Deploying ASA

ASA Deployment Modes in ACI Fabric

The following ASA deployment modes are supported in the Cisco Application Centric Infrastructure (ACI) fabric:

- Single context and multiple context modes with the ASA device package version 1.2 or later.

  Both context modes use VLAN sub-interfaces to separate traffic of different tenants.

- Transparent (bump in the wire) mode for "GoThrough" insertion.
  - Forwarding is done based on MAC address, but the routing table is needed for NAT and application inspection.
  - Flooding must be enabled in the ACI bridge domains.

- Routed (Layer 3 hop) mode for "GoTo" insertion.

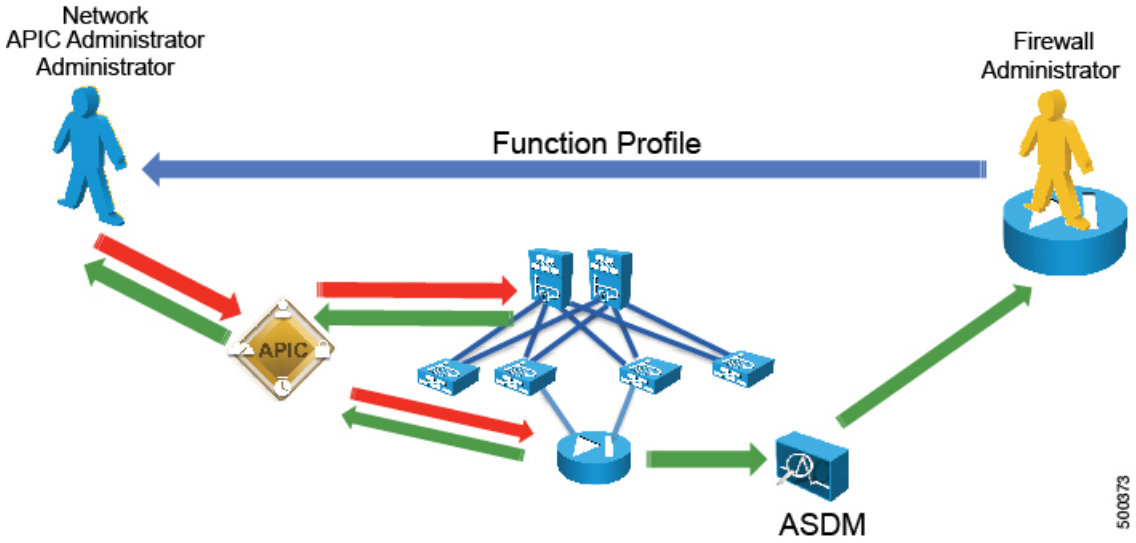
  You can configure only a single routing table per context, so you must specify destination static routes for target endpoint group subnets, or you can use dynamic routing with the ASA device package version 1.2 or later.

Note You do not need to create multiple contexts to create multiple service graphs. You can create multiple service graphs within a single context as long as the interface and ACL names are unique.

About the ASA Operational Model

In the ASA operational model, the ASA configuration is managed through the Application Policy Infrastructure Controller (APIC). The following figure illustrates the ASA operational model:

Figure 1: ASA Operational Model



The ASA administrator provides the XML or JSON function profile configuration to the APIC administrator who then pushes the function profile through the APIC to the ASA device.

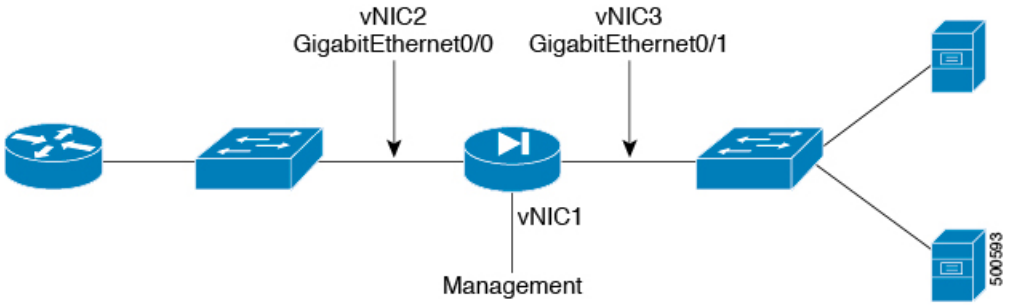
Translation of ASA Terminology

The following table translates which vNIC corresponds to which interface in Cisco ASAv and Cisco Application Centric Infrastructure (ACI):

Interface	VMware	ASAv	ACI	IP address is entered as
Management	vNIC1	Management	N/A	N/A
Outside	vNIC2	GigabitEthernet0/0	GigabitEthernet0/0	ExternalIf
Inside	vNIC3	GigabitEthernet0/1	GigabitEthernet0/1	InternalIf

The following figure illustrates the naming convention for the interfaces in the case of a Cisco ASAv firewall:

Figure 2: ASAv Firewall Interface Naming Convention



About ASA Multi-Context Mode

You can partition a single physical ASA into multiple virtual firewalls, known as security/virtual contexts. Each context acts as an independent device with its own security policy, interfaces, and management IP address. You can use ASA multi-context capability in Cisco Application Centric Infrastructure (ACI) along with an ASA service graph. This configuration is supported with an ASA 5500-X device and ASA device package 1.2 or later.

ASA supports multi-context by adding individual ASA contexts as `Cdev` objects under the Layer 4 to Layer 7 devices. The Layer 4 to Layer 7 parameter configuration is pushed to individual ASA contexts, not to the "Admin" context. ACI pushes the "allocate-interface" configuration to the "Admin" context for the other contexts. This means that the IP address of the "Admin" context must be entered as the management IP address for the logical device configuration.

About ASA High Availability and Scalability

Failover provides simple device-level redundancy. Failover peers are adjacent on data interfaces and have the same active IP address or MAC address. An active/standby failover pair can be initially configured and managed through the Application Policy Infrastructure Controller (APIC). You must first register both ASAs with the APIC. Active/active failover not supported.

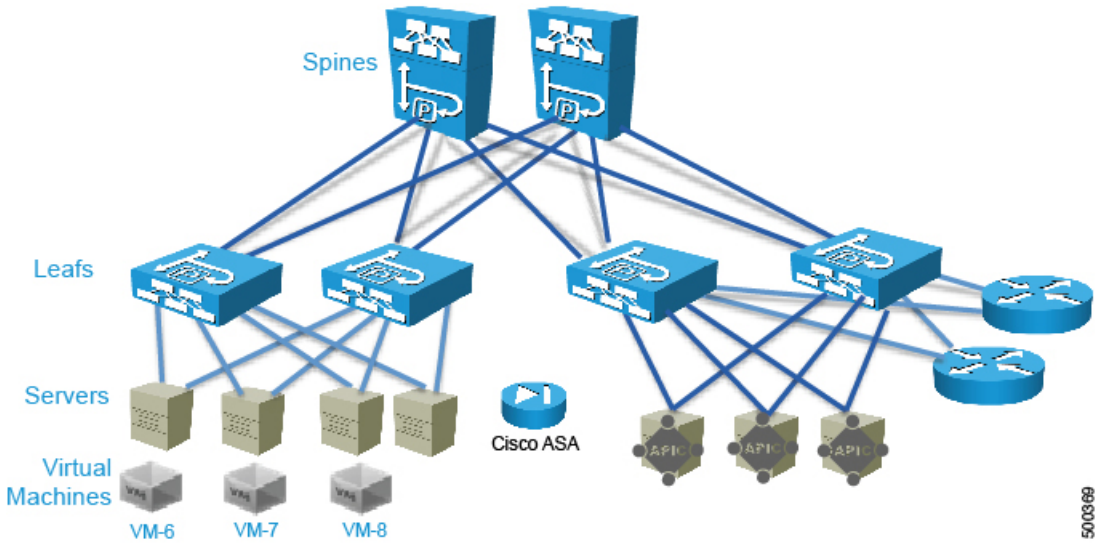
The ASA cluster must be deployed out of band, but the APIC can manage the cluster once it is deployed.

