# Table of Contents

About this Guide .............................................................................................................. 4  
Appliances Supported ........................................................................................................ 4  
Microsoft Lync 2010 – Software Versions Supported ......................................................... 4  
Loadbalancer.org – Software Versions Supported ............................................................... 4  
Microsoft Lync 2010 ........................................................................................................... 5  
  Microsoft Lync 2010 Editions ......................................................................................... 5  
    Standard Edition ........................................................................................................... 5  
    Enterprise Edition ...................................................................................................... 5  
Microsoft Lync 2010 & Loadbalancer.org ......................................................................... 5  
Microsoft Lync 2010 Server Roles ..................................................................................... 6  
Load Balancing Lync 2010 .................................................................................................. 8  
  Load Balancing Methods Supported ............................................................................. 8  
    DNS Load Balancing .................................................................................................. 8  
    Hardware Load Balancing (HLB) ................................................................................ 8  
Load Balancing Considerations ......................................................................................... 8  
  Load Balancer Configuration Mode .............................................................................. 8  
  Load Balanced Roles ..................................................................................................... 9  
  Persistence (aka Server Affinity) .................................................................................... 9  
  TCP Timeout Settings ................................................................................................... 9  
  Reverse Proxy Server .................................................................................................... 10  
    Lync 2010 Web Services ............................................................................................ 10  
    Simple URLs ............................................................................................................... 10  
Load Balanced Ports / Protocols ......................................................................................... 11  
  Front End Servers ......................................................................................................... 11  
    Required .................................................................................................................... 11  
    Optional ..................................................................................................................... 11  
  Director Servers ............................................................................................................ 12  
    Required .................................................................................................................... 12  
    Optional ..................................................................................................................... 12  
  Edge Servers (Internal Access) ...................................................................................... 12  
  Edge Servers (External Access) ...................................................................................... 12  
Deployment Architecture .................................................................................................. 13  
  Loadbalancer.org test Environment .............................................................................. 13  
    Overview .................................................................................................................... 13  
    Front End Pool – the Details ...................................................................................... 14  
    Director Pool – the Details ....................................................................................... 15  
    Internal Edge – the Details ....................................................................................... 16  
    External Edge – the Details ...................................................................................... 17  
    Lync Topology Builder ............................................................................................... 18  
    DNS Configuration .................................................................................................... 18  
Loadbalancer.org Appliance – the Basics .......................................................................... 19  
  Network Configuration .................................................................................................. 19  
  Accessing the Web User Interface (WUI) ....................................................................... 21  
  Clustered Pair Configuration ......................................................................................... 22  
Loadbalancer.org Appliance – Configuring for Lync 2010 .................................................. 23  
  STEP 1 – Configure Layer 7 Global Settings ............................................................... 24  
  STEP 2 – Configuring the Load Balanced Front End Services ......................................... 25  
    Virtual Server/Service (VIP) List ............................................................................... 25  
    Virtual Server/Service (VIP) Configuration ............................................................... 25  
    Real Server (RIP) Configuration ............................................................................... 27
About this Guide
This guide details the configuration of Loadbalancer.org appliances for deployment with Microsoft Lync 2010. It includes details of ports/services that must be load balanced, topology considerations for the various Lync 2010 server roles and also steps on how to configure the appliances.

For an introduction on setting up the appliance as well as additional technical information, please also refer to our quick-start guides and full administration manuals which are available at the following links:

**Version 7.x**


**Version 6.x**

Quickstart guide: http://www.loadbalancer.org/pdf/quickstep

**Appliances Supported**
Due to the number of Virtual Servers/Services (VIPs) required for Lync 2010, the Enterprise R16 is not supported. All other models can be used with Lync 2010 as listed below:

- Enterprise
- Enterprise MAX
- Enterprise 10G
- Enterprise VA

For a full specification comparison of these models please refer to: http://www.loadbalancer.org/matrix.php

**Microsoft Lync 2010 – Software Versions Supported**

- Microsoft Lync 2010 – all versions

**Loadbalancer.org – Software Versions Supported**

- v7.4.3 and later
- v6.21 and later
Microsoft Lync 2010

Microsoft Lync 2010 is an Enterprise level real-time communications server, providing the infrastructure for enterprise instant messaging, presence, file transfer, peer-to-peer and multiparty voice and video calling, ad-hoc and structured conferences (audio, video and web) and PSTN (Public Switched Telephone Network) connectivity. These features are available within an organization, between organizations, and with external users on the public internet, or standard phones, using the PSTN or via SIP trunking.

Microsoft Lync 2010 Editions

*Standard Edition*

Standard Edition server is designed for small organizations, and for pilot projects of large organizations. It enables many of the features of Lync Server 2010, including the necessary databases, to run on a single server. This enables you to have Lync Server functionality for a lesser cost, but does not provide a true high-availability solution.

*Enterprise Edition*

For a high-availability solution Lync 2010 Enterprise Edition is required. Load balancing is required to load balance the Front End pools, Director pools and Edge Server pools.

Microsoft Lync 2010 & Loadbalancer.org

Deploying Microsoft Lync 2010 with Loadbalancer.org appliances enables organizations to create a feature rich highly resilient solution that ensures that wherever staff are located and however they connect, they can depend on a platform that allows seamless communications wherever and whenever needed using the communications medium of their choice.

Loadbalancer.org appliances are configured to present a series of Virtual Servers/Services (VIPs). These VIPs become the connection points for internal and external clients. The load balancer is then able to distribute requests to the Lync servers that make up the various pools.
Microsoft Lync 2010 Server Roles

System functionality is split into multiple roles as shown in the following table. For the Standard edition, all roles are installed on a single server, for the Enterprise edition, roles can be distributed across multiple servers depending on the number of end-users, server performance and HA requirements.

The table also summarizes the scalability, HA & co-location options for each role.

<table>
<thead>
<tr>
<th>Role</th>
<th>Details</th>
</tr>
</thead>
</table>
| **Front End Server**  | *Purpose*: As the core server role, the Front End Server runs many Lync Server services. This role along with the back-end SQL server are the minimum required roles for Lync.  
*Scalability*: Each front end server can support up to 10,000 users. When configured in a pool, up to 80,000 users are supported.  
*High Availability*: Use a pool of servers with a load balancer. |
| **Back End Server**   | *Purpose*: The back-end SQL Server hosts various databases to keep track of Lync's configuration and state information.  
*Scalability*: Microsoft recommends using an SQL cluster for high availability.  
*High Availability*: Use clustering / Mirroring techniques. |
| **A/V Conferencing Server** | *Purpose*: Provides Audio / Visual conferencing functionality to Lync clients.  
*Scalability*: Microsoft recommends a separate dedicated server for more than 10,000 users. Each dedicated A/V server supports up to 20,000 users.  
*High Availability*: Use a pool of servers (no load balancer is required).  
*Co-location*: By default this role is co-located with the Front End Server, but can also be deployed separately. |
| **Edge Server**       | *Purpose*: Enables users to communicate and collaborate with users outside the organization's firewalls. These external users can include the organization’s own users who are currently working off-site, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Lync Server deployment. This role also enables connectivity to public IM connectivity services, including Windows Live, AOL, and Yahoo!.  
*Scalability*: One Edge Server for every 15,000 users who will access a site remotely. As a minimum, Microsoft recommend two Edge Servers for high availability.  
*High Availability*: Use a pool of servers with a load balancer. |
<table>
<thead>
<tr>
<th>Role</th>
<th>Purpose</th>
<th>Scalability</th>
<th>High Availability</th>
<th>Co-location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mediation Server</td>
<td>Enables Enterprise Voice and dial-in conferencing. Mediation Server translates signaling and, in some configurations, media between your internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk.</td>
<td>A dedicated Mediation Server supports up to 1200 users. Co-located with a Front End Server, it supports up to 226 users.</td>
<td>Use a pool of servers with a load balancer.</td>
<td>By default this role is co-located with the Front End Server, but can also be deployed separately, which for larger deployments making a large number of calls is recommended.</td>
</tr>
<tr>
<td>Monitoring Server</td>
<td>This role collects data from the Lync infrastructure and allows administrators to run reports. This information can help to provide the best possible media experience for users and maximize the return on investment of your deployment as well as helping to plan future growth.</td>
<td>One physical Monitoring Server can support up to 250,000 users if not co-located with Archiving Server. If co-located, it can support up to 100,000 users.</td>
<td>Use a standby server (messages are queued on the Front-End servers if a failure occurs).</td>
<td>Can be co-located with Archiving Server.</td>
</tr>
<tr>
<td>Archiving Server</td>
<td>Enables archiving of IM communications and meeting content for compliance reasons. If you do not have legal compliance concerns, you do not need to deploy Archiving Server.</td>
<td>One physical Archiving Server can support up to 500,000 users if not co-located with Monitoring Server. If co-located, it can support up to 100,000 users.</td>
<td>Use a standby server (messages are queued on the Front-End servers if a failure occurs).</td>
<td>Can be co-located with Monitoring Server.</td>
</tr>
<tr>
<td>Director Server</td>
<td>This is a required role when Edge Servers are deployed. In this case Director authenticates the external users, and then passes their traffic on to the internal servers. Directors are also deployed with Front End pools to streamline authentication requests and improve performance. In this scenario, all requests go first to the Director, which then routes them to the correct Front End pool.</td>
<td>One Director for every 15,000 users who will access a site remotely. As a minimum, Microsoft recommend two Directors for high availability.</td>
<td>Use a pool of servers with a load balancer.</td>
<td></td>
</tr>
</tbody>
</table>
Load Balancing Lync 2010

