



Deploying Microsoft Office Live Communications Server 2005 and the F5 BIG-IP System

- Introducing the BIG-IP and Live Communications Server 2005 Enterprise Edition configuration
- Configuring the BIG-IP and Live Communications Server for deployment
- Using Access Proxy and Director with the BIG-IP system for remote access
- Appendix A: Backing up and restoring the BIG-IP system configuration

Introducing the BIG-IP and Live Communications Server 2005 Enterprise Edition configuration

Microsoft® and F5 have collaborated on a highly effective way to intelligently direct traffic for Microsoft Office Live Communications Server 2005 Enterprise Edition with the F5 BIG-IP® application traffic management device. Microsoft and F5 Networks have conducted interoperability testing between the BIG-IP system and Microsoft Live Communications Server 2005. Organizations using the BIG-IP system benefit from mission-critical availability, intelligent traffic management, simple scalability, and enhanced security for Live Communications Server deployments.

Live Communications Server provides organizations with voice, video, chat, and an extensible platform that connects people, information, and business processes—enabling better decisions faster. With a familiar user experience integrated into Microsoft Office System programs, Live Communications Server allows people to communicate without the constraints of geography, office location, or time zone.

For more information on Live Communications Server, see <http://www.microsoft.com/livecomm>.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The BIG-IP system must be running version 4.5 or later (the step-by-step configuration procedures in this Deployment Guide are for 4.5 or later, but do not include configuration steps for BIG-IP version 9.0 and later).
- ◆ The Live Communications Server must be running the 2005 Enterprise Edition.
- ◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing this configuration.

◆ Note

This document is written with the assumption that you are familiar with both the BIG-IP system and the Live Communications Server 2005. For more information on configuring these products, consult the appropriate documentation.

Configuration example

The Live Communications Server 2005 Enterprise Edition introduces the concept of a pool. Multiple Live Communications Servers communicate with a single back-end SQL Server. **Pool** is used to describe this collection of multiple Live Communications Servers tied to a single back-end. Users are now homed to a pool as opposed to individual Live Communications Servers. This allows users to login using any Live Communications Server in a pool. Pools allow flexibility by increasing the capacity of the service by adding more Live Communications Servers on the fly. Failure of one or more Live Communications Servers will have a minimal effect on service availability, as the load is balanced between the remaining Live Communications Servers.

This configuration example shows a typical configuration with a BIG-IP system and Microsoft Live Communications Server. With multiple Live Communications Servers in a Pool there is now a need for distributing the incoming session requests among the Live Communications Servers. Figure 1.1 shows how a BIG-IP device is located in front of a pool of Live Communications Servers.

◆ Tip

Although only one BIG-IP device is necessary for this configuration, we strongly recommend a redundant BIG-IP device for the highest level of availability.

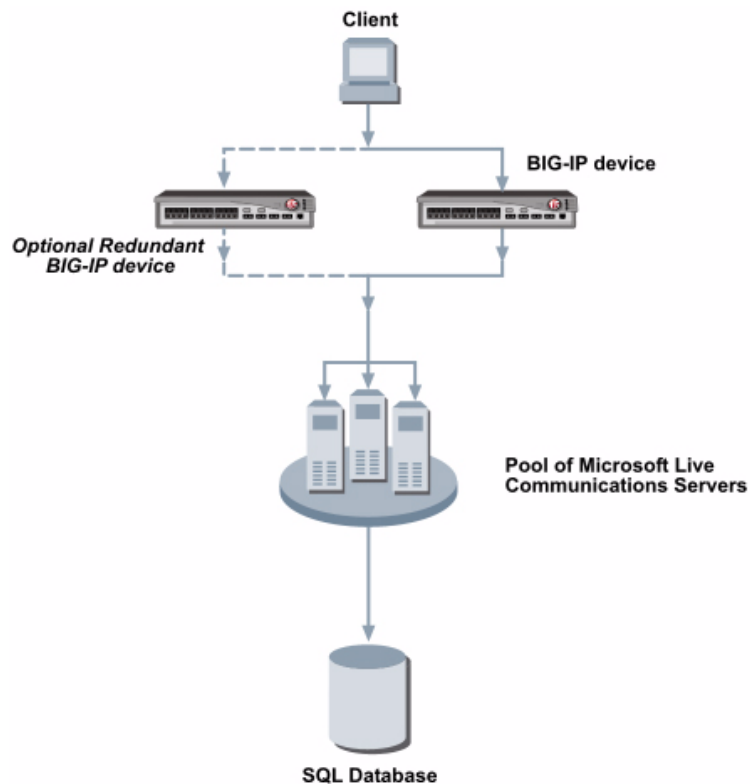


Figure 1.1 BIG-IP Live Communications Server logical configuration

Configuring the BIG-IP and Live Communications Server for deployment

To configure the BIG-IP and Live Communications Server for integration, you need to complete the following procedures:

- *Connecting to the BIG-IP device*
- *Creating a VLAN*
- *Creating a self IP*
- *Creating pools*
- *Creating virtual servers*
- *Creating a default SNAT*
- *Configuring a health monitor*
- *Synchronizing the BIG-IP configuration if using a redundant system*

◆ Tip

*We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. To save your BIG-IP configuration, see **Appendix A: Backing up and restoring the BIG-IP system configuration**, on page 1-40.*

The BIG-IP system offers both Web-based and command line configuration tools, so that users can work in the environment that they are most comfortable with. This Deployment Guide contains procedures to configure the BIG-IP system using both the BIG-IP Web-based Configuration utility using a browser and the BIG-IP **bigpipe** command line interface. Unless you are familiar with using the **bigpipe** command line interface, we recommend using the Configuration utility.

Connecting to the BIG-IP device

The first step in this configuration is to connect to the BIG-IP system. You can connect to the BIG-IP system using the Configuration utility or the command line.

Connecting to the BIG-IP device using the Configuration utility

Use the following procedure to access the BIG-IP Web-based Configuration utility using a Web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the BIG-IP device>
A Security Alert dialog box appears, click **Yes**.
The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
The Configuration Status screen opens.

Once you are logged onto the BIG-IP system, the initial screen, called the Configuration Status page, opens. From the Configuration status page, you can access the Configuration utility, documentation such as manuals and release notes, and software downloads.
3. From the Configuration Status screen, click **Configure your BIG-IP (R) using the Configuration utility**.
The Configuration utility opens to the Network Map screen.

Connecting to the BIG-IP device using the bigpipe command line interface

You can access the **bigpipe** command line utility on a BIG-IP system with connections for a monitor and keyboard. For a system without a monitor and keyboard attached, like the IP Application Switch, you can access **bigpipe** through an SSH shell from a remote administrative host. For specific information on how to access **bigpipe** through an SSH shell, consult the *BIG-IP Reference Guide*.

Creating a VLAN

A VLAN is a grouping of separate networks that allows those networks to behave as if they were a single local area network, whether or not there is a direct ethernet connection between them.

The next step in this configuration is to create a VLAN on the BIG-IP system. You can create a VLAN from the Configuration utility or the command line.

To create a VLAN on the BIG-IP system using the Configuration utility

1. On the navigation pane, click **Network**.
The Network screen displays the VLAN list.
2. Click the **Add** button.
The Add VLAN dialog box opens.
3. In the **VLAN Name** box, type a name for the VLAN.
In our example, we type **lcs_vlan**.
4. In the **Tag** box, type the tag for the VLAN. If you do not know the tag, check with the system administrator.
In our example, we use **4091**.

5. In the **Resources** section, select the interface that will have access to tagged traffic, and click the **tagged >>** button.
In our example, we select **1.15**.
6. Click the **Done** button.
The new VLAN appears in the list. See Figure 1.2.