ASA in GoTo Mode

About Deploying ASA in GoTo Mode

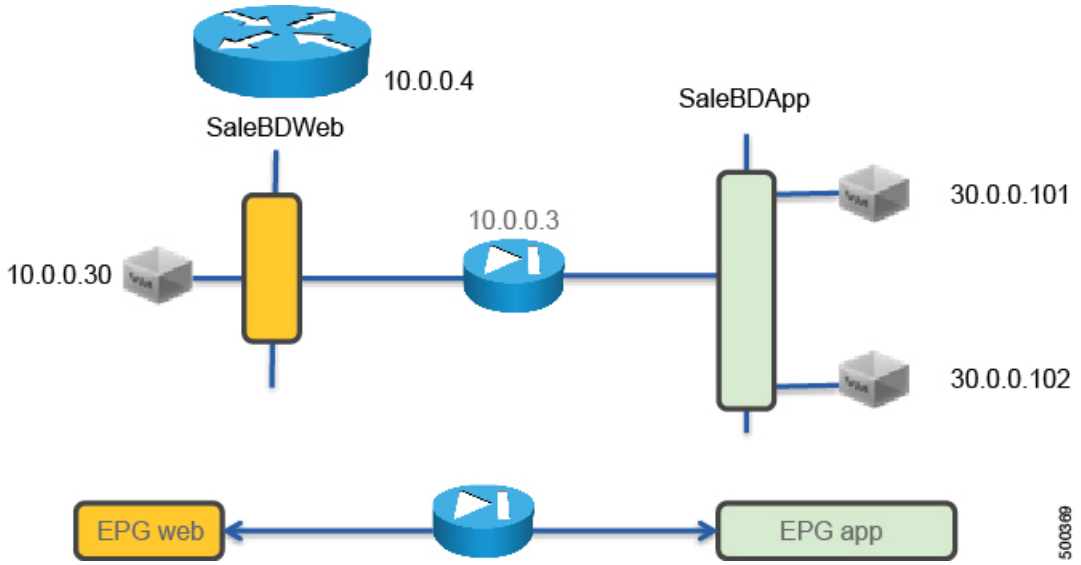
The following figure illustrates the topology for deploying Cisco Application Centric Infrastructure (ACI) fabric with ASA devices:

Figure 3: ACI Fabric with ASA Devices



The following figure illustrates the logical topology of an ASA GoTo deployment:

Figure 4: Logical Topology of an ASA GoTo Deployment



To deploy an ASA device in the GoTo mode, you must do the following things:

- Configure 2 bridge domains
- Configure 2 endpoint groups with each one associated with a different bridge domain
- Configure the ASA device as a GoTo device
- Set up NAT with a public IP on the same subnet as the bridge domain that ASA connects to on the outside (or consumer side)
- Configure the contract between the outside and inside endpoint group (or server side or provider side)
- Associate the service graph with the contract
- Associate the external logical interface with GigabitEthernet0/0 (which in the case of ASAv is Network Adapter 2)
- Associate the internal logical interface with GigabitEthernet0/1 (which in the case of ASAv is Network Adapter 3)

Overview of Preparing an ASA Device in GoTo Mode

ASA and ASAv do not have the concept of VRF management. If ASA or ASAv are deployed in GoTo mode you might want to use "inband" management to ASA to avoid conflicting entries in the routing table. If you are using the service device in transparent mode, you do not need to use "inband" management because there is no need for VRF management.

The following procedure provides of overview of preparing an ASA device to be deployed in GoTo mode.

Procedure

Step 1 Enable SSH.

Step 2 Enable HTTP access.

Step 3 Configure the credentials.
You do not need to configure the interfaces, VLANs, or IP addresses.

Step 4 Enter the following commands to create the initial configuration:

```
asa1(config)# no firewall transparent
asa1(config)# Interface Management0/0
asa1(config)# nameif management
asa1(config)# no shut
asa1(config)# hostname ASAv
asa1(config)# route management 0.0.0.0 0.0.0.0 192.168.11.254
asa1(config)# user admin password tme12345
asa1(config)# enable password tme12345
asa1(config)# aaa authentication ssh console LOCAL
asa1(config)# http server enable
asa1(config)# http 0.0.0.0 0.0.0.0 management
asa1(config)# ssh 0.0.0.0 0.0.0.0 management
```

Configuring Bridge Domains for ASA in GoTo Mode

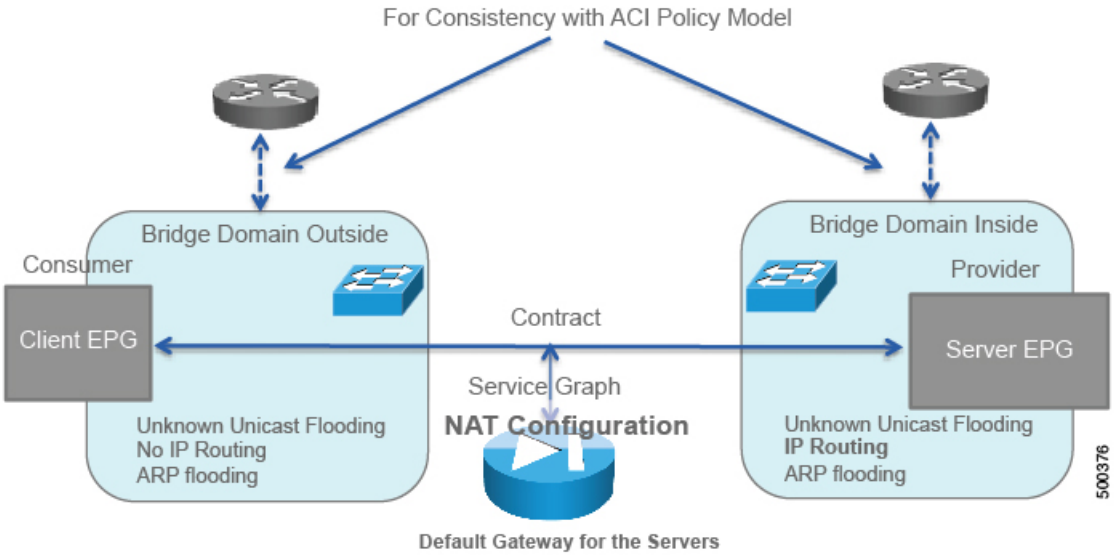
When you configure the bridge domains for ASA in GoTo mode, configure the bridge domains as you would for a generic configuration, except as follows:

- **L2 Unknown Unicast** radio buttons—Choose **Flood**.
- **ARP Flooding** check box—Put a check in the check box.
- **Unicast Routing** check box—Put a check in the check box if you need to configure an L3Out or for the endpoint attach feature.

For information on how to configure bridge domains, see Creating Bridge Domains and VRFs Using the GUI.

The following figure illustrates the bridge domain configuration for ASA in GoTo mode:

Figure 5: Bridge Domain Configuration for ASA in GoTo Mode



If you need the mapping database, such as for using traceroute or endpoint attach, you must enable unicast routing in the bridge domains.

Tuning the Server-Side Bridge Domain for Flood Removal for ASA in GoTo Mode

In GoTo mode you might want to optimize flooding. This tuning is meaningful only in the case of a service graph with GoTo mode, because in GoThrough mode Cisco Application Centric Infrastructure (ACI) sets the bridge domains to unknown unicast flooding.