Load Balancing Methods Supported
Microsoft Lync 2010 supports two types of load balancing solutions: Domain Name System (DNS) load balancing and Hardware Load Balancing (HLB).

DNS Load Balancing
Lync 2010 DNS load balancing is typically implemented at the application level. When the application (for example, a Lync 2010 client) queries DNS for the pool members IP address, all member addresses are returned. Then, the client attempts to establish a TCP connection to one of the IP addresses. If that fails, the client tries the next IP address in the cache. If the TCP connection succeeds, the client negotiates TLS to connect to the Front End Server. If it gets to the end without a successful connection, the user is notified that no servers running Lync Server 2010 are available at the moment.

It's not possible to use DNS load balancing for client to server HTTP / HTTPS traffic because these are session state oriented protocols. In this case a Hardware Load Balancer must be used.

Hardware Load Balancing (HLB)
As mentioned above, hardware based load balancing is required for Web traffic. Therefore it's possible to use a HLB in a hybrid mode where the HLB balances web traffic and DNS load balancing is used for all other services, or in exclusive mode where the HLB is used to balance all services.

N.B. The configuration presented in this manual uses hardware load balancing for all load balanced services.

Load Balancing Considerations

Load Balancer Configuration Mode
Direct Return (DR) mode aka Direct Server Return (DSR) mode is not supported for Lync 2010. Modes that are supported are as follows:

- Full-NAT mode (also known as proxy, secure NAT, source NAT, or SNAT mode). In full-NAT mode, both the source and IP destinations are changed as packets pass through the load balancer.

  N.B. Loadbalancer.org refer to this mode as 'Layer 7 SNAT mode'

- Half-NAT mode (also known as transparency, destination NAT or DNAT mode). In half-NAT mode, the destination IP address is changed as packets pass through the load balancer, but the source IP address remains intact.

  N.B. Loadbalancer.org refer to this mode as 'Layer 4 NAT mode'
The following table describes the supported configurations for full-NAT and half-NAT modes:

<table>
<thead>
<tr>
<th>Load Balanced Pools</th>
<th>Supported Modes</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Pools</td>
<td>Full-NAT</td>
<td>Half-NAT is not supported for load balancing of internal pools because inter-server communications within an internal pool fail when servers in the pool try to connect to their own VIP.</td>
</tr>
<tr>
<td>Edge Pools</td>
<td>Full-NAT &amp; Half-NAT</td>
<td>The VIP for the external interface of Edge Servers should be set to half-NAT or full-NAT only for traffic to the Edge (for each VIP that is used for Edge Servers and HTTP). Also, NAT is not supported for the IP address of the external interface of the A/V Edge Server of an Edge Server, so the IP address of the external interface of the A/V Edge service on each Edge Server must be publicly routable (no NAT).</td>
</tr>
</tbody>
</table>

**Load Balanced Roles**

The following pools / servers require load balancing:

**The Enterprise Pool with multiple Front End Servers:** The hardware load balancer serves as the connectivity point to multiple Front End Servers in an Enterprise pool. For Web Services, the simple URLs can either be directed at the Front End Servers or the Director Servers. However, when Director Servers are deployed then it is recommend that these requests are forwarded to the Director Pool.

**The Director Pool with multiple Director Servers:** The hardware load balancer serves as the connectivity point to multiple Directors in an array and also for the external Web Services typically forwarded from a DMZ based Reverse Proxy such as Microsoft TMG.

**The Edge Pool with multiple Edge Servers:** The hardware load balancer acts as the connectivity point to both the internal and external NICs for multiple Edge Servers in an array. Different hardware load balancers can be used to load balance Edge Servers, one for the internal NICs and one for the external NICs of the Edge Server.

**Persistence (aka Server Affinity)**

Most Lync protocols are configured using source IP address persistence. If the mobility features available in Lync Server 2010 CU4 are used, this requires cookie-based persistence for external connections to Lync Web Services. Therefore SSL must be terminated at the load balancer to allow the cookie to be inserted, then re-encrypted before reaching the Front End Servers. This is covered in the Appendix.

**TCP Timeout Settings**

The TCP idle time-out should be set to be at least 20 minutes. This value should be above the Maximum SIP connection idle timeout which is typically set to 20 minutes. In this guide, TCP related idle timeouts are set to 30 minutes.
Reverse Proxy Server

Lync 2010 Web Services

A Reverse Proxy server is required to enable external access to the Lync 2010 Web Services. This can be achieved using Microsoft Forefront Threat Management Gateway (TMG) 2010. Microsoft recommends that all Web Services in all pools should be published. One publishing rule for each Front End pool and Director pool is required.

Simple URLs

In addition, the simple URLs must also be published. When Director Servers are deployed, the reverse proxy should listen for HTTP/HTTPS requests to the simple URLs and should proxy them to the external Web Services virtual directory on the Director pool rather than to the Front End pool.

For additional details on Reverse Proxy requirements please refer to the following Microsoft Technet article:

Setup Reverse Proxy Servers:

For additional details on load balancing requirements please refer to the following Microsoft Technet articles:

Lync 2010 – Load Balancing Requirements:

Components Required for External User Access:
## Load Balanced Ports / Protocols

### Front End Servers

#### Required

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>135</td>
<td>TCP/DCOM/RPC</td>
<td>Various DCOM based operations</td>
</tr>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>Internal Web Services</td>
</tr>
<tr>
<td>444</td>
<td>TCP/HTTPS</td>
<td>Used for the Focus (conference state server) &amp; FE server to Survivable Branch Appliances</td>
</tr>
<tr>
<td>5061</td>
<td>TCP/TLS/MTLS/SIP</td>
<td>Various SIP based communication</td>
</tr>
<tr>
<td>5065</td>
<td>TCP/MTLS/SIP</td>
<td>Incoming SIP listening requests for application sharing</td>
</tr>
<tr>
<td>5069</td>
<td>TCP/SIP</td>
<td>Used by the QoE Agent on the Front End Servers</td>
</tr>
<tr>
<td>4443</td>
<td>TCP/HTTPS</td>
<td>External Web Services – from Reverse Proxy</td>
</tr>
<tr>
<td>8080</td>
<td>TCP/HTTP</td>
<td>External Web Services – from Reverse Proxy</td>
</tr>
</tbody>
</table>

#### Optional

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP/HTTP</td>
<td>Various HTTP based Services</td>
</tr>
<tr>
<td>448</td>
<td>TCP</td>
<td>Used for call admission control by the Lync Server Bandwidth Policy Service</td>
</tr>
<tr>
<td>5060</td>
<td>TCP/SIP</td>
<td>Unsecured SIP Traffic</td>
</tr>
<tr>
<td>5067</td>
<td>TCP/TLS/MTLS/SIP</td>
<td>Incoming SIP requests from the PSTN gateway to the Mediation Server</td>
</tr>
<tr>
<td>5068</td>
<td>TCP/SIP</td>
<td>Incoming SIP requests from the PSTN gateway to the Mediation Server</td>
</tr>
<tr>
<td>5070</td>
<td>TCP/SIP</td>
<td>Incoming requests from the Front End Server to the Mediation Server</td>
</tr>
<tr>
<td>5071</td>
<td>TCP/SIP</td>
<td>Incoming SIP requests for the Response Group application</td>
</tr>
<tr>
<td>5072</td>
<td>TCP/SIP</td>
<td>Incoming SIP requests for Microsoft Lync 2010 Attendant (dial in conferencing)</td>
</tr>
<tr>
<td>5073</td>
<td>TCP/SIP</td>
<td>Incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing)</td>
</tr>
<tr>
<td>5075</td>
<td>TCP/SIP</td>
<td>Incoming SIP requests for the Call Park application</td>
</tr>
<tr>
<td>5076</td>
<td>TCP/SIP</td>
<td>Incoming SIP requests for the Audio Test service</td>
</tr>
<tr>
<td>5080</td>
<td>TCP</td>
<td>Used for call admission control by the Bandwidth Policy service for A/V Edge TURN traffic</td>
</tr>
</tbody>
</table>
# Director Servers