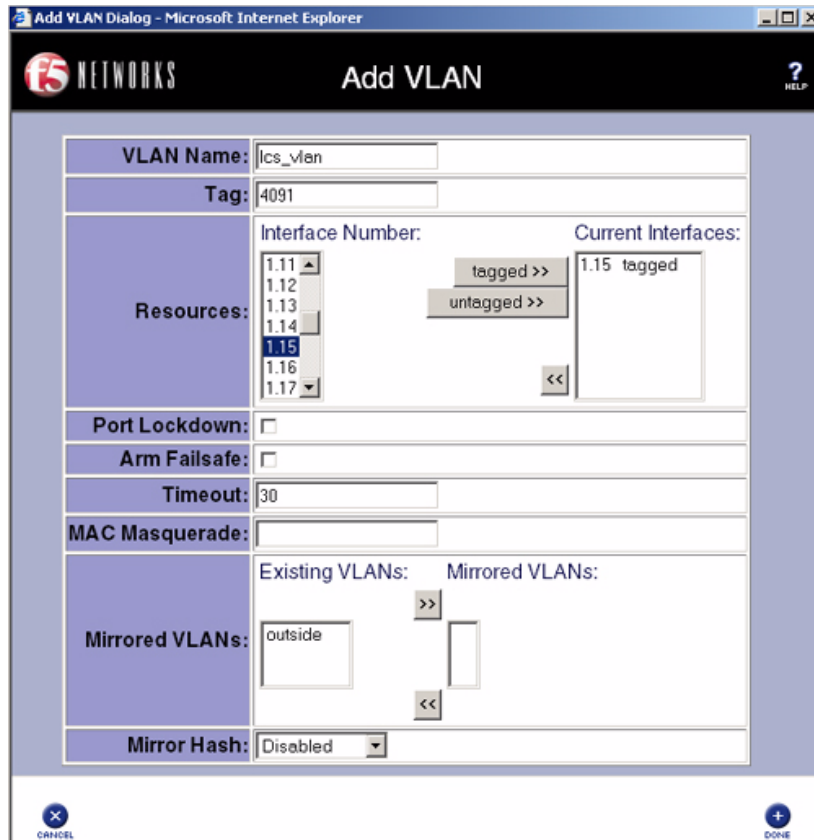


Figure 1.2 Adding a VLAN in the BIG-IP Configuration utility

To create a VLAN tag from the command line

1. To create a VLAN that supports tag-based access from the command line, use the following syntax:
b vlan <vlan name> tag <xxxx>
In our example, we use:
b vlan lcs_vlan tag 4091
2. The next step is to add the interface to the VLAN **lcs_vlan** as a tagged interface. This is done by specifying the VLAN name, the **tagged** keyword, and the interfaces to be tagged:
b vlan <vlan name> interfaces add tagged <x.x>
In our example, we use:
b vlan lcs_vlan interfaces add tagged 1.15

Creating a self IP

Self IP addresses are the IP addresses owned by the BIG-IP system that you use to access the internal and external VLANs. The next step in this configuration is to create a self IP address for the VLAN we created in the preceding procedure.

To create a self IP address using the Configuration utility

1. On the navigation pane, click **Network**.
The Network screen displays the VLAN list.
2. Click the Self IP Addresses tab.
The self IP addresses screen opens.
3. Click the **Add** button.
The Add Self IP Address dialog box opens.
4. In the **IP Address** box, type a static IP address in the VLAN you created in the preceding procedure. Note that this needs to be on the same network as the Live Communications Server devices.
In the Netmask box, type the corresponding subnet mask. The Broadcast address is automatically calculated.
In our example, we use **10.10.10.1** with a Netmask of **255.255.255.0**.
5. In the **SNAT Automap** section, click the box to enable **SNAT Automap**. With SNAT automap enabled, the BIG-IP device uses the self IP addresses in place of the client IP address, ensuring that responses from servers arrive back at the BIG-IP device.
6. In the VLAN section, select the VLAN you created in the *Creating a VLAN* procedure.

7. Click the **Done** button.
The new self IP address appears in the list.



Figure 1.3 Adding a self IP address in the BIG-IP Configuration utility

To create a self IP on the BIG-IP system using the command line

1. To create a self IP address on the BIG-IP system, use the following syntax

```
b self <IP address> VLAN <VLAN Name>
```

In our example, we use:

```
b self 10.10.10.1 VLAN lcs_vlan
```

Creating pools

The BIG-IP system also uses the term *pool* for a group of devices. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. You must create a separate pool for each service on which there will be traffic. In this configuration, we configure three pools on the BIG-IP device that contain the Live Communications Servers, one for TLS (Transport Layer Security) traffic, one for RPC (Remote Procedure Call) traffic, and one for IP forwarding.

Creating the TLS pool

The first pool we create is for TLS traffic. You can create this pool from the Configuration utility or the command line.

To create a pool from the Configuration utility

1. In the navigation pane, click **Pools**.
The Pools screen opens.
2. Click the **Add** button.
The Add Pool screen opens.
3. In the **Pool Name** box, enter a name for your pool.
In our example, we use **tls_pool**.
4. In the **Load Balancing Method** box, enter your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).

For this configuration, we recommend selecting Least Connections. In Least Connections mode, the BIG-IP system passes a new connection to the node that has the least number of current connections. Least Connections mode works best in environments where the servers or other equipment you are load balancing have similar capabilities. Using Live Communications Server, traffic from servers to clients is roughly the same on each connection.

5. In the **Resources** section, you add the Live Communications Servers to the pool.
 - a) In the **Member Address** box, type the IP address of the Live Communications Server.
In our example, we type **10.10.10.11**.
 - b) In the **Service** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list (for example **5061**). In our example, we type **5061**, the port for TLS traffic.
 - c) The **Member Ratio** and **Member Priority** boxes are optional.
 - d) Click the Add button (>>) to add the member to the **Current Members** list.
 - e) Repeat steps a-d for each Live Communications Server you want to add to the pool. In our example, we repeat these steps twice for the other two Live Communications Servers (**10.10.10.12** and **10.10.10.13**). See Figure 1.4.
6. In the **Enable NAT** section, click to clear the box.
7. In the **Enable SNAT** section, click to clear the box.
8. The other fields in the Add Pool screen are optional. Configure these fields as applicable for your network. (For additional information about configuring a pool, click the **Help** button.)

9. Click the **Done** button.

Member Address:	Service:	Member Ratio:	Member Priority:	Current Members:
10.10.10.13	5061			10.10.10.11:5061 r1 p1 10.10.10.12:5061 r1 p1 10.10.10.13:5061 r1 p1
or choose...	or choose...			

Figure 1.4 Adding a pool for TLS traffic in the BIG-IP Configuration utility

To create the TLS pool from the command line

To create the pool from the command line, use the following syntax

```
b pool <pool name> { [lb_method <load balancing method>] member <IP address>:<port> [nat disable snat disable] }
```

In our example,:

```
b pool tls_pool { lb_method least_conn member 10.10.10.11:5061 member 10.10.10.12:5061 member 10.10.10.13:5061 nat disable snat disable }
```

Creating the RPC pool

The next step is to create a pool for RPC traffic. Again, you can create the pool from the Configuration utility or from the command line.

To create a pool from the Configuration utility

1. In the navigation pane, click **Pools**.
The Pools screen opens.
2. Click the **Add** button.
The Add Pool screen opens.
3. In the **Pool Name** box, enter a name for your pool.
In our example, we use **rpc_pool**.
4. In the **Load Balancing Method** box, enter your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).

For this configuration, we recommend selecting Least Connections. In Least Connections mode, the BIG-IP system passes a new connection to the node that has the least number of current connections. Least Connections mode works best in environments where the servers or other equipment you are load balancing have similar capabilities.

5. In the **Resources** section, you add the device to the pool.
 - a) In the **Member Address** box, type the IP address of the Live Communications Server device.
In our example, we type **10.10.10.11**.
 - b) In the **Service** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list (for example **135**). In our example, we type **135**, the default port for **RPC**.
 - c) The **Member Ratio** and **Member Priority** boxes are optional.
 - d) Click the Add button (>>) to add the member to the **Current Members** list.
 - e) Repeat steps a-d for each Live Communications Server you want to add to the pool. In our example, we repeat these steps twice for the other two Live Communications Servers (**10.10.10.12** and **10.10.10.13**).
6. In the **Enable NAT** section, click to clear the box. For the RPC pool, leave the **Enable SNAT** box checked (see Figure 1.5).

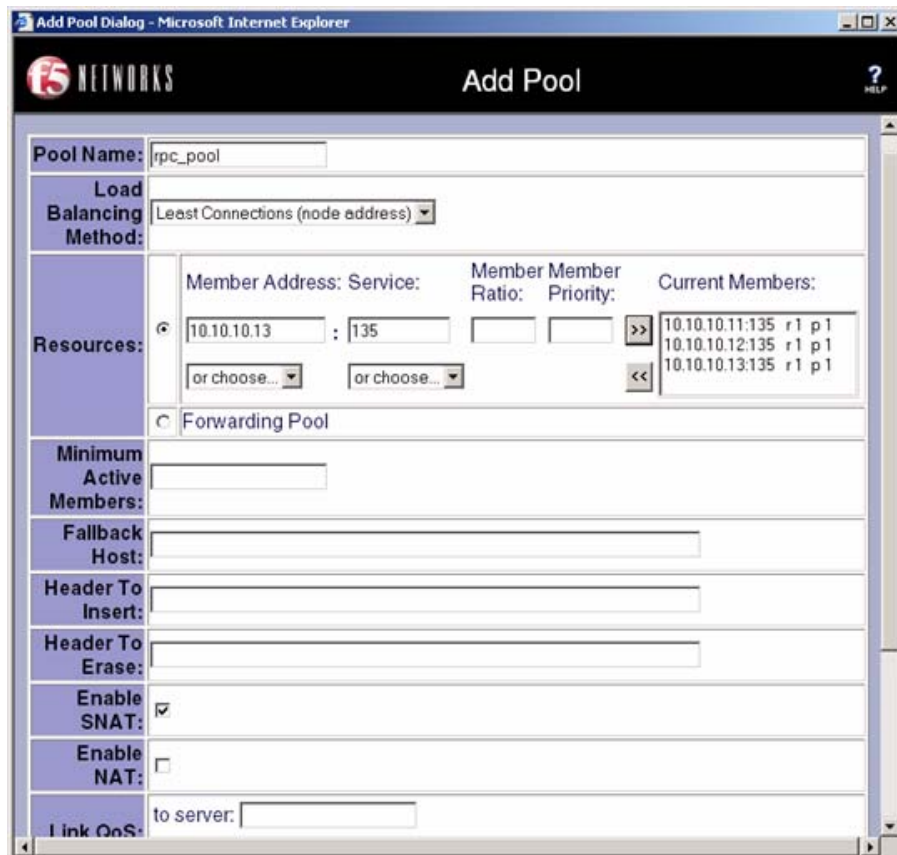


Figure 1.5 Adding a pool for RPC traffic in the BIG-IP Configuration utility

7. The other fields in the Add Pool screen are optional. Configure these fields as applicable for your network. (For additional information about configuring a pool, click the **Help** button.)
8. Click the **Done** button.

