



# Deploying Layer 4 to Layer 7 Services

- [Overview, on page 1](#)
- [Deploying a Service Graph, on page 4](#)

## Overview

The Cisco Cloud APIC enables you to deploy Layer 4 to Layer 7 service devices to the public cloud. This initial release supports application gateway deployments in Azure.

## About Application Gateways

An application gateway is a Layer 7 load balancer that inspects packets and creates access points to HTTP and HTTPS headers. It also identifies the load and spreads it out to the targets with higher efficiency. You deploy an application gateway using a service graph, which enables you to define how you want traffic to come into the network, the devices that the traffic passes through, and how the traffic leaves the network. You specify these actions by configuring one or more listeners.

Listeners enable you to specify the ports and protocols (HTTP or HTTPS) that the application gateway accepts traffic on. When specifying HTTPS, you also choose a security policy and an SSL certificate.



---

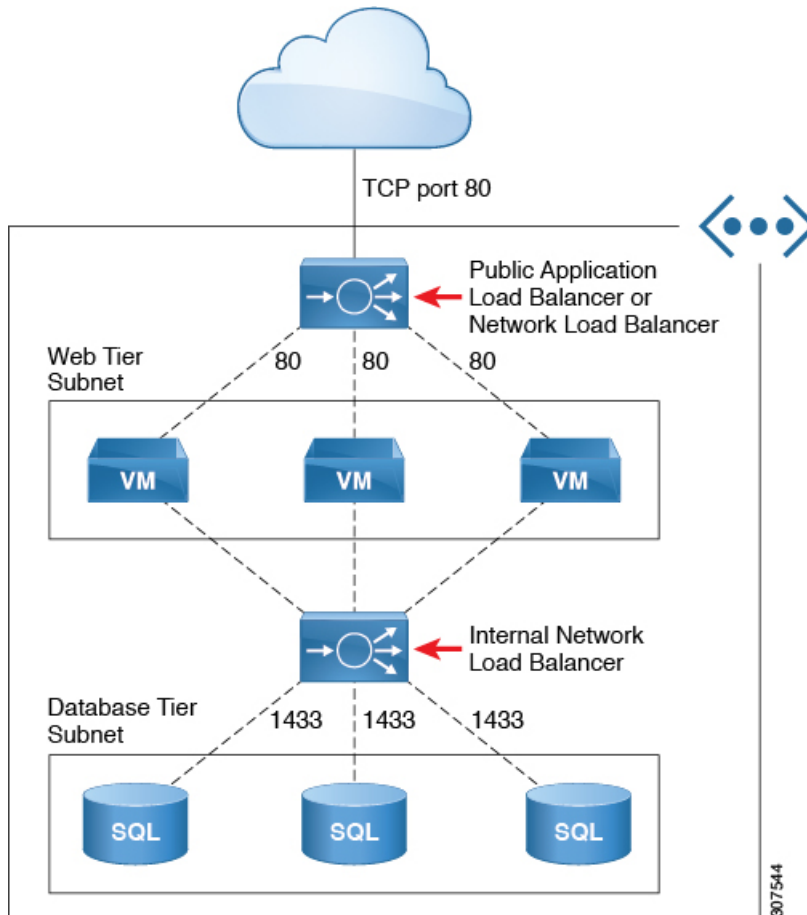
**Note** A listener can have multiple certificates.

---

All listeners require you to configure at least one rule (a default rule, which does not have a condition). Rules enable you to specify the action that the load balancer takes when a condition is met. For example, you can create a rule that redirects traffic to a specified URL when a request is made to a specified hostname or path.

There are two deployment types: internet-facing and internal-facing. An internet-facing deployment inserts the application gateway as a service between the consumer external EPG and the provider cloud EPG. An internal-facing deployment inserts the application gateway as a service between the consumer cloud EPG and the provider cloud EPG. The following figure shows the contract configuration within the VRF and the application gateway as a service inserted between the consumer external EPG and the provider cloud EPG. The following figure also shows the contract configuration within the VRF and the application gateway as a service inserted between the consumer cloud EPG and provider cloud EPG.