### Required

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>5061</td>
<td>TCP/TLS/MTLS/SIP</td>
<td>Internal SIP communications between servers and for client connections</td>
</tr>
<tr>
<td>4443</td>
<td>TCP/HTTPS</td>
<td>External Web Services (including Simple URLs) – from Reverse Proxy</td>
</tr>
<tr>
<td>8080</td>
<td>TCP/HTTP</td>
<td>External Web Services (including Simple URLs) – from Reverse Proxy</td>
</tr>
</tbody>
</table>

### Optional

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>TCP/SIP</td>
<td>Unsecured SIP Traffic</td>
</tr>
</tbody>
</table>

---

# Edge Servers (Internal Access)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP/STUN</td>
<td>Audio/Visual service</td>
</tr>
<tr>
<td>3478</td>
<td>UDP/STUN</td>
<td>Audio/Visual service</td>
</tr>
<tr>
<td>5061</td>
<td>TCP/MTLS/SIP</td>
<td>Access (SIP proxy) service</td>
</tr>
<tr>
<td>5062</td>
<td>TCP/MTLS/SIP</td>
<td>Audio/Visual authentication service</td>
</tr>
<tr>
<td>8057</td>
<td>TCP/MTLS</td>
<td>Web Conferencing</td>
</tr>
</tbody>
</table>

# Edge Servers (External Access)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP/TLS/STUN/SIP</td>
<td>Access (SIP proxy), Web Conferencing, Audio/Visual services</td>
</tr>
<tr>
<td>3478</td>
<td>UDP/STUN</td>
<td>Audio/Visual service</td>
</tr>
<tr>
<td>5061</td>
<td>TCP/MTLS/SIP</td>
<td>Access (SIP proxy) service</td>
</tr>
</tbody>
</table>

N.B. For further details on server port requirements please also refer to the following Microsoft links:


Deployment Architecture

Loadbalancer.org test Environment

Overview

Main Components:

- Enterprise Pool with multiple Front End Servers
  - Includes the co-located A/V conferencing Server
  - Includes the co-located Mediation Server
- Director Pool with multiple Director Servers
- Edge Server Pool with Multiple Edge Servers
- Reverse Proxy – used to forward External Web Service requests on ports 80 & 443 to the Front End / Director Servers on ports 8080 & 4443
- Load Balancer Clustered Pair 1 – Used to load balance the Internal Edge, the Director Servers and the Enterprise Front End Servers
- Load Balancer Clustered Pair 2 – Used to load balance the External Edge
**Front End Pool – the Details**

**NOTES:**

- Services are deployed using both a one-arm (the LAN based internal VIP) and two-arm (the 2 x External Web Services VIPs) configuration
- Layer 7 VIPs act as a proxy so both client-to-server and server-to-client traffic passes via the load balancer
- If Lync's Mobility features are used, please refer to the Appendix for details on setting up SSL Offload, cookie insertion and SSL re-encryption

**NOTE:** Prior to v7.5 a VIP is known as a 'Virtual Server', from v7.5 onwards it's known as a 'Virtual Service'.

---

**Diagram Description:**

- **Internal Router / Firewall**
- **Load Balancer**:
  - 192.168.10.30/24 (135,443,444,5061,5065,5069)
  - 192.168.20.30/24 (4443)
  - 192.168.20.30/24 (8080)
- **LAN**
- **Front End Pool**
  - **Front End 1**
  - **Front End 2**
- **Enterprise Front End Pool**
- **Internal Lync test clients**

A single VIP with all required ports is used for the Front-End Pool services. Two VIPs are used for the Front-End Pool External Web Services.
**NOTES:**

- Services are deployed using both a one-arm (the LAN based internal VIP) and two-arm (the 2 x External Web Services VIPs) configuration
- Layer 7 VIPs act as a proxy so both client-to-server and server-to-client traffic passes via the load balancer
- If Lync's Mobility features are used, please refer to the Appendix for details on setting up SSL Offload, cookie insertion and SSL re-encryption

**NOTE:** Prior to v7.5 a VIP is known as a 'Virtual Server', from v7.5 onwards it's known as a 'Virtual Service'.
**Internal Edge – the Details**

**NOTES:**

- All services are deployed using a two-arm configuration
- Internal clients must be able to access the Edge Servers via the load balanced VIP and also directly.
  - When accessing the Edge Servers directly, the load balancer acts as a router and forwards packets accordingly
    - To allow internal Lync Clients to access the Edge Servers directly, static routes are added to the internal test clients
      - 192.168.100.0/24 via 192.168.10.1/24
      - and to the load balancer
        - 192.168.100.0/24 via 192.168.20.2/24
  - To allow Edge Server return traffic to reach internal clients, static routes are added to:
    - each Edge Server
      - 192.168.20.0/24 via 192.168.100.1/24
      - 192.168.10.0/24 via 192.168.100.1/24
    - the router
      - 192.168.10.0/24 via 192.168.20.1/24
- A default gateway is not set on the internal interface of the Edge Servers, this should be configured on the external interface only

---

**NOTE:** Prior to v7.5 a VIP is known as a 'Virtual Server', from v7.5 onwards it's known as a 'Virtual Service'.
**NOTES:**

- All services are deployed using a two-arm configuration
- External clients must be able to access the Edge Servers via the load balanced VIP and also directly
  - When accessing the Edge Servers directly, the load balancer acts as a router and forwards packets accordingly
    - To allow external clients to access the Edge Servers directly, a static route is added to the external router
      - 10.20.0.0/16 via 10.25.1.1/16
- External test clients have their default gateway set as the external router / firewall
- In a production deployment Public IP addresses are required for the 3 Edge Service VIPs and also for each corresponding service on the real servers. In the above example this means a total of 9 public IP addresses
- The default gateway of the Edge Servers is set to be the load balancer – set this on the external NIC and do not set a default gateway on the internal NIC
- The default gateway of the load balancer is set to be the external router/firewall

---

**NOTE:** Prior to v7.5 a VIP is known as a 'Virtual Server', from v7.5 onwards it's known as a 'Virtual Service'.
**DNS Configuration**

Internal DNS records must be modified to ensure that the various FQDNs defined in the Topology Builder are set to point at the relevant Virtual Server/Service (VIP) created on the load balancer. Additional internal records are also manually added:

- `sip internaltls._tcp.robstest.com → pool1.robstest.com`
- `pool1.robstest.com → Enterprise Pool VIP on the load balancer`

On the external test clients, DNS entries are configured in the local hosts file:

- `sip.robstest.com → points to the external IP for the Access Edge`
- `webconf.robstest.com → points to the external IP for the Web Conf. Edge`
- `av.robstest.com → points to the external IP for the AV Edge`
- `meet.robstest.com → points to the reverse-proxy (Simple URL → Director Pool)`
- `dialin.robstest.com → points to the reverse-proxy (Simple URL → Director Pool)`
- `dirpool1.robstest.com → points to the reverse-proxy (Front End Pool)`
- `admin.robstest.com → points to the reverse-proxy (Front End Pool)`
- `pool1.robstest.com → points to the reverse-proxy (Front End Pool)`
Loadbalancer.org Appliance – the Basics

Network Configuration

The IP address, default gateway and DNS settings can be configured in several ways depending on the version as detailed below.

v7.5 & Later

Configure the IP address, Default Gateway & DNS Settings

Using the Network Setup Wizard at the console:
After boot, follow the console instructions to configure the IP address, gateway and DNS settings.