To create the RPC pool from the command line

To create this pool from the command line, use the following syntax

```
b pool <pool name> { [lb_method <load balancing method>] member <IP address>:<port> nat
  disable }
```

In our example, we type:

```
b pool rpc_pool { lb_method least_conn member 10.10.10.11:135 member 10.10.10.12:135
  member 10.10.10.13:135 nat disable }
```

Creating the Forwarding pool

The last pool in this configuration is a Forwarding pool. In this configuration, we create the Forwarding pool to enable cross-pool communications as well as load balancing of certain management operations.

To configure the IP forwarding pool from the Configuration utility

1. In the navigation pane, click **Pools**.
The Pools screen opens.
2. Click the **Add** button.
The Add Pool screen opens.
3. In the **Pool Name** box, enter a name for your pool.
In our example, we use **fwd_pool**.
4. In the **Load Balancing Method** box, leave the setting at Round Robin. As this is a forwarding pool, the load balancing method does not apply.
5. In the **Resources** section, click the **Forwarding Pool** option button.
6. In the **Enable NAT** section, click to clear the box.
7. In the **Enable SNAT** section, click to clear to the box (see Figure 1.6).
8. Click the **Done** button.

The screenshot shows the 'Add Pool' configuration window. The 'Pool Name' is 'fwd_pool'. The 'Load Balancing Method' is set to 'Round Robin'. In the 'Resources' section, the 'Forwarding Pool' radio button is selected and circled in blue. Below this, the 'Enable SNAT' and 'Enable NAT' checkboxes are also circled in blue. Other fields include 'Minimum Active Members', 'Fallback Host', 'Header To Insert', 'Header To Erase', 'Link QoS', 'IP ToS', and 'Clone Pool'.

Figure 1.6 Adding the Forwarding Pool in the Configuration utility with NAT and SNAT disabled

To create the Forwarding pool from the command line

To create the Forwarding pool from the command line, type the following command:

```
pool fwd_pool { forward nat disable snat disable }
```

Creating virtual servers

A virtual server with its virtual address is the visible, routable entity through which the Live Communications Servers in a load balancing pool are made available to the client.

The next step in this configuration is to define virtual servers that reference the pools. As with a pool, you must create a virtual server for each service. Again, you can define virtual servers from the Configuration utility or the command line.

Creating the TLS virtual server

The first virtual server we create references the **tls_pool** we created earlier.

To create the TLS virtual server using the Configuration utility

1. In the navigation pane, click **Virtual Servers**.
The Virtual Servers screen opens.
2. Click the **Add** button.
The Add Virtual Server screen opens.
3. Enter the IP address and service for the virtual server, and then click the **NEXT** button.
In our example, we use **192.168.10.16** with service of **5061**.
The Configure Basic Properties screen opens.
4. In the **Enable Reset on Timeout** section, click to clear the box.
Click the **NEXT** button.
The Select Physical Resources screen opens.
5. Click the **Pool** option button, and from the list, select the pool you created in the *Creating the TLS pool* section above.
In our example, we select **tls_pool** (see Figure 1.7).

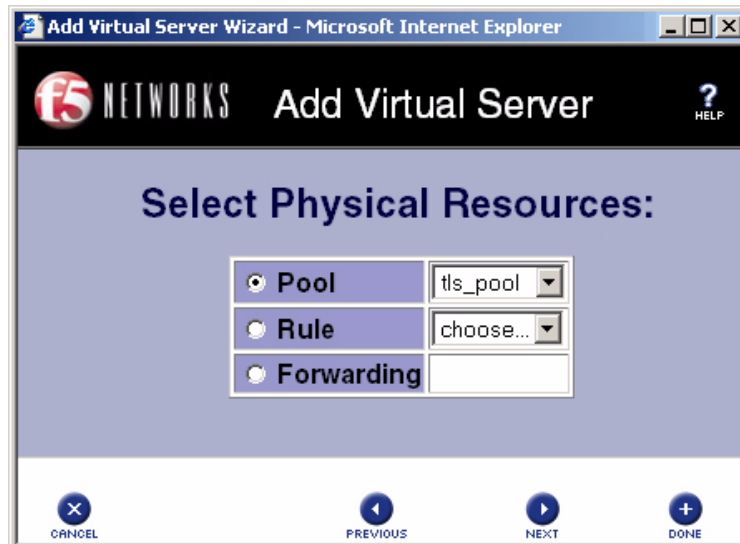


Figure 1.7 Selecting the **tls_pool** while creating the virtual server

- Click the **Done** button.
For additional information about configuring a virtual server, click the **Help** button.

To view the newly created virtual server, click the virtual server in the virtual server list. In our example, our virtual server properties are shown in Figure 1.8.

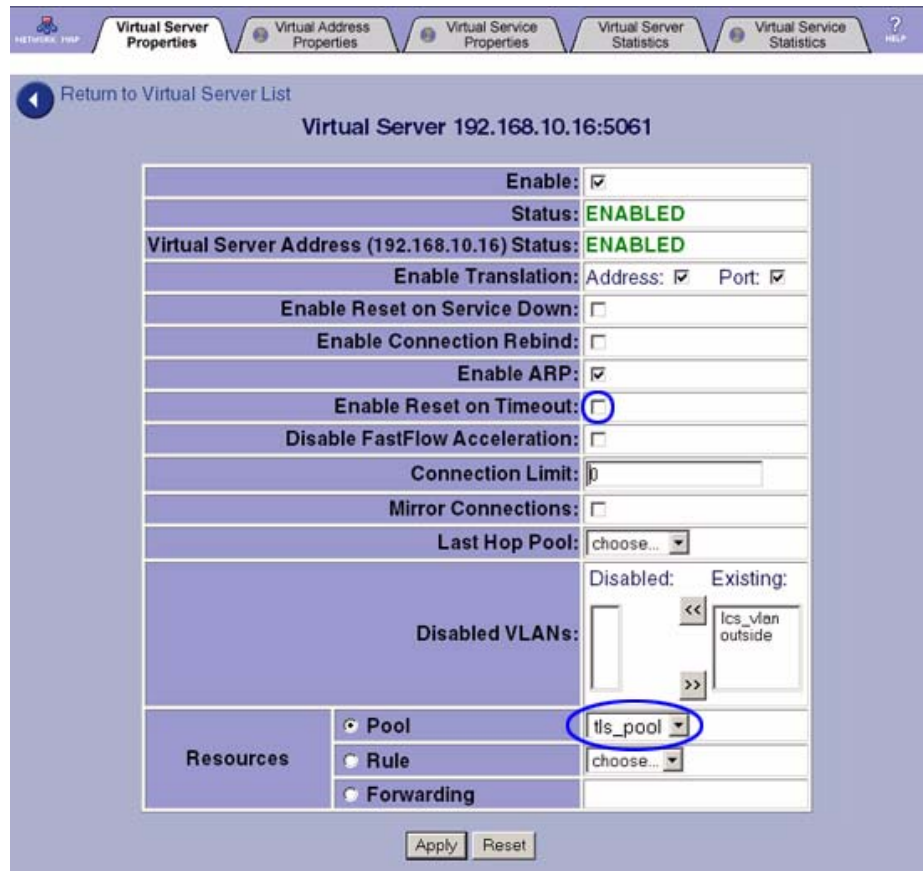


Figure 1.8 The TLS virtual server in the BIG-IP Configuration utility.

To create the TLS virtual server from the command line

Use the bigpipe **virtual** command as shown below. You can use standard service names in place of port numbers. If you have DNS configured, you can also use host names in place of IP addresses.

```
b virtual <virtual IP address>:<port> use pool <pool_name> [timeout resets disable]
```

In our example, we use:

```
b virtual 192.168.10.16:5061 use pool tls_pool timeout resets disable
```

Creating the RPC virtual server

The next virtual server references the **rpc_pool**.

To create the RPC virtual server using the Configuration utility

1. In the navigation pane, click **Virtual Servers**.
The Virtual Servers screen opens.
2. Click the **Add** button.
The Add Virtual Server screen opens.
3. Enter the IP address and service for the virtual server, and then click the **NEXT** button.
In our example, we use **192.168.10.17** with service of **135**.
The Configure Basic Properties screen opens.
4. In the **Enable Reset on Timeout** section, click to clear the box.
Click the **NEXT** button.
The Select Physical Resources screen opens.
5. Click the **Pool** option button, and from the list, select the pool you created in the *Creating the RPC pool* section above.
In our example, we select **rpc_pool**.
6. Click the **Done** button.
For additional information about configuring a virtual server, click the **Help** button.