On the server-side bridge domain, it can be beneficial to reduce flooding for unknown unicast packets. To do this, you can enable hardware proxy on the bridge domain. You should keep ARP flooding enabled because it might be necessary in the presence of ASA deployed in HA pairs.

Adding Endpoint Attach Support for ASA in GoTo Mode

You can deploy an ASA device in a service graph in a way that the endpoints that are discovered in the provider endpoint group are automatically added to an object group. In the ASA device, this feature is called "endpoint attach".

The object group is given a name in the following format:

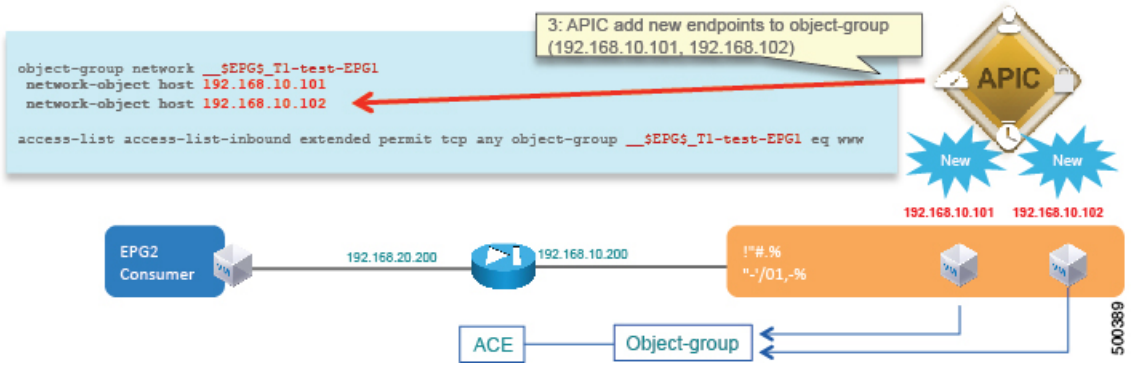
tenant_name-application_profile_name-EPG_name

For example:

```
ciscoasa# show run object-group
object-group network __$EPG$_T1-test-EPG1
  network-object host 192.168.10.100
```

The ACL will then reference this object group. The endpoint group detects the endpoint and populates the ACL. The Application Policy Infrastructure Controller (APIC) dynamically detects the new endpoint, then the endpoint is automatically added to the object group for ACE.

Figure 6: Example of the APIC Adding New Endpoints to the Object Group



The following procedure enables endpoint attach.

Procedure

Step 1 On the menu bar, choose **Tenants** > **All Tenants**.

Step 2 In the Work pane, double click the tenant's name.

Step 3 In the Navigation pane, choose **Tenant** *tenant_name* > **L4-L7 Services** > **L4-L7 Service Graph Template** > ***service_graph_template_name*** > **Function Node -** *node_name* > **provider**.

Step 4 In the Work pane, choose the connector's properties.

Step 5 Put a check in the **Attachment Notification** check box.

Step 6 Click **Submit**.

Step 7 Configure Layer 4 to Layer 7 parameters for ASA. The bridge domain must have routing enabled.

Step 8 Configure the ACE by defining the Device Config > Access List > Access Control Entry > Destination Address > Endpoint Group parameter as `epg_name` and set the value equal to the object group name in the following format:

tenant_name-application_profile_name-EPG_name

For example:

```
<!-- destination address: any or dynamically populated -->
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="destination_address"
 name="dest-address" nodeNameOrLbl="ASA-1-node" >
    <!-- destination address: autopopulated from the EPG endpoints -->
    <!-- Format is Tenant-applicationprofile-EPG -->
    <vnsParamInst  key="epg_name"   name="epg_name"  value="Sales-orderingtool-app"/>
    <!-- destination address: any -->
    <!-- vnsParamInst key="any" name="any"  value="any" -->
</vnsFolderInst>
```

ASA GoTo Mode Design Examples

The following figures illustrate ASA GoTo mode deployments with various scenarios: some with the client connected directly to the fabric, some with the fabric providing routing to the outside, and some with an external router. The figures include the recommended bridge domain settings for both client and server-side bridge domains.

The settings for the server-side or provider-side (also known as the internal bridge domain, `BD2`) include IP routing in case you decide to use the endpoint attach feature. If you do not want to use endpoint attach and

you do not care about flood reduction in the server-side bridge domain, you can configure the bridge domain without IP routing.

Figure 7: GoTo Mode with Client VMs (Split VRF)

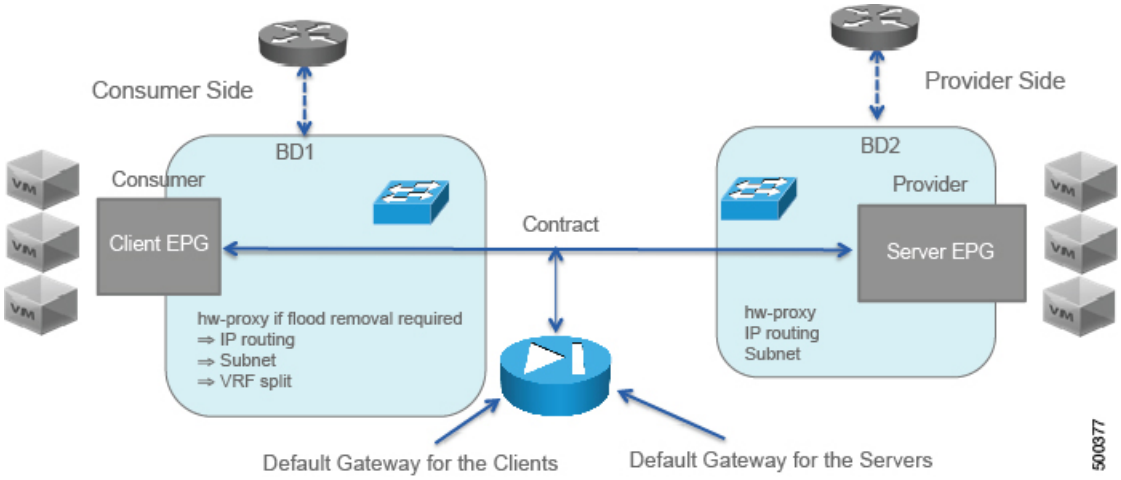


Figure 8: GoTo Mode with L3out option 1 with NAT and a single VRF)