Using the WUI:
Using a browser, connect to the WUI on the default IP address/port: http://192.168.2.21:9080
to set the IP address use: Local Configuration > Network Interface Configuration
to set the default gateway use: Local Configuration > Routing
to configure DNS settings use: Local Configuration > Hostname & DNS

Using Linux commands:
At the console, set the initial IP address using the following command:
```
ip addr add <IP address>/<mask> dev eth0
e.g. ip addr add 192.168.2.10/24 dev eth0
```
At the console, set the initial default gateway using the following command:
```
route add default gw <IP address> <interface>
e.g. route add default gw 192.168.2.254 eth0
```
At the console, set the DNS server using the following command:
```
echo nameserver <IP address> >> /etc/resolv.conf
e.g. echo nameserver 192.168.64.1 >> /etc/resolv.conf
```

N.B. If this method is used, you must also configure these settings using the WUI, otherwise settings will be lost after a reboot

v7.4.3

Configure the IP address & Default Gateway

Using the Network Setup Wizard at the console:
After boot, follow the console instructions to configure the IP address and gateway using the Network Setup Wizard.

N.B. For these software versions the network setup wizard does not support DNS server configuration. DNS servers must be defined using the WUI or Linux commands as explained below.
Configure the IP address, Default Gateway & DNS Settings

Using the WUI:
Using a browser, connect to the WUI on the default IP address:port: http://192.168.2.21:9080

to set the IP address use: Edit Configuration > Network Interface Configuration
to set the default gateway use: Edit Configuration > Routing
to configure DNS settings use: Edit Configuration > Hostname & DNS

Using Linux commands:
At the console, set the initial IP address using the following command:
\[ \text{ip addr add <IP address>/<mask> dev eth0} \]
e.g. \[ \text{ip addr add 192.168.2.10/24 dev eth0} \]

At the console, set the initial default gateway using the following command:
\[ \text{route add default gw <IP address> <interface>} \]
e.g. \[ \text{route add default gw 192.168.2.254 eth0} \]

At the console, set the DNS server using the following command:
\[ \text{echo nameserver <IP address> >> /etc/resolv.conf} \]
e.g. \[ \text{echo nameserver 192.168.64.1 >> /etc/resolv.conf} \]

N.B. If this method is used, you must also configure these settings using the WUI, otherwise settings will be lost after a reboot

v6.x

Configure the IP address, Default Gateway & DNS Settings

Using the WUI:
Using a browser, connect to the WUI on the default IP address:port: http://192.168.2.21:9080

to set the IP address & default gateway use: Edit Configuration > Network Interface Configuration
to configure DNS settings use: Edit Configuration > DNS & Hostname

N.B. The Virtual Appliance attempts to use DHCP to obtain its initial IP address, default gateway and DNS settings. The IP address allocated will be displayed on the console once the boot process is complete

Using Linux commands:
At the console, set the initial IP address using the following command:
\[ \text{ifconfig eth0 <IP address> netmask <netmask> up} \]
e.g. \[ \text{ifconfig eth0 192.168.2.10 netmask 255.255.255.0 up} \]

At the console, set the initial default gateway using the following command:
\[ \text{route add default gw <IP address> <interface>} \]
e.g. \[ \text{route add default gw 192.168.2.254 eth0} \]

At the console, set the DNS server using the following command:
\[ \text{echo nameserver <IP address> >> /etc/resolv.conf} \]
e.g. \[ \text{echo nameserver 192.168.64.1 >> /etc/resolv.conf} \]

N.B. If this method is used, you must also configure these settings using the WUI, otherwise settings will be lost after a reboot
Accessing the Web User Interface (WUI)

The WUI can be accessed from a browser at:  \texttt{http://192.168.2.21:9080/lbadmin}

* Note the port number → 9080

(replace 192.168.2.21 with the IP address of your load balancer if its been changed from the default)

\textbf{Username:} loadbalancer

\textbf{Password:} loadbalancer

Once you have entered the logon credentials the Loadbalancer.org Web User Interface will be displayed as shown below:

\textit{v7.x}

The screen shot below shows the v7.5 WUI once logged in:
v6.x

The screen shot below shows the V6.21 WUI once logged in:

![Screen Shot of V6.21 WUI](image)

**Clustered Pair Configuration**

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide's single unit is deployed first, adding a secondary slave unit is covered in section 6 of the Appendix.
Loadbalancer.org Appliance – Configuring for Lync 2010

NOTE: It's highly recommended that you have a working Lync 2010 environment first before implementing the load balancer.

N.B. The steps presented in this section cover versions 6.x, 7.4.3 and 7.5 & later of the Appliance.
STEP 1 – Configure Layer 7 Global Settings

To configure the TCP timeouts required by Lync 2010, HAProxy’s client and server timeouts must be changed from their default values.

v7.x

- v7.5 & later – Go to Cluster Configuration > Layer 7 – Advanced Configuration
- v7.4.3 – Go to Edit Configuration > Layer 7 – Advanced Configuration

<table>
<thead>
<tr>
<th>Layer 7 (HAProxy):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock HAPerxy Configuration</td>
</tr>
<tr>
<td>Logging</td>
</tr>
<tr>
<td>Log Only Errors</td>
</tr>
<tr>
<td>Redispatch</td>
</tr>
<tr>
<td>Connection Timeout</td>
</tr>
<tr>
<td>Client Timeout</td>
</tr>
<tr>
<td>Real Server Timeout</td>
</tr>
</tbody>
</table>

- Change **Client Timeout** to **1800000** as shown above (i.e. 30 minutes)
- Change **Server Timeout** to **1800000** as shown above (i.e. 30 minutes)
- Click the **Update** button to save the settings

v6.x

- Using the WUI, go to: Edit Configuration > Global Settings > Layer 7 (HAProxy)

<table>
<thead>
<tr>
<th>Layer 7 (HAProxy):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
</tr>
<tr>
<td>Redispatch</td>
</tr>
<tr>
<td>continueout</td>
</tr>
<tr>
<td>clitimeout</td>
</tr>
<tr>
<td>srvtimeout</td>
</tr>
</tbody>
</table>

- Change **clitimeout** to **1800000** as shown above (i.e. 30 minutes)
- Change **srvtimeout** to **1800000** as shown above (i.e. 30 minutes)
- Click the **Update** button to save the settings
STEP 2 – Configuring the Load Balanced Front End Services

**Virtual Server/Service (VIP) List**

The table below shows VIPs that must be created:

<table>
<thead>
<tr>
<th>VIP Name (Label)</th>
<th>IP Address</th>
<th>Port(s)</th>
<th>Layer</th>
<th>Layer 7</th>
<th>Persistence Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>FrontEndPool</td>
<td>192.168.10.30</td>
<td>135, 443, 444, 5061, 5065, 5069</td>
<td>7</td>
<td>Other TCP</td>
<td>Source IP address</td>
</tr>
<tr>
<td>FePoolExtWebSvcs8080</td>
<td>192.168.20.30</td>
<td>8080</td>
<td>7</td>
<td>Other TCP</td>
<td>Source IP address</td>
</tr>
<tr>
<td>FePoolExtWebSvcs4443</td>
<td>192.168.20.30</td>
<td>4443</td>
<td>7</td>
<td>Other TCP</td>
<td>Source IP address *</td>
</tr>
</tbody>
</table>

* If the mobility features available in Lync Server 2010 CU4 are used, this requires cookie-based persistence for external connections to Lync Web Services. Therefore SSL must be terminated at the load balancer to allow the cookie to be inserted, then re-encrypted before reaching the Front End Servers. To Set this up, it's recommended to first add the services listed above and verify their operation without SSL offload, then to follow the steps in the Appendix to configure SSL offload.

**Virtual Server/Service (VIP) Configuration**

The following steps show how to create the first VIP in the table above. Once created, use the same method to create all other VIPs listed in the table (3 total) noting the specific settings required for each.

**v7.x**

| NOTE: Prior to v7.5 a VIP is known as a 'Virtual Server', from v7.5 onwards it's known as a 'Virtual Service'. For simplicity the configuration steps below refer to 'Virtual Service' for both. |

- v7.5 & later – Using the WUI, go to **Cluster Configuration > Layer 7 – Virtual Service** and click **[Add a New Virtual Service]**
- v7.4.3 – Using the WUI, go to **Edit Configuration > Layer 7 – Virtual Servers** and click **[Add a New Virtual Server]**
- Enter the following details:
• Enter an appropriate label for the VIP, e.g. **FrontEndPool**
• Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.10.30**
• Set the **Virtual Service Ports** field to **135,443,444,5061,5065,5069**
• Set **Persistence mode** to **Source IP**
• Click **Update**
• Now click [Modify] next to the newly created VIP
• Change **Layer 7 Protocol** to **Other TCP**
• Set the **Check Port** field to **5061**
• Click **Update**

Now repeat these steps to add the other Virtual Services listed in the table above.

