

Organizations can use the Barracuda Load Balancer to enhance the scalability and availability of their Microsoft® Lync™ Server 2010 deployments (formerly known as Microsoft Office Communications Server).

Barracuda Networks has conducted interoperability tests between the Barracuda Load Balancer and Lync Server 2010. This guide describes how to deploy the Barracuda Load Balancer to provide scaling in a Lync environment.

Microsoft Lync Server Overview

Organizations use solutions like Microsoft Lync to allow them to effectively disseminate information and enhance collaborative efforts among their employees. Microsoft Lync Server 2010 offers functionality such as VoIP, instant messaging and Web collaboration. All these services may be accessed by clients from either the internal office network or from the Internet.

For companies that want a scalable solution, Microsoft recommends using a hardware load balancer to distribute the traffic among multiple Lync Servers.

Prerequisites

- Microsoft Lync Server 2010 Enterprise Edition
- Barracuda Load Balancer running firmware version 3.6.1.009 or higher
- Barracuda Load Balancer model 340 or above
- *For Internal Lync Server Deployment:* Minimum one Barracuda Load Balancer, two recommended for high availability
- *For both Internal Lync Server Deployment and Edge Deployment:* Minimum two Barracuda Load Balancers, four recommended for high availability. In order to maintain the integrity of the edge security model, separate load balancers are required for the internal traffic and the edge traffic.
- *For Internal Lync Server Deployment, Edge Deployment, and non-colocated A/V Services:* Minimum three Barracuda Load Balancers, six recommended for high availability. In order to maintain the integrity of the edge security model, separate load balancers are required for the internal traffic, the edge traffic and the non-colocated A/V Services.

This document assumes that you have installed your Barracuda Load Balancer(s), have connected to the Web interface, and activated your subscription(s). If you are planning to deploy Office Communications Server with high availability, you must first cluster your Barracuda Load Balancers. See the [Barracuda Load Balancer Administrator's Guide](#) for assistance with clustering.

Do not run the Lync Topology Builder until instructed to in this deployment guide. All of the Services on the Barracuda Load Balancer must be configured before running the Topology Builder.

Additional References

- Barracuda Load Balancer Administrator's Guide:
 - http://www.barracudanetworks.com/documentation/#Load_Balancer
- A description of the ports and protocols used by the servers, load balancers, and clients in a Microsoft Lync deployment environment.
 - <http://technet.microsoft.com/en-us/library/gg398833.aspx>
- Microsoft Lync Server 2010 Documentation
 - <http://technet.microsoft.com/en-us/library/gg398616.aspx>

Terminology

The following table explains some of the terms used in this document.

Table 1: Terminology

Definitions	
Front-End Server	A Lync Server in the internal network running the Front End Lync Services.
Edge Server	A Lync Server deployed in the perimeter network running the Edge Lync Services.
Fully Qualified Domain Name (FQDN)	The unique name for a specific computer or host that can resolve to an IP address, e.g. <code>www.example.com</code>
Service	A combination of a virtual IP (VIP) address and one or more TCP/UDP ports that the Barracuda Load Balancer listens on. Traffic arriving over the specified port(s) to a Service is directed to one of the Real Servers associated with a particular Service.

Deployment Options

The supported deployments of the Lync Server and the Barracuda Load Balancer are described in the following sections.

Lync Server Front-End Server Deployment Options

As the servers in a Lync Server enterprise pool communicate with each other using the VIP address of the pool, create a TCP Proxy Service and associate the servers with it to facilitate this communication. The servers and the Barracuda Load Balancer must be deployed using a **one-armed** topology in either a single or multiple subnet configuration.

Deploying internal Lync pools using a two-armed Route-Path topology, Direct Server Return (DSR) or Bridge Mode **does not work** and is not supported.

Lync Edge Server Deployment Options

Load balanced Edge deployments are supported using either a **one-armed** Route-Path topology using a TCP Proxy Service or a **two-armed** Route-Path topology using a Layer 4 Service. For maximum performance, a two-armed Route-Path topology is recommended.