Figure 1: Internet-Facing and Internal-Facing Deployment



**Note** You can find more information about application gateways in the documentation on the Azure website.

## Dynamic Server Attachment to Server Pool

Servers in the server pool or target group are dynamically added. You do not need to specify the IP addresses or instance IDs for the targets. The relation from a listener rule to a provider cloud EPG is used for the dynamic selection of endpoints. The relation is also used for adding the endpoints to the target group. By default, the endpoints are registered with the port number 80.

Based on the target group-to-security group (application security group/network security group) association that is provided in the application gateway, and the EPG (security group) of the endpoint, the VM instance (server) is associated to the target group dynamically on the target group's default port. Alternatively, instead of registering the VM instance on the target group port, you can attach the custom port by specifying the ports in the following table:

You can specify `EPGMap:<EpgDN>` as the tag and the list of ports to be registered on the target group as a list separated by commas.

## About Service Graphs

The Cisco Application Centric Infrastructure (ACI) treats services as a part of an application. Any services that are required are treated as a service graph that is instantiated on the Cisco ACI fabric from the Cisco APIC. You define the service for the application while service graphs identify the set of network or service functions that the application needs.

A service graph represents the network using the following elements:

- **Function node**—A function node represents a function that is applied to the traffic, such as a load balancer. A function within the service graph might require one or more parameters and have one or more connectors.
- **Terminal node**—A terminal node enables input and output from the service graph.
- **Connector**—A connector enables input and output from a node.

After the graph is configured, the Cisco APIC automatically configures the services according to the service function requirements that are specified in the service graph. The Cisco APIC also automatically configures the network according to the needs of the service function that is specified in the service graph, which does not require any change in the service device.

A service graph is represented as two or more tiers of an application with the appropriate service function inserted between them.

A service appliance (device) performs a service function within the graph. One or more service appliances might be required to render the services required by a graph. A single-service device can perform one or more service functions.

Service graphs and service functions have the following characteristics:

- Traffic sent or received by an endpoint group can be filtered based on a policy, and a subset of the traffic can be redirected to different edges in the graph.
- Service graph edges are directional.
- Logical functions can be rendered on the appropriate (physical or virtual) device, based on the policy.
- The service graph supports splits and joins of edges, and it does not restrict the administrator to linear service chains.
- Traffic can be reclassified again in the network after a service appliance emits it.

By using a service graph, you can install a service, a load balancer, once and deploy it multiple times in different logical topologies. Each time the graph is deployed, Cisco ACI takes care of changing the configuration on the service device to enable the forwarding in the new logical topology.

## About Function Nodes

A function node represents a single service function. A function node has function node connectors, which represent the network requirement of a service function.

A function node within a service graph can require one or more parameters. An EPG, an application profile, or a tenant VRF can specify the parameters. Function parameters can be specified when the service graph is rendered. For example, if the function node is a load balancer, the listener and its rule can be specified for the function node at the time the graph is rendered.

## About Terminal Nodes

Terminal nodes connect a service graph with the contracts. You can insert a service graph for the traffic between two application cloud EPGs by connecting the terminal node to a contract. Once connected, traffic between the consumer cloud EPG and provider cloud EPG of the contract is redirected to the service graph.

## Deploying a Service Graph

The service graph enables you to define how traffic flows between devices, how the traffic comes into the network, which devices the traffic passes through, and how the traffic leaves the network.

Before you can deploy a service graph, you must configure the following:

1. A tenant
2. An application profile
3. A consumer EPG
4. A provider EPG
5. A cloud context profile
6. A cloud load balancer
7. A contract with a filter
8. A service graph

## Deploying the Service Graph Using the Cloud APIC GUI

### Creating a Load Balancer Using the Cisco Cloud APIC GUI

This section explains how to create a load balancer using the Cisco Cloud APIC GUI.