---

**v6.x**

• Using the WUI, go to **Edit Configuration > Virtual Servers (HAProxy)** and click [Add a New Virtual Server]

• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>FrontEndPool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Server (ipaddress:port)</td>
<td>192.168.10.30:135</td>
</tr>
<tr>
<td>Persistence mode</td>
<td>Source IP</td>
</tr>
<tr>
<td>Fallback</td>
<td>127.0.0.1:9081</td>
</tr>
</tbody>
</table>

• Enter an appropriate label for the VIP, e.g. **FrontEndPool**
• Change the **Virtual Server (ipaddress:port)** field to <the required IP>:135, e.g. **192.168.10.30:135**
• Set **Persistence mode** to **Source IP**
• Click **Update**
• Now click [Modify] next to the newly created VIP
• In the **Extra Ports** field enter the other required ports separated by commas, i.e. **443,444,5061,5065,5069**
• Change **Layer 7 Protocol** to **Other TCP**
• Set the **Check Port** field to **5061**
• Click **Update**

Now repeat these steps to add the other Virtual Servers listed in the table above.
Real Server (RIP) Configuration

Real Servers (RIPS) must now be defined for each Virtual Server/Service created. The number of RIPS defined depends on the number of Front End Servers in your deployment, the test deployment used for this guide has 2 Front End servers so each VIP requires 2 RIPS to be configured.

v7.x

- v7.5 & later – Using the WUI, go to Cluster Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP
- v7.4.3 – Using the WUI, go to Edit Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>FE-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.10.31</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>1</td>
</tr>
<tr>
<td>Weight</td>
<td></td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the RIP, e.g. FE-1
- Change the Real Server IP Address field to the required IP address, e.g. 192.168.10.31
- Leave the Real Server Port field blank
- Click Update
- Repeat the above steps to add your other Front End Servers

Now repeat these steps to add RIPS for the other Virtual Services.

v6.x

- Using the WUI, go to Edit Configuration > Real Servers (HAProxy) and click [Add a new Real Server] next to the newly created VIP
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>FE-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server (ipaddress:port)</td>
<td>192.168.10.31</td>
</tr>
</tbody>
</table>
• Enter an appropriate label for the RIP, e.g. FE-1
• Change the Real Server (ipaddress:port) field as required (leaving the port blank) e.g. 192.168.10.31
• Click Update
• Repeat the above steps to add your other Front End Servers

Now repeat these steps to add RIPS for the other Virtual Servers.

STEP 3 – Configuring the Load Balanced Director Services

Virtual Server/Service (VIP) List

The table below shows all VIPs that must be created:

<table>
<thead>
<tr>
<th>VIP Name (Label)</th>
<th>IP Address</th>
<th>Port(s)</th>
<th>Layer</th>
<th>Layer 7 Protocol</th>
<th>Persistence Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectorPool</td>
<td>192.168.10.20</td>
<td>5061</td>
<td>7</td>
<td>Other TCP</td>
<td>Source IP address</td>
</tr>
<tr>
<td>DirPoolExtWebSvcs8080</td>
<td>192.168.20.20</td>
<td>8080</td>
<td>7</td>
<td>Other TCP</td>
<td>Source IP address</td>
</tr>
<tr>
<td>DirPoolExtWebSvcs4443</td>
<td>192.168.20.20</td>
<td>4443</td>
<td>7</td>
<td>Other TCP</td>
<td>Source IP address *</td>
</tr>
</tbody>
</table>

* If the mobility features available in Lync Server 2010 CU4 are used, this requires cookie-based persistence for external connections to Lync Web Services. Therefore SSL must be terminated at the load balancer to allow the cookie to be inserted, then re-encrypted before reaching the Director Servers. To Set this up, it's recommended to first add the services listed above and verify their operation without SSL offload, then to follow the steps in the Appendix to configure SSL offload.

Virtual Server/Service (VIP) Configuration

The following steps show how to create the first VIP in the table above. Once created, use the same method to create all other VIPs listed in the table (5 total) noting the specific settings required for each.

v7.x

NOTE: Prior to v7.5 a VIP is known as a 'Virtual Server', from v7.5 onwards it's known as a 'Virtual Service'. For simplicity the configuration steps below refer to 'Virtual Service' for both.

• v7.5 & later – Using the WUI, go to Cluster Configuration > Layer 7 – Virtual Services and click [Add a New Virtual Service]
• v7.4.3 – Using the WUI, go to Edit Configuration > Layer 7 – Virtual Servers and click [Add a New Virtual Server]
• Enter the following details:
Enter an appropriate label for the VIP, e.g. DirectorPool
Set the Virtual Service IP address field to the required IP address, e.g. 192.168.10.20
Set the Virtual Service Ports field to 5061
Set Persistence mode to Source IP
Click Update
Now click [Modify] next to the newly created VIP
Change Layer 7 Protocol to Other TCP
Click Update

Now repeat these steps to add the other Virtual Services listed in the table above.

v6.x

Using the WUI, go to Edit Configuration > Virtual Servers (HAProxy) and click [Add a New Virtual Server]

Enter the following details:

- Enter an appropriate label for the VIP, e.g. DirectorPool
- Change the Virtual Server (ipaddress:port) field to <the required IP>:5060, e.g. 192.168.10.20:5061
- Set Persistence mode to Source IP
• Click Update
• Now click [Modify] next to the newly created VIP
• Change Layer 7 Protocol to Other TCP
• Click Update

Now repeat these steps to add the other Virtual Servers listed in the table above.

Real Server (RIP) Configuration

Real Servers (RIPs) must now be defined for each Virtual Server/Service created. The number of RIPs defined depends on the number of Director Servers in your deployment, the test deployment used for this guide has 2 Director servers so each VIP requires 2 RIPs to be configured.

v7.x

• v7.5 & later – Using the WUI, go to Cluster Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP
• v7.4.3 – Using the WUI, go to Edit Configuration > Layer 7 – Real Servers and click [Add a new Real Server] next to the newly created VIP
• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>DIR-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.10.21</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>5061</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
</tr>
</tbody>
</table>

• Enter an appropriate label for the RIP, e.g. DIR-1
• Change the Real Server IP Address field to the required IP address, e.g. 192.168.10.21
• Set the Real Server Port field to 5061
• Click Update
• Repeat the above steps to add your other Director Servers

Now repeat these steps to add RIPs for the other Virtual Services.
v6.x

• Using the WUI, go to Edit Configuration > Real Servers (HAProxy) and click [Add a new Real Server] next to the newly created VIP
• Enter the following details:

  ![Label](DIR-1)

  ![Real Server (ipaddress:port)](192.168.10.21:5061)

  ![Weight](1)

  ![Update](Update)

  • Enter an appropriate label for the RIP, e.g. DIR-1
  • Change the Real Server (ipaddress:port) field to <the required IP>:5061 e.g. 192.168.10.21:5061
  • Click Update
  • Repeat the above steps to add your other Director Servers

Now repeat these steps to add RIPS for the other Virtual Servers.

STEP 4 – Configuring the Load Balanced Edge Pool Services (Internal)

Virtual Server/Service (VIP) List

The table below shows all VIPs that must be created:

<table>
<thead>
<tr>
<th>VIP Name (Label)</th>
<th>IP Address</th>
<th>Port</th>
<th>Protocol</th>
<th>Layer</th>
<th>Persistence Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntEdgeAccess5061</td>
<td>192.168.10.10</td>
<td>5061</td>
<td>TCP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
<tr>
<td>IntEdgeWebConf8057</td>
<td>192.168.10.10</td>
<td>8057</td>
<td>TCP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
<tr>
<td>IntEdgeAv443</td>
<td>192.168.10.10</td>
<td>443</td>
<td>TCP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
<tr>
<td>IntEdgeAv3478</td>
<td>192.168.10.10</td>
<td>3478</td>
<td>UDP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
<tr>
<td>IntEdgeAv5062</td>
<td>192.168.10.10</td>
<td>5062</td>
<td>TCP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
</tbody>
</table>

** IMPORTANT **   Make sure that you change the protocol for the Audio Visual VIP 'IntEdgeAv3478' from the default setting 'TCP' to 'UDP'.

