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 1: 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 2: 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 3: 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 4: 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.