- 
- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.  
A list of **Application Management** options appear in the **Intent** menu.
- Step 3** From the **Application Management** list in the **Intent** menu, click **Services > Devices > Create Device**. The **Create Device** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create Device Dialog Box Fields* table then continue.

**Table 1: Create Device Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of the load balancer.

Properties	Description
<b>Tenant</b>	To choose a tenant: <ol style="list-style-type: none"> <li>Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog appears.</li> <li>From the column on the left, click to choose a tenant.</li> <li>Click <b>Select</b>. You return to the <b>Create Device</b> dialog box.</li> </ol>
<b>Settings</b>	
<b>Service Type</b>	Choose <b>Application Gateway</b> .
<b>Scheme</b>	Choose <b>Internet Facing</b> or <b>Internal</b> .
<b>Region</b>	To choose a region: <ol style="list-style-type: none"> <li>Click <b>Select Region</b>. The <b>Select Region</b> dialog box appears.</li> <li>From the <b>Select Region</b> dialog, click to choose a region in the left column then click <b>Select</b>. You return to the <b>Create Cloud Context Profile</b> dialog box.</li> </ol>
<b>Subnet</b>	To choose a subnet: <ol style="list-style-type: none"> <li>Click <b>Select Subnet</b>. The <b>Select Subnet</b> dialog box appears.</li> <li>From the column on the left, click to choose a subnet.</li> <li>Click <b>Select</b>. You return to the <b>Create Device</b> dialog box.</li> <li>Click <b>Add</b> to add the region and subnet.</li> </ol>
<b>VM Instance Count</b>	Enter a number in the <i>VM Instance Count</i> text box.
<b>VM Instance Size</b>	Click the radio button for the VM instance size you want to choose: <b>large</b> , <b>medium</b> , or <b>small</b> .

**Step 5** Click **Save** when finished.

## Creating a Service Graph Template Using the Cisco Cloud APIC GUI

This section explains how to configure a service graph template using the Cisco Cloud APIC GUI.

### Before you begin

You have already created a device.

- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Application Management**.  
A list of **Application Management** options appear in the **Intent** menu.
- Step 3** From the **Application Management** list in the **Intent** menu, click **Services > Service Graph > Create Service Graph**. The **Create Service Graph** dialog box appears.
- Step 4** Enter the appropriate values in each field as listed in the following *Create Service Graph Dialog Box Fields* table then continue.

**Table 2: Create Service Graph Dialog Box Fields**

Properties	Description
<b>General</b>	
<b>Name</b>	Enter the name of service graph template.
<b>Tenant</b>	To choose a tenant: <ol style="list-style-type: none"> <li>Click <b>Select Tenant</b>. The <b>Select Tenant</b> dialog appears.</li> <li>From the column on the left, click to choose a tenant.</li> <li>Click <b>Select</b>. You return to the <b>Create Service Graph</b> dialog box.</li> </ol>
<b>Description</b>	Enter a description of the service graph template.
<b>Settings</b>	
<b>Select a Device</b>	To choose a device: <ol style="list-style-type: none"> <li>Click <b>Select Device</b>. The <b>Select Device</b> dialog appears.</li> <li>From the column on the left, click to choose a device.</li> <li>Click <b>Select</b>. You return to the <b>Create Service Graph</b> dialog box.</li> </ol>

- Step 5** Click **Save** when finished.

## Deploying Layer 4 to Layer 7 Services Using the Cisco Cloud APIC GUI

This section explains how to deploy Layer 4 to Layer 7 services.

### Before you begin

- You have configured a device.
- You have configured a service graph.