** IMPORTANT **   Make sure that you change the protocol for the Audio Visual VIP 'IntEdgeAv3478' from the default setting 'TCP' to 'UDP'.
NOTE: Prior to v7.5 a VIP is known as a 'Virtual Server', from v7.5 onwards it's known as a 'Virtual Service'. For simplicity the configuration steps below refer to 'Virtual Service' for both.

- v7.5 & later – Using the WUI, go to Cluster Configuration > Layer 4 – Virtual Services and click [Add a New Virtual Service]
- v7.4.3 – Using the WUI, go to Edit Configuration > Layer 4 – Virtual Servers and click [Add a New Virtual Server]

Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>IntEdgeAccess5061</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP address</td>
<td>192.168.10.10</td>
</tr>
<tr>
<td>Virtual Service Ports</td>
<td>5061</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>NAT</td>
</tr>
<tr>
<td>Persistent</td>
<td>yes</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
</tr>
</tbody>
</table>

- Enter an appropriate label for the VIP, e.g. IntEdgeAccess5061
- Change the Virtual Service IP address field to the required IP address, e.g. 192.168.10.10
- Set the Virtual Service Ports field to 5061
- Change the Forwarding Method to NAT
- Set Persistence to yes
- Ensure that Protocol is set to TCP
- Click Update
- Now click [Modify] next to the newly created VIP
- Change Persistence Timeout to 1800
- Click Update

Now repeat these steps to add the other Virtual Services listed in the table above.

v6.x

- Using the WUI, go to Edit Configuration > Virtual Servers and click [Add a New Virtual Server]

- Enter the following details:
Enter an appropriate label for the VIP, e.g. **IntEdgeAccess5061**
• Change the **Virtual Server (ipaddress:port)** field to `<the required IP>:5061`, e.g. **192.168.10.10:5061**
• Set **Persistence** to **yes**
• Click **Update**
• Now click [**Modify**] next to the newly created VIP
• Change **Persistence Timeout** to **1800** (30 minutes)
• Change **Scheduler** to **wlc** (Weighted Least Connection)
• Change **Forwarding Method** to **NAT**
• Click **Update**

Now repeat these steps to add the other Virtual Servers listed in the table above.

**Real Server (RIP) Configuration**

Real Servers (RIPs) must now be defined for each Virtual Server/Service created. The number of RIPs defined depends on the number of Director Servers in your deployment, the test deployment used for this guide has 2 Front Director so each VIP requires 2 RIPs to be configured.

**v7.x**

• **v7.5 & later** – Using the WUI, go to **Cluster Configuration > Layer 4 – Real Servers** and click [**Add a new Real Server**] next to the newly created VIP
• **v7.4.3** – Using the WUI, go to **Edit Configuration > Layer 4 – Real Servers** and click [**Add a new Real Server**] next to the newly created VIP
• Enter the following details:
• Enter an appropriate label for the RIP, e.g. **EDGE-1**
• Change the *Real Server IP Address* to the required IP address, e.g. **192.168.100.10**
• Set the *Real Server Port* field to **5061**
• Click **Update**
• Repeat the above steps to add your other Edge Servers

Now repeat these steps to add RIPs for the other Virtual Services.

---

v6.x

• Using the WUI, go to *Edit Configuration > Real Servers* and click **[Add a new Real Server]** next to the newly created VIP
• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>EDGE-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server (ipaddress:port)</td>
<td>192.168.100.10:5061</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>NAT</td>
</tr>
</tbody>
</table>

• Enter an appropriate label for the RIP, e.g. **EDGE-1**
• Change the *Real Server (ipaddress:port)* field to `<the required IP>:5061`, e.g. **192.168.100.10:5061**
• Change *Forwarding Method* to **NAT**
• Click **Update**
• Repeat the above steps to add your other Edge Servers

Now repeat these steps to add RIPs for the other Virtual Servers.
**STEP 5 – Configuring the Load Balanced Edge Pool Services (External)**

**Virtual Server/Service (VIP) List**

The table below shows all VIPs that must be created:

<table>
<thead>
<tr>
<th>VIP Name (Label)</th>
<th>IP Address</th>
<th>Port</th>
<th>Protocol</th>
<th>Layer</th>
<th>Persistence Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtEdgeAccess443</td>
<td>10.25.1.10</td>
<td>443</td>
<td>TCP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
<tr>
<td>ExtEdgeAccess5061</td>
<td>10.25.1.10</td>
<td>5061</td>
<td>TCP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
<tr>
<td>ExtEdgeWeb443</td>
<td>10.25.1.11</td>
<td>443</td>
<td>TCP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
<tr>
<td>ExtEdgeAv443</td>
<td>10.25.1.12</td>
<td>443</td>
<td>TCP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
<tr>
<td>ExtEdgeAv3478</td>
<td>10.25.1.12</td>
<td>3478</td>
<td>UDP</td>
<td>4</td>
<td>Source IP address</td>
</tr>
</tbody>
</table>

**Virtual Server/Service (VIP) Configuration**

The following steps show how to create the first VIP in the table above. Once created, use the same method to create all other VIPs listed in the table. **Note that three different IP's are used for the five VIPs.**

**IMPORTANT** Make sure that you change the protocol for the Audio Visual VIP 'IntEdgeAv3478' from the default setting 'TCP' to 'UDP'.

**v7.x**

NOTE: Prior to v7.5 a VIP is known as a 'Virtual Server', from v7.5 onwards it's known as a 'Virtual Service'. For simplicity the configuration steps below refer to 'Virtual Service' for both.

- v7.5 & later – Using the WUI, go to **Cluster Configuration > Layer 4 – Virtual Services** and click [Add a New Virtual Service]
- v7.4.3 – Using the WUI, go to **Edit Configuration > Layer 4 – Virtual Servers** and click [Add a New Virtual Server]

- Enter the following details:
• Enter an appropriate label for the VIP, e.g. **ExtEdgeAccess443**
• Change the **Virtual Service IP address** field to the required IP address, e.g. **10.25.1.10**
• Set the **Virtual Service Ports** field to **443**
• Change the **Forwarding Method** to **NAT**
• Set **Persistence** to **YES**
• Ensure that **Protocol** is set to **TCP**

Now repeat these steps to add the other Virtual Services listed in the table above.

---

**v6.x**

• Using the WUI, go to **Edit Configuration > Virtual Servers** and click **[Add a New Virtual Server]**
• Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>ExtEdgeAccess443</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Server (ipaddress:port)</td>
<td>10.25.1.10:443</td>
</tr>
</tbody>
</table>

| Persistent | yes |

• Enter an appropriate label for the VIP, e.g. **ExtEdgeAccess443**
• Change the **Virtual Server (ipaddress:port)** field to `<the required IP>:443`, e.g. **10.25.1.10:443**
• Set **Persistence mode** to **Source IP**
• Click **Update**
• Now click **[Modify]** next to the newly created VIP
• Change **Persistence Timeout** to **1800** (30 minutes)
• Change **Scheduler** to **wlc** (Weighted Least Connection)
• Change **Forwarding Method** to **NAT**
• Click **Update**

Now repeat these steps to add the other Virtual Servers listed in the table above.
**Real Server (RIP) Configuration**

Real Servers (RIPs) must now be defined for each Virtual Server/Service created. The number of RIPs defined depends on the number of Director Servers in your deployment, the test deployment used for this guide has 2 Director servers so each VIP requires 2 RIPs to be configured.

**v7.x**

- v7.5 & later – Using the WUI, go to *Cluster Configuration > Layer 4 – Real Servers* and click *[Add a new Real Server]* next to the newly created VIP
- v7.4.3 – Using the WUI, go to *Edit Configuration > Layer 4 – Real Servers* and click *[Add a new Real Server]* next to the newly created VIP
- Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>EDGE-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>10.20.1.10</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>443</td>
</tr>
<tr>
<td>Weight</td>
<td>1</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

  - Enter an appropriate label for the RIP. e.g. **EDGE-1**
  - Change the **Real Server IP Address** field to the required address, e.g. **10.20.1.10**
  - Set the **Real Server Port** field to **443**
  - Click **Update**
  - Repeat the above steps to add your other Edge Servers

Now repeat these steps to add RIPs for the other Virtual Services.