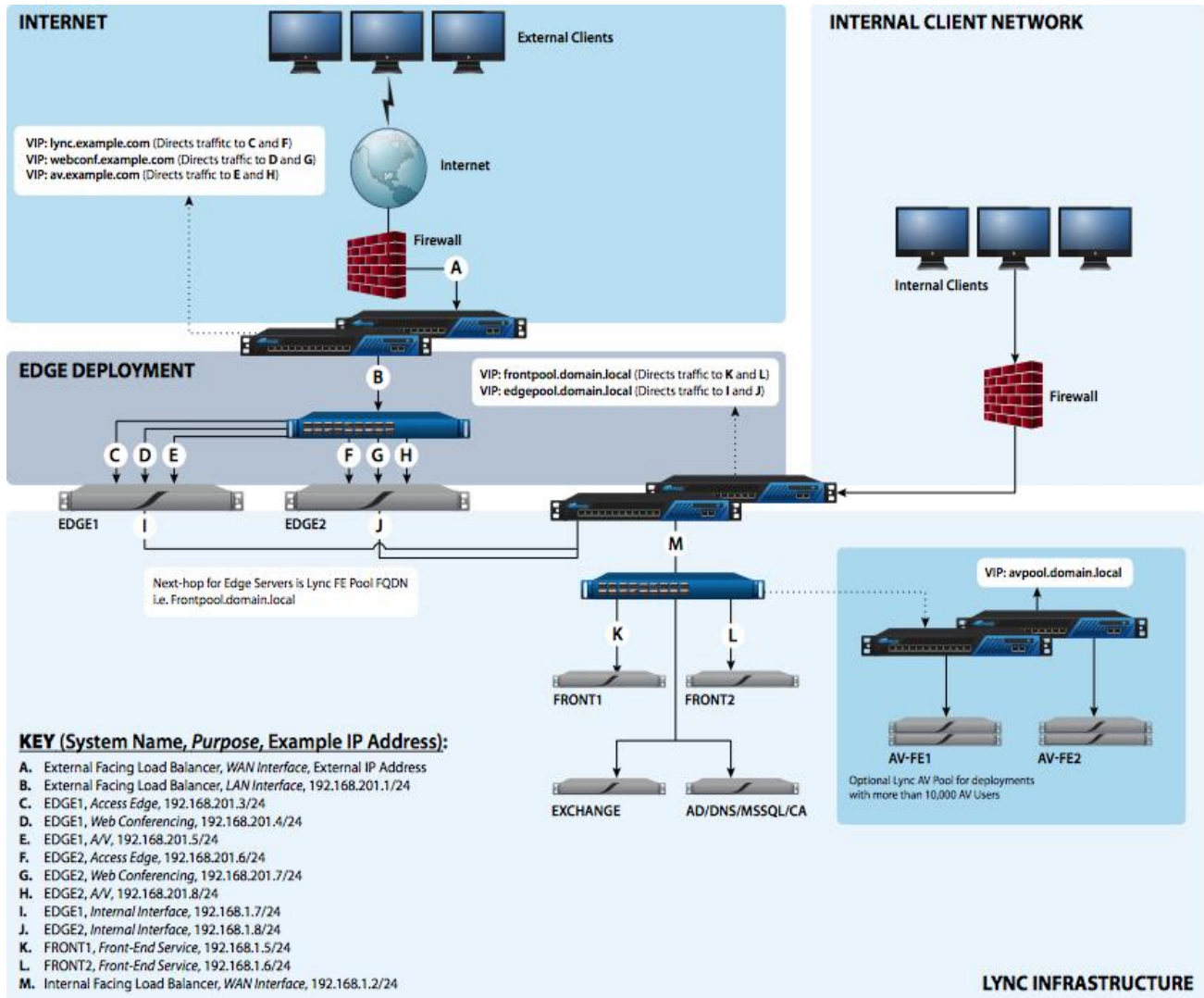
Bridge Mode and Direct Server Return deployments **do not work** and are not supported.

Deployment Example

Figure 1: Lync Deployment Example shows an example of a complete Lync deployment with Barracuda Load Balancers. This example is referenced in the deployment tasks detailed in the next sections.

Note that in this example, the Edge deployment uses a two-armed topology while the Front-End deployment uses a one-armed configuration.

