1 About the ASA Integration with the APIC

The Cisco Application Policy Infrastructure Controller (APIC) automates insertion of services (such as an ASA firewall) 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.

Note If you try to create a configuration that is not supported on your current ASA version, an error similar to the following could appear on the APIC:

```
" *Major script error: Configuration error: …. ERROR: % Invalid input detected at
'^' marker. "
```

See your ASA version documentation for supported features.

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*.

Available APIC Products

Starting with release 1.2(7.8), there are two versions of the Cisco ASA Device Package software for ACI:

- Cisco ASA Device Package software for ACI - Same as the original version that was available with version 1.2(6) and earlier. This version allows you to configure many important features of ASA from APIC, including but not limited to the following:
  - Interface
  - Routing
  - Access-list
  - NAT
  - TrustSec
  - Application inspection
  - NetFlow
  - High availability
- Cisco ASA Device Package Fabric Insertion software for ACI - This version contains the following subset of features of the original version:
  - Interface
  - Dynamic routing
  - Static routing

Supported Versions of the Cisco ASA Software and Features

The following table lists the supported versions of the Cisco ASA Software for each of the supported platforms.

Platform	Software Version
Cisco ASA 5500-X (5512 through 5555)	ASA software Version 8.4(x) and later
Cisco ASA 5585-X (SSP 10 through SSP 60)	
Cisco Firepower 9300 Security Appliance	ASA software Version 9.6(1) and later
Cisco Firepower 41xx Security Appliance	
Cisco ASAv	See the "ASA and ASDM Compatibility" section of the *Cisco ASA Compatibility Matrix*.

The following table lists the supported features for the ASAv and the ASA 5585-X. For releases that support BGP and OSPF, see the *Release Notes for the Cisco ASA Device Package Software, Version 1.2(1) for ACI*.

Feature	ASAv Support (Yes/No)	ASA 5500-X/5585-X Support (Yes/No)
Service Policies	Yes	Yes
Access Lists and Groups	Yes	Yes
Application Inspection	Yes	Yes
BGP	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	Active/Standby only
Interface Configuration	Yes	Yes
IP Audit	Yes	Yes
IPv6	Yes	Yes
Logging	Yes	Yes

Feature	ASAv Support (Yes/No)	ASA 5500-X/5585-X Support (Yes/No)
Multiple Contexts	No	Yes
NAT/Twice NAT	Yes	Yes
Netflow	Yes	Yes
Network and Service Objects and Groups	Yes	Yes
NTP	Yes	Yes
OSPF	Yes	Yes
Protocol Timeouts	Yes	Yes
Shared AnyConnect Premium Licenses	No	Yes
Smart Call Home Enable	Yes	Yes
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, which the APIC uses to access the ASA:

```
ciscoasa(config)# username username password password privilege 15
```


Note The user is not required to be the "management-user." Any user is acceptable.

Step 9 Create an AAA authentication that allows APIC to have HTTP console access using LOCAL authentication:

```
ciscoasa(config)# aaa authentication http console LOCAL
```

Step 10 Verify that there is crypto key. If it does not exist, generate one using the following commands:

```
ciscoasa(config)# show crypto key mypubkey rsa
ciscoasa(config)# crypto key generate rsa
```

Step 11 Verify that the Encryption-DES and Encryption-3DES-AES are enabled using the following command on the ASA:

```
ciscoasa(config)# show version
```

If they are disabled, generate a new license.

4 Configure Jumbo Frame Support

To use Ethernet packets larger than 1500 bytes, you must configure jumbo frame support.

Step 1 Enable jumbo frames:

```
ciscoasa(config)# jumbo-frame reservation
```

Step 2 Save the running configuration:

```
ciscoasa(config)# write memory
```

Step 3 Reboot the ASA:

```
ciscoasa(config)# reload
```

5 Configure Multiple Context Mode

Step 1 To configure multi-context mode, see the "High Availability and Scalability" chapter in the *Cisco ASA Series General Operations CLI Configuration Guide* for instructions, at:

http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/configuration/general/asa-general-cli/ha-contexts.html

The instructions at this link describe how to configure interfaces in system mode, assign them to contexts, and configure the interfaces in each context. Those are all steps that will be done by the Device Package.

The Device Package is responsible for allocating and configuring interfaces used in each service graph in multi-context mode. However, the system administrator is responsible for the following provisioning of a multi-context ASA before registering it to the APIC:

Step 2 Create the required user contexts. (The device package does not create or delete any context.)

Step 3 For each context, make the provisioning similar to that for a single context ASA.

a. Allocate a management interface to it from the admin context.

Example configuration:

```
context tenant1
    allocate-interface Management0/1
    config-url disk0:/tenant1.cfg
```

b. In the user context, configure the management interface with **nameif** as "management," and specify a static IP address.

Example configuration:

```
interface management 0/1
    nameif management
    ip address 10.1.1.1 255.255.255.0
    security-level 100
```

c. In the user context, enable HTTPS access to the management interface.

Example configuration:

```
http server enable
http 0.0.0.0 0.0.0.0 management
```

d. Set user credentials and create AAA authentication that allows APIC to have access to the HTTP console using LOCAL authentication

```
username username password password privilege 15
aaa authentication http console LOCAL
```

e. Set up the management route.

f. Verify that there is crypto key. If it does not exist, generate one using the following commands:

```
show crypto key mypubkey rsa
crypto key generate rsa
```

6 Configure an ASA Cluster

To configure an ASA cluster, see the "ASA Cluster" chapter of the *Cisco ASA Series General Operations CLI Configuration Guide* for instructions, at:

http://www.cisco.com/c/en/us/td/docs/security/asa/asa94/configuration/general/asa-general-cli/ha-cluster.html

7 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*.

8 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.