- Step 1** Click the **Intent** icon. The **Intent** menu appears.
- Step 2** Click the drop-down arrow below the **Intent** search box and choose **Configuration**.  
A list of **Configuration** options appear in the **Intent** menu.
- Step 3** From the **Configuration** list in the **Intent** menu, click **EPG Communication**. The **EPG Communication** dialog box appears with the **Consumer EPGs**, **Contract**, and **Provider EPGs** information.
- Step 4** To choose a contract:  
a) Click **Select Contract**. The **Select Contract** dialog appears.  
b) In the pane on the left side of the **Select Contract** dialog, click to choose a contract then click **Select**. The **Select Contract** dialog box closes.
- Step 5** To add a consumer EPG:  
a) Click **Add Consumer EPGs**. The **Select Consumer EPGs** dialog appears.  
b) In the pane on the left side of the **Select Consumer EPGs** dialog, click to place a check in a check box to choose a cloud EPG (for an internal facing load balancer) or a cloud external EPG (for an internet facing load balancer) then click **Select**. The **Select Consumer EPGs** dialog box closes.
- Step 6** To add a provider EPG:  
a) Click **Add Provider EPGs**. The **Select Provider EPGs** dialog appears.  
b) In the pane on the left side of the **Select Provider EPGs** dialog, click to place a check in a check box to choose a provider EPG then click **Select**. The **Select Provider EPGs** dialog box closes.
- Step 7** To choose a service graph:  
a) From the **EPG Communication Configuration** dialog, click **Select Service Graph**. The **Select Service Graph** dialog box appears.  
b) In the pane on the left side of the **Select Service Graph** dialog, click to choose a service graph then click **Select**. The **Select Service Graph** dialog box closes.
- Step 8** Under **Service Graph Preview**, click **Add Cloud Load Balancer Listener**. The **Add Cloud Load Balancer Listener** dialog appears that enables you to add listeners.  
Listeners are the ports and protocols that the device will work on.
- Step 9** Enter the appropriate values in each field as listed in the following *Add Cloud Load Balancer Listener Dialog Box Fields* table then continue.

**Table 3: Add Cloud Load Balancer Listener Dialog Box Fields**

Properties	Description
<b>Name</b>	Enter the name of the listener.
<b>Port</b>	Enter the port that the device will accept traffic on.
<b>Protocol</b>	Click to choose <b>HTTP</b> or <b>HTTPS</b> .
<b>Security Policy</b>	Click the drop-down list and choose a security policy (only available when <b>HTTPS</b> is chosen).

Properties	Description
<b>SSL Certificate</b>	<p>To choose an SSL certificate(only available when <b>HTTPS</b> is chosen):</p> <ol style="list-style-type: none"> <li>a. Click <b>Add SSL Certificates</b>.</li> <li>b. Click to place a check mark in the check box of the certificates you want to add.</li> <li>c. Choose a key ring: <ol style="list-style-type: none"> <li>1. Click <b>Select Key Ring</b>. The <b>Select Key Ring</b> dialog appears.</li> <li>2. From the <b>Select Key Ring</b> dialog, click to choose a key ring in the left column then click <b>Select</b>. The <b>Select Key Ring</b> dialog box closes.</li> </ol> </li> <li>d. Click the <b>Certificate Store</b> drop-down list and choose a certificate.</li> </ol> <p><b>Note</b> A listener can have multiple certificates.</p>
<b>Add Rule</b>	<p>To add rule settings to the device listener, click <b>Add Rule</b>. A new row appears in the <b>Rules</b> list an the <b>Rules Settings</b> fields are enabled.</p>