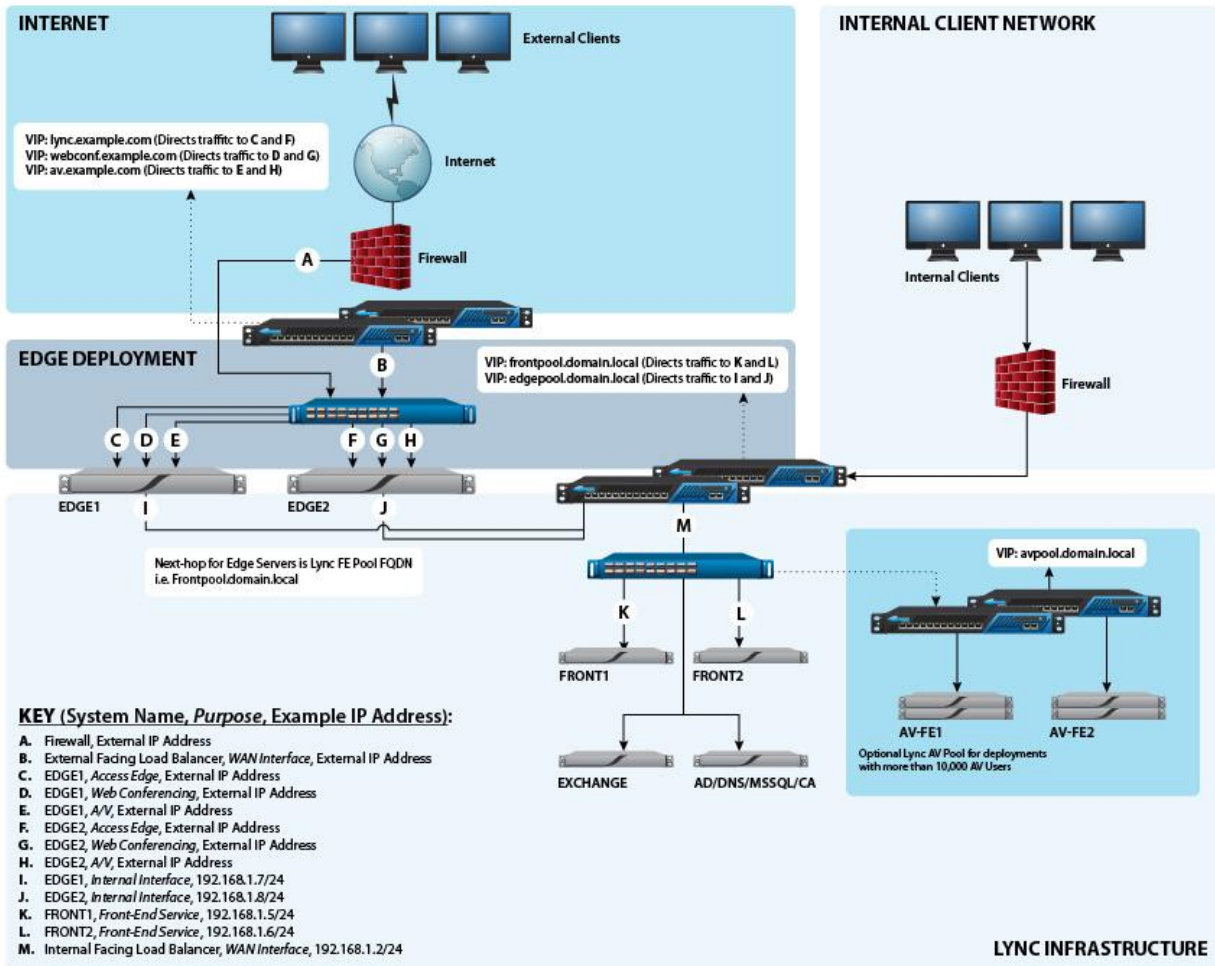
Figure 1: Lync Deployment Example



Note: The inbound firewall should not NAT inbound traffic addressed to the Edge deployment.

Figure 2: Lync Deployment Example One-armed Edge shows another example of a very similar Lync deployment with Barracuda Load Balancers. In this example, the only difference is that the Edge deployment uses a one-armed topology. The same references can be used in the deployment tasks detailed in the next sections.

Figure 2: Lync Deployment Example One-armed Edge



Deployment Tasks

Table 2: Deployment tasks lists the tasks required to deploy the Barracuda Load Balancer in a Lync environment. Complete these tasks using the instructions in the rest of this document.