To create the RPC virtual server from the command line

Use the bigpipe **virtual** command as shown below. You can use standard service names in place of port numbers. If you have DNS configured, you can also use host names in place of IP addresses.

```
b virtual <virtual IP address>:<port> use pool <pool_name> [timeout resets disable]
```

In our example, we use:

```
b virtual 192.168.10.17:135 use pool rpc_pool timeout resets disable
```

Creating a wildcard virtual server for the Forwarding pool

The final virtual server in this configuration is a wildcard virtual server and references the **fwd_pool**. We recommend you configure this pool from the Configuration utility.

To create a virtual server for the Forwarding pool

1. In the navigation pane, click **Virtual Servers**.
The Virtual Servers screen opens.
2. Click the **Add** button.
The Add Virtual Server screen opens.

- In the IP address section, enter **0.0.0.0** to specify a wildcard virtual server.
In the Service section, enter **0** to specify a wildcard service for the virtual server, and then click the **NEXT** button.
The Associate Wildcard VLAN screen opens.

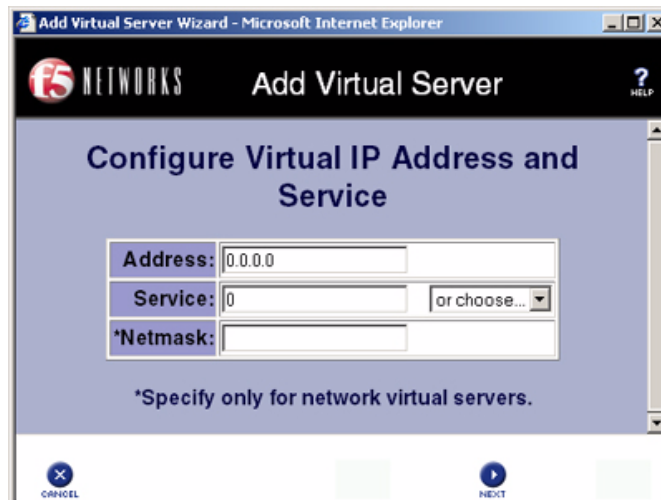


Figure 1.9 Configuring the wildcard virtual server

- Leave the VLAN box at **all**, and click the **Next** button.
The Configure Basic Properties screen opens.
- In the **Enable Address Translation**, **Enable Port Translation**, and **Enable ARP** sections, click to clear the boxes to disable Address and Port Translation, and ARP, and then click the **Next** button.
- Click the **Pool** option button, and from the list, select the pool you created in the *Creating the Forwarding pool* section above.
In our example, we select **fwd_pool**.
- Click the **Done** button.
You return to the Virtual Server list.
- From the Virtual Server List screen, click the **0.0.0.0:0** virtual server you just created.
The Virtual Server Properties screen opens.
- Click the Virtual Address Properties tab.
The Global Virtual Address 0.0.0.0 screen opens.
- In the **Any IP Traffic** section, click a check in the **Enable** box.
- Click the **Apply** button.
- Click the Virtual Service Properties tab.
The Global Virtual Service 0 properties screen opens.
- In the **TCP Enabled** and **UDP Enabled** sections, make sure there are checks in both boxes. If either box does not have a check, click a check in the appropriate box.

14. Click the **Apply** button.

Creating a default SNAT

A secure network address translation (SNAT) provides the ability to perform certain Live Communications Server pool-level management operations from the servers in the pool.

To create a default SNAT from the Configuration utility

1. From the navigation pane, click **NATs**.
The NAT screen opens.
2. Click the SNATs tab.
The SNAT screen opens.
3. Under **Current List**, check to see if a default SNAT is present.
 - If a default SNAT is not present, use the following procedure:
 - a) Click the **Add Default** button in the upper left portion of the screen.
The Add Default SNAT dialog box opens.
 - b) In the **Translation** section, click the **Automap** option button to select Automap.
 - c) Click the **Done** button.
 - If a default SNAT is present, make sure that the **SNAT Address** is set to **Auto**.

Configuring a health monitor

The next step in this configuration is to configure a health monitor on the BIG-IP system for the Live Communications Servers. We use the template for the TCP Extended Content Verification (ECV) monitor to create the monitor.

For this monitor, the TCP timeout for the **5061** service needs to be set to a value greater than the maximum Registration Timeout refresh interval configured in Live Communications Server global settings. This is necessary to ensure that a Registration Timeout refresh occurs before the BIG-IP system terminates a TCP connection due to inactivity.

We recommend you configure the health monitor from the Configuration utility. For information on how to configure the health monitor from the command line, see the ***BIG-IP Reference Guide***.

To configure a health monitor using the BIG-IP Configuration utility.

1. In the navigation pane, click **Monitors**.
The Network Monitors screen opens.

2. Click the **Add** button.
The Add Monitor dialog box opens.
3. In the Add Monitor screen, type the name of your monitor (it must be different from the monitor template name), in our example, we type **sip_monitor**.
In the **Inherits From** box, select the **tcp** monitor template from the list. Click the **Next** button.

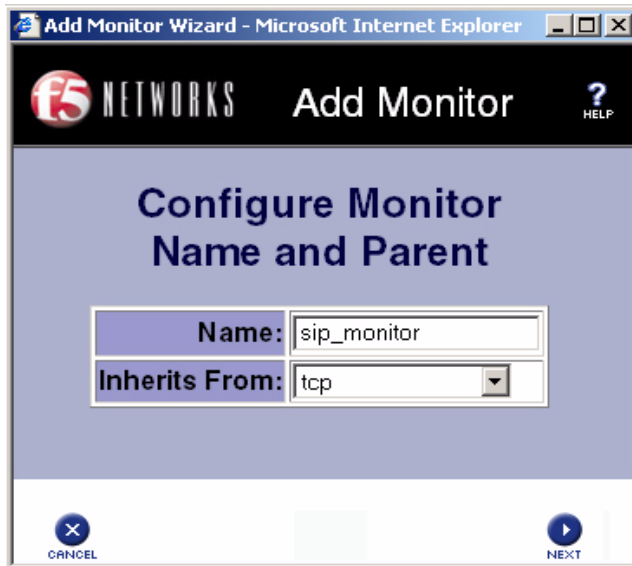


Figure 1.10 Creating the SIP monitor in the BIG-IP Configuration utility

4. In the Configure Basic Properties section, in the **Interval** box, type **10**, for a 10 second interval. In the **Timeout** box, type a value that is greater than the default maximum for a Registration Timeout refresh in the Live Communications Server global settings.
In our example, we type **32**, for a 32 second timeout.
Click the **Next** button.
The Configure ECV TCP Monitor screen opens.
5. Click the **Next** button again.
The Configure Destination Address and Service (Alias) screen opens.
6. In the **Destination Service** box, type **5061** (see Figure 1.11), and then click the **Done** button.
The Add Monitor dialog box closes, and you return to the Network Monitors screen.

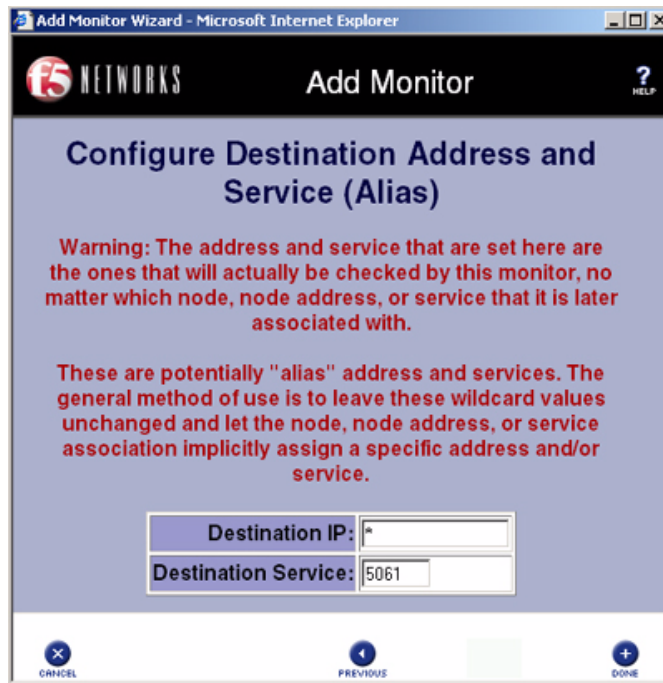


Figure 1.11 Configuring the Destination service for the monitor

7. From the Network Monitors screen, click the Basic Associations tab.
The Basic Association screen opens.
8. In the **Node Address** section, from the list, select the name of the monitor you created in Step 3. In our example, we select **sip_monitor**.
9. In the Node Address column, locate the Live Communications Server nodes, and click a check in the **Add** box for each node.

In our example, we check the Add box for the **10.10.10.11**, **10.10.10.12**, and **10.10.10.13** Node Addresses.

