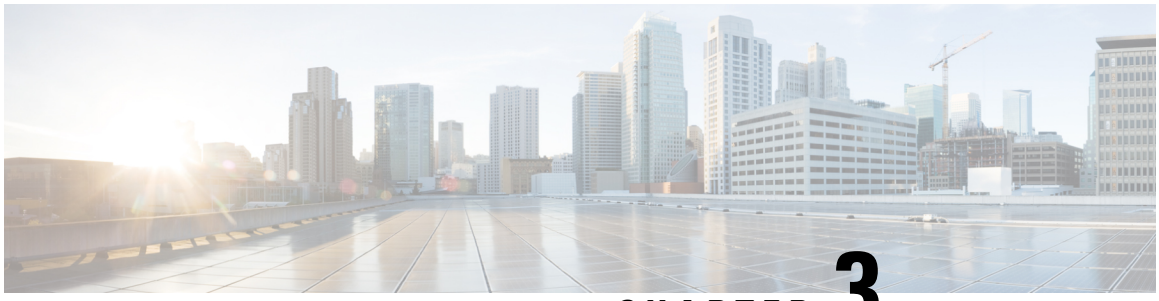
Service Policy, Connection Settings, Threat Detection

The following table lists some loosely-related features that control some aspects of connections that go through the device. Most of these settings have defaults that work in most cases.

Table 12: Service Policy, Connection Settings, Threat Detection Features

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Global Timeouts	**Global Timeouts** UI path: **Devices** > **Platform Settings**, **Timeouts** page. See: Platform Settings.	Platform settings is a shared policy. These setttings are applied to each device assigned the policy.

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Service Policy for connection settings	**Threat Defense Service Policy** UI path: **Policies** > **Access Control**, then while editing a policy, find **Threat Defense Service Policy** under the **Advanced Settings**. See: Service Policies.	These settings include **TCP State Bypass**, **TCP Sequence Randomization**, **TCP Intercept**, **Dead Connection Detection (DCD)**, **TCP Normalization**, and general connection limits and timeouts per traffic class. The Threat Defense Service Policy is defined as part of the access control policy, which is a shared policy you assign to one or more device. Any rules that you constrain to specific interfaces are configured only on those devices that include the interface. Global rules are applied to every device assigned to the access control policy.
Quality of Service (QoS)	**Quality of Service (QoS)** UI path: **Devices** > **QoS**. See: Quality of Service.	The QoS policy is shared, but each rule in the policy must specify one or more interface. A rule is configured on a device only if the rule includes an interface on the device.
Threat Detection (the **threat-detection** command).	**Threat Detection** UI path: **Policies** > **Access Control**, then while editing a policy, find **Threat Detection** under the **Advanced Settings**. See: Threat Detection.	The Secure Firewall Threat Defense feature is not an exact overlap with the ASA feature, but includes new abilities. You can also use FlexConfig to deploy the ASA command versions.



CHAPTER 3

Virtual Private Network Features

This chapter provides high-level information to configure the ASA Virtual Private Network features in Secure Firewall Threat Defense using Secure Firewall Management Center.

Site-to-Site VPN

Table 13: Site-to-Site VPN

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
LAN-to-LAN IPsec	**Policy-based VPN** UI path: **Devices** > **Site To Site** > **Policy Based (Crypto Map)**. See: Configure a Policy-based Site-to-Site VPN. How-To: Configure a Policy-based Site-to-Site VPN, Customize IKE Options for an Existing Site-to-Site VPN Deployment, Customize IPsec Options for an Existing Site-to-Site VPN Deployment, Customize Advanced Settings for an Existing Site-to-Site VPN Deployment	The management centerprovides a single wizard to configure VPN on the peers.
Virtual Tunnel Interface (VTI)	**Route-based VPN** UI path: **Devices** > **Site To Site** > **Route Based (VTI)**. See: Create a Route-based Site-to-Site VPN. How-To: Create a route-based VPN (VTI), Configure a Static Route for VTI, Configure BGP routing for VTI, Configure an access control rule to allow encrypted traffic over VTI	Creating a VPN between a hub with a dynamic VTI and spokes with static VTIs is much easier in management center using the wizard. There is no wizard in ASDM.
Umbrella SASE	**Deploy a SASE Tunnel on Umbrella** UI path: **Devices** > **VPN** > **Site To Site** > **+SASE Topology**. See: Deploy a SASE Tunnel on Umbrella.	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Monitor Site-to-Site VPN	**Monitor the Site-to-Site VPN** UI path: **Overview** > **Dashboards** > **Site to Site VPN**. See: Monitor the Site-to-Site VPN.	

Remote Access VPN

Table 14: Remote Access VPN

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Remote Access IPsec (IKE v2) VPN	**Remote Access VPN Policy** UI path: **Devices** > **VPN** > **Remote Access** > **Policy Assignment** > **VPN Protocols** > **IPsec-IKEv2**. See: Configuring a Remote Access VPN Connection. How-To: • Configuring Traffic Filtering for Remote Access (RA) VPN Connections—Creating an Extended Access List for Filtering Traffic on an RA VPN Connection, Adding an Extended Access List to a Group Policy for Filtering Traffic on an RA VPN Connection • Certificate Authentication for Remote Access (RA) VPN—Creating a Certificate Map for Certificate Authentication in RA VPN, Associating a Certificate Map to a Connection Profile • Create and Install an Identity Certificate on Device for Remote Access VPN Configuration—PKCS12 Cert Enrollment Object, Manual Cert Enrollment Object, Self-signed Cert Enrollment Object, SCEP Cert Enrollment Object, Install Manual Certificate, Install PKCS12, SCEP, or Self-Signed Certificate, Configure Remote Access VPN • Configuring VPN—Renew a certificate using manual re-enrollment, Renew a certificate using Self-signed, SCEP, or EST enrollment, Configure LDAP attribute map for remote access VPN, Add SAML Single Sign-On server object, Configure Dynamic Access Policy for Remote Access VPN	Configuring a connection profile and a group policy object remains the same in the management center as in the ASA. You must create a realm object for creating local users and Active Directory/LDAP. Realms are connections between the management center and the user accounts on the servers.
Remote Access SSL VPN	**Remote Access VPN Policy** UI path: **Devices** > **VPN** > **Remote Access** > **Policy Assignment** > **VPN Protocols** > **SSL**. See: Configuring a Remote Access VPN Connection. How-To: Configure Remote Access VPN.	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
VPN Load Balancing	**VPN Load Balancing** UI path: Edit the remote access VPN policy. **Advanced** > **Load Balancing**. See: Configuring VPN Load Balancing.	VPN load balancing is a mechanism for equitably distributing remote-access VPN traffic among the devices in a VPN load-balancing group.
Dynamic Access Policies	**Dynamic Access Policies** UI path: **Devices** > **Dynamic Access Policy**. See: Dynamic Access Policies. How-To: Configure Dynamic Access Policy for Remote Access VPN.	Enables you to configure authorization that addresses the dynamics of VPN environments.
Monitor VPN	**Remote Access VPN Dashboard** UI path: **Overview** > **Dashboards** > **Remote Access VPN** See: Remote Access VPN Monitoring.	
Secure Client Hostscan	**VPN File Objects** UI path: **Objects** > **Object Management** > **VPN** > **Secure Client File**. See: File Objects.	
Secure Client Custom Attributes	**Secure Client Custom Attributes Objects** UI path: **Objects** > **Object Management** > **VPN** > **Custom Attribute**. Secure Client Custom Attributes Objects.	