A worksheet is provided in Appendix A that you can use to record your configuration. Barracuda Networks recommends completing this worksheet as you perform these tasks. It will assist you when running the Topology Builder in Step 7.

Table 2: Deployment tasks

Task	Where
1. Modify TCP and UDP Connections Settings.	Do this on all active Barracuda Load Balancers, both internal and external.
2. Configure Enterprise Pool Services.	Do this on the internal-facing Barracuda Load Balancer.
If you did not colocate A/V services on your Front End Servers, you must also do the following:	
3. Configure Internal A/V Services (if applicable).	Do this on the A/V Pool Barracuda Load Balancer
If you have an edge deployment you must also do the following tasks:	
4. Configure Internal Edge Services.	Do this on the internal-facing Barracuda Load Balancer.
5. Configure External Edge Services.	Do this on the external-facing Barracuda Load Balancer.
If you have deployed Director servers you must also do the following task:	
6. Configure Director Services.	Do this on the Director Barracuda Load Balancer.
All users should do these tasks after all Services are configured on the Barracuda Load Balancer:	
7. Run Topology Builder.	Do this on the server where Topology Builder is installed.
8. Enable Cookie Persistence.	Do this on the internal-facing Barracuda Load Balancer.

Note: If your Barracuda Load Balancers are clustered, the configuration between the active and passive systems is synchronized. There is no need to modify any passive Barracuda Load Balancers.

1. Modify TCP and UDP Connections Settings

Do the following on all active Barracuda Load Balancers, both internal (the Barracuda Load Balancer configured with the Front-End servers) and external (if there is a Barracuda Load Balancer deployed with Edge servers).

The Barracuda Load Balancer comes configured with default settings that work with most applications. Lync requires changes to the default TCP and UDP connection settings on the Barracuda Load Balancer to ensure compliance with Microsoft specifications.

To modify the TCP and UDP Connections settings on the System Settings page:

- 1.1. Go to the **Advanced > System Settings** tab in the Web interface.
- 1.2. In the **TCP Connections Timeout** box, enter 1800 (30 minutes).
- 1.3. In the **UDP Connections Timeout** box, enter 1800 (30 minutes).

2. Configure Enterprise Pool Services

Do the following on the internal-facing Barracuda Load Balancer.

To configure all the Services needed for an internal Lync deployment, perform the following steps on the internal-facing Barracuda Load Balancer:

- 2.1. Go to the **Basic > Services** page in the Web interface.
- 2.2. Add each Service listed in *Table 3: Required Services for internal Lync deployment* - they are all **required**. To add a Service:
 - In the **Service Name** box, enter the name for the Service.
 - In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal Lync Pool.
 - Select the protocol and in the **Port** box, enter the port for the Service in the table.
 - In the **Real Servers** box, enter the IP address for every Front-End server in your Lync Pool.


Table 3: Required Services for internal Lync deployment

Service Name	Virtual IP Address	Protocol	Port	Real Servers
MTLS Front	IP for FQDN of Internal Enterprise Lync Pool e.g. 192.168.1.11/24 for frontpool.domain.local	TCP	5061	IP Addresses of your Front-End servers (K and L from the example)
DCOM WMI Front	IP for FQDN of Internal Enterprise Lync Pool	TCP	135	IP Addresses of your Front-End servers (K and L from the example)
Internal Conf Front	IP for FQDN of Internal Enterprise Lync Pool	TCP	444	IP Addresses of your Front-End servers (K and L from the example)
HTTPS Front	IP for FQDN of Internal Enterprise Lync Pool	TCP	443	IP Addresses of your Front-End servers (K and L from the example)

2.3. The Services in *Table 4: Optional Services for internal Lync deployment* are **optional**. Add each Service only if you have deployed that feature.

