Quick Start Guide

Cisco ASA Integration with the APIC

Version 1.0(1)

Released: August 6, 2014

Updated December 1, 2014

1 About the ASA Integration with the APIC

The Cisco Application Policy Infrastructure Controller (APIC) automates insertion of services (such as an ASA firewall) northbound between applications, also called End Point Groups (EPGs). The APIC uses northbound APIs for configuring the network and services. You use these APIs to create, delete, and modify a configuration using managed objects.

When configuration is controlled through the APIC, you cannot change the configuration through the ASA CLI. This means that the CLIs for any feature that you configure through the APIC are disabled on the ASA. However, you may use the CLI to configure management access to the ASA. Operational and status commands, such as troubleshooting commands and **show** commands, are also available through the CLI.

Note With APIC integration, you can only use ASDM for monitoring purposes. You cannot change the configuration using ASDM.

For information about how to use ASDM for monitoring, see the *Cisco ASA Series General Operations ASDM Configuration Guide* for the specified feature and release that you are using.

Service Function Insertion

When a service function is inserted in the service graph between applications, traffic from these applications is classified by the APIC and identified using a tag in the overlay network. Service functions use the tag to apply policies to the traffic. For the ASA integration with the APIC, the service function forwards traffic using either routed or transparent firewall operation.

For information about the APIC, see the “Cisco Application Centric Infrastructure” chapter of the *ACI Fundamentals* guide.

For information about service graphs, see the “Configuring a Service Graph” chapter of the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.*

For information about the insertion of Layer 4 to Layer 7 services, see the “Overview” chapter of the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.

Supported ASA Models and Features

The following table lists the supported ASA models.

ASA Model	Software Version
ASA 5585-X (SSP 10 through SSP 60)	ASA software Version 8.4(x) and later
ASAv	

The following table lists the supported features for the ASAv and the ASA 5585-X.

Feature	ASAv Support (Yes/No)	ASA 5585-X Support (Yes/No)
Access Control Policies	Yes	Yes
Access Lists and Groups	Yes	Yes
Application Inspection	Yes	Yes
Clustering	No	Yes
Connection Limits	Yes	Yes
DNS Clients	Yes	Yes
EtherChannels	No	Yes
High Availability (Active/Active, Active/Standby)	Active/Standby only	Yes
Interface Configuration	Yes	Yes
IP Audit	Yes	Yes
IPv6	Yes	Yes
Logging	Yes	Yes
NAT/Twice NAT	Yes	Yes
Netflow	Yes	Yes
Network and Service Objects and Groups	Yes	Yes
NTP	Yes	Yes
Protocol Timeouts	Yes	Yes
Shared AnyConnect Premium Licenses	No	Yes
Smart Call Home Enable	Yes	Yes

Feature	ASAv Support (Yes/No)	ASA 5585-X Support (Yes/No)
Static Routing	Yes	Yes
TCP Intercept (Embryonic Connection Limits)	Yes	Yes
Threat Detection	Yes	Yes

2 Deploy the ASA

- ASAv—See the *Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide* for installation procedures, at the following URL:

  http://www.cisco.com/c/en/us/support/security/virtual-adaptive-security-appliance-firewall/products-installation-guides-list.html

  Note During ASAv deployment, you must define the value of the nameif property for the management interface as *management*. If you define the interface name as anything other than *management*, the device cluster will be stuck in AuditRequested/AuditPending state, and the fault will indicate that the read operation timed out. The management interface and default gateway configuration are deleted from the ASAv, and the interface is shut down.

- ASA 5585-X—See the *Cisco ASA 5585-X Quick Start Guide* for installation procedures, at the following URL:

  http://www.cisco.com/go/asa5585x-quick

3 Configure Management Access to the ASA

You must configure management access to the ASA so that the APIC can manage the ASA.

To configure management access to the ASAv, see Deploy the ASA.

To configure management access to the ASA 5585-X, see the following procedure:

Step 1 Remove any existing configuration:

```
ciscoasa(config)# clear configure all
```

Step 2 (Optional) Set the firewall mode to transparent firewall mode:

```
ciscoasa(config)# firewall transparent
```

Step 3 Configure the IP address and subnet mask on the management interface. The ASA needs to be on the same subnet as the APIC:

```
ciscoasa(config)# interface management {0/0 | 0/1}
ciscoasa(config-subif)# ip address ip_address subnet_mask
```

Step 4 Name the interface "management:"

```
ciscoasa(config-subif)# nameif management
```

Step 5 Enable the interface:

```
ciscoasa(config-if)# no shutdown
```

Step 6 Enable the ASA HTTPS server:

```
ciscoasa(config)# http server enable
```

Step 7 Enable an APIC to access the ASA. Repeat this step for each APIC in the APIC cluster:

```
ciscoasa(config)# http apic_address 255.255.255.255 management
```

Step 8 Create the user, "management-user," which the APIC uses to access the ASA:

```
ciscoasa(config)# username management-user password password privilege 15
```

4 Install the ASA Device Package

Each service node type must provide a device package, which includes two parts: a device specification and a device script. Service nodes of the same type are bound to a single device package.

The ASA device package enables you to perform the following tasks:

- Configure an ASA.
- Register the ASA with the APIC.

Step 1 Review the prerequisites for installing device packages.

See the "Overview" chapter and the "Prerequisites" chapter of the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.

Step 2 Download the ASA device package, a .zip file that is available from Cisco.com, at the following URL:

http://www.cisco.com/go/asa-software

Step 3 Install the ASA device package.

See the “Importing a Device Package” chapter of the *Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*.

Step 4 Register the ASA with the APIC.

See the “Fabric Connectivity” chapter of the *Cisco APIC Layer 4 to Layer 7 Device Package Development Guide*.

5 Configure the ASA within the APIC

Use the northbound API to configure the security policy, specifically for service graphs.

For information about how to use northbound APIs, see the *Cisco APIC Management Information Model Reference*.

For XML samples of ASA-specific northbound APIs, see the *Cisco ASA API Reference for APIC Integration*.

For APIC documentation, see http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.