Configure

Background

The ACI fabric provides for integration of L4-L7 services as an integral part of an application. This is accomplished through the use of an APIC-managed service graph, which requires a L4-L7 device package. The imported device package exposes configuration parameters in APIC, and allows it to orchestrate a given configuration onto the device.

To install the L4-L7 service graph, register a L4-L7 device with the APIC, add its configuration as part of a Function Profile or L4-L7 Service Parameters, and link those two with a service graph. Once you apply this L4-L7 service graph to a contract, the APIC renders it in the fabric by tagging device interfaces and stitching them to appropriate consumer and provider EPGs. The APIC then applies a given configuration to the registered device in an automated fashion. Once all of the configuration is applied to the ACI fabric and the L4-L7 device, the ACI fabric directs traffic defined by the contract to a given device for inspection. The ACI also allows you to chain multiple services together under a single service graph.

Configure Management Access to the ASA

Configure management access to the ASA so that the APIC can manage the ASA.

- To configure management access to an ASAv, see the respective Quick Start Guide:

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

- To configure management access to an ASA 5585-X, follow the steps in this section.

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-subif)# 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. The user is not required to be the management user. Any user is acceptable.

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

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

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

Step 10 Verify that there is crypto key. If it doesn't exist, generate one using:

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

Step 11 Verify that Encryption-DES and Encryption-3DES-AES are enabled. If they're disabled, generate a new license.

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

Configure Jumbo Frame Support

To use Ethernet packets larger than 1500 bytes, 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
```

Configure Multiple Context Mode

To configure multi-context mode, see the High Availability and Scalability chapter in the Cisco ASA Series General Operations CLI Configuration Guide for instructions.

The instructions 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 provisioning a multi-context ASA before registering it to the APIC.

Step 1 Create the required user contexts. The device package does not create or delete any context.

Step 2 For each context, make the provisioning similar to that for a single-context ASA.

1. Allocate a management interface to it from the admin context. For example:

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

2. In the user context, configure the management interface with **nameif** as **management** and specify a static IP address. For example:

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

3. In the user context, enable HTTPS access to the management interface. For example:

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

4. Set user credentials, and create an 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
```

5. Set up the management route.
6. Verify that there is crypto key. If it doesn't exist, generate one using:

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

Configure an ASA Cluster

To configure an ASA cluter, see the ASA Cluster chapter of the Cisco ASA Series General Operations CLI Configuration Guide for instructions.

Configure the ASA From the APIC

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

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

Refer to the APIC documentation for more information.