Table 4: Optional Services for internal Lync deployment


Service Name	Virtual IP Address	Protocol	Port	Real Servers
Application Sharing (optional)	IP for FQDN of Internal Enterprise Lync Pool	TCP	5065	IP Addresses of your Front-End servers (K and L from the example)
QoE Agent (optional)	IP for FQDN of Internal Enterprise Lync Pool	TCP	5069	IP Addresses of your Front-End servers (K and L from the example)
Response Group Service (optional)	IP for FQDN of Internal Enterprise Lync Pool	TCP	5071	IP Addresses of your Front-End servers (K and L from the example)
Conferencing Attendant (optional)	IP for FQDN of Internal Enterprise Lync Pool	TCP	5072	IP Addresses of your Front-End servers (K and L from the example)
Conferencing Announcement (optional)	IP for FQDN of Internal Enterprise Lync Pool	TCP	5073	IP Addresses of your Front-End servers (K and L from the example)
Outside Voice Control (optional)	IP for FQDN of Internal Enterprise Lync Pool	TCP	5074	IP Addresses of your Front-End servers (K and L from the example)

2.4. For each Service created, edit the Service by clicking the **Edit**  graphic next to the Service entry in the table. On the **Service Detail** page that appears, for all Services except for the HTTPS Front Service:

- In the **General** section, set **Service Type** to **TCP Proxy**.
- In the **Persistence** section, set **Persistence Type** to **Client IP** and **Persistence Time** to **1200**.
- In the **Advanced Options** section, set **Session Timeout** to 0 (session never times out).

For the HTTPS Front Service only:

- In the **General** section, set **Service Type** to **Layer 7 - HTTPS**.
- In the **Persistence** section, set **Persistence Type** to **HTTP Cookie** and **Persistence Time** to **1200**. Leave **Cookie Name** blank.
- In the **Advanced Options** section, set **Session Timeout** to 0 (session never times out).

2.5. For the DCOM WMI Front Service only, edit each Real Server associated with the Service by clicking the **Edit**  graphic next to each Real Server entry in the table. On the **Real Server Detail** page that appears:

- In the **Server Monitor** section, set the **Testing Method** to **TCP Port Check**.
- In the **Port** field, enter the value **5061**. It is better to test port 5061 for this Service because port 135 always passes the TCP port check, even if Lync Services are not responding.

3. Configure Internal A/V Services (if applicable)

If you have more than 10,000 users in this pool, it is recommended that you separate the A/V Services of your Internal Lync Pool and do not colocate the A/V services on the Front End pool. If you choose to colocate A/V Services on your Front End Pool, no further changes to the configuration are required.

Separating out the A/V Services into its own pool will require two more Barracuda Load Balancers operating as a High Availability pair. Contact Barracuda Technical Support if your deployment has more than 10,000 A/V users for assistance.

4. Configure Internal Edge Services

Do the following on the internal-facing Barracuda Load Balancer.

To configure all the Services needed for a load-balanced Lync Edge deployment, perform the following steps on the internal-facing Barracuda Load Balancer:

- 4.1. Go to the **Basic > Services** page in the Web Interface.
- 4.2. For each entry in *Table 5: Services for Lync Edge deployment on the internal-facing Barracuda Load Balancer*, add a Service. To add a Service:
 - In the **Service Name** box, enter the name for the Service.
 - In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal Edge Lync Pool.
 - In the **Port** box, enter the port for that Service in the table.
 - In the **Real Servers** box, enter the internal IP address for every Edge server.

Table 5: Services for Lync Edge deployment on the internal-facing Barracuda Load Balancer

Service Name	Virtual IP Address	Protocol	Port	Real Server
MTLS Edge	IP for FQDN of Internal Edge Enterprise Lync Pool e.g.192.168.1.12/24 for edgepool.domain.local	TCP	5061	Internal IP addresses of your Edge Servers (I and J from the example)
AV Auth Edge	IP for FQDN of Internal Edge Enterprise Lync Pool	TCP	5062	Internal IP addresses of your Edge Servers (I and J from the example)
RTP HTTPS Edge	IP for FQDN of Internal Edge Enterprise Lync Pool	TCP	443	Internal IP addresses of your Edge Servers (I and J from the example)
HTTPS	IP for FQDN of Internal Edge Enterprise Lync Pool	TCP	4443	Internal IP addresses of your Edge Servers (I and J from the example)
Web Conferencing Edge	IP for FQDN of Internal Edge Enterprise Lync Pool	TCP	8057	Internal IP addresses of your Edge Servers (I and J from the example)
RDP Media Edge	IP for FQDN of Internal Edge Enterprise Lync Pool	UDP	3478	Internal IP addresses of your Edge Servers (I and J from the example)

4.3. For each **TCP** Service created, edit the Service by clicking the **Edit**  graphic next to the Service entry in the table. On the **Service Detail** page that appears:

For all Services except for the HTTPS and RTP HTTPS Edge Service:

- In the **General** section, set **Service Type** to **TCP Proxy**.
- In the **Persistence** section, set **Persistence Type** to **Client IP** and **Persistence Time** to **1200**.
- In the **Advanced Options** section, set **Session Timeout** to 0 (session never times out).