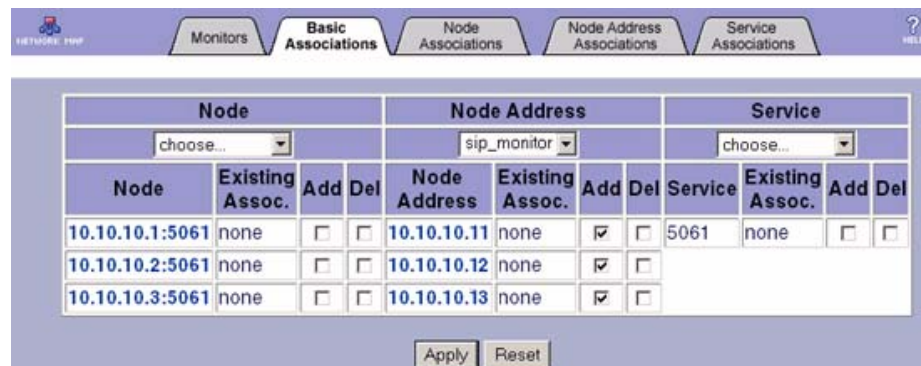


Figure 1.12 Monitors - Basic Associations tab showing the sip_monitor associations

-
10. Click **Apply**.

You now see the **sip_monitor** in the Existing Associations column of the **Node Address** section for each of the Live Communications Servers (as in Figure 1.13).

Node Address			
choose...			
Node Address	Existing Assoc.	Add	Del
10.10.10.11	sip_monitor	<input type="checkbox"/>	<input type="checkbox"/>
10.10.10.12	sip_monitor	<input type="checkbox"/>	<input type="checkbox"/>
10.10.10.13	sip_monitor	<input type="checkbox"/>	<input type="checkbox"/>

Figure 1.13 Live Communications Server nodes associated with the *sip_monitor*

For additional information associating a monitor, click the **Help** button.

Synchronizing the BIG-IP configuration if using a redundant system

If you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

To synchronize the configuration using the Configuration utility

1. In the navigation pane, click **System**.
The Network Map screen opens.
2. Click the Redundant Properties tab.
The Redundant Properties screen opens.
3. Click the **Synchronize Configuration** button.

To synchronize the configuration from the command line

Synchronize the configuration from the command line using the **bigpipe config sync** command:

```
bigpipe config sync all
```

The **bigpipe config sync all** command synchronizes the following configuration files:

- The common **bigdb** keys
- All files in **/config** (except **bigip_base.conf**)

Use the **bigpipe config sync** command without the all option to synchronize only the boot configuration file **/config/bigip.conf**.

◆ **Important**

If you have a redundant BIG-IP configuration (active-active or active-standby), you must also perform the first two procedures (Creating a VLAN and Creating a self IP) on both devices. The rest of the procedures only need to be performed on one BIG-IP device. The first two procedures are not included in the items that are synchronized between the BIG-IP devices.

Using Access Proxy and Director with the BIG-IP system for remote access

The Live Communications Server 2005 product allows the network of an organization to federate (peer) with other Live Communications Server-enabled networks for core presence and instant messaging.

This feature is enabled using a proxy server, Microsoft® Office Live Communications Server 2005 Access Proxy, using TLS/MTLS (Mutually Authenticated Transport Layer Security) for connections on both internal and external interfaces. Outside legs and inside legs are designated by different IP addresses, on two separate Network Interface Cards (NICs) or both addresses on the same NIC.

The Access Proxy functions as a reverse-proxy operation, when outside users (users of an enterprise outside the enterprise's network) need access into the enterprise's internal Live Communications Server service. Employees traveling, or working from home or in remote offices, can use the 'outside user' mode to remotely access the service.

A Microsoft® Office Live Communications Server 2005, **Director** is a Live Communications Server 2005 device with no locally homed users that communicates with the Access Proxy to provide additional security for the internal network. The Director authenticates and authorizes external SIP traffic coming from the Access Proxy to prevent unauthenticated traffic from reaching the internal Live Communications Servers.

Access Proxies and Directors can be connected in tandem to provide scalability and availability. The distribution of new connections and routing of traffic on existing connections is performed using a BIG-IP system.

The Access Proxy is the entry point into the enterprise Live Communications Server deployment. Its main role is to secure the internal network, these are some of the tasks performed by the Access Proxy:

- The Access Proxy performs connection management.
- Only TLS connections are accepted for connections from remote users and MTLS connection from federated servers.
- The Access Proxy ensures that when receiving a message from a server, it is from a well known server that has been configured by the administrator.
- The Access Proxy also blocks all messages coming from domains on its block list.

For specific information on how to configure the Access Proxy or Director devices, see the Microsoft documentation.

◆ **Important**

This section is only necessary if your configuration contains Access Proxy devices to allow remote users to use the internal Live Communications Server system.

◆ **Note**

*More than one Access Proxy device in a cluster is called a **Array**.*

Configuration example

In this configuration, there are BIG-IP devices on both sides of the array of Access Proxy devices, to direct traffic for inbound and outbound traffic.

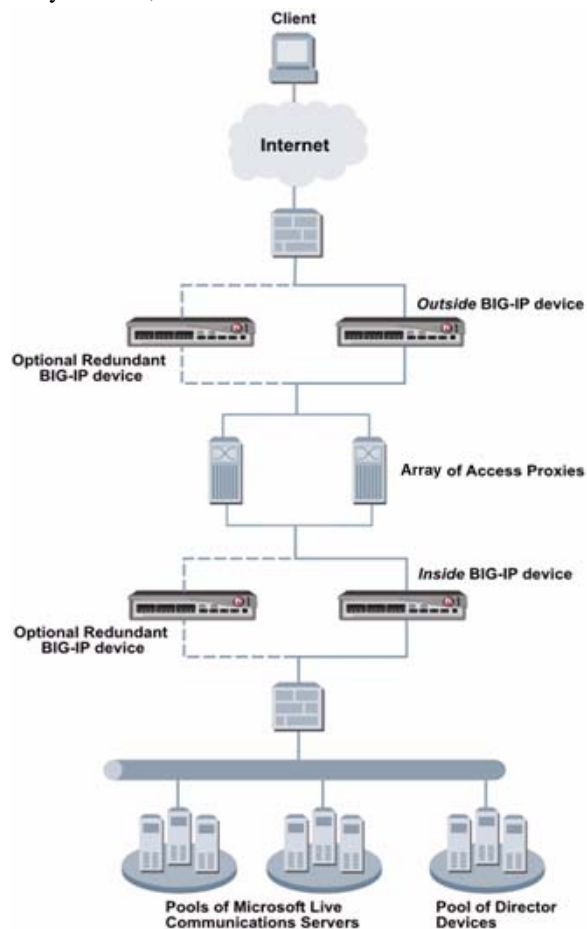


Figure 1.14 Deploying BIG-IP systems with Access Proxy and Director devices

◆ **Tip**

*To configure the BIG-IP system to provide high availability for firewalls, we recommend a BIG-IP Firewall Sandwich configuration. For more information on the Firewall Sandwich and for configuration instructions, see the **BIG-IP Solutions Guide**.*

Prerequisites

The following are prerequisites to the Access Proxy configuration.

- ◆ In the following procedures, we assume you have already created pools for the Live Communications Servers, as shown in **Creating pools**, on page 1-7, and virtual servers, as shown in **Creating virtual servers**, on page 1-13.
If you have additional pools of Live Communications Servers, repeat the procedures in **Creating pools**, on page 1-7, and **Creating virtual servers**, on page 1-13 for the additional Live Communications Server pools, and then return to this section.
- ◆ If you have a firewall in your network in between the Internet and the BIG-IP system (as shown in Figure 1.14), the firewall needs to be configured to allow TCP traffic on port **5061** in both directions, and TCP/UDP traffic on port **53** for outbound traffic only.
- ◆ If you have a firewall in your network between the Access Proxy devices and the inside BIG-IP system (as shown in Figure 1.14), the firewall should be configured to allow only port **5061** traffic in both directions.
- ◆ The default gateway on the Access Proxy devices should be the IP address of the internal facing self IP on the *outside* BIG-IP system.
- ◆ If you are using a Director in your deployment, you must modify the Hosts file on the Access Proxy devices to resolve the Director fully qualified domain name (FQDN) to the virtual server address of the Director.

Configuring the BIG-IP systems to direct traffic for the Access Proxy

Note that this Best Practice configuration requires two additional BIG-IP systems to load balance traffic to the Access Proxy devices.

In the following sections, we first configure the outside BIG-IP system, then the inside BIG-IP system.

◆ **Important**

*We assume the BIG-IP systems are already installed in the network, and that you have created (or are using the default) VLANs on the external and internal network. If you need to create additional VLANs, see **Creating a VLAN**, on page 1-4*

Configuring the outside BIG-IP system

We begin this deployment by configuring the *outside* BIG-IP system (as shown in Figure 1.14). On the outside BIG-IP system, you need to complete the following procedures:

- *Creating the self IP on the outside BIG-IP system*
- *Creating a pool for the Access Proxy devices on the outside BIG-IP system*
- *Creating the virtual server on the outside BIG-IP system*
- *Creating a SNAT on the outside BIG-IP system*
- *Enabling port lockdown on the outside BIG-IP system*

Creating the self IP on the outside BIG-IP system

The first step is to create a self IP address on the outside BIG-IP system.