Properties	Description
Rule Settings	

Properties	Description
	<p>The <b>Rule Settings</b> pane contains the following options:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Enter a name for the rule.</li> <li>• <b>Host</b>—Enter a hostname to create a host-based condition. When a request is made for this hostname, the action you specify is taken.</li> <li>• <b>Path</b>—Enter a path to create a path-based condition. When a request is made for this path, the action you specify is taken.</li> <li>• <b>Type</b>—The action type tells the device which action to take. The action type options: <ul style="list-style-type: none"> <li>• <b>Return fixed response</b>—Returns a response using the following options: <ul style="list-style-type: none"> <li>• <b>Fixed Response Body</b>—Enter a response message.</li> <li>• <b>Fixed Response Code</b>—Enter a response code.</li> <li>• <b>Fixed response Content-Type</b>—Choose a content type.</li> </ul> </li> <li>• <b>Forward</b>—Forwards traffic using the following options: <ul style="list-style-type: none"> <li>• <b>Port</b>—Enter the port that the device will accept traffic on.</li> <li>• <b>Protocol</b>—Click to choose <b>HTTP</b> or <b>HTTPS</b>.</li> <li>• <b>Provider EPG</b>—The EPG with the web server that handles the traffic.</li> <li>• <b>EPG</b>—To choose an EPG: <ol style="list-style-type: none"> <li>a. Click <b>Select EPG</b>. The <b>Select EPG</b> dialog box appears.</li> <li>b. From the <b>Select EPG</b> dialog ox, click to choose an EPG in the left column then click <b>Select</b>. The <b>Select EPG</b> dialog box closes.</li> </ol> </li> </ul> </li> <li>• <b>Redirect</b>—Redirects requests to another location using the following options: <ul style="list-style-type: none"> <li>• <b>Redirect Code</b>—Click the <b>Redirect Code</b> drop-down list and choose a code.</li> </ul> </li> </ul> </li> </ul>

Properties	Description
	<ul style="list-style-type: none"> <li>• <b>Redirect Hostname</b>—Enter a hostname for the redirect.</li> <li>• <b>Redirect Path</b>—Enter a redirect path.</li> <li>• <b>Redirect Port</b>—Enter the port that the device will accept traffic on.</li> <li>• <b>Redirect Protocol</b>—Click to the <b>Redirect Protocol</b> drop-down list and choose <b>HTTP</b>, <b>HTTPS</b>, or <b>Inherit</b>.</li> <li>• <b>Redirect Query</b>—Enter a redirect query.</li> </ul> <p>Click <b>Add Rule</b> when finished.</p>

**Step 10** Click **Add** when finished.  
The service graph is deployed.

## Deploying a Service Graph Using the REST API

### Creating an Internal-Facing Load Balancer Using the REST API

This example demonstrates how to create an internal-facing load balancer using the REST API.

To create an internal-facing load balancer:

**Example:**

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />

    <cloudLB scheme="internal" type="application" name="alb-151-15" status="">
      <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus15/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]"/>
      </cloudLB>

    </fvTenant>
  </polUni>
```

### Configuring an Internet-Facing Load Balancer Using the REST API

This example demonstrates how to create an internet-facing load balancer using the REST API.

To create an internet-facing load balancer:

**Example:**

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">
    <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />

    <cloudLB scheme="internet" type="application" name="alb-151-15" status="">
      <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus15/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]"/>
    </cloudLB>

  </fvTenant>
</polUni>
```

## Creating a Service Graph Using the REST API

This example demonstrates how to create a service graph using the REST API.

To create a service graph:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">

    <vnsAbsGraph name="c15_g1" type="cloud" status="">
      <vnsAbsTermNodeProv name="p1">
        <vnsAbsTermConn/>
      </vnsAbsTermNodeProv>
      <vnsAbsTermNodeCon name="c1">
        <vnsAbsTermConn/>
      </vnsAbsTermNodeCon>
      <vnsAbsNode managed="yes" name="N1" funcType="GoTo">
        <vnsRsNodeToCloudLDev tDn="uni/tn-tn15/clb-alb-151-15"/>
        <vnsAbsFuncConn name="provider"/>
        <vnsAbsFuncConn name="consumer"/>
      </vnsAbsNode>
      <vnsAbsConnection connDir="consumer" connType="external" name="con1">
        <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeCon-c1/AbsTConn"/>
        <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-consumer"/>
      </vnsAbsConnection>
      <vnsAbsConnection connDir="provider" connType="internal" name="con2">
        <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeProv-p1/AbsTConn"/>
        <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-provider"/>
      </vnsAbsConnection>
    </vnsAbsGraph>

  </fvTenant>
</polUni>
```

## Attaching a Service Graph Using the REST API

This example demonstrates how to attach a service graph using the REST API.

To attach a service graph:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
  <fvTenant name="tn15">

    <vzBrCP name="c1">
      <vzSubj name="c1">
        <vzRsSubjGraphAtt tnVnsAbsGraphName="c15_g1"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>
```

## Configuring an HTTP Service Policy Using the REST API

This example demonstrates how to create an HTTP service policy using the REST API.