**v6.x**

- Using the WUI, go to *Edit Configuration > Real Servers* and click *[Add a new Real Server]* next to the newly created VIP
- Enter the following details:
Enter an appropriate label for the RIP. e.g. **EDGE-1**

- Change the **Real Server (ipaddress:port)** field to `<the required IP>:443`, e.g. **10.20.1.10:443**
- Change **Forwarding Method** to **NAT**
- Click **Update**
- Repeat the above steps to add your other Edge Servers

Now repeat these steps to add RIPv2s for the other Virtual Servers.

**STEP 6 – Finalizing the Configuration**

To apply the new settings for the Layer 7 based VIPs, HAPROXY must be restarted as follows:

**v7.x**
- Go to **Maintenance > Restart Services** and click **Restart HAPROXY**

**v6.x**
- Go to **Maintenance > Restart HAPROXY (Hard restart)**
Testing & Validation

Client connections bypass the load balancer

It's important to note that client connections can bypass the load balancer and connect directly to one of the Front End servers (this will be the users home server if available). This is normal and expected behavior and is explained in the 'Client Registration' section of the following technet article:


Taking Servers Offline

As explained in the section above, client connections can be direct to one of the Front End servers. In this case, taking a server offline using only the load balancer will have no effect. Therefore, a two step approach is suggested:

• **Drain the server using the Lync Control Panel** – this will cause all clients to reconnect to one of the other Front-End servers. Note that active calls and conferencing session should remain active until closed

• **Take the server offline (Drain) using System Overview in the load balancer's WUI** – this will ensure that existing connections can continue until closed, new connections that pass via the load balancer will be directed to a different Front End server

Microsoft Lync Testing Tool

The Microsoft Lync 2010 / OCS 2007 R2 Remote Connectivity Analyzer tool is a very useful Web-based Microsoft tool designed to help IT Administrators troubleshoot their Lync 2010 deployments. It's available at the following link:

https://www.testocsconnectivity.com/

Lync Diagnostics Tools

Microsoft's Lync Server 2010 Logging Tool enables logs to be captured and analyzed. It's a very effective way to analyze Lync client / server communications when diagnosing any issues.

For example, Lync 2010 looks for the optimum path for client communication. Direct communication is preferred over relaying, UDP is preferred over TCP. The logging and analysis tools can be used to verify that optimum methods are used for client communications. The following screen shot shows communication between an external and internal client, in this case UDP was selected indicating optimum path.
For additional guidelines on using the logging tool refer to the following link:


N.B. to be able to analyze the logs, download and install the Microsoft Lync Server 2010 Resource Kit Tools from the following link:


Wireshark Protocol Analyzer

Wireshark is an excellent tool that can be used to analyze network traffic when diagnosing any network related issues. Wireshark is available for download at the following link:

http://www.wireshark.org/download.html

Other Useful Resources

Microsoft Lync Server 2010 Resource Kit documentation:


Testing & verifying Lync 2010 Edge Server:


Testing Web Services:

Technical Support
For more details or assistance with your deployment please don't hesitate to contact our support team using the following email address: support@loadbalancer.org

Conclusion
Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Microsoft Lync Server 2010 environments.
Appendix

1 – Mobility Services – Configuring SSL Offload, Cookie Insertion & SSL Re-encryption

To enable support for the mobility features available in Lync Server 2010 CU4 a number of settings need to be changed on the load balancer. Currently, this also includes manually editing the load balancer’s underlying configuration files.

For the External Web Services SSL must be terminated at the load balancer to allow the cookie to be inserted, then re-encrypted before reaching the Front End & Director Servers.

HTTPS Traffic Flow – without SSL Offload

Without offload (as per the config on pages 25 & 28), 2 VIPs are used – one for HTTP and one for HTTPS.

HTTPS Traffic Flow – with SSL Offload & Re-encryption

With SSL offload & Re-encryption, the HTTPS flow is modified as shown below for the Front End Server External Web Services. The Director Servers must also be configured in the same way.

NOTES:

1. The SSL certificate & private key must be exported from one of the Front End Servers and imported into the load balancer
2. Pound is used on the load balancer to terminate SSL on port 4443
3. The HAProxy VIPs created previously to listen on port 4443 must be modified to listen on a different port, 8081 is used in this example. The existing RIPv must also be changed to be the Pound Re-encrypt listeners
4. The Pound Re-encrypt listeners connect to the Front End Servers on port 4443 and re-encrypt the traffic using the certificate installed on these servers
5. The HAProxy VIPs must be configured to use HTTP cookie persistence
6. The Reverse Proxy should re-map ports, i.e. 80 → 8080 & 443 → 4443
**Internal Load balancer Configuration Steps**

*N.B. Where there are differences between product versions, these are noted in the steps below.*

1) **Create the Pound SSL Virtual Server/Service (VIP)** – follow the steps listed below:

**v7.x**

- v7.5 & later – Using the WUI go to *Cluster Configuration > SSL Termination*
- v7.4.3 – Using the WUI go to *Edit Configuration > SSL Termination*
- Click **[Add a new Virtual Service]**
- Enter details as shown below, changing names and IPs as needed:

<table>
<thead>
<tr>
<th>Label</th>
<th>FEWebSvcs Offload4443</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP address</td>
<td>192.168.20.30</td>
</tr>
<tr>
<td>Virtual Service Port</td>
<td>4443</td>
</tr>
<tr>
<td>Backend Virtual Service IP Address</td>
<td>192.168.20.30</td>
</tr>
<tr>
<td>Backend Virtual Service Port</td>
<td>8081</td>
</tr>
<tr>
<td>Ciphers to use</td>
<td></td>
</tr>
<tr>
<td>Do not insert empty fragments</td>
<td></td>
</tr>
<tr>
<td>SSL Terminator</td>
<td>Pound STunnel</td>
</tr>
<tr>
<td>Enable WebDAV Verbs</td>
<td></td>
</tr>
<tr>
<td>Rewrite HTTP Redirects</td>
<td>✓</td>
</tr>
<tr>
<td>Honor Cipher Order</td>
<td></td>
</tr>
<tr>
<td>Allow Client Renegotiation</td>
<td>No Client Renegotiation</td>
</tr>
<tr>
<td>Disable SSLv2 Ciphers</td>
<td>✓</td>
</tr>
<tr>
<td>Disable SSL Compression</td>
<td>✓</td>
</tr>
</tbody>
</table>

- **Click Update**

Now repeat the above steps for the Director server based External Web Services (DirPoolExtWebSvcs4443).
v6.x

- Using the WUI go to Edit Configuration > SSL Termination (Pound)
- Click [Add a new Virtual Server]
- Enter details as shown below, changing names and IPs as needed:

<table>
<thead>
<tr>
<th>Virtual Server (ipaddress:port)</th>
<th>192.168.20.30:4443</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backend Cluster</td>
<td>FePoolExtWebSvcs4443 - 192.168.20.30:8081</td>
</tr>
<tr>
<td>Ciphers to use</td>
<td></td>
</tr>
<tr>
<td>Rewrite HTTP Redirects</td>
<td>✓</td>
</tr>
<tr>
<td>Honor Cipher Order</td>
<td></td>
</tr>
<tr>
<td>Allow Client Renegotiation</td>
<td>No Client Renegotiation</td>
</tr>
<tr>
<td>Disable SSLv2 Ciphers</td>
<td></td>
</tr>
</tbody>
</table>

- For the Backend Cluster select FePoolExtWebSvcs4443 – 192.168.20.30:8081 as shown
- Click Update

2) Disable the ability for the system to re-write the Pound Configuration – this ensures that the manual configuration changes described in the following sections are not overwritten by the system:

v7.x

- v7.5 & later – Using the WUI, go to: Cluster Configuration > SSL – Advanced Configuration, and set Disable Write to on
- v7.4.3 – Using the WUI, go to: Edit Configuration > SSL – Advanced Configuration, and set Disable Write to on
  - Click Update to save the changes

v6.x

- This step is not applicable to v6.x. Note that any changes made to the Pound configuration via the WUI will overwrite any manual changes made to the configuration file.

3) Create the Pound Re-encrypt listeners – Using an editor such as vi or vim at the console or via an ssh session, or using the default built-in editor included with WinSCP (not Notepad) modify the Pound configuration file as follows:
Navigate to the directory `/etc/pound` then edit the file named `pound.cf`. Now using the editor, copy & paste the text below into the end of that file.

**v6.x**

Navigate to the directory `/usr/local/etc` then edit the file named `pound.cf`. Now using the editor, copy & paste the text below into the end of that file.