For the HTTPS and RTP HTTPS Edge Services only:

- In the **General** section, set **Service Type** to **Layer 7 - HTTPS**.
- In the **Persistence** section, set **Persistence Type** to **HTTP Cookie** and **Persistence Time** to **1200**. Leave **Cookie Name** blank.
- In the **Advanced Options** section, set **Session Timeout** to 0 (session never times out).

4.4. No change is required for RDP Media Edge, which is a Layer 4 - UDP Service.

5. Configure External Edge Services

Do the following on the external-facing (Internet-facing) Barracuda Load Balancer.

The Real Servers should be physically connected to a switch which is connected to the LAN port (for two-armed deployment) or the WAN port (one-armed deployment) of the Barracuda Load Balancer.

To configure all the Services needed for a load balanced Edge Deployment of Lync Server, perform the following steps on the external-facing Barracuda Load Balancer:

5.1. Go to the **Basic > Services** page in the Web interface.

5.2. For each entry in *Table 6: Services for load balancing Edge Deployment of Lync*, add a Service. To add a Service:

- In the **Service Name** box, enter the name for the Service.
- In the **Virtual IP Address** box, enter the IP address for the FQDN of your Internal Edge Lync Pool.
- In the **Port** box, enter the port for that Service in the table.
- In the **Real Servers** box, enter the internal IP address for every Edge server.

Note: Each Service must have its own VIP Address in the table listed below

Table 6: Services for load balancing Edge Deployment of Lync

Service Name	Virtual IP Address	Protocol	Port	Real Server
Access Edge	IP for FQDN of Access Edge e.g. IP address for lync.example.com	TCP	443	IP address of Access Edge NICs on each Edge Server (C and F from the example)

Service Name	Virtual IP Address	Protocol	Port	Real Server
Access Edge <i>(This Service is required if you have enabled federation on your Enterprise Edge Pool).</i>	IP for FQDN of Access Edge e.g. IP address for lync.example.com	TCP	5061	IP address of Access Edge NICs on each Edge Server (C and F from the example)
Web Conferencing Edge	IP for FQDN of WebConf Edge e.g. IP address for webconf.example.com	TCP	443	IP address of WebConf NICs on each Edge Server (D and G from the example)
A/V Edge	IP for FQDN of AV Edge e.g. IP address for av.example.com	TCP	443	IP address of AV NICs on each Edge Server (E and H from the example)
A/V UDP Edge	IP for FQDN of AV Edge e.g. IP address for av.example.com	UDP	3478	IP address of AV NICs on each Edge Server (E and H from the example)

5.3. For each **TCP** Service created, edit the Service by clicking the **Edit**  graphic next to the Service entry in the table. On the **Service Detail** page that appears,

For a two-armed deployment:

- In the **Persistence** section, set **Persistence Type** to **Client IP** and **Persistence Time** to **1200**

For a one-armed deployment:

- In the **General** section, set **Service Type** to **TCP Proxy**
- In the **Persistence** section, set **Persistence Type** to **Client IP** and **Persistence Time** to **1200**
- In the **Advanced Options** section, set **Session Timeout** to **0** (session never times out).

5.4. No further modifications need to be made to the default settings for the TCP Services or the UDP Service.

6. Configure Director Services

Do the following on the Director Barracuda Load Balancer.

To configure all the Services needed for Director Services, perform the following steps on the Director Barracuda Load Balancer:


6.1. Go to the **Basic > Services** page in the Web interface.

6.2. For each entry in *Table 7: Services for load balancing Director Services*, add a Service:

- In the **Service Name** box, enter the name for the Service.
- In the **Virtual IP Address** box, enter the IP address for the FQDN of your Director Service.
- In the **Port** box, enter the port for that Service in the table.
- In the **Real Servers** box, enter the IP address for every Director server.