To create a self IP address using the Configuration utility

1. On the navigation pane, click **Network**.
The Network screen displays the VLAN list.
2. Click the Self IP Addresses tab.
The self IP addresses screen opens.
3. Click the **Add** button.
The Add Self IP Address dialog box opens.
4. In the **IP Address** box, type a static IP address in the external facing VLAN.
In the Netmask box, type the corresponding subnet mask. The Broadcast address is automatically calculated.
In our example, we use **172.168.10.1** with a Netmask of **255.255.255.0**.
5. In the **SNAT Automap** section, click the box to enable **SNAT Automap**.
6. In the VLAN section, select the name of the external facing VLAN.
7. Click the **Done** button.
See Figure 1.15.

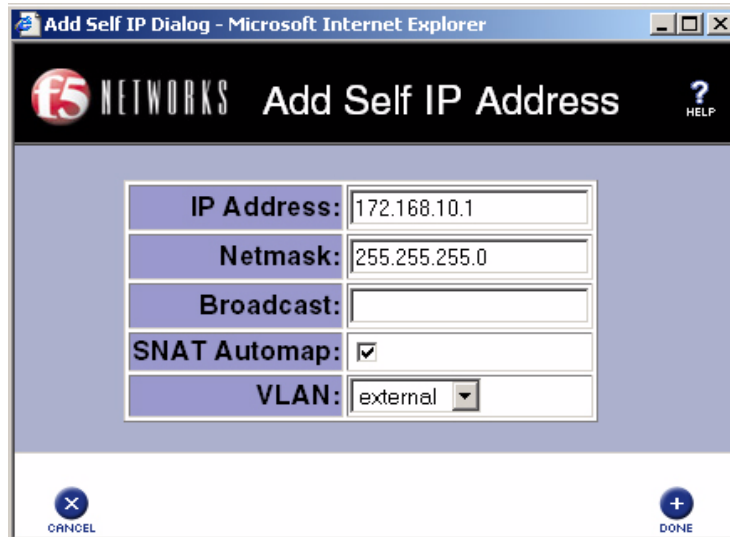


Figure 1.15 Creating a self IP address on the Outside BIG-IP system

To create a self IP on the BIG-IP system using the command line

1. To create a self IP address on the BIG-IP system, use the following syntax

```
b self <IP address> VLAN <VLAN Name>
```

In our example, we use:

```
b self 172.168.10.1 VLAN external netmask 255.255.255.0
```

You must also have a self IP address for the BIG-IP system's internal facing VLAN. Repeat the preceding procedure, but in Step 4, type a static IP address in the internal facing VLAN (in our example we use **192.168.10.1**), and in Step 6, select the internal facing VLAN.

Creating a pool for the Access Proxy devices on the outside BIG-IP system

The next step is to create a BIG-IP pool for the Access Proxy devices.

To create a pool for the Access Proxy devices from the Configuration utility

1. In the navigation pane, click **Pools**.
The Pools screen opens.
2. Click the **Add** button.
The Add Pool screen opens.
3. In the **Pool Name** box, enter a name for your pool.
In our example, we use **ap_pool_outside**.

4. In the **Load Balancing Method** box, enter your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).

For this configuration, we recommend selecting Least Connections.

5. In the **Resources** section, you add the IP address and service of the Access Proxy servers to the pool.
 - a) In the **Member Address** box, type the IP address of the external interface of the Access Proxy server.
In our example, we type **192.168.10.100**.
 - b) In the **Service** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list. In our example, we type **5061**.
Note: If you are using HTTPS tunneling, use 443 for the service.
 - c) The **Member Ratio** and **Member Priority** boxes are optional.
 - d) Click the Add button (>>) to add the member to the **Current Members** list.
 - e) Repeat steps a-d for each Access Proxy device you want to add to the pool. In our example, we repeat these steps once for the other external interface of the Access Proxy: **192.168.10.101**.
6. In the **Enable NAT** and **Enable SNAT** sections, make sure that the boxes are *not* checked. If necessary, click both boxes to clear the check.

Member Address:	Service:	Member Ratio:	Member Priority:	Current Members:
192.168.10.101	5061	1	1	192.168.10.100:5061 r1 p1
192.168.10.100	5061	1	1	192.168.10.101:5061 r1 p1

Figure 1.16 Adding the Access Proxy pool in the BIG-IP Configuration utility

The other fields in the Add Pool screen are optional. Configure these fields as applicable for your network. (For additional information about configuring a pool, click the **Help** button.)

7. Click the **Done** button. The pool is added to the list.

To create the Access Proxy pool from the command line

To create the pool from the command line, use the following syntax

```
b pool <pool name> { [lb_method <load balancing method>] member <IP address>:<port> nat
  disable snat disable }
```

In our example,:

```
b pool ap_pool_outside { lb_method least_conn member 192.168.10.100:5061 member
  192.168.10.101:5061 nat disable snat disable }
```

Creating the virtual server on the outside BIG-IP system

After you define the pool, the next step is to define the following virtual server on the BIG-IP devices to load balance the traffic to the Access Proxy pool.

To create the virtual server for the Access Proxy pool on the outside BIG-IP device using the Configuration utility

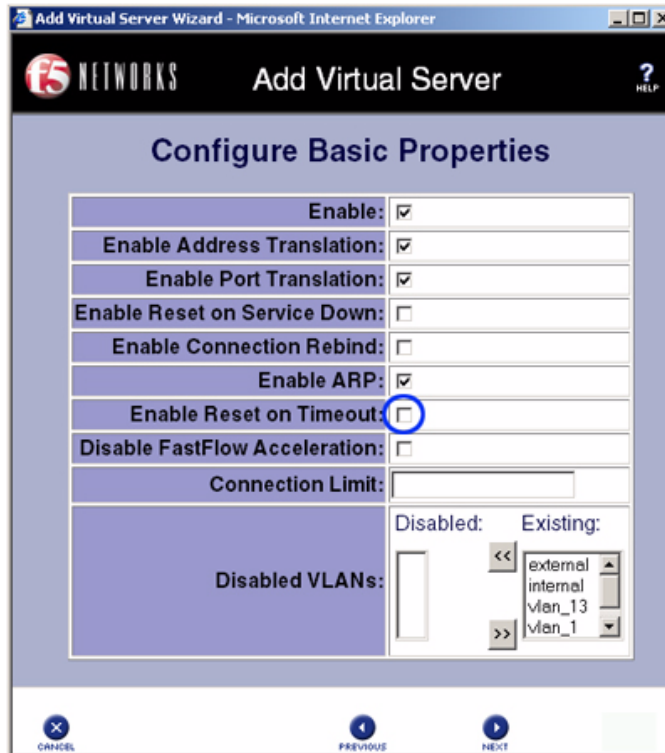
1. In the navigation pane, click **Virtual Servers**.
The Virtual Servers screen opens.
2. Click the **Add** button.
The Add Virtual Server screen opens.
3. Enter the IP address and service for the virtual server, and then click the **NEXT** button.

In our example, we use **172.168.10.100** with service of **5061**.
The Configure Basic Properties screen opens.

The screenshot shows the 'Add Virtual Server' configuration utility. The main heading is 'Configure Virtual IP Address and Service'. Below this, there are three input fields: 'Address' containing '172.168.10.100', 'Service' containing '5061' and a dropdown menu labeled 'or choose...', and '*Netmask' which is empty. At the bottom of the form, there are two buttons: 'CANCEL' and 'NEXT'.

Figure 1.17 Adding the virtual server on the outside BIG-IP system

- In the **Enable Reset on Timeout** section, click to clear the box. Click the **NEXT** button. The Select Physical Resources screen opens.



- Click the **Pool** option button, and from the list, select the pool you created in the *Creating a pool for the Access Proxy devices on the outside BIG-IP system* section above. In our example, we select **ap_pool_outside**.



Figure 1.18 Adding the Access Proxy pool to the virtual server

6. Click the **Done** button.

For additional information about configuring a virtual server, click the **Help** button.

To view the newly created virtual server, click the virtual server in the virtual server list. In our example, our virtual server properties are shown in Figure 1.19.