**Text to copy:**

```
ListenHTTP
Address 192.168.20.231
Port 8080
Service
BackEnd
Address 192.168.20.31
HApport 4443
Port 4443
HTTPS
End
End
End
ListenHTTP
Address 192.168.20.232
Port 8080
Service
BackEnd
Address 192.168.20.32
HApport 4443
Port 4443
HTTPS
End
End
End
ListenHTTP
Address 192.168.20.221
Port 8080
Service
BackEnd
Address 192.168.20.21
HApport 4443
Port 4443
HTTPS
End
End
End
ListenHTTP
Address 192.168.20.222
Port 8080
Service
BackEnd
Address 192.168.20.22
HApport 4443
Port 4443
HTTPS
End
End
End
```
Once the above lines have been added, save the file.

N.B. If you have more than 2 Front End / Director servers, you will need to add and customize additional Listen sections, e.g. if you have 3 Front End servers and 3 Director servers, you will need a total of 6 listen sections.

4) Customize the Pound Re-encrypt listeners – the lines above contains 4 ‘ListenHTTP’ sections. In this example which is from the Loadbalancer.org test environment, the first 2 listen sections correspond to the 2 x Front End Servers, the second 2 listen sections correspond to the 2 x Director Servers.

The 'BackEnd' IP addresses are the real server IP addresses (i.e. the Front End & Director Servers) and should also be configured to suit your environment.

5) Add Floating IPs for the Pound Re-encrypt listeners – follow the steps listed below:

\[v7.x\]
- v7.5 & later – Using the WUI go to: Cluster Configuration > Floating Ips
- v7.4.3 – Using the WUI go to: Edit Configuration > Floating IPs

\[v6.x\]
- Using the WUI go to: Edit Configuration > Floating IPs
- Add a floating IP for each Pound Re-encrypt listener – in the Pound configuration above, the IPs used are: 192.168.20.221, 192.168.20.222, 192.168.20.231, 192.168.20.232

6) Modify the original HTTPS Web Services VIPs (FePoolExtWebSvcs4443 & DirPoolExtWebSvcs4443) – follow the steps listed below:

- Using the WUI modify these VIPs to listen on port 8081 instead of 4443
- Using the WUI modify the associated RIPS to be the Pound Re-encrypt listeners. For the test environment in this guide:
  - for FePoolExtWebSvcs4443 the existing RIPS need to be changed to:
    192.168.20.231:8080
    192.168.20.232:8080
  - for DirPoolExtWebSvcs4443 the existing RIPS need to be changed to:
    192.168.20.221:8080
    192.168.20.222:8080
- Using the WUI modify these VIPs to use HTTP cookie persistence:
  - using the WUI change Layer 7 Protocol to HTTP and set Persistence mode to HTTP Cookie
• v7.5 & later only – Using the WUI change HTTP pipeline mode from the default value **Close both client and server** to **No change**

  *N.B. other version require a manual config as described later in step 11*

• v7.5 & later only – Using the WUI change the default cookie name from **SERVERID** to **MS-WSMAN**

  *N.B. other version require a manual config as described later in step 11*

• Using the WUI modify these VIPs to use an HTTP based health check – this ensure that both the Pound re-encrypt listeners and the back-end Lync servers are health-checked. Configure the following fields:

  *Request to send* – set to: **dialin/**
  *Response Expected* – set to: **Conference**

This configures HAProxy to attempt to open the page http://<Lync server IP address>/dialin/ and look for the word 'Conference', if successful the health check has passed

• Click **Update** to save the changes

7) **Export the SSL Certificate from one of the Front End Servers** – note the following points:

• When exporting the certificate from Windows:
  ◦ Make sure that the private key is included
  ◦ Tick the option *Include all certificates in the certification path if possible*

8) **Convert the SSL Certificate from .pfx format to PEM format (required by the load balancer)** – follow the steps listed below:

• Using Openssl on a Windows PC, convert the certificate using the following command:

  openssl pkcs12 -in c:\certs\certificate.pfx -nodes -out c:\certs\certificate.pem

  *N.B. Openssl can be downloaded from: http://slproweb.com/products/Win32OpenSSL.html – you can use either the 'light' version or the 'full' version*

9) **Import the SSL Certificate to the Load Balancer** – follow the steps listed below:

  *v7.x*

• v7.5 & later – Using the WUI goto: **Cluster Configuration > SSL Termination**, click **[Certificate]** next to the new SSL VIP

• v7.4.3 – Using the WUI goto: **Edit Configuration > SSL Termination**, click **[Certificate]** next to the new SSL VIP

• Using the browse option, navigate to and select the .pem file created in the previous step

• Click **Upload PEM file**
v6.x
• Using the WUI goto: Edit Configuration > SSL Termination (Pound), click [Modify] next to the newly created VIP
• Using the browse option, navigate to and select the .pem file created in the previous step
• Click Upload PEM file

10) Disable the ability for the system to re-write the HAProxy Configuration – this ensures that the manual configuration changes described in the following section are not overwritten by the system.

v7.x
• v7.5 & later – Using the WUI, go to: Cluster Configuration > Layer 7 – Advanced Configuration, and set Disable Write to on
• v7.4.3 – Using the WUI, go to: Edit Configuration > Layer 7 – Advanced Configuration, and set Disable Write to on
• Click Update to save the changes

v6.x
• This step is not applicable to v6.x. Note that any changes made to the Layer 7 (HAProxy) configuration via the WUI will overwrite any manual changes made to the configuration file.

11) Customize the HAProxy configuration for the External Web Services HTTPS VIPs (FePoolExtWebSvcs4443 & DirPoolExtWebSvcs4443) – follow the steps listed below:

v7.x
• v7.5 & later – No configuration is required since the required settings have already been configured in step 6.

v6.x & v7.4.3
• Using an editor, edit the file HAProxy.cfg located in /etc/haproxy
  ◦ Set the cookie name for these VIPs:
    ▪ Change all occurrences of SERVERID to MS-WSMAN – this sets the cookie name as required by Microsoft for the External Web Services
  ◦ Modify the default HTTP behavior for these VIPs:
    ▪ Remove the line: option httpclose
• Save the file
12) Restart Pound & HAProxy – follow the steps listed below:

**v7.x**
- Using the WUI go to: *Maintenance > Restart Services*
- click *Restart Pound*
- click *Restart HAProxy*

**v6.x**
- Using the WUI go to: *Maintenance > Restart Pound-SSL*
- Using the WUI go to: *Maintenance > Restart HAProxy (hard restart)*

2 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave, please refer the section ‘Adding a slave unit after the master has been configured’ in the v7.x administration manual which is available at the following link: [http://www.loadbalancer.org/pdf/loadbalanceradministrationv7.pdf](http://www.loadbalancer.org/pdf/loadbalanceradministrationv7.pdf).

For v6.x the procedure is similar although there is no system status bar that displays the unit and interface status as in v7.x.

Don't hesitate to contact our support team if you need any further assistance: support@loadbalancer.org
## 3 – Company Contact Information

<table>
<thead>
<tr>
<th>Country</th>
<th>Address</th>
<th>Tel</th>
<th>Fax</th>
<th>Email (sales)</th>
<th>Email (support)</th>
</tr>
</thead>
</table>
| **North America (US)** | Loadbalancer.org, Inc.  
270 Presidential Drive  
Wilmington,  
DE 19807  
USA  
Tel : +1 866.229.8562 (24x7)  
Fax : +1 302.213.0122  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |                      |                      |                |                 |
| **North America (Canada)** | Loadbalancer.org Ltd.  
300-422 Richards Street  
Vancouver, BC  
V6B 2Z4  
Canada  
Tel : +1 604.629.7575  
Fax : +1 302.213.0122  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |                      |                      |                |                 |
| **Europe (UK)** | Loadbalancer.org Ltd.  
Portsmouth Technopole  
Kingston Crescent  
Portsmouth  
PO2 8FA  
England, UK  
Tel : +44(0)870 4438779 (24x7)  
Fax : +44(0)870 4327672  
Email (sales) : sales@loadbalancer.org  
Email (support) : support@loadbalancer.org |                      |                      |                |                 |
| **Europe (Germany)** | Loadbalancer.org GmbH  
Alt Pempelfort 2  
40211 Düsseldorf  
Germany  
Tel : +49 (0)221 9793 7203  
Fax : +49 (0)30 9203 836495  
Email (sales) : vertrieb@loadbalancer.org  
Email (support) : support@loadbalancer.org |                      |                      |                |                 |