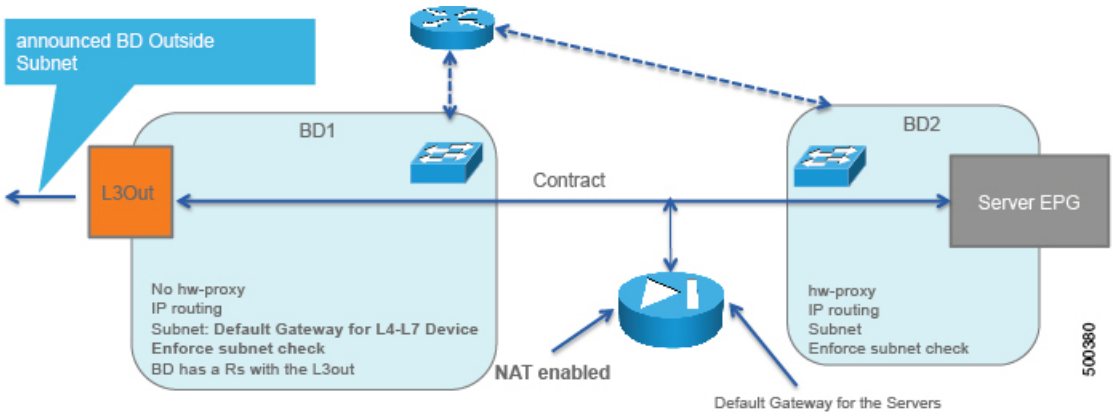


Figure 9: GoTo Mode Using Two VRFs

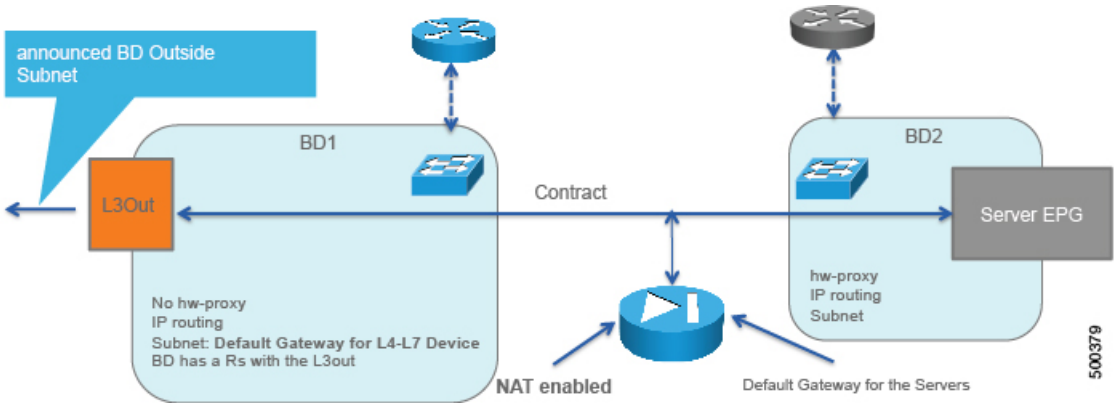
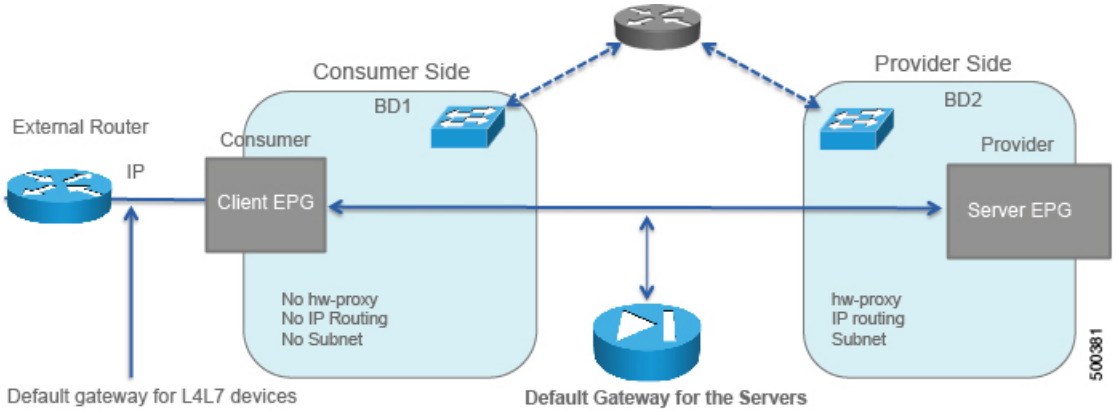


Figure 10: GoTo Mode with External Router



Deploying ASA in GoTo Mode

The tasks that you must perform to deploy ASA in GoTo mode are nearly identical to the tasks for generically deploying a service graph, with a few differences. The following procedure provides the generic service graph deployment tasks, along with information about what you must do differently to deploy ASA in GoTo mode.

Procedure

Step 1 Import the device package.
See Importing a Device Package Using the GUI.

Step 2 Create the bridge domains and VRFs.
See Creating Bridge Domains and VRFs Using the GUI.

a) For the inside bridge domain, enable **Unicast Routing** if you plan to use endpoint attach.
b) Associate the bridge domain with a VRF, which is necessary because of the object model. The hardware will not program the VRF if the bridge domain is configured only as Layer 2.

Step 3 Create endpoint groups and contracts.
See Creating Endpoint Groups and Contracts Using the GUI.

Step 4 Configure logical devices and concrete devices.
See Creating a Logical or Concrete Device Using the GUI.

a) For a concrete device, in the **Service Type** drop-down list, choose **Firewall**.
b) For the **Function Type** buttons, click **GoTo**.
c) For the Layer 4 to Layer 7 parameters, for the Host Name parameter, set the value to the host name of the ASA device.

If you have not yet applied the service graph template, a concrete device will have a health score of 0. This indicates the vNICs are not yet connected to a valid port group, which is normal since the graph has not been applied yet. As long as the device has a **Device State** of `stable`, then the communication between Application Policy Infrastructure Controller (APIC) and the device is working.

Step 5 Create or import a function profile.
See Creating a Function Profile Using the GUI or Importing a Function Profile Using the GUI.

- The configuration parameters for the firewall at the `CDev` level include the port channel, but they do not include the IP address. The reason is that the IP address of the firewall can change depending on where it is deployed, such as in which graph or tenant it is deployed.
- In this configuration, you must configure the device parameters for the port channel by using the "ALL parameters" field and set the LACP maximum to "8".
- You need to define each LACP member in the parameters.
- The VLAN on the port channel is automatically created in the rendering phase based on the bridge domain information and based on the physical domain information.

The following table describes the mandatory Layer 4 to Layer 7 parameters and provides examples of possible values that you must change for your specific configuration:

Table 1: Layer 4 to Layer 7 Parameters for ASA in GoTo Mode

L4-L7 Parameter or Folder	ASA Usage and Notes
`Device Config` folder	Define as `Device`.
`Device Config > Access List` folder	Define as `access-list-inbound`.
`Device Config > Access List > Access Control Entry` folder	Define as `permit-icmp`. Expand this folder to enter the Application Control Engine (ACE) parameters.
`Device Config > Access List > Access Control Entry` folder	Define as `permit-ssh`. Expand this folder to enter the ACE parameters.
`Device Config > NAT Rules List` folder	Define as `NATList-A`.

L4-L7 Parameter or Folder	ASA Usage and Notes
`Device Config > NAT Rules List > NAT Rule` folder	Define as `NATRule1`.
`Device Config > NAT Rules List > NAT Rule > Destination Address Translation > Mapped Object > Network Object` parameter	Define as `object_name` with a value of `Server1OutsideIP`. This is a traffic selection object.
`Device Config > NAT Rules List > NAT Rule > Destination Address Translation > Real Object > Network Object` parameter	Define as `object_name` with a value of `Server1InsideIP`. This is a traffic selection object.
`Device Config > Network Object` folder	Define as `ServerInsideP`.
`Device Config > Network Object > Host IP Address` parameter	Define as `host_ip_address` with a value of `30.0.0.101`.
`Device Config > Network Object` folder	Define as `ServerOutsideP`.
`Device Config > Network Object > Host IP Address` parameter	Define as `host_ip_address` with a value of `10.0.0.11`.
`Interface Related Configuration` folder for externalIf	Define as `externalIf`.
`Interface Related Configuration > Access Group` folder	Define as `ExtAccessGroup`.
`Interface Related Configuration > Access Group > Inbound Access List` parameter	Define as `name` with a value of `access-list-inbound`.

L4-L7 Parameter or Folder	ASA Usage and Notes
`Interface Related Configuration > Interface Specific Configuration` folder	Define as `externalIfCfg`.
`Interface Related Configuration > Interface Specific Configuration > IPv4 Address Configuration` folder	Define as `IPv4Address`.
`Interface Related Configuration > Interface Specific Configuration > IPv4 Address Configuration > IPv4 Address` parameter	Define as `ipv4_address` with a value of `10.0.0.3/255.255.255.0`. This mask value must follow this exact format.
`Interface Related Configuration` folder for internalIf	Define as `internalIf`.
`Interface Related Configuration > Interface Specific Configuration` folder	Define as `internalIfCfg`.
`Interface Related Configuration > Interface Specific Configuration > IPv4 Address Configuration` folder	Define as `IPv4Address`.
`Interface Related Configuration > Interface Specific Configuration > IPv4 Address Configuration > IPv4 Address` parameter	Define as `ipv4_address` with a value of `30.0.0.3/255.255.255.0`. This mask value must follow this exact format. The internalIf does not require parameters for an ACL.

L4-L7 Parameter or Folder	ASA Usage and Notes
`Function Config` folder	Define as `Function`. From this folder, you must reference the interfaces and the NAT configuration. In this folder, do the following things: 1 Define the `NAT Policy` folder as `NATPolicy`. 2 Define the NAT Policy > NAT Rules List parameter as `nat_list_name` with a value of `NATList-A`.
`Function Config > NAT Policy` folder	Define as `NATPolicy`.
`Function Config > NAT Policy > NAT Rules List` parameter	Define as `nat_list_name` with a value of `NATList-A`.

The following XML illustrates an example of Layer 4 to Layer 7 parameters configuration for the ASA deployment in GoTo mode:

```
<!-- RELATION TO THE EXTERNAL AND INTERNAL INTERFACES  -->
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="ExIntfConfigRelFolder" name="ExtConfig" nodeNameOrLbl="ASA-1-node" >
    <vnsCfgRelInst key="ExIntfConfigRel" name="ExtConfigrel" targetName="externalIf"/>
</vnsFolderInst>
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="InIntfConfigRelFolder" name="IntConfig" nodeNameOrLbl="ASA-1-node" >
    <vnsCfgRelInst key="InIntfConfigRel" name="InConfigrel" targetName="internalIf"/>
</vnsFolderInst>

<!-- ACL DEFINITION, ACL NAME "access-list-inbound" -->
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="AccessList"
name="access-list-inbound" nodeNameOrLbl="ASA-1-node" >

<!-- ACE "permit-ssh" -->
    <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="AccessControlEntry" name="permit-ssh" nodeNameOrLbl="ASA-1-node" >
        <vnsParamInst key="order" name="order1"  value="10"/>
        <!-- protocol -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="protocol"
 name="tcp" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="name_number" name="tcp"  value="tcp"/>
        </vnsFolderInst>
        <!-- source address -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="source_address" name="src-address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="any" name="any"  value="any"/>
        </vnsFolderInst>
        <!-- destination address -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="destination_address" name="dest-address" nodeNameOrLbl="ASA-1-node" >
```

```
            <vnsParamInst key="any" name="any"  value="any"/>
        </vnsFolderInst>
        <!-- destination L4 port -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="destination_service" name="dest-service" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="operator" name="op"  value="eq"/>
            <vnsParamInst key="low_port" name="port"  value="22"/>
        </vnsFolderInst>
        <!-- action permit or deny -->
        <vnsParamInst key="action" name="action-permit"  value="permit"/>
    </vnsFolderInst>
    <!-- ACE "permit-icmp" -->
    <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="AccessControlEntry" name="permit-icmp" nodeNameOrLbl="ASA-1-node" >
        <vnsParamInst key="order" name="order1"  value="10"/>
        <!-- protocol -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="protocol"
 name="icmp" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="name_number" name="icmp"  value="icmp"/>
        </vnsFolderInst>
        <!-- source address -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="source_address" name="src-address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="any" name="any"  value="any"/>
        </vnsFolderInst>
        <!-- destination address -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed"
key="destination_address" name="dest-address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="any" name="any"  value="any"/>
        </vnsFolderInst>
        <!-- action -->
        <vnsParamInst key="action" name="action-permit"  value="permit"/>
    </vnsFolderInst>
</vnsFolderInst>

<!-- EXTERNAL INTERFACE  -->
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="Interface"
name="externalIf" nodeNameOrLbl="ASA-1-node" >
   <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="InterfaceConfig"
 name="externalIfCfg" nodeNameOrLbl="ASA-1-node" >
        <!-- security level -->
        <vnsParamInst key="security_level" name="external_security_level"  value="50"/>
        <!-- IP ADDRESS-->
       <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="IPv4Address"
 name="IPv4Address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="ipv4_address" name="ipv4_address"
value="10.0.0.3/255.255.255.0"/>
        </vnsFolderInst>
    </vnsFolderInst>
    <!-- access-group  -->
    <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="AccessGroup"
name="ExtAccessGroup" nodeNameOrLbl="ASA-1-node" >
        <vnsCfgRelInst key="inbound_access_list_name" name="name"
targetName="access-list-inbound"/>
    </vnsFolderInst>
```

```
</vnsFolderInst>
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="Interface"
name="internalIf" nodeNameOrLbl="ASA-1-node" >
   <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="InterfaceConfig"
 name="internalIfCfg" nodeNameOrLbl="ASA-1-node" >
        <!-- security level -->
        <vnsParamInst key="security_level" name="internal_security_level"  value="100"/>
        <!-- IP ADDRESS-->
       <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-routed" key="IPv4Address"
 name="IPv4Address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="ipv4_address" name="ipv4_address"
value="30.0.0.3/255.255.255.0"/>
        </vnsFolderInst>
    </vnsFolderInst>
</vnsFolderInst>
```

Step 6 Create a service graph template and either use a function profile or enter the Layer 4 to Layer 7 parameters by hand.
See Creating a Layer 4 to Layer 7 Service Graph Template Using the GUI.

a) Drag the defined logical device to the canvas.

Step 7 Apply the service graph template.
See Applying a Service Graph Template to Endpoint Groups Using the GUI.

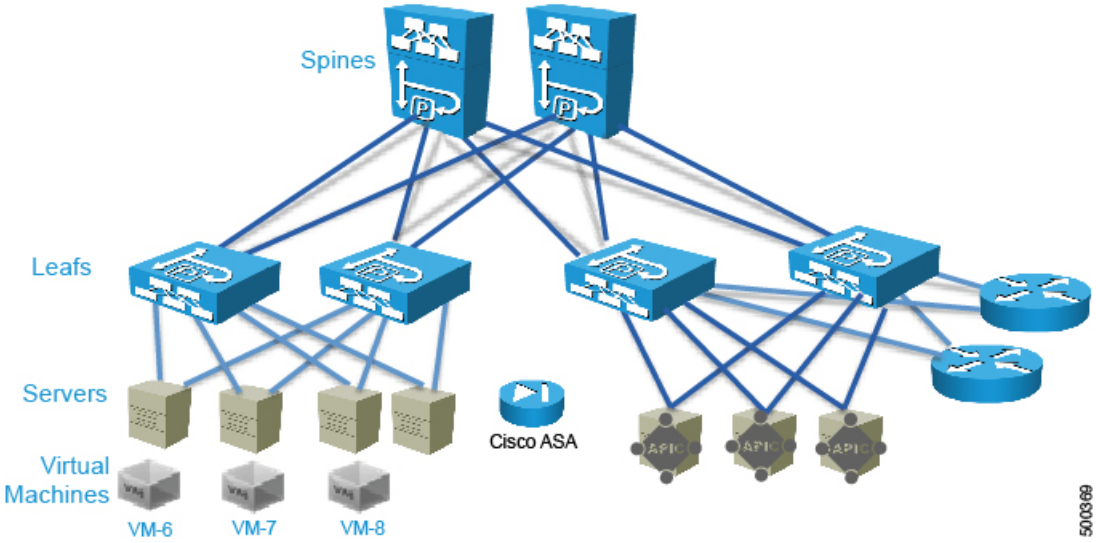
Step 8 Verify that the configuration deployed successfully.
See Verifying the Configuration for an ASA Device, on page 25.

ASA in GoThrough Mode

About Deploying ASA in GoThrough Mode

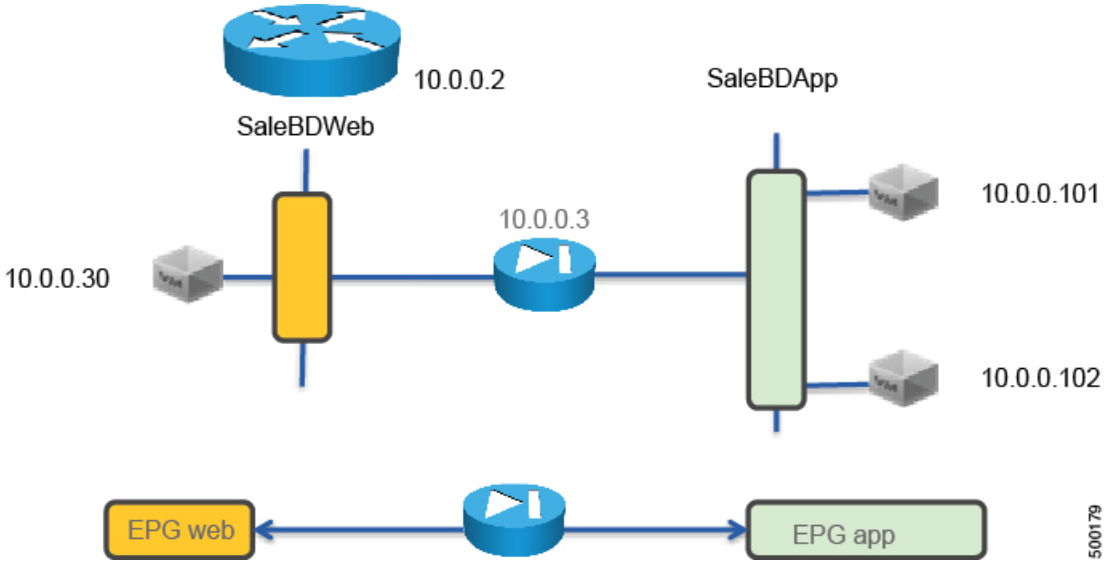
The following figure illustrates the topology for deploying Cisco Application Centric Infrastructure (ACI) fabric with ASA devices:

Figure 11: ACI Fabric with ASA Devices



The following figure illustrates the logical topology of an ASA GoThrough deployment:

Figure 12: Logical Topology of an ASA GoThrough Deployment



To deploy an ASA device in the GoThrough mode, you must do the following things:

- Configure 2 bridge domains
- Configure 2 endpoint groups with each one associated with a different bridge domain
- Enable routing on only one of the two bridge domains, which normally would be the outside bridge domain for the purpose of an L3Out
- Enable ARP flooding and unknown unicast flooding on both bridge domains
- Configure the ASA device as a GoThrough device
- Configure the contract between the outside and inside endpoint group (or server side or provider side)
- Associate the service graph with the contract
- Associate the external logical interface with GigabitEthernet0/0 (which in the case of ASAv is Network Adapter 2)
- Associate the internal logical interface with GigabitEthernet0/1 (which in the case of ASAv is Network Adapter 3)

Overview of Preparing an ASA Device in GoThrough Mode

ASA and ASAv do not have the concept of VRF management. For GoThrough mode, you do not need to use "inband" management because there is no need for VRF management.

The following procedure provides of overview of preparing an ASA device to be deployed in GoThrough mode.

Procedure

Step 1 Enable SSH.

Step 2 Enable HTTP access.

Step 3 Configure the credentials.
You do not need to configure the interfaces, VLANs, or IP addresses.

Step 4 Enter the following commands to create the initial configuration:

```
asa1(config)# firewall transparent
asa1(config)# Interface Management0/0
asa1(config)# nameif management
asa1(config)# ip address 192.168.12.120 255.255.255
asa1(config)# no shut
asa1(config)# hostname ASAv
asa1(config)# route management 0.0.0.0 0.0.0.0 192.168.12.254
asa1(config)# user admin password tme12345
asa1(config)# enable password tme12345
asa1(config)# aaa authentication ssh console LOCAL
asa1(config)# http server enable
asa1(config)# http 0.0.0.0 0.0.0.0 management
asa1(config)# ssh 0.0.0.0 0.0.0.0 management
```

Configuring Bridge Domains for ASA in GoThrough Mode

While you can optimize the bridge domain settings for GoThrough mode and optimize flooding, in practice the GoThrough service graph modifies the bridge domains to enable unknown unicast flooding and ARP flooding. ARP flooding is needed to make sure that if a firewall changes its MAC address while keeping the same IP address as a result of a failover, the gratuitous ARP can reach all the servers in the bridge domain to get updated to point to the new MAC address. With ARP flooding enabled, hypothetically unknown unicast flooding would not be needed, but it is assumed that the firewall relies on flooding to discover where each MAC address is and to build the forwarding table.

IP routing can be enabled on both bridge domains if each bridge domain had a different VRF. However, the service graph for GoThrough mode changes the bridge domain settings and does not render if both bridge domains have IP routing enabled.

When you configure the bridge domains for ASA in GoThrough mode, configure the bridge domains as you would for a generic configuration, except as follows:

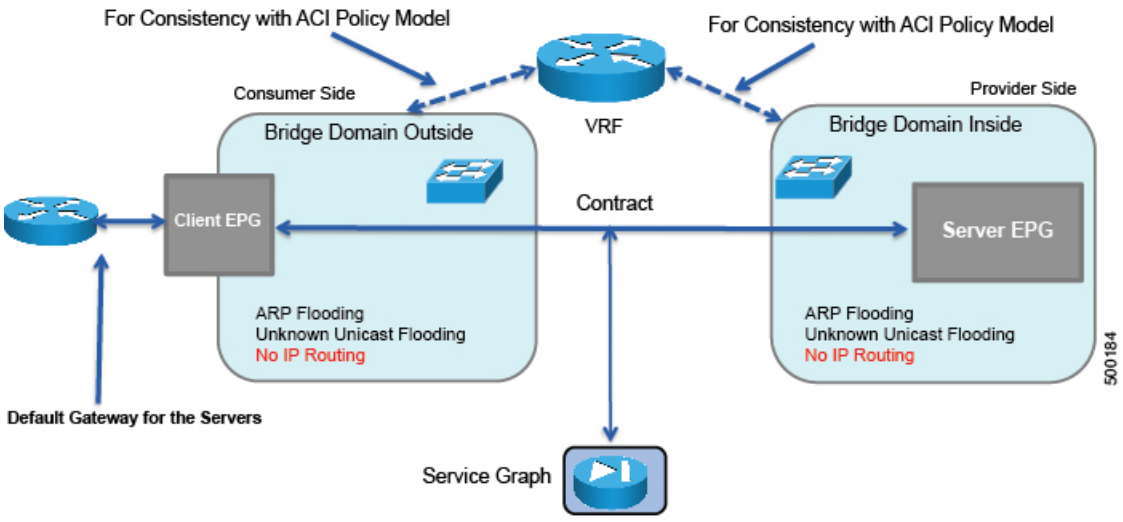
- **L2 Unknown Unicast** radio buttons—Choose **Flood**.
- **ARP Flooding** check box—Put a check in the check box.
- **Unicast Routing** check box—Put a check in the check box.
- **Unicast Routing** check box—Put a check in the check box if you are configuring the outside bridge domain and the Cisco Application Centric Infrastructure (ACI) fabric is the default gateway for the servers.

The GoThrough mode service graph does not render if IP routing is enabled on both bridge domains, and endpoint attach is not designed to work with GoThrough mode.

For information on how to configure bridge domains, see Creating Bridge Domains and VRFs Using the GUI.

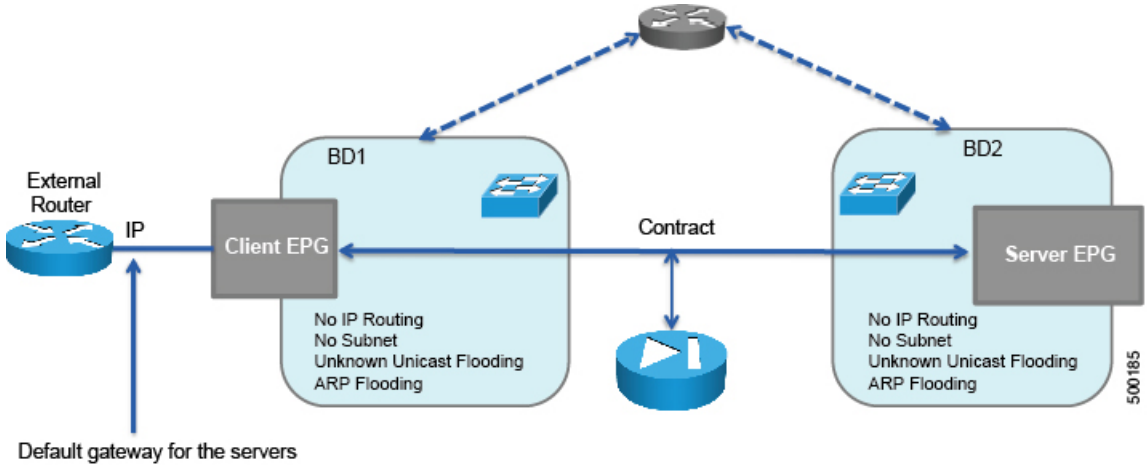
The following figure illustrates the simplest bridge domain configuration for ASA in GoThrough mode:

Figure 13: Simplest Bridge Domain Configuration for ASA in GoThrough Mode



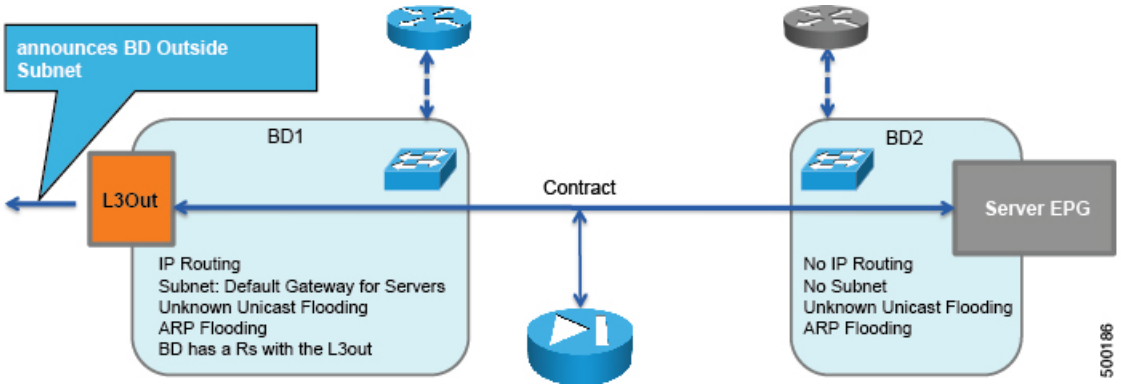
The following figure illustrates the bridge domain configuration for ASA deployment in GoThrough mode with an external router:

Figure 14: Bridge Domain Configuration for ASA in GoThrough Mode with an External Router



The following figure illustrates the bridge domain configuration for ASA deployment in GoThrough mode with an L3Out:

Figure 15: Bridge Domain Configuration for ASA in GoThrough Mode with an L3Out



Deploying ASA in GoThrough Mode

The tasks that you must perform to deploy ASA in GoThrough mode are nearly identical to the tasks for generically deploying a service graph, with a few differences. The following procedure provides the generic service graph deployment tasks, along with information about what you must do differently to deploy ASA in GoThrough mode.

Procedure

Step 1 Import the device package.

See Importing a Device Package Using the GUI.

Step 2 Create the bridge domains and VRFs.
See Creating Bridge Domains and VRFs Using the GUI.

a) Associate the bridge domain with a VRF, which is necessary because of the object model. The hardware will not program the VRF if the bridge domain is configured only as Layer 2.

Step 3 Create endpoint groups and contracts.
See Creating Endpoint Groups and Contracts Using the GUI.

Step 4 Configure logical devices and concrete devices.
See Creating a Logical or Concrete Device Using the GUI.

a) For a concrete device, in the **Service Type** drop-down list, choose **Firewall**.
b) For the **Function Type** buttons, click **GoThrough**.
c) For the Layer 4 to Layer 7 parameters, for the Host Name parameter, set the value to the host name of the ASA device.

If you have not yet applied the service graph template, a concrete device will have a health score of 0. This indicates the vNICs are not yet connected to a valid port group, which is normal since the graph has not been applied yet. As long as the device has a **Device State** of `stable`, then the communication between Application Policy Infrastructure Controller (APIC) and the device is working.

Step 5 Create or import a function profile.
See Creating a Function Profile Using the GUI or Importing a Function Profile Using the GUI.

- The configuration parameters for the firewall at the `CDev` level include the port channel, but they do not include the IP address. The reason is that the IP address of the firewall can change depending on where it is deployed, such as in which graph or tenant it is deployed.
- In this configuration, you must configure the device parameters for the port channel by using the "ALL parameters" field and set the LACP maximum to "8".
- You need to define each LACP member in the parameters.
- The VLAN on the port channel is automatically created in the rendering phase based on the bridge domain information and based on the physical domain information.

The following table describes the mandatory Layer 4 to Layer 7 parameters and provides examples of possible values that you must change for your specific configuration:

Table 2: Layer 4 to Layer 7 Parameters for ASA in GoThrough Mode

L4-L7 Parameter or Folder	Usage and Notes
`Device Config` folder	Define as `Device`.
`Device Config > Access List > Access Control Entry` folder	Define as `permit-icmp`. Expand this folder to enter the Application Control Engine (ACE) parameters.
`Device Config > Access List > Access Control Entry` folder	Define as `permit-ssh`. Expand this folder to enter the ACE parameters.

L4-L7 Parameter or Folder	Usage and Notes
`Device Config > Bridge Group Interface` folder	Define as `1`.
`Device Config > Bridge Group Interface > IPv4 Address Configuration > IPv4 Address` parameter	Define as `ipv4_address` with a value in the following format: *`a.b.c.d/e.f.g.h`* *a.b.c.d* is the IPv4 address, while *e.f.g.h* is the mask. For example: `10.0.0.2/255.255.255.0` .
`Interface Related Configuration` folder for externalIf	Define as `externalIf`.
`Interface Related Configuration > Access Group` folder	Define as `ExtAccessGroup`.
`Interface Related Configuration > Interface Specific Configuration` folder	Define as `externalIfCfg`.
`Interface Related Configuration > Interface Specific Configuration > Bridge Group Interface` parameter	Define as `extbridge` with a value of the bridge group number that you defined for the `Device Config > Bridge Group Interface` folder.
`Interface Related Configuration` folder for internalIf	Define as `internalIf`. The internalIf does not require parameters for an ACL.
`Interface Related Configuration > Interface Specific Configuration` folder	Define as `internalIfCfg`.
`Interface Related Configuration > Interface Specific Configuration > Bridge Group Interface` parameter	Define as `intbridge` with a value of the bridge group number that you defined for the `Device Config > Bridge Group Interface` folder.

The following XML is an example of a Layer 4 to Layer 7 parameters configuration:

```
<!-- RELATION TO THE EXTERNAL AND INTERNAL INTERFACES  -->
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
key="ExIntfConfigRelFolder" name="ExtConfig" nodeNameOrLbl="ASA-1-node" >
    <vnsCfgRelInst key="ExIntfConfigRel" name="ExtConfigrel" targetName="externalIf"/>
</vnsFolderInst>
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
key="InIntfConfigRelFolder" name="IntConfig" nodeNameOrLbl="ASA-1-node" >
    <vnsCfgRelInst key="InIntfConfigRel" name="InConfigrel" targetName="internalIf"/>
</vnsFolderInst>

<!-- ACL DEFINITION, ACL NAME "access-list-inbound" -->
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged" key="AccessList"
name="access-list-inbound" nodeNameOrLbl="ASA-1-node" >

<!-- ACE "permit-ssh" -->
    <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
key="AccessControlEntry" name="permit-ssh" nodeNameOrLbl="ASA-1-node" >
        <vnsParamInst key="order" name="order1"  value="10"/>
        <!-- protocol -->
       <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged" key="protocol"
 name="tcp" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="name_number" name="tcp"  value="tcp"/>
        </vnsFolderInst>
        <!-- source address -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
key="source_address" name="src-address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="any" name="any"  value="any"/>
        </vnsFolderInst>
        <!-- destination address -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
key="destination_address" name="dest-address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="any" name="any"  value="any"/>
        </vnsFolderInst>
        <!-- destination L4 port -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
key="destination_service" name="dest-service" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="operator" name="op"  value="eq"/>
            <vnsParamInst key="low_port" name="port"  value="22"/>
        </vnsFolderInst>
        <!-- action permit or deny -->
        <vnsParamInst key="action" name="action-permit"  value="permit"/>
    </vnsFolderInst>
    <!-- ACE "permit-icmp" -->
    <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
key="AccessControlEntry" name="permit-icmp" nodeNameOrLbl="ASA-1-node" >
        <vnsParamInst key="order" name="order1"  value="10"/>
        <!-- protocol -->
       <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged" key="protocol"
 name="icmp" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="name_number" name="icmp"  value="icmp"/>
        </vnsFolderInst>
        <!-- source address -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
```

```
key="source_address" name="src-address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="any" name="any"  value="any"/>
        </vnsFolderInst>
        <!-- destination address -->
        <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged"
key="destination_address" name="dest-address" nodeNameOrLbl="ASA-1-node" >
            <vnsParamInst key="any" name="any"  value="any"/>
        </vnsFolderInst>
        <!-- action -->
        <vnsParamInst key="action" name="action-permit"  value="permit"/>
    </vnsFolderInst>
</vnsFolderInst>

<!-- BRIDGE-GROUP 1 -->
<vnsFolderInst  ctrctNameOrLbl="webtoapp"  graphNameOrLbl="FW-bridged" key="BridgeGroupIntf"
 name="1" nodeNameOrLbl="ASA-1-node" scopedBy="epg">
    <vnsParamInst  key="ipv6_nd_dad_attempts"  name="ipv6_nd_dad_attempts" validation=""
value="1"/>
    <!-- IP ADDRESS-->
   <vnsFolderInst  ctrctNameOrLbl="webtoapp"  graphNameOrLbl="FW-bridged" key="IPv4Address"
 name="IPv4Address" nodeNameOrLbl="ASA-1-node" scopedBy="epg">
        <vnsParamInst  key="ipv4_address"  name="ipv4_address" validation=""
value="30.0.0.254/255.255.255.0"/>
    </vnsFolderInst>
</vnsFolderInst>

<!-- EXTERNAL INTERFACE  -->
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged" key="Interface"
name="externalIf" nodeNameOrLbl="ASA-1-node" >
   <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged" key="InterfaceConfig"
 name="externalIfCfg" nodeNameOrLbl="ASA-1-node" >
        <!-- BRIDGE-GROUP CONFIGURATION -->
        <vnsCfgRelInst  key="bridge_group"  name="extbridge" targetName="1"/>
        <!-- security level -->
        <vnsParamInst key="security_level" name="external_security_level"  value="50"/>
    </vnsFolderInst>
    <!-- access-group  -->
    <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged" key="AccessGroup"
 name="ExtAccessGroup" nodeNameOrLbl="ASA-1-node" >
        <vnsCfgRelInst key="inbound_access_list_name" name="name"
targetName="access-list-inbound"/>
    </vnsFolderInst>
</vnsFolderInst>
<vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged" key="Interface"
name="internalIf" nodeNameOrLbl="ASA-1-node" >
   <vnsFolderInst ctrctNameOrLbl="webtoapp" graphNameOrLbl="FW-bridged" key="InterfaceConfig"
 name="internalIfCfg" nodeNameOrLbl="ASA-1-node" >
        <!-- BRIDGE-GROUP CONFIGURATION -->
        <vnsCfgRelInst  key="bridge_group"  name="intbridge" targetName="1"/>
        <!-- security level -->
        <vnsParamInst key="security_level" name="internal_security_level"  value="100"/>
    </vnsFolderInst>
</vnsFolderInst>
```

Step 6 Create a service graph template and either use a function profile or enter the Layer 4 to Layer 7 parameters by hand.
See Creating a Layer 4 to Layer 7 Service Graph Template Using the GUI.

a) Drag the defined logical device to the canvas.
b) In the **ASA Cluster Information** section, for the **Firewall** radio buttons, choose **Two-Arm**.

Step 7 Apply the service graph template.
See Applying a Service Graph Template to Endpoint Groups Using the GUI.

You cannot configure an "any" virtual IP or port. You can only choose **TCP** or **UDP** option; there is no "all IP protocol" value.

Step 8 Verify that the configuration deployed successfully.
See Verifying the Configuration for an ASA Device, on page 25.

Verifying the Configuration for an ASA Device

After you deployed an ASA device in any mode, you can verify that the configuration is functioning properly by using the following procedure. If you encounter an issue, you can try troubleshooting by viewing the Application Policy Infrastructure Controller (APIC) log that is at the following location:

```
/data/devicescript/CISCO.ASA.1.2/logs/debug.log
```

Procedure

Step 1 In the APIC GUI, on the menu bar, choose **Tenants** > **All Tenants**.

Step 2 In the Work pane, double click the tenant's name.

Step 3 In the Navigation pane, choose **Tenant** ***tenant_name*** > **L4-L7 Services** > **Deployed Graph Instances** > ***ASA_graph_name***.

Step 4 In the Work pane, in the **Cluster Interfaces** section, ensure that the logical interfaces appear.

Step 5 In the Navigation pane, choose **Tenant** ***tenant_name*** > **L4-L7 Services** > **Deployed Devices** > ***ASA_device_name***.

Step 6 In the Work pane, view the ASA device's properties. The health score should be 100.

Step 7 In the ASA GUI, choose the **Virtual Hardware** tab.
Verify that the vNICs were automatically placed in the shadow EPGs.

Step 8 In the Cisco Adaptive Security Device Manager (ASDM) GUI, choose **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**.
In the Work pane, verify that you can see the `externalIf` and `internalIf` interfaces.

Undoing a Service Graph Configuration for ASA

To undo a service graph configuration for ASA, in the Application Policy Infrastructure Controller (APIC) GUI, delete the service graph template.

See Undoing a Service Graph Configuration Using the GUI.