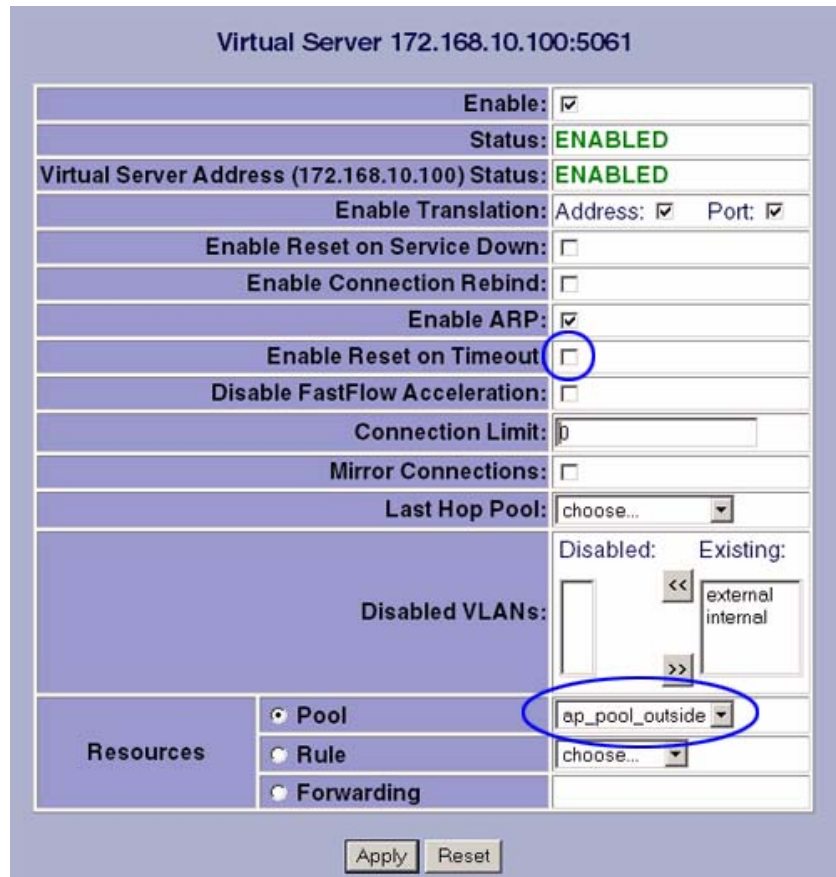


Figure 1.19 The Access Proxy virtual server on the Outside BIG-IP system

To create the Access Proxy virtual server from the command line

Use the bigpipe **virtual** command as shown below. You can use standard service names in place of port numbers. If you have DNS configured, you can also use host names in place of IP addresses.

```
b virtual <virtual IP address>:<port> use pool <pool_name> [timeout resets disable]
```

In our example, we use:

```
b virtual 172.168.10.100:5061 use pool ap_pool_outside timeout resets disable
```

Creating a SNAT on the outside BIG-IP system

The next step is to configure a default SNAT.

To create a default SNAT from the Configuration utility

1. From the navigation pane, click **NATs**.
The NAT screen opens.
2. Click the SNATs tab.
The SNAT screen opens.
3. Under **Current List**, check to see if a default SNAT is present.
 - If a default SNAT is not present, use the following procedure:
 - a) Click the **Add Default** button in the upper left portion of the screen.
The Add Default SNAT dialog box opens.
 - b) In the **Translation** section, click the **Automap** option button to select Automap.
 - c) Click the **Done** button.
 - If a default SNAT is present, make sure that the **SNAT Address** is set to **Auto**.

Enabling port lockdown on the outside BIG-IP system

The next step in the configuration of the outside BIG-IP system is to enable port lockdown on all VLANs. Port Lockdown enables you to lock down a VLAN to prevent direct connection to the BIG-IP system through that VLAN.

To enable port lockdown on the outside BIG-IP system from the Configuration utility

1. In the navigation pane, click **Network**.
The VLAN screen opens.
2. Click the VLAN name in the list.
The properties screen for that VLAN opens.
3. To enable port lockdown, check the **Port Lockdown** box.
4. Click **Done**.
5. Repeat these steps for each VLAN.

To enable or disable port lockdown from the command line

To enable port lockdown, type:

```
b vlan <vlan_name> port_lockdown enable
```

Repeat this command for each VLAN.

Configuring the inside BIG-IP system

The next section of this deployment is to configure the *inside* BIG-IP system (as shown in Figure 1.14). On the inside BIG-IP system, you need to complete the following procedures:

- *Creating self IPs on the inside BIG-IP system*
- *Creating the pools on the inside BIG-IP system*
- *Creating the virtual servers on the inside BIG-IP system*
- *Creating a default SNAT on the inside BIG-IP system*
- *Enabling port lockdown on the inside BIG-IP system*, on page 1-37

Creating self IPs on the inside BIG-IP system

The first step in configuring the inside BIG-IP system is to configure self IP addresses.

To configure the self IPs on the inside BIG-IP system, follow the same procedure as *Creating the self IP on the outside BIG-IP system*, on page 1-26, using the appropriate IP addresses. In our example, we create an external facing (**10.10.10.1**) and an internal facing (**157.168.10.1**) self IP address.

◆ Important

Ensure that SNAT Automap is enabled on the self IPs.

Creating the pools on the inside BIG-IP system

On the inside BIG-IP system, you need to configure a pool for Access Proxy devices and a pool for the next hop server in the enterprise network. The next hop server could be the IP address of a Standard Edition server or the virtual IP address of an Enterprise Edition pool. The Standard Edition server or the Enterprise Edition pool could be acting as Directors.

Creating a pool for the Access Proxy devices on the inside BIG-IP system

To configure a pool for the Access Proxy devices, follow the same procedure as *Creating a pool for the Access Proxy devices on the outside BIG-IP system*, on page 1-27, but naming the pool **ap_pool_inside** and typing the IP address of the internal interface of the Access Proxy servers.

To create a pool for the Access Proxy devices from the Configuration utility

1. In the navigation pane, click **Pools**.
The Pools screen opens.
2. Click the **Add** button.
The Add Pool screen opens.

3. In the **Pool Name** box, enter a name for your pool.
In our example, we use **ap_pool_inside**.
4. In the **Load Balancing Method** box, enter your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).

For this configuration, we recommend selecting Least Connections.

5. In the **Resources** section, you add the IP address and service of the Access Proxy servers to the pool.
 - a) In the **Member Address** box, type the IP address of the internal interface of the Access Proxy server. In our example, we type **10.10.10.100**.
 - b) In the **Service** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list. In our example, we type **5061**.
Note: If you are using HTTPS tunneling, use 443 for the service.
 - c) The **Member Ratio** and **Member Priority** boxes are optional.
 - d) Click the Add button (>>) to add the member to the **Current Members** list.
 - e) Repeat steps a-d for each Access Proxy device you want to add to the pool. In our example, we repeat these steps once for **10.10.10.101**.
6. In the **Enable NAT** box, make sure that the box is *not* checked. If necessary, click the box to clear the check.
7. **Enable SNAT** box, click a check in the box to enable SNAT.
The other fields in the Add Pool screen are optional. Configure these fields as applicable for your network. (For additional information about configuring a pool, click the **Help** button.)
8. Click the **Done** button. The pool is added to the list.

To create the Access Proxy pool from the command line

To create the pool from the command line, use the following syntax

```
b pool <pool name> { [lb_method <load balancing method>] member <IP address>:<port> nat  
  disable snat enable }
```

In our example, we type:

```
b pool ap_pool_inside { lb_method least_conn member 10.10.10.100:5061 member  
  10.10.10.101:5061 nat disable snat enable }
```

Creating a pool for the next hop server in the enterprise network

The next step is to create a pool to access the next hop server in the enterprise network. The next hop server could be the IP address of a Standard Edition server or the virtual IP address of an Enterprise Edition pool. The Standard Edition server or the Enterprise Edition pool could be acting as Directors.

A **Director** is a Pool (typically a Enterprise Edition server) with no locally homed users, and acts as a authorization/AD-routing proxy for outside users and domains, protecting internal Live Communications Servers against unauthenticated SIP traffic. A Director is typically needed when there are outside users and multiple pools (or servers) within an enterprise. Although a Director is not a requirement, it increases the security and manageability of the deployment.

To create a pool for the next hop server in the enterprise network

1. In the navigation pane, click **Pools**.
The Pools screen opens.
2. Click the **Add** button.
The Add Pool screen opens.
3. In the **Pool Name** box, enter a name for your pool.
In our example, we use **internal_nexthop_pool**.
4. In the **Load Balancing Method** box, enter your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).

For this configuration, we recommend selecting Least Connections.

5. In the **Resources** section, you add the IP address and service of the Access Proxy servers to the pool.
 - a) In the **Member Address** box, type the IP address of either the Standard Edition server or the virtual IP address of an Enterprise Edition pool. In our example, we use **157.168.10.100**.
 - b) In the **Service** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list. In our example, we type **5061**.
Note: If you are using HTTPS tunneling, use 443 for the service.
 - c) The **Member Ratio** and **Member Priority** boxes are optional.
 - d) Click the Add button (>>) to add the member to the **Current Members** list.
6. In the **Enable NAT** box, make sure that the box is *not* checked. If necessary, click the box to clear the check.
7. **Enable SNAT** box, click a check in the box to enable SNAT.

The other fields in the Add Pool screen are optional. Configure these fields as applicable for your network. (For additional information about configuring a pool, click the **Help** button.)

8. Click the **Done** button. The pool is added to the list.

To create the Access Proxy pool from the command line

To create the pool from the command line, use the following syntax

```
b pool <pool name> { [lb_method <load balancing method>] member <IP address>:<port> nat
  disable snat enable }
```

In our example, we type:

```
b pool internal_nexthop_pool { lb_method least_conn member 157.168.10.100:5061 nat
  disable snat enable }
```

Creating the virtual servers on the inside BIG-IP system

After you create the pools, you configure the virtual servers on the inside BIG-IP system.

Creating the Access Proxy virtual server on the inside BIG-IP system.

The next step is to define a virtual server on the inside BIG-IP system to load balance the traffic to the inside Access Proxy pool.

To create the virtual server for the Access Proxy pool on the inside BIG-IP device using the Configuration utility

1. In the navigation pane, click **Virtual Servers**.
The Virtual Servers screen opens.
2. Click the **Add** button.
The Add Virtual Server screen opens.
3. Enter the IP address and service for the virtual server, and then click the **NEXT** button.
In our example, we use **157.168.10.200** with service of **5061**.
The Configure Basic Properties screen opens.
4. In the **Enable Reset on Timeout** section, click to clear the box.
Click the **NEXT** button.
The Select Physical Resources screen opens.
5. Click the **Pool** option button, and from the list, select the pool you created in the *Creating a pool for the Access Proxy devices on the outside BIG-IP system* section above.
In our example, we select **ap_pool_inside**.
6. Click the **Done** button.
For additional information about configuring a virtual server, click the **Help** button.

To create the Access Proxy virtual server from the command line

Use the bigpipe **virtual** command as shown below. You can use standard service names in place of port numbers. If you have DNS configured, you can also use host names in place of IP addresses.

```
b virtual <virtual IP address>:<port> use pool <pool_name> [timeout resets disable]
```

In our example, we use:

```
b virtual 157.168.10.200:5061 use pool ap_pool_inside timeout resets disable
```

Creating a virtual server for the next hop pool

Next, you need a virtual server on the inside BIG-IP system to load balance traffic to the next hop pool.

To configure this virtual server, use the procedure *Creating the Access Proxy virtual server on the inside BIG-IP system.*, on page 1-36, but you need to configure the virtual server to reference the pool created in *Creating a pool for the next hop server in the enterprise network*, on page 1-35. In our example, this is **internal_nexthop_pool**, the virtual server address is **10.10.10.200** with a service of **5061**.

Creating a default SNAT on the inside BIG-IP system

To create a default SNAT on the inside BIG-IP system, follow the procedure *Creating a SNAT on the outside BIG-IP system*, on page 1-32.

Enabling port lockdown on the inside BIG-IP system

The next step in the configuration of the outside BIG-IP system is to enable port lockdown on all VLANs. Port Lockdown enables you to lock down a VLAN to prevent direct connection to the BIG-IP system through that VLAN.

To enable port lockdown, follow the procedure *Enabling port lockdown on the outside BIG-IP system*, on page 1-32.

Configuring a health monitor

The next step in this configuration is to configure health monitors on both the outside and inside BIG-IP systems for the Live Communications Servers. Again, we use the template for the TCP Extended Content Verification (ECV) monitor to create the monitor.

We recommend you configure the health monitor from the Configuration utility. For information on how to configure the health monitor from the command line, see the *BIG-IP Reference Guide*.

To configure a health monitor for the Live Communications servers using the Configuration utility

1. In the navigation pane, click **Monitors**.
The Network Monitors screen opens.
2. Click the **Add** button.
The Add Monitor dialog box opens.
3. In the Add Monitor screen, type the name of your monitor (it must be different from the monitor template name), in our example, we type **sip_monitor**.
In the **Inherits From** box, select the **tcp** monitor template from the list. Click the **Next** button.
4. In the Configure Basic Properties section, in the **Interval** box, type **10**, for a 10 second interval. In the **Timeout** box, type a value that is greater than the default maximum for a Registration Timeout refresh in the Live Communications Server global settings.
In our example, we type **32**, for a 32 second timeout.
Click the **Next** button.
The Configure ECV TCP Monitor screen opens.
5. Click the **Next** button again.
The Configure Destination Address and Service (Alias) screen opens.
6. In the **Destination Service** box, type **5061**, and then click the **Done** button.

The Add Monitor dialog box closes, and you return to the Network Monitors screen.
7. From the Network Monitors screen, click the Basic Associations tab.
The Basic Association screen opens.
8. In the **Node Address** section, from the list, select the name of the monitor you created in Step 3. In our example, we select **sip_monitor**.
9. In the Node Address column, locate all the Live Communications Servers, and click a check in the **Add** box for each node. In our example, we click checks in the **192.168.10.100** and **192.168.10.101** boxes on the outside BIG-IP system.
10. Click **Apply**.
You now see the **sip_monitor** in the Existing Associations column of the **Node Address** section for each of the Live Communications Servers.
For additional information associating a monitor, click the **Help** button.

-
11. Repeat this procedure on the other BIG-IP system. In our example, we repeat this procedure on the inside BIG-IP system, and in Step 9, we click checks in the **10.10.10.100**, **10.10.10.101**, and **157.168.10.100** boxes.

 **Important**

It is extremely important to repeat this procedure on both the inside and outside BIG-IP systems.

Synchronizing the BIG-IP configuration

If you are using redundant BIG-IP systems, the final step is to synchronize the configuration to the redundant BIG-IP device. Refer to the *Synchronizing the BIG-IP configuration if using a redundant system*, on page 1-21 for instructions, and synchronize the configuration of both the inside and outside BIG-IP systems.

Appendix A: Backing up and restoring the BIG-IP system configuration

We recommend saving your BIG-IP configuration before you begin this configuration. When you save the BIG-IP configuration, it collects the following critical data and compress it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files
- BIG-IP license and passwords
- SSL certificates
- SSH keys

Saving up and restoring the BIG-IP configuration using the Configuration utility

The Configuration Management screen allows you to save and restore all configuration files that you may edit to configure a BIG-IP system. These configuration files are called a User Configuration Set (UCS). The Configuration Management screen contains sections for saving and restoring a configuration. The list boxes in these sections display only files in the `/usr/local/ucs` directory. If you want to save or restore files from another directory, you must type the full path in the box.

To save the BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
The User Administration screen opens.
2. Click the Configuration Management tab.
The Configuration Management screen opens.
3. In the **Save Current Configuration** section, type the path where you want your configuration file saved or choose a path from the list box. If no path is specified, the BIG-IP saves files to `/usr/local/ucs`. The BIG-IP appends the extension `.ucs` to file names without it. In our example, we type `preLCS_backup.ucs`.

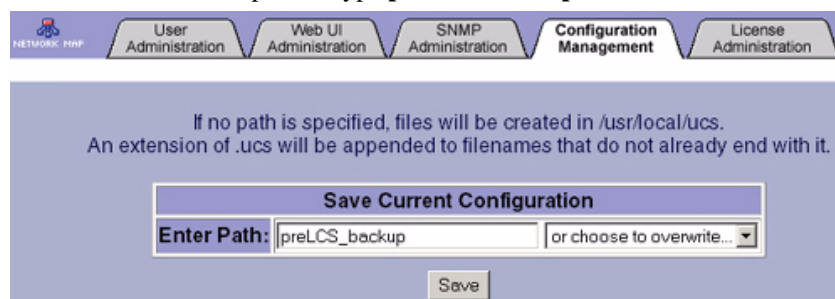


Figure 1.20 Saving the BIG-IP configuration

-
4. Click the **Save** button to save the configuration file.

To restore a BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
The User Administration screen opens.
2. Click the Configuration Management tab.
The Configuration Management screen opens.
3. In the **Restore a Configuration** section, choose the configuration file you want to restore from the list box, or type the path where your configuration files were saved.
4. Click the **Restore** button.
To check the status of the restoration, click the **View Log** button. You should wait a few moments for the log file to start generating before you click **View Log**. Repeated clicking of this button will update your screen with the most current log file information until the restoration is complete.

Saving and restoring the BIG-IP configuration using the bigpipe command line interface

You can also save and restore your configuration using the **bigpipe** command line.

To save and backup your BIG-IP configuration data from the command line

1. From the command line, use the following syntax:

```
bigpipe config save <filename>
```

Where **<filename>** is the name of the your saved configuration.

In our example, we type:

```
bigpipe config save preLCS_backup
```

Note: By default, BIG-IP saves the UCS to the following location: /usr/local/ucs. F5 Networks recommends that you use this default.

2. Copy the UCS file to a remote location.

Important

Important: The UCS file contains both authorization data and configuration files. It is critical that you safely store this file in a remote location.

To reinstall configuration data from the command line

To reinstall the UCS file that you created and stored during the backup procedure, perform the following steps:

1. Verify that the BIG-IP system has an IP address and route to the remote host on which the UCS file is located.
2. Copy the UCS file from the remote host to the **local /usr/local/ucs** directory.
3. If the hostname of the local system has changed since you created the original UCS file, you must set the hostname back to the original name. To change the hostname, type the following command, where `<fully-qualified-hostname>` is the original hostname:

```
hostname <fully-qualified-hostname>
```

***Important:** If you do not set the hostname back to the original name, the BIG-IP device will only perform a partial installation of the configuration files.*

4. Type the following command to decompress the UCS file and save the configuration files on the BIG-IP:

```
bigpipe config install <filename>
```

5. Reboot the system by typing the following:

```
reboot
```

For more information on saving and restoring a configuration file using the command line (including instructions on how to reinstall the BIG-IP system from scratch and a special case if you are using a BIG-IP version 4.5 RMA system), visit the F5 Networks Technical Support Web site (requires registration) and refer to Solution 1493.