Table 7: Services for load balancing Director Services

Service Name	Virtual IP Address	Protocol	Port	Real Servers
Director MTLS	IP for FQDN of the Director Service	TCP	5061	IP addresses of your Director Servers
Director MTLS Legacy <i>Add this Service if you need to support Office Communications Server prior to 2007 R2. If you only have versions of OCS that are 2007 R2 or later (including Lync), do not add this Service.</i>	IP for FQDN of the Director Service	TCP	5060	IP addresses of your Director Servers

6.3. For each Service created, edit the Service by clicking the **Edit**  graphic next to the Service entry in the table. On the **Service Detail** page that appears:

- In the **General** section, set the Service Type to **TCP Proxy**.
- In the **Persistence** section, set **Persistence Type** to **Client IP** and **Persistence Time** to **1200**
- In the **Advanced Options** section, set **Session Timeout** to 0 (session never times out).

7. Run Topology Builder

Now that all of the Services have been configured on the Barracuda Load Balancer, run Lync Topology Builder. Use the configuration information that you have recorded in the worksheet in Appendix A to assist you in filling out the required fields.

8. Enable Cookie Persistence

In this step you will install an SSL certificate on the internal-facing Barracuda Load Balancer to enable cookie persistence for the Layer 7 – HTTPS Services that were partially configured previously. You will also configure backend SSL on the Real Servers. The Barracuda Load Balancer will use the certificate that you install to decrypt the SSL traffic directed to Layer 7 – HTTPS Services. It will check for a persistence cookie and then re-encrypt the traffic before sending it to a server in the pool.

Each of the front-end Lync servers should have the pool name in its certificate. Export a certificate, making sure it has the pool name, from one of the front-end servers:

8.1. Using the Certificates Microsoft Management Console (MMC), export a certificate along with its private key.

To enable cookie persistence, perform the following steps on the internal-facing Barracuda Load Balancer:

8.2. Import the certificate using the **Basic > Certificates** page.

8.3. Go to the **Basic > Services** page and edit the HTTPS Front Service. On the **Service Detail** page, in the **SSL Offloading** section, select the SSL certificate from the SSL Certificate list.

- 8.4. Go the **Basic > Services** page and edit each Real Server that is associated with the HTTPS Front Service. On the **Real Server Detail** page, set **Enable HTTPS/SSL** to **Yes** so that the Barracuda Load Balancer will re-encrypt the traffic sent to the Real Server.

If you deployed edge services on the internal-facing Barracuda Load Balancer, identify the certificate for the HTTPS and RTP HTTPS Edge Services:

- 8.5. Go to the **Basic > Services** page and edit the HTTPS and RTP HTTPS Edge Services. On the **Service Detail**, in the **SSL Offloading** section, select the SSL certificate from the SSL Certificate list.
- 8.6. Go the **Basic > Services** page and edit each Real Server that is associated with each of these Services. On the **Real Server Detail** page, set **Enable HTTPS/SSL** to **Yes** so that the Barracuda Load Balancer will re-encrypt the traffic sent to the Real Server.

Your installation is now complete.

Appendix A: IP Worksheet

As you perform the deployment tasks, record your IP Addresses on this worksheet. It will assist you when you run the Topology Builder.

Configured Barracuda Load Balancer	FQDN	IP Address	Associated Topology Builder Step or Steps	Notes
Internal-facing Barracuda Load Balancer			Front End Pool wizard	Pool FQDN
Internal-facing Barracuda Load Balancer	Usually this is the same as your pool FQDN unless your organization has also implemented SIP DNS load balancing.		Front End Pool wizard	External Base URL
A/V Barracuda Load Balancer (if configured)			Front End Pool wizard, Define the new A/V Conferencing Server	A/V Conferencing Pool
Internal-facing Barracuda Load Balancer			New Edge Pool wizard	Edge Pool FQDN
External-facing Barracuda Load Balancer			New Edge Pool, External FQDNs	Edge SIP Access
External-facing Barracuda Load Balancer			New Edge Pool, External FQDNs	Edge Web Conferencing
External-facing Barracuda Load Balancer			New Edge Pool, External FQDNs	Edge Audio/Video