To create an HTTP service policy:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="http_listener1" port="80" protocol="http" status="">
            <cloudListenerRule name="rule1" priority="10" default="yes" status="">
              <cloudRuleAction type="forward" port="80" protocol="http"
                epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
            </cloudListenerRule>
            <cloudListenerRule name="redirectRule" priority="20">
              <cloudRuleCondition type="path" value="/img/*"/>
              <cloudRuleAction type="redirect" RedirectPort="8080"/>
            </cloudListenerRule>
            <cloudListenerRule name="FixedRspRule" priority="30">
              <cloudRuleCondition type="host" value="example.com"/>
              <cloudRuleAction type="fixedResponse" FixedResponseCode="200"/>
            </cloudListenerRule>
            <cloudListenerRule name="redirectHPRule" priority="40" status="">
              <cloudRuleCondition type="host" value="example.com"/>
              <cloudRuleCondition type="path" value="/img/*"/>
              <cloudRuleAction type="forward" port="80" protocol="http"
                epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
            </cloudListenerRule>
          </cloudListener>
        </cloudSvcPolicy>
      </vnsAbsNode>
    </vnsAbsGraph>
```

```
</fvTenant>
</polUni>
```

## Configuring a Key Ring Using the REST API

This example demonstrates how to configure a key ring using the REST API. For more information about key ring configuration, see the *Cisco APIC Basic Configuration Guide*.

To configure a key ring:

```
<polUni>
  <fvTenant name="tn15" >
    <cloudCertStore>
      <pkiKeyRing status="" name="lbCert" tp="lbTP" key="-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA4DGxaK+RHv/nToHLnmDBq2BfLimgX/zNJC9bGuzr8Mj7dm0
XuHfQYGv0h1PtL4Pdx5f5qjB0NBHjAVB1Gw8cDiErEgAXy9Km27ySo2foKryNqCRE
Ginn/CgF75QPfEd568eScNDZPt/eMeHAuRX/PykKUatWWncGanJvHqc+SOLPF6TD
gQ5nwOHFFvym2DY8bfYWrWmGsO7JqZzbPMptA2QWb1ILsSoIrdkI Igf6ZfyY/EN
bH+nYN2rJT81zYszz0YmR0oRQHTiN2NiDY/ZV63yxCXfLg9qpNZCuD8KOfdCZPEq
8takiWBxiR5/HRPscWAdWQsoiKgG1k4NEbFA9QIDAQABAoIBAQQDQqA9IslYrdtqN
q6mZ3s2BNfF/4kgb7gn0Dws+9EJJLCJNZVhFEo2ZxxyfPp6HRnjYS50W83/E1anD
+GD1bSucTuxqFIQVh7r1ebYZIWK+NYSjr5yNVxux8U2hCNV8WWVqkJjKcUqICB
Bm47FKj53LV46ze0gyCaibFrYxZJ9+farGneyBdnoV+3thmez7534KCi0t3J3Eri
lgSY3ql6hPXB2ZXAP4jdAoLgWDU4I1M6OqOiWopZM/QYIE/WtPYyJ0QzNCXObtc5
FboDcvedsgd4x5G1fV2A4xTBQMCTZUZJ9fyAcFogTZXD+UVqxorh47tf/mz+1fjq
f1XphED1AoGBAPVlvkFGW46qqRnYovfryxxz40M1sVsgcJpQTQtBQi2koJ8OwEZJ
2s+CX0r+oDqwP23go/QEVYVkcic9RGkJBNGel+dm/bTjzgmQYtqSCNtecTsZD5JN
yljkciiZznDkjcjReS22kh3dGXIBRiYk7ezp2z7EKfDrHe5x5ouGMgCnAoGBAOnh
buDEohv8KJJaB+DiUfhtoa3aKNPBO+zWPCHP0HFGjPXshJcIYZc1GycyumuDKVnNd
MxhE/yOnQHowi4T9FMLpz5yh5zucUVqOBgB1P6Mzbc5t5MtLrEYr/AqFN11CqyXQ
cVcT6iCW1OAFJRW3c/OiESwLMzchsl8RnbwOie6kDAoGBANv1zmPb07zB3eGTCU0t
KGIqWFLncUkVaDZRFZYPPnwiRkoe73j9brkNbgCqx+NLP5UjoeFry0N6y106q/
ZA4I7FnXryLBW2HYu41Vix1+XOZ/HeO3RmFN1z717dGmaGbv43aKIB9x+X5n8wF
6z1NtBhmBk7yNwomlRaglsbAoGAX0p4cJ/tJNXSe7AswHDQCL68uimJddfz5nKG
k83nE+Qc0qQozDJAmCiSfmuSNRnSep3FiafjBFXK0X4h+mdBJC7bagRnI92Mh0X
mOwsp4P2GdywkZwdbuHQ6UBp1Ferf9aztZtn+as6xKOUATEezy9DK9zMWzQhhtaY
m9yZTp0CgYEA1UtcpWjAzQbXODJGmxGdAAakPpeiKw/Da3MccrTdGJt88ezM1Oej
Pdoab0G2PcfGjZotSGk7N4XARVKeq7pgZ0kwcYAsh06A2Hal+D1z/bGoZP+kmD/x
Ny82phxVOXCNc5Vv921U59+j7e067UFLAYJe6fu+oFImvofRnP4DIQ=
-----END RSA PRIVATE KEY-----" cert="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBACTCFNBhbiBk3N1MRIWEAYDVQQK
Ew1NeUNvbXBhbnkxDjAMBGNVBA5TBU15T3JnMRgwFgYDVQDFA8qLmFtYXpvbM3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEWEXJhbXNoYWhAY21zY28uY29tMB4XDTE4MTA
wMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjI
wMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTM
wNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV
0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xM
jE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4
MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTM
wMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwM
jIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjI
wMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwMTMwNV0xMjE4MTMwMjIwM
T3JnMRgwFgYDVQDFA8qLmFtYXpvbM3cy5jb20xIDAeBgkqhkiG9w0BCQEWEWEX
JhbXNoYWhAY21zY28uY29tggkApY20n/9qsGwwDAYDVR0TBAUuAwEB/zANBgkqhkiG
9w0B
```





**Note** A listener can have multiple certificates. The certificate options are:

- ELBSecurityPolicy-2016-08 – The default when no security policy is chosen.
- ELBSecurityPolicy-FS-2018-06
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-2-Ext-2018-06
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2015-05
- ELBSecurityPolicy-TLS-1-0-2015-04

If you use multiple certificates, you must specify the default certificate. The default is specified using the **defaultCert** property in **cloudRsListenerToCert**.

### Before you begin

You have already configured a key ring certificate.

To create an HTTPS service policy:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="https_listener" port="443" protocol="https"
secPolicy="eLBSecurityPolicy-2016-08" status="">
            <cloudRsListenerToCert defaultCert="yes" certStore="default"
tDn="uni/tn-t2/certstore/keyring-lbCert" status=""/>
              <cloudListenerRule name="defaultRule" default="yes" priority="100" status="">
                <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t1/cloudapp-ap/cloudepg-ep1">
                  </cloudRuleAction>
                </cloudListenerRule>
              </cloudListener>
            </cloudSvcPolicy>
          </vnsAbsNode>
        </vnsAbsGraph>
      </fvTenant>
